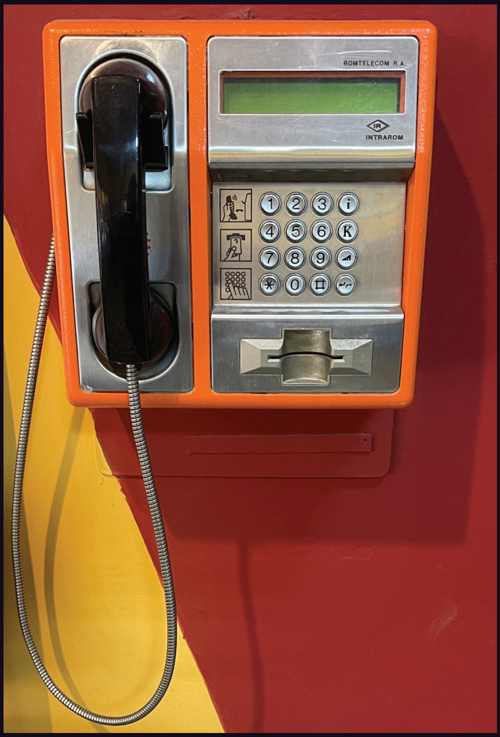
Volume Thirty-Nine, Number Two
DIGITAL EDITION

2600
The Hacker Quarterly

AI model drawing images from any prompt!

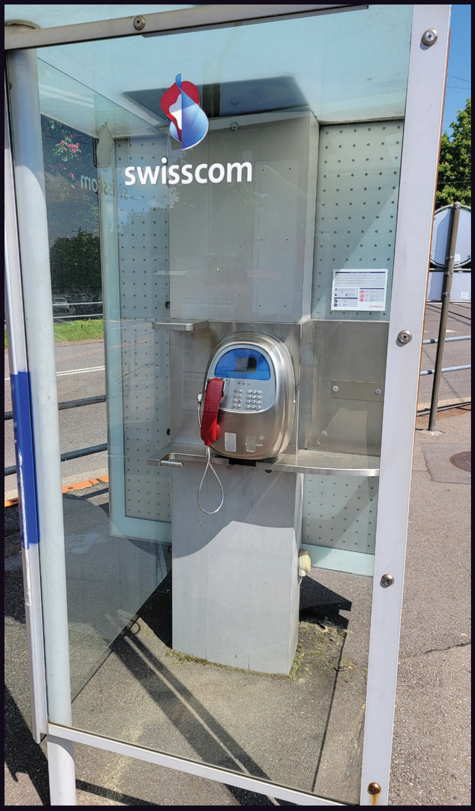
S C O U T S

Working Payphones



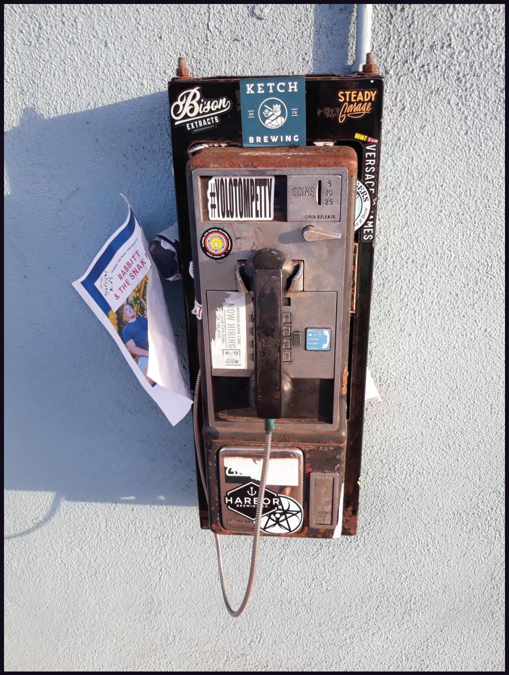
Romania. This cheerful looking phone was found inside a university hospital in Bucharest. We're told it's in pretty good condition and that there are not very many left.

Photo by Daniel Cioaca



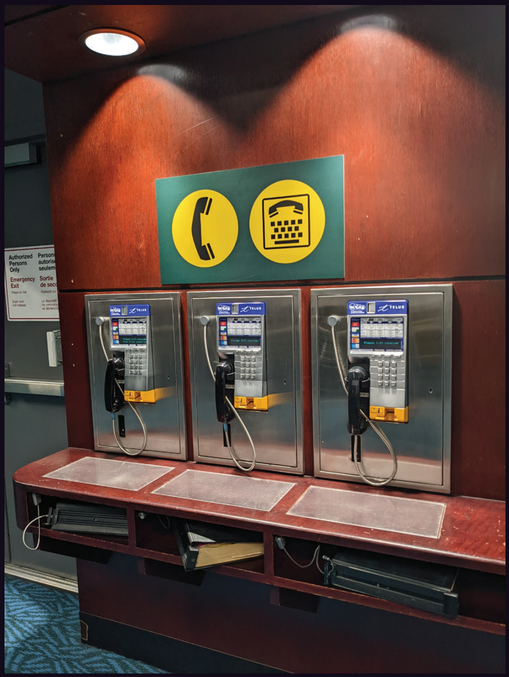
Switzerland. Spotted at the Thunplatz train and bus area in Bern, this efficient looking model looks like it's prepared for just about anything.

Photo by Tom Dalton



United States. Seen on the Hawaiian island of Maui in the town of Paia, you would never think this phone was actually in working order. But it is! And it moonlights as a bulletin board.

Photo by Jim



Canada. These win the prize as they're all working. You'll have to go to the B gates at Vancouver International Airport to see them, but it's well worth the trip.

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 (Do not send us links as photos must be previously unpublished.)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)

Operations

Social Media Is Neither

Let's be honest. We've all benefited in some way from social media. Whether it's staying in contact with a select group of people or being more tied into what's going on in a particular community or movement, we cannot deny that through social media we have the means of connecting in a far more efficient and accurate manner than ever before.

But it's this very allure which draws us in and helps to set us up for a nightmare that eclipses all of the good. Virtually every negative aspect of society has become orders of magnitude more amplified owing to the ability of instantly rounding up a huge number of like-minded people - as well as artificial constructs that can often carry the same weight as real individuals.

Mob rule is never a good thing. The least common denominator becomes the default and any signs of independent thought are quickly quelled. Forums like Twitter and Facebook make it really simple to whip up outrage and shut down an opponent or even an entire opposing line of thought. There are occasions where this is warranted, but there are many others where it is not. Hatred, racism, bullying - these are easy to understand concepts that shouldn't be tolerated in any forum. But then the tables get turned and, through social media, people are told that up is now down and 2+2=5. Because of the mob mentality, few dare to question what is obviously wrong. Most are content with being in a group where they feel they belong and where there's a target of "others" who are the threat and who must be stopped.

Nobody is immune from this. We've seen it happen on all sides of the political and social spectrum. Just as we once told ourselves that fascist rhetoric could never take hold in our country, we now make a similar miscalculation in concluding that whatever side we're on is safe from undue peer pressure through social media. While there are certainly perceptible differences in the degree that we're all affected, a seed is still a seed. As long as we hand over this much power and influence to this means of communication, we risk losing a great deal before we even realize there's a threat.

When "alternative facts" become legitimized through over-tolerance or by convincing people that they're constantly being lied to, almost everything can be turned into reality for a significant part of the population. This is how a fair election can be seen as a stolen one by huge numbers of people; those saying otherwise are lying and making up facts - and simply saying so is enough to convince those who have signed on to the right social media faction. We saw the same thing with vaccines and how all kinds of easily disproved "facts" were being spread and believed, despite what health experts worldwide were saying; the health experts were in on the conspiracy, after all. Suspicion and mistrust, coupled with instant access to millions of believers and sharing legitimate-looking stories, made actual facts no longer necessary. As Russia continues its brutal onslaught in Ukraine, its citizens continue to believe the official version of events, despite what on-the-scene journalists, witnesses, and actual unedited footage are saying. This is actually an older strategy of simply shutting down the independent voices and only permitting state propaganda to be heard. It's historically how populations have been controlled and it continues to be an effective means of manipulation across the planet. Control of social media only makes this tactic easier.

When we say that social media is neither, what we mean is that there is nothing social about blindly following and never questioning what you're told by the people you find yourself allied with. We know this is not how everyone uses the tool, but a significant percentage of the population does. And as for media, let's just say this is not the kind that you should rely upon to tell you the truth or to uncover actual facts, particularly those you may not want to hear. *That* form of media is comprised of people who spend their lives pursuing facts, questioning what they're told, often putting themselves in danger, and reporting what they find - regardless of who benefits and who wins or loses. Yes, we can still “become the media” and uncover those truths that mainstream media overlooks for one reason or another. But this is an earned position, not one that you get simply because you want it. Unfortunately, the lines have been blurred to such a degree that it’s almost impossible to tell true journalists from entertainers - or even highly delusional individuals.

The risks to all of us if this continues are great. In the past, we’ve warned of the potential abuses of new technology by asking readers to imagine what might have happened had the Nazis had such tools at their disposal. Now try to imagine what they would have done with the power of social media. And realize that there are many regimes that are at this moment refining their skills in that particular realm so that their message becomes the only one that spreads and weaponizes. In the past, you simply had to have a dictatorial form of government where the population and the media were controlled in order to turn lies into truth. But now, all you need is a way of reaching susceptible people through social media, along with a message of suspicion and fear that will motivate them to follow you and do whatever you say. And once that’s perfected, the dictatorial power will inevitably follow, as the mindset for it has already been established.

It’s a scary prospect, but it’s not an inevitable one. We have the ability to fight back. We just have to believe in ourselves as individuals who aren’t desperate to win acceptance. We don’t have to keep going down this road.

This means taking social media a whole lot less seriously. It means actually *talking* to people one on one and not just going with what’s popular or trending. It means not being afraid to speak your mind and to not feel the need to punish others when they do so. Arguing is great. Shaming is a tool often used by bullies who can’t win an argument with words, so they turn to mobs. We can do better.

It may seem comical and almost fun to watch how crazy things can possibly get. We used to believe that to a degree years ago. But if the nonsense leads to the wrong people being in the wrong positions and making the wrong decisions, it very quickly stops being funny. And it’s damn difficult to untangle the ensuing mess.

We’re living through a lot of those consequences today and the situation may seem hopeless at times. It’s not. It just requires that we work together so that a degree of sanity can once again prevail. That means being able to distinguish fact from fiction, to respect the words of those who have devoted themselves to true research, and to always continue questioning what you’re told. That latter part should apply to everyone, not just those you don’t trust. Most of all, we have to learn how to communicate with people again, not just usernames.

Social media started with such promise. We gave it too much power. It’s well past time we took that back.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for October 1, 2022. Annual subscription price $31.00.

1. Mailing address of known office of publication is Box 752, Middle Island, New York 11953.
2. Mailing address of the headquarters or general business offices of the publisher is 2 Flowerfield, St. James, NY 11780.
3. The names and addresses of the publisher, editor, and managing editor are: Publisher and Editor: Emmanuel Goldstein, Box 99, Middle Island, New York 11953. Managing Editor: Eric Corley, 2 Flowerfield, St. James, NY 11780
4. The owner is Eric Corley, 2 Flowerfield, St. James, NY 11780
5. Known bondholders, mortgagees, and other security holders owning or holding more than 1 percent or more of total amount of bonds, mortgages, or other securities are: none.
6. Extent and nature of circulation:

	Average No. Copies each issue during preceeding 12 months	Single Issue nearest to filing date
A. Total Number of Copies	21063	20000
B. Paid and/or Requested Circulation		
1 Paid/Requested Outside-County Mail Subscriptions	5442	5389
2 Paid In-County Subscriptions	0	0
3 Sales Through Dealers and carries, street vendors, and counter sales	14169	12880
4 Other Classes Mailed Through the USPS	0	0
C. Total Paid and/or Requested Circulation	19611	18269
D. Free Distribution by Mail and Outside the Mail		
1 Outside-County	123	122
2 In-County	0	0
3 Other Classes Mailed Through the USPS	0	0
4 Outside the Mail	920	914
E. Total free distribution	1043	1036
F. Total distribution	20654	19305
G. Copies not distributed	409	695
H. Total	21063	20000
I. Percent Paid	95	95

7. I certify that the statements made by me above are correct and complete.
(Signed) Eric Corley, Owner.

Phishing in 2022

by Jeff Barron   jeffbarron@protonmail.com   @_jeffaf

Phishing remains the most effective way to penetrate an organization from the outside. The Verizon 2021 Data Breach Investigations Report (DBIR) states that a median average of 3.5 percent of users click the phishing link. This was a median; some organizations had clickthrough rates of greater than 40 percent. It's funny, even if you don't follow the tips in this article and your phish ends up in spam, you still have a chance. Phishing is alive and well in 2022. In this article, I will show you how to do it. No more cloning websites. Two-factor authentication? We can beat that.

OK, so you have your target? Well, there is a bunch of OSINT to be done before you can even set up your domain. A sock puppet account on LinkedIn is really good for mapping out relationships inside of the target organization. Other social media can reveal useful things for the target as well, but I mostly stay with LinkedIn.

Using the website `phonebook.cz`, I discovered 307 email addresses for `2600.com`. Now, I have no interest or intention of phishing the good folks at *2600* or anyone that isn't paying me to do so. However, it shows how effective `phonebook.cz` is at quickly displaying email addresses by just providing a domain name. Another commonly used tool is "theHarvester" which is available on GitHub and packaged with Kali.

OK, so you've got emails and maybe some information for pretexts from your OSINT analysis. This is the point where you should search for breached credentials for your target. If you haven't been collecting breach dumps and don't know anyone who has, then I recommend an awesome service: Dehashed. You can get an account for $5 at `dehashed.com` and it's well worth it. You can also check for the existence of breached credentials without paying anything. Once you have obtained your breached creds, then it's time to try them out. If you can send an email as someone in the organization, then that will add credibility to your phish.

It's time to register a domain. The first thing we want to do is examine our target domain name. Can we get a different TLD? Using a tool at `dnstwist.it`, one can see that there are some shady *2600* domains like `2600.cn` and `2600.eu` that are likely not related to `2600.com`. You may get lucky and get the .ORG or .NET version of your target. It is also worth checking for expired domains. You can find those on `expireddomains.net`.

As far as registrars, I don't really have an opinion. The cheaper the better. I've used Namecheap in the past and it's done the job. After you register your domain, the next step is to sit on it for at least seven days. If your domain is less than seven days old when your phish goes out, it will be sent straight to spam.

The next thing you'll want to do is to get a VPS for your domain. I use Digital Ocean droplets, but there are probably better and cheaper options out there. On your Linux-based VPS, you'll want to install Postfix and Mailutils. (Mailutils is the package name for Debian/Ubuntu-based distros.)

Setting up Postfix is out of the scope of this article. I'll include an awesome reference at the end of this article for those who want to learn more about how to do it. Essentially, it boils down to adding your domain to three files (/etc/postfix/transport, /etc/postfix/virtual_domains, and /etc/postfix/virtual_regexp). Remember to configure hostname and mailname properly in /etc/ as well.

We need DNS entries! You'll want to configure your DNS to have an A record pointing towards the IP address of your VPS. You'll also want an MX record pointing at mail.evildomain.tld. Unfortunately, there is still more DNS work to do. We must have SPF, DMARC, and DKIM records for our shady domain! This is fairly easy to do and, again, I point you to the first reference at the bottom of this article for more details from `Hacktricks.xyz`. After you have set up SPF, DMARC, and DKIM records, then you also need a Reverse DNS entry or rDNS PTR record that resolves the IP address of the VPS to the domain.

So we have finished our setup. It's time to *test* our mail and see how well it will do with spam filters. `Hacktricks.xyz` recommends a website called `mail-tester.com`. You can send an email to it and similar services from the command line with Mailutils.

```
echo "my test message" |
➥mail -s "My test message"
➥generatedAddress@mail-tester.com
```

After testing the email, there is one more thing I do on my VPS box. I use iptables to block AWS, Azure, and GCP. I don't have good data on this, but I strongly believe this allows my evil domains to live longer without getting burned by threat intelligence companies scanning the Internet for bad domains like ours.

Pretexts! So what are we going to say to get the user to click? I have two trusty pretexts that are effective. They are "Hey, I'm (insert name of IT person found on LinkedIn) and I noticed some unusual activity on your o365 account. Would you help me out and check and see if this is you?

Thank you so much! (insert link)" and "Hey, we are resetting all passwords as we integrate our new vendors. Please go to (insert link) and follow the prompts as soon as possible. Thanks! (Insert name of IT person you found on LinkedIn.)" It's good to personalize the email as much as possible and say Hi (name of victim), but that can be tedious so I usually just make it generic for all, then send the phish to everyone (except the IT department).

At this point, we have most of what we need to begin this engagement. But what are we linking to? We haven't cloned any websites! The reason we haven't is that we are going to use evilginx2. From the GitHub page, the project self describes as follows: "Standalone man-in-the-middle attack framework used for phishing login credentials along with session cookies, allowing for the bypass of 2-factor authentication."

Evilginx2 is amazing. Imagine our victim uses o365. We can generate a link with evilginx2 that when the user clicks it, will be redirected through our site and get proxied to the actual site itself. So on one side we have the victim user, in the middle is our VPS, and on the other side is o365. It looks identical because it *is* the actual site. Because of where the VPS sits during this attack, you can also capture session cookies generated if the victim user gets a push notification or enters a code - since we are proxying the connection, we will get that cookie too and be able to bypass multi-factor authentication in this way. Evilginx2 will also download TLS/SSL certs for you when you run it. I prefer running it from docker as it's quick and easy. The evilginx2 GitHub page has great videos explaining how to use it and how it works under the hood.

All right, so if you've gotten this far, you now have everything you need to conduct a modern, MFA-bypassing, phishing attack. Please use this power for good. I recommend reading through the references for more detailed information on some of the areas I glossed over. If you want to talk more about offensive security, please feel free to shoot me an email.

A big shout out and thank you to the folks who helped teach me this stuff: Critical Path Security, Black Hills Infosec, the amazing folks at hacktricks.xyz, Kuba Gretsky of the evilginx2 project, and *2600 Magazine,* which inspired a 12-year-old version of me to build a red box.

So long, and thanks for all the phish.

References

- `book.hacktricks.xyz/generic-` `➥methodologies-and-resources/` `➥phishing-methodology`
- `github.com/kgretzky/evilginx2`

Plain Text in Plain Sight: Smaller Alternatives to the World Wide Web

by Colin Cogle

What's wrong with the World Wide Web? You open a browser, connect to a server (usually securely), and interact with content. With a few clicks, you can get news, sports scores, movies, inane updates from people you may know, cat pictures, hacker magazines, dinner... what's not to love?

Sir Tim Berners-Lee published the first website in December 1990, where he described his new document management system, hypertext, and the markup language for it. Though he continues to shape the incessantly-evolving ecosystem as the head of the World Wide Web Consortium, there are problems with the modern Web which will likely outlive us: ads, trackers, megabytes of JavaScript bloat, DRM, cookies, nonconsensual data collection and analytics, pop-ups, pop-overs, pop-unders, autoplaying music, commercialization, compartmentalization, autoplaying video in the corners of news articles, top-ten lists spread across 11 pages, ugly Facebook share buttons everywhere (even on PornHub for some reason, in case someone out there thinks their family and friends will love this video). And that's just off the top of my head.

It's easy to be an old man yelling at a cloud. It should surprise no one that the World Wide Web is here to stay. However, that doesn't mean we can't come up with alternatives. In fact, we already have - and I'm not talking about mobile apps or Tor Browser.

Go For Gopher

When you strip away everything superfluous, you're left with plain text. No formatting, no scripting, just words on a page. That was the idea behind Gopher. Named for the University of Minnesota's mascot (in case you were wondering), Gopher is a filesystem-inspired protocol to make your computer "gofer" information online.

Gopher sites (sometimes called Gopher holes, because why not) are typically presented as a text-based menu. You have words, and you have links to folders, files, or other sites. That's it. Unlike the Web, all Gopher sites look the same and navigate identically. It's truly a product of a time when NFT stood for nice fucking Tamagotchi.

This forced simplicity is part of the reason why it failed. While HTML is forgiving of mistakes, Gophermaps are strict and make you follow RFC 1436 to a "T." Needless to say, once customizing your MySpace pages became a thing, Gopher was looking very long in the tooth. Browsers eventually removed support for it, getting rid of it like an unwanted rodent.

Somehow, though, Gopherspace isn't dead. In the past 15 years, the number of Gopher servers online has tripled. Servers, clients, and (ironically) Web browser extensions continue to be developed. Most notably, the Playdate handheld gaming system had its release notes only available via Gopher, leading to [some news coverage for the plaintext protocol] (`theregister.com/2022/05/23/the_return_of_the_gopher/`)!

Gopher is more than nostalgia for the days when the Internet made noise when you turned it on. You can find news, weather, search engines, home pages, phlogs (the equivalent of blogs), and more. Perhaps this little rodent living under the Web isn't so dead after all.

Blast Off With Gemini

Fast-forward to 2019. A person by the handle Solderpunk was frustrated with the WWW and how crazy things were getting. In an interview, he said, "Visiting websites is basically a matter of downloading and running software, without any way to know in advance what that software might do, and very little ability to pick and choose which things you let it do." However, he also thought Gopher was too rigid and restrictive. The community sat down and thought up something like "'the web, stripped right back to its essence' or as 'Gopher, souped up and modernized just a little.'" The result was something these outer space buffs called Project Gemini.

Like Gopher, it's another simple text-based protocol that was designed to be intentionally difficult to expand, to avoid the feature creep that the WWW underwent. However, Gemini sites (called "capsules") are more modern, featuring Unicode, free-flowing text, gemtext (think: Markdown), virtual hosting, TLS 1.3, and more.

In three short years, Gemini has gone from IRC discussions to something implemented by over 2,000 servers, and it shows no signs of slowing down. More capsules and gemlogs (again, "blogs") are rocketing off into Geminispace every day.

So the Web Is Dead, Right?

No, and far from it. For general browsing, the World Wide Web is going nowhere, and that's fine. I've spent this article trashing it, but the good still vastly outweighs the bad. My bank will never implement Gopher. Amazon won't be selling products on Gemini anytime soon. Despite the big Web, there is definitely a place for the "small web" these days.

Consider:

- Has your computer gotten too slow to run Google Chrome? Is that old Android tablet struggling? Did Apple cut off macOS updates for your perfectly good laptop? Don't fork over your hard-earned cash and make more e-waste. A Gemini browser would make that old device feel like new - and put less strain on the old battery.
- Perhaps you want to get your vintage computer or old cell phone back online, but good luck using a 25-year-old Web browser. Gopher was made for retrocomputing!
- Traveling out to the boonies and stuck with dial-up or a 2G phone signal? It's rare, but it happens. You could spend an hour watching one web page open, or use Gemini and get it done in seconds.
- Do you prefer the command line? Text-mode web browsers can be cumbersome, but Gemini and Gopher were *built* for the terminal.

If you feel like everything online is getting bloated, and everyone wants to track you and sell you their crap, there are thinner alternatives. We can chat on IRC, talk on newsgroups, send email instead of signing our lives away to Meta - and now, we have some alternatives to the ever-expanding Web. However you choose to do it, happy browsing!

Battle for Better Batteries

by Hydrolycus

Rechargeable batteries are found in all the things, big and small, that make modern societies tick. Thanks to their ubiquity, it is easy to take batteries for granted, but in doing so we ignore the undeniable fact that our choice of rechargeable battery is a choice that has real-life consequences in environmental, financial, as well as geopolitical terms.

So let's start at the very beginning, allegedly a very good place to start.

The Heavy Metal Era

The lead-acid battery was the first practical rechargeable battery. Invented by the Frenchman Planté in the late 1850s, it's inexpensive to manufacture and capable of delivering plenty of current features that have led to it still being the most widespread battery used in internal combustion vehicles and stationary installations.

In spite of its popularity, it's not without problems. First of all, it has a poor power-to-weight ratio. Lead, one of the battery's principal components, is as heavy as - well, lead actually, a fact that makes it unsuitable for portable devices.

It gets worse. The other principal component is sulfuric acid. In practical terms, a leaky battery in your phone could give you a one-time free dermabrasion. The charge/discharge cycle of a lead-acid battery releases highly combustible hydrogen gas, creating a potential Hindenburg scenario in poorly ventilated spaces. And then there's the disposal problem. Lead in all its forms is poisonous to humans and many other living organisms, necessitating strict disposal and recycling protocols for the batteries.

Nickel Ain't Worth a Dime

Nickel is a much lighter metal than lead. It's relatively inexpensive, and nickel oxide hydroxide also happens to be a good material to make battery electrodes from. Several different chemistries have been developed, and such batteries can be made quite small, making them viable in portable devices.

But as you probably guessed, nickel-based batteries have their own set of problems. The batteries have very real limits on the number of times they can be fully recharged from a partial discharge, the "memory effect" we've all come to hate. They also have problems with polarity reversal if they are discharged too deeply, a phenomenon that can kill sensitive electronics along with the battery. The trick would be to discharge the batteries fully but not too fully before recharging. And even if you are astute enough to pull that off, there's a gotcha: self-discharge through internal leak currents.

Although nickel isn't very toxic by itself, it is often partnered with cadmium in batteries, and cadmium is an extremely toxic metal that you don't want in your local landfill, unless you have a fetish for kidney failure and spontaneous bone fractures.

A Cure for the Blues: Lithium

So far we've painted a pretty depressing picture of rechargeable batteries (pun intended), but for the longest time it was all we had and we learned to live with it. Then the 1980s came upon humanity, bringing with it blessings like big hair, Members Only jackets, boom-boxes, ferns, and *Full House*. And lithium.

Lithium is the lightest of all the metals, juxtaposing it as a Barry Manilow to a heavy metal like lead's Iron Maiden. It is also happy to give away and accept back electrons, with none of nickel oxide hydroxide's fussiness. Put those facts together and we could have a recipe for battery chemistries suitable for portable devices as well as electric vehicles. And, sure enough, there are dozens of battery types based on lithium. So all's well, then?

Hardly. Lithium is a poisonous metal, posing a danger in humans to the kidneys and the nervous system. Somebody might protest that the small quantities used in, for example, a cell phone or a music player aren't a big deal in the overall scheme of things. But imagine the day when discarded lithium-based batteries of tens of millions of electric cars and other vehicles end up in landfills across the globe.

Disposal is not the only problem associated with lithium. The mining and refining process of lithium consumes mind-boggling amounts of another scarce resource: water. It takes two million liters of fresh water to make one ton of lithium. One ton of lithium is a lot, right? Actually, no it's not. One ton of lithium is barely enough to make batteries for perhaps 90 small passenger cars.

Then there are the financial considerations, and those include more than just the high cost of extraction. Lithium is a relatively rare metal. The worldwide reserves are on the order of 20 million metric tons. Most of the reserves are located in China, with other extractable deposits in Australia, Chile, Argentina, and the Democratic Republic of Congo. Much of China's production is earmarked for domestic consumption, and a sizable chunk of the contracts for the output of other countries is already spoken for by a handful of corporations. In effect, there's a monopoly in place, keeping prices artificially high.

China's dominance in the lithium market has obvious geopolitical consequences, as it could be used to pressure other countries, especially with the world's growing dependency on lithium batteries.

Similar situations exist for many of the other key ingredients in lithium batteries, such as cobalt, copper, graphite, and others.

Finally, we have to mention lithium-based batteries' claim to popular infamy. They're prone to runaway thermal reactions that can cause them to catch fire. Your ears could literally be burning if that happens to your phone's battery.

At this point, it would be fair to ask if there is a way to make good, usable, rechargeable batteries without either killing the planet, going bankrupt, or starting World War III. It turns out that there might be.

Sodium: A Salt and Battery

The metal sodium sits on the next rung of the periodic table right above lithium. Given that position, it's reasonable to ask if it has chemical properties similar to lithium. The answer is that it does. It's highly reactive in the sense that it's willing to give up electrons, but also take them back - the fundamental idea of rechargeability. In fact, metallic sodium is so reactive that it will catch fire if exposed to air!

Sodium is abundant on our planet, and not only in cheap snack foods and hipster spas. Our oceans are full of sodium, and there are rock deposits all over the world. Thus, there are no geopolitical complications to overcome. Our blood and the cells of our bodies are jam-packed with sodium chloride, as are all other living cells, living proof that it's not toxic if enjoyed in moderation. And to top it off, it's relatively inexpensive to extract from the many sources that exist.

So the final question then becomes: Could we make sodium based batteries? We not only can, we already *are* making them. CATL, the world's largest battery producer has developed the technology, and by the time you're reading this they have probably reached the market. But they were not first. Several companies, for example British firm Faradion, are already shipping large-capacity sodium-based batteries to customers.

The Low-Sodium Alternative

There is even more good news on the horizon. Several companies are making progress developing "green" batteries from organic sources. Huh? Organic batteries?

One of the most promising organic battery technologies is based on peptides. Peptides are simply chains of amino acids, the stuff that proteins are made of. There are 20 naturally occurring amino acids, and each have slightly different chemical properties.

Depending on the order in which the specific amino acids are linked together, we end up with peptides and proteins with widely varying characteristics, some of which can be used to make rechargeable batteries. This is thanks to the electrical properties of various amino acids. Some of them - for example aspartate and glutamate - have a negative electric charge, whereas others - for example histidine, arginine, and lysine - have a positive electric charge.

What's so great about organic batteries? First of all, the chemicals inside them are fully biodegradable. There are no poisonous metals to worry about.

Second, since proteins are the building blocks of all living matter, there are plenty of cheap amino acids to go around if you know where to look for them. Batteries have successfully been created from farm- and forestry-waste that would otherwise be burned or left to rot! Nobody goes to war over farm waste.

One final, very interesting property of peptide-based batteries is that the charge time is much lower than what we get from lithium batteries. Imagine fully charging your Tesla in 30 minutes!

This technology is developing rapidly, and there are several pilot studies underway, primarily targeted at making batteries for electric vehicles.

All in all, there is hope for a future beyond lithium and lead. It's not a matter of technology anymore, it's a matter of economic and political initiative.

Shout outs to Joao, Saravanan, Rav, John, and Kirk.

Command Line Unminifier

by Gearbox

JavaScript and CSS files are usually posted online in minified format (minimum number of spaces and everything on a single line) in order to save transfer bandwidth. This makes it hard to analyze. Even though there are online tools to unminify such files, using a command line utility to do this work has the advantage of integration with already existing CLI tools (via pipes or command calls) and the potential to work in bulk.

Such a CLI tool can take the minified content of a JS or CSS file using the standard input and output the unminified content using the standard output. The default space indentation can be set to two spaces, but can be overridden via an input parameter ("indent"). For example, if we name the tool script webballoon.py to unminify the content of a file, we can call it on Linux or Mac like:

```
cat script.min.js | ./webballoon.py
```

or to use a custom indent of four spaces:

```
cat script.min.js | ./webballoon.py --indent 4
```

For implementation, Python 3 is a great choice, as it is installed by default on most Linux distros and has a huge number of packages for pretty much everything.

We start with the Python "shebang" line (`#!/usr/bin/python3`), which tells Bash to use the Python 3 interpreter if the file is called directly without passing it as a parameter to Python 3 (e.g. "./webballoon.py" instead of "python3 ./webballoon.py").

Next, we import the packages we need:

- *argparse* - to add support for input parameter parsing (for the "indent" optional parameter that we are going to use).
- *sys* - in order to use the standard input, output, and error streams and to specify script error code in case of unexpected input.

Although it might seem overkill to use a parameter parsing package for a single input parameter, the application might be further extended in the future, plus there's the advantage that you can call the script with a "-h" or "--help" parameter and it displays automatically generated help.

The `_get_indent_size` function is used to retrieve the value of the indent input parameter (defaults to 2 if the parameter is not specified). It uses the `_check_larger_than_zero` helper function to validate that the indent parameter has a specified value that's numeric and greater than zero.

We then use the `_get_indent_spaces` helper function to get a white space string of variable size that can be use to display the indent and the `_print_to_stream` helper function to print text to standard output stream without adding a new line at the end.

The core functionality resides in the main function. It is the module entry point and contains the input processing logic. It parses the input character-by-character and, based on the encountered characters, generates the output as follows:

1. In case the "{" character is encountered, it means that what will follow is in an inner scope, so we output "{", move to the next line, and output an increased indent.
2. In case the "}" character is encountered, it means that what will follow is in an outer scope, so we move to the next line, output a decreased indent, "}", move to the next line, and output the current indent.
3. In case the ";" character is encountered, it means that what will follow is on a separate line at the same indent, so we output ";", move to the next line, and output the indent.
4. In case the "," character is encountered, it means that multiple elements are separated, so we output a space followed by ",".
5. Any other character is outputted as is.

The full code listing below is available under Boost Software License 1.0 and is also available online at: `github.com/gearbx/webballoon`.

```
#!/usr/bin/python3

import argparse
import sys

_BAD_INPUT_ERROR_CODE = 1

def _check_larger_than_zero(value) -> int:
try:
v = int(value)
if v <= 0:
print(f"Invalid parameter value {value}", file=sys.stderr)
sys.exit(_BAD_INPUT_ERROR_CODE)
return v
except Exception:
print(f"Invalid parameter value {value}", file=sys.stderr)
sys.exit(_BAD_INPUT_ERROR_CODE)

def _get_indent_size() -> int:
parser = argparse.ArgumentParser()
parser.add_argument("--indent", type=_check_larger_than_
➥zero, default=2, help="the indent size in spaces.(default 2)")
args = parser.parse_args()
return args.indent

def _get_indent_spaces(indent: int) -> str:
return " " * indent

def _print_to_stream(text: str):
print(text, end="", file=sys.stdout)

def main():
indent_increase = _get_indent_size()
indent = 0
for line in sys.stdin:
for character in line:
if character == "{":
indent += indent_increase
_print_to_stream(" {\n" + _get_indent_spaces(indent))
elif character == "}":
indent = max(0, indent - indent_increase)
_print_to_stream("\n" + _get_indent_spaces(indent) + "}\n" +
➥_get_indent_spaces(indent))
elif character == ";":
_print_to_stream(";\n" + _get_indent_spaces(indent))
elif character == ",”:
_print_to_stream(", ")
else:
_print_to_stream(character)

if __name__ == "__main__":
Main()
```

Telecom Informer

by The Prophet

Hello, and greetings from the Central Office! It's summer here in the Pacific Northwest, and eagles are making my life miserable. The local eagle population has decided that our cell towers are a good spot to watch for rabbits, whose populations exploded over the spring. 5G equipment is particularly sensitive to line-of-sight interference, and eagles an automatic yellow card for interference. But they're a national symbol and a protected species and I can't do a single thing about them.

The eagles probably aren't responsible for unexpected roaming by our customers onto Canadian carriers, but they're as good a reason to blame as any around here, where radio signals scatter through trees and skip happily for miles across bodies of water. For a long while, this wasn't much of a problem, because U.S. carriers programmed their handsets not to easily roam onto Canadian networks. In fact, they did the opposite (and still do to some degree) and would lock onto the home network with a death grip.

These days, for whatever reason, our customers on the "borderlands" (as they are locally called) are landing on Canadian networks more often. Canadian carriers have gone on a building spree lately, investing heavily in growing network coverage as they build out their 5G networks while some have also added 700MHz 4G coverage. Frequencies are coordinated along the border, but Canadian carriers definitely aim for maximum advantage in covering the U.S. Our service is carefully tuned to stop working almost exactly when you cross the border. Depending upon where you are, theirs can be usable up to 20 miles inside the U.S. border.

Unexpected international roaming used to be something that carriers scrupulously avoided, and to some extent they still do. It created massive customer service problems whenever the bill showed up, given expensive international roaming charges. However, with the advent of cheap roaming agreements between North American carriers, U.S. carriers introduced service plans that include free roaming across North America. This means that a lot less effort is put into hunting down areas where Canadian carriers are effectively providing service to the U.S. side (not that much is likely to be done about these places anyway, because it'd involve investing in infrastructure, something U.S. carriers aren't especially inclined to do).

All of this is fine until someone calls 911, which creates a massive problem. People in panicked, stressed situations aren't always situationally aware of whether they are using a Canadian tower, and a lot of place names sound the same in Washington and British Columbia. So it can take awhile for the 911 operator to work out what's happening and where the caller is, and transfer them to the correct Public Safety Access Point (PSAP). That is, if they even know the correct PSAP. Often they don't. A 911 caller in western Washington will usually be in either San Juan or Whatcom counties, but not necessarily. This could mean a merry-go-round of transfers between PSAPs before a distressed caller (potentially in a life-or-death situation) is connected to the correct first responders.

Enter Northern911, which is based in Sudbury, Ontario. This company has provided PSAP services to independent and VoIP carriers for decades, and is essentially the "oddball PSAP." Owing to the geographically vast territory that they serve, their dispatchers are much more geographically aware than most and have an index of every PSAP in North America, along with the ability to transfer over primary e911 trunks into most of them. In fact, they operate a freemium "911 for 911" service, where 911 operators can call 1-866-869-9959 for assistance with properly routing the call. This is much faster than other commonly used methods such as NENA directory searches, and is likely to yield more accurate information (given that Northern911 dispatchers have considerable human expertise in which PSAPs serve what geographies). Up to five calls per month are free, after which Northern911 operates on a subscription model.

In emergencies, seconds can matter, and chat bots haven't been able to effectively replace 911 operators yet. And if you're having an emergency along the Canadian border and end up with a 911 dispatcher on the wrong side, there's a very good chance that some folks in Sudbury will be involved in figuring out where you are, and which first responders will be helping you. And with that, if you're one of the thousands of people swarming to the borderlands to enjoy the great outdoors this summer, please enjoy them safely. There are any number of emergencies that simply didn't need to happen or result in a 911 call, particularly those involving cliff diving, guns, and fireworks.

One thing that will be safe this summer? A New HOPE! Hopefully, I will have seen you there in New York when it happened in July. And with that, I'll be back to doing everything I legally can to encourage these eagles to fly north across the border and harass a Canadian carrier's towers.

WRITERS NEEDED!

There are so many topics in the hacker world that capture our interest. And everyone reading this has their own story to tell involving technology and their adventures with it. We need more of you to send us those stories so we can keep capturing and inspiring the imagination of many readers to come!

Send your articles to us via email at **articles@2600.com**

We prefer ASCII but can read any format. Most articles are between 1000-2000 words, but we have many that are fewer and a bunch that are more. What's important is that you add your voice to those who have written for *2600* over the years. (We've never heard anyone say they've regretted it.)

For those without Internet access,
our editorial department can be
snail mailed at:
2600 Editorial, PO Box 99,
Middle Island, NY 11953 USA

All writers whose articles are printed will receive a one year subscription (or back issues) plus a t-shirt of their choice.

The Problem of Effective and Usable Strong Passwords

by William Ben Bellamy Jr.

Note that in this article the word "password" is used for both singular words (strings) and phrases that are used as a password.

This article will focus on the following points:

- How are passwords attacked
- What makes a password strong
- Suggestions for building effectively strong passwords

Problem Statement

Typically, we each have dozens of passwords that we use regularly. Passwords help to protect the confidentiality, integrity, and availability of the systems and services we rely on.

For the past few decades we have been indoctrinated to think that each system requires a password that is:

- unique
- at least eight characters long
- composed from several character sets
- changed regularly

Compounding the problem is that each system/service that requires password authentication can enforce different requirements.

This is not sustainable. It forces the typical person to cut corners and look for "easy" passwords which leads to writing passwords onto paper near their systems, and using easily guessable words and phrases.

I propose that a practical and sustainable solution involves taking into account the techniques that password attacks (cracking) employ, and avoiding those techniques in order to produce passwords that are unlikely to be guessed.

How Passwords Work

When you type in your password, which is simply a string of characters, your system immediately calculates the hash value of that string. A hash value is produced by an algorithm that accepts any type or amount of material and outputs a fixed length value that uniquely represents the input material, but that cannot be reversed to find the original input material. It then sends the hash value to another system as proof that you are who you say you are - someone with permissions to access that system or service. That system - and network - only ever sees the hash value of your password, never the actual password.

The backend system compares the hash value you provided with its own stored copy of your password's hash value. If the two match, it can be assumed that you typed the correct password and have some degree of authorization on that system. If they do not match, then the correct password was not provided and no access is granted.

How Passwords Are Cracked

An attacker who has access to the password hash for an account/service will attempt to "crack" the hash value in order to learn the original password that was used to create that hash value and consequently have access to that protected resource or system.

There are two main approaches to cracking passwords: online and offline.

- Offline cracking generates the hash value of each password candidate and compares it to the hash value being cracked. Tools include John the Ripper, Hashcat, and rainbow tables.
- Online cracking submits generated hash values of password candidates to an online system in real-time until access is granted. Tools include Hydra.

Passwords usually are represented by their "hash value." A hash is a mathematical function that accepts any amount or type of material and produces a fixed length value that identifies the input material - both the content and the order - and which is computationally infeasible to reverse the process to determine a password given its hash value. If any portion of that material is changed, the fresh hash will be dramatically different from the previous. Also, it is mathematically infeasible to reverse a hash back to its original input. So a hash is like an absolutely precise fingerprint of the original material.

"Password cracking" is the process of working through a word list, and taking each word and hashing it in the same way that an unknown password was hashed. The two hashes are then compared and, if they match, you now know the original password. If they do not match, you try the next word in your list.

In addition, “rules” are applied to each word from your list. These rules describe how the initial word should be modified, manipulated, or in some way changed. These changes are intended to test variations on a word in ways that a person is likely to modify a common word in order to harden their password. The language used for rules is rather obscure and difficult to master. So most crackers will rely on existing rule sets rather than fine-tune them for a specific target. The actual word list, however, is often created with a specific target in mind.

These manipulations include, along with many, many more:

- changing letter case
- appending numerals or spaces
- prepending numerals
- inserting special characters

In this way, a single word from a word list can be morphed into hundreds of variations, most of which the attacker might never think of.

What Makes a Password “Strong”?

There are at least four factors that we can easily control that determine how strong a password is.

1. *The number of characters making up the password*. The more the better. Each additional character astronomically multiples the number of guesses required. Eventually the attacker will reach a point of diminishing returns and terminate the attack.

2. *The size of character sets*. A character set is a collection of related characters. For example, uppercase English letters, lowercase English letters, Arabic numerals, Roman numerals, special characters, and so on.

The more character sets we use in a password, the stronger it will be.

It takes ten symbols to represent the Arabic numerals 0-9. It takes 26 symbols to represent the lowercase English alphabet. So, in general, it is better to use larger character sets, and several of them.

- Alpha (upper and lower) =52 (a-z and A_Z)
- Numerals =10 (0-9)
- Roman Numerals =3 characters in 4 combinations and 1-4 symbols (I-X) (there is no zero)
- Typable special characters =~32
- Alt-characters (extended ASCII) (~129-255) 126 (`sites.psu.edu/➥symbolcodes/windows/➥codealt`, `www.alt-codes.net`)
- Unicode - astronomical count, but often impractical to type. (Unicode charts: `www.unicode.org/charts`) (Typing Unicode: `en.wikipedia.org/wiki/➥Unicode_input`)

So the size of a character space composed of upper and lower alpha, numerals, and special characters combined is ~94 potential characters.

3. *Length of the password*. It is that simple, yet extremely powerful. The longer the better. Every additional character dramatically increases the number of possible character combinations (complexity), making it increasingly computationally infeasible to successfully crack/guess.

4. *Frequency of Change*. A password is effective only for as long as it takes to crack/guess it. The previous steps will increase the time necessary to crack/guess your password to the point it is no longer feasible for an attacker to continue.

A Suggested Solution

The following suggestions will help create effectively strong passwords. You can use some or all of these to build a password. Remember that the key to an effectively strong password is the length of the string and the size of the character space.

Assuming your password is effectively attack-resistant to the point it is unlikely to be cracked, you can consider using a single password on many systems, and for a long time. And in any case, if it is cracked, the information about you on one system usually does point to the other systems you use.

General Suggestions

- Use all the character sets you can. This increases the overall character space size.
- Build a password that is at least 16 characters in length - preferably more than 24 (more on how to make that usable and practical towards the end).

The Detailed Steps

- *Decide on more than two core words/strings that will make up your password*. Select words/strings that together give you at least 16 to 24 or more characters. When choosing these words, try to have the first word begin with a lower case letter greater than “m”. That way, if the word list is sorted, about the first half of the word list will be processed needlessly. Consider the following:

  - an obscure word you would like to learn to spell

  - the name of a plant, insect, location, star, element...
  - a favorite song title or phrase, a short portion from a poem, scripture...

- *Include a random string at some point*. Consider:
  - random keystrokes
  - a car license plate number or portion you happen to see (i.e., YEO-862)
  - keyboard geometry
  - product serial number
  - a MAC network address
  - the year of your favorite movie
- *Include spaces as delimiters between the words*. For extra strength, use two or more characters (space, underscore, hyphen...) as mixed delimiters.
- *Include an alt character*. This is very powerful since it is seldom in a password cracker's rules set, and it expands the character space astronomically. You will need to research how to enter ALT characters on your particular system. (One way to make entering ALT and Unicode characters easier is to, in some very secure way, save your full password and simply copy and paste it when needed.)
- *Even better, include an obscure Unicode character*. Again, you will need to research how to enter Unicode characters on your particular system.
- *Use geeking*. Geeking is the practice of exchanging regular characters for others of similar shape or sound. When using geeking, do not use the first opportunity, or all opportunities. For example, if you could geek five characters, then actually only geek two. Below are just a few examples:

```
0 - O
7 - T
@ - a
Vv - w
Nn - m
$ - S
/ - l
( - c
```

In addition, you can use the core portion of a password over and over and simply increment one character, the salt:

- Increment for each new password. For example, left to right across the shifted top row of numerals (~ to +). This is much more powerful than simply incriminating a numeral.
- Increment through the alphabet (a, b, c...) rather than numerically.

Things Not to Include in Building a Password

- unaltered dictionary words, even in combination
- regional terms ("go cats", "go cards")
- simple misspelled words (hackorz)
- nomenclature (leet, script kitty)

An Example

In this example, note that I am not using all of the possible suggestions. Use those that will help create a long and complex string that frustrates the techniques attackers use to crack/guess passwords.

- *Choose three core words*. Let's use "mood hack coffee". In this case, "mood hack" is a phrase with meaning, and coffee is (sort of) unrelated. This also starts with an "m" or beyond.
- *Add a random string (keyboard geometry):* "[poi". This give me "mood hack [poi coffee".
- *Mixed letter case:* "mood Hack [poi Coffee". Here I change only two letters to uppercase.
- *Geeking:* "nnood Ha(k [poi Coffee". Now I change "m" to "nn" giving me an extra character along with geeking, and is also later than "m" in the alphabet. I also change "c" to "(".
- *Include numerals:* "nnood Ha(k [poi C0ffee". Simply a "o" to an "0". Again geeking, but for the purpose of including at least one numeral.
- *Large string length (more than 16):* is now 22.
- *Use more than one character set:* Here I have uppercase, lowercase, special characters, numerals. That is a character space of ~94 characters.
- *Then for good measure, I append two spaces:* "nnood Ha(k [poi C0ffee ". This gives me 24 characters. That means that this password is one out of ~94 to the power of 24 (divided by two if you want to account for the average number of guesses) possible combinations. That is a really big number of guesses on average to discover this password.

How to Remember a Strong Password

So far, great. We have the information for developing a functionally strong password, one that is crack/guess-resistant. But, now we have to remember that long string of characters. Regardless of how effective a password is, if it is not easy to remember and use, it won't remain effective.

Fortunately, there is no real difference between the words and phrases we have already learned as language and those that are contrived for use as passwords. So to "learn" these stronger passwords, simply use the techniques we used to memorize all of the words and phrases we already know.

1. *Keep the length relatively short: 24-32 characters*. Balance the number or words with their aggregate length. For example, two short words and one long word, or two long words and one short word. I find that less than 33 characters is comfortable as long as there is a meaning underneath that makes sense to me.

2. *Make the component words memorable*. The password needs to be thought of as a single idea rather than a bunch of keystrokes.

In the example "nnood Ha(k [poi C0ffee ", the core idea is "Mood hack with coffee". "Mood" uses "nn". "Hack" uses "(". "[poi" is just easy to type filler. "Coffee" simply uses a zero. Then end with two spaces. And spaces used as delimiters. Just a few tweaks on three words that constitute a meaningful phrase.

3. *Muscle memory*. Open an editor and type your new password over and over until your fingers are comfortable with the movements that are used. Start slow and deliberate, and increase the speed as you are comfortable. The key is that after a short while you will stop thinking about the individual characters you are typing and begin to understand them as a few words, and finally as one movement.

For example, type the following:

```
the dir path xcopy format
➥python list computer host
```

Notice how your mind and fingers know commonly typed material as a single movement (each word is a single movement). You do not think about each letter or the order of letters, you simply think about the word. It is the same as playing a musical instrument. Your hands know how to play an F chord rather than getting each finger to a particular place on your instrument. A G major scale is one long movement rather than a bunch of delicate movements.

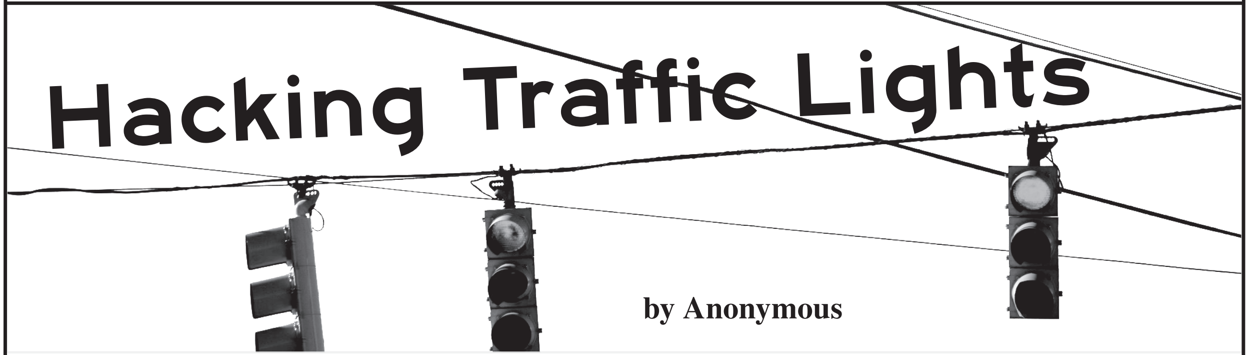
So practice typing your new password until it is more automatic than deliberate.

Conclusion

This approach, or some variation on it, should allow you to consider using a single password on several systems, and for a longer time. That is because if your password hash is stolen, the attacker is unlikely to crack/guess such a long complex password.

This approach should also help make longer more complex passwords memorable and usable.

Hacking Traffic Lights



by Anonymous

Ah, the lowly traffic light. Faithfully rotating through a sequence of colored patterns, hour by hour, day by day. Being found at nearly every busy intersection, we think nothing special of them. Even less attention is paid to the nondescript metal cabinet resting just off the side of the road by every traffic light. This cabinet is generally the size of a refrigerator if standing alone, or a microwave if on a light pole. Most are unpainted plain metal boxes, designed to not attract attention. Do not be fooled, friend! Inside this cabinet, hidden in plain sight, is a wonderland of blinken lights, electronics, and computers!

But alas, the cabinet is locked. Do not be dismayed! It is but a simple tumbler, easily conquered. And if you are lazy, you can purchase a key for a few dollars online, as nearly all cabinets use one of a handful of keys. If you do obtain a key, you may find that it also opens other nearby cabinets. Even without a key, the thin sheet metal of the cabinet affords little real security from a determined individual.

Once inside the cabinet, you will find a hacker's dreamland of lights, wires, and switches. How does all this work? I am glad you asked! The heart of it all is the signal controller. This single machine controls all of the traffic lights. In the old days, these were mechanical, much like a clock. Later, microcontrollers were introduced and some still use these. However, today the trend is to use controllers with embedded Linux.

Oh, did I mention these controllers are often networked together? Let that sink in a bit. Across the USA in particular, traffic lights are being controlled by networked Linux computers. Do you suppose these are installed by security professionals who change default passwords, disable SSH, HTTP admin portals, etc.? Or are they installed wide open as to be operated by city or town workers over a supposed "secure" network?

But wait, there's more! Consider that some traffic lights are remotely accessed via public IP address and connection from an Internet provider. One wonders if a security professional has configured and installed a firewall for these devices? Some, if not most, traffic controllers can be set with a password. This is often just a four-digit PIN. A look around the cabinet and you might even find it sketched on a scrape of paper.

The bottom of the cabinet contains rows of flashing metal "bricks." These are the load switches which translate the low voltage of the controller signal to 110 or 220 for the traffic light to operate. Be very careful! You will also find several switches on the inside of the cabinet door or just inside the cabinet. These may be used to reset the signal controller, manually cycle the signal, or place the traffic light in all red flash! Nearly every modern cabinet has a monitor that will not allow the traffic lights to go "all green" and in general will prevent any dangerous combination of lights to appear. If you try, the signal will enter "all red flash" as a protection. For your own safety, it is best to avoid this section of the cabinet.

Traffic lights are controlled by a combination of "detection" and "timing." The traffic light may have a timing cycle which runs from one to three minutes. Within this "cycle," a predetermined slice of the cycle is given to each light. However, if a vehicle is "detected," more time may be given to a particular light. Detection may be by buried wire loops which detect the metal of a vehicle. These wires are fed back to the cabinet into a "detector" (more blinken lights!) that tells the controller a vehicle has arrived. However, sophisticated camera systems are increasingly in use. You may find a video monitor in the cabinet which you may use to monitor the video from each camera. If not, every video system has a processor which can be accessed with a computer via serial or local Ethernet link. From this interface, you can view and edit the zones where the vehicles are detected. Microwave radar systems are also used to detect vehicles at traffic signals. These systems also have processors and, much like the video processors described above, can be accessed from the cabinet (or even remotely if networked). There are even Infrared and AI powered systems in some locations.

Most of the devices described above communicate over Ethernet. However, in many cabinets the primary communication protocol is Serial Data Link Control (SDLC) bus. SDLC is a fascinating protocol from the early years of computer networking. Unless you have been working with computers for a very long time, you probably have no idea what an SDLC bus is. As a quick introduction, SDLC is a 1970s-era frame-based data bus created by IBM to network machines over phone lines, satellite, and inter-building links (think Cold War, missile silos and PDP-11s). Hardly anything modern uses this protocol, save traffic lights. That said, SDLC is a very robust, well documented protocol and preserves a good deal of networking history. Along with SDLC, you will find RS-232 and RS-485 serial protocols commonly used to network within and between cabinets. As a rule, these protocols work with no authentication or encryption.

Traffic cabinets, in the USA at least, are a relic of a simpler time when high security meant a five pin brass tumbler lock. The serious truth is that traffic cabinets are ridiculously insecure, physically. Once physical access is gained, the cabinet is pwned. Even more disturbing is that if one cabinet in a series of network cabinets is breached, all of the cabinets are now pwned. If one of these cabinets has Internet access and this Internet connection is breached, the entire network of traffic signals will be compromised, without the need for physical access. I should not need to elaborate further the seriousness of such a situation for public safety.

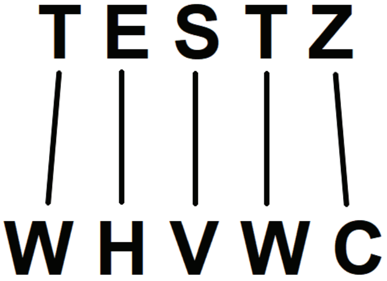
Considering how vulnerable and valuable these systems are, why are we not seeing more attacks? Either these system have not caught the eye of would-be attackers, or they have already been compromised. Which do you think is more likely?

I'll Take Some Vigenère With My Caesar

by snooze

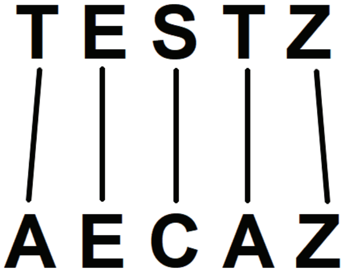
To brush up on my (extremely minimal) crypto skills, I recently began reading *Serious Cryptography*, which made me want to implement some of the concepts I was learning. For those of you who are unaware of what a Caesar cipher is, it is a pretty simple concept. You basically "encrypt" a message by rotating each letter of an input plaintext by three characters each time, and wrap around to the beginning of the alphabet if your "plus three" rotation ends after "Z."

For example, the letter A becomes D, and Z becomes C, so on and so forth. You would see the following in a Caesar encrypted message:



If you are familiar with this concept, you might also know it to be referred to as "ROT-3" encoding, where the ROT stands for Rotation and the number 3 refers to the amount of characters. Note that since there are 26 characters in the alphabet, you can expand on the Caesar cipher by changing that particular variable.

What I wanted to discuss next is what happens when we actually use a "key" to determine how much each letter gets rotated by since this is a bit more interesting. Pretend we had a key of "HAK" for the same "TESTZ" string above. "H," "A," and "K" give us ROT-7, ROT-0, and ROT-10, respectively. Since TESTZ has more characters than our key, we simply repeat the key the length of TESTZ, which would be "H A K H A." That results in the following output:



This is an example of the Vigenère cipher which, while more "secure" than the Caesar/ROT-3 cipher that came before it, is still comically insecure by today's standards and should not be used for anything remotely important. That said, I wanted to see if I could write an algorithm that accepts a key as input from a user, then encrypt a plaintext using said key, providing the corresponding ciphertext as output.

Grabbing user input and validating the key as alphabetical is easy enough:

```
import string
alpha = string.ascii _ lowercase

plainText = input("Enter your
➥plaintext to be encrypted: ")
userKey = input("Enter your
➥alphabetical key; exits on
➥invalid character: ")
cipherText = ''

# Check validity of key; for
➥demonstration purposes I only
➥accept alphabet characters

for char in userKey:
 if char.lower() not in alpha:
  print("Invalid key;
quitting.")
  quit()
 else:
  rot = alpha.index(char)
  print(rot)
```

If you run the above, you see that we get the "ROT" numbers as listed (7, 0, 10) previously. Now the first dilemma comes up; we need to repeat the key "HAK" once it runs out of characters due to our plaintext being longer than the key itself. After some sleuthing, it appears itertools.cycle is a great answer for this problem.

```
from itertools import cycle
cyc = cycle(userKey)

for char, rot in zip(plainText,
➥cyc):
 print(char, alpha.index(rot))
```

This gives us the following output and provides the logic we are looking for:

```
Enter your plaintext to be
➥encrypted: testz
Enter your alphabetical key;
➥exits on invalid character:
hak
t 7
e 0
s 10
t 7
z 0
```

Now it is time to utilize a ROT encoding algorithm which, as mentioned, I wrote previously. That said, I just added it to my code as a function called rotateChar and made some modifications to handle non-alphabetical characters and varying letter case. The full, somewhat commented code:

```
from itertools import cycle
import string
alpha = string.ascii _ lowercase

plainText = input("Enter your
➥plaintext to be encrypted: ")
userKey = input("Enter your
➥alphabetical key; exits on
➥invalid character: ").lower()
cipherText = ''
cycKey = cycle(userKey)

# Caesar/ROT Function

def rotateChar(s: str, rotate:
➥int):
 out = ''
 boolUpper = s.isupper()
 s = s.lower()
 if s not in alpha:
  out = s
 elif s in alpha and alpha.
➥index(s) + rotate > 25:
  if boolUpper:
   out = alpha[((alpha.index(s)
+ ➥rotate) - 25) - 1].upper()
  else:
   out = alpha[((alpha.index(s)
+ ➥rotate) - 25) - 1]
 else:
  if boolUpper:
   out = alpha[alpha.index(s) +
➥rotate].upper()
  else:
   out = alpha[alpha.index(s) +
➥rotate]
 return out

# Check validity of key; for
➥demonstration purposes I only
➥accept alphabet characters

for char in userKey:
 if char.lower() not in alpha:
  print("Invalid key;
quitting.")
  quit()

# Create nested list(s) with
➥the proper ROT number for
each ➥string in the plaintext

refList = []

for char, rot in zip([char for
➥char in plainText if char.
➥lower() in alpha], cycKey):
 if char.lower() in alpha:
  refList.append([char, alpha.
➥index(rot)])

# Iterate through original
➥plaintext and rotate when a
➥legal character is at index 0
➥of refList then pop index 0.

for char in plainText:
 if refList and char ==
➥refList[0][0]:
  cipherText +=
rotateChar(char, refList[0][1])
  refList.pop(0)
 else:
  cipherText += char

print("Ciphertext:", cipherText)
```

You can save the above code to a new file and run it with python3 /path/to/file.py - otherwise, my sample output below:

```
$ python3 vigcipher.py
Enter your plaintext to be
➥encrypted: Testing our CIPHER!
Enter your alphabetical key;
➥exits on invalid character:
➥secret
Ciphertext: Liukmgy swi GBHLGI!
```

Overall, this was a fun exercise and I look forward to implementing more cryptographic algorithms in the future!

Applications, Places, System: A Personal View of Linux

by Matt Johnson ech0plex88@protonmail.com

It's June 26, 2002. My freshman year of college is over and a summer of relaxation begins. One year of college, one year of independence, one year of downloading MP3s through Kazaa, LimeWire, Grokster, Audiogalaxy, and others at 1.544 MBPS. I fell in love with electronic music in high school, and college amplified that emotion. It wasn't just trance but breakbeat and ambient via Musicforhackers.com; tagline "Soundscapes for compromising a remote host." When you're trudging through calculus homework, you can benefit from Aphex Twin or Brian Eno.

In Ottawa, Canada, the GNOME (GNU Network Object Model Environment) Foundation released version 2.0 of their desktop. As foundation president Miguel de Icaza stated, "The GNOME 2.0 project is the culmination of a major effort which had the dual objectives of dramatically improving developer productivity and significantly enhancing the GNOME user experience."[1]

Unfortunately, the significance was lost on me because I was only vaguely aware of Linux's existence. Beginning with my first family PC in 1995, a Packard Bell 486, I explored Windows 3.1 and 95. The world of DOS became clear, and I was able to configure boot disks with autoexec.bat and config.sys with ease. Whatever it took to run *Star Wars: TIE Fighter*, *Silent Service II*, *F117 Stealth Fighter 2.0*, or any number of 90s simulators. By the time I graduated high school, my PC skills were based in Windows. Our school had Apple PCs with those hockey puck mice, but they were oddities, like a Fiji mermaid or pickled cyclops piglet in a circus sideshow.

Then I was a college freshman with a brand new Compaq desktop running Windows XP, sifting through our campus LAN looking for unprotected folders full of MP3s. My games of choice were *Half-Life*, *Return to Castle Wolfenstein*, *American McGee's Alice* and *Quake III Arena*. Everything Just Worked. In the spring of 2002, a teacher's assistant offered a recommendation. "You should try this," he suggested, like a street corner pusher in a rain-soaked city.

It was a Knoppix live CD, a weird fascinating experience. What is this desktop environment? What's with this penguin? At the time, I didn't know it was a Debian-based distribution using KDE. I only knew it wasn't Windows and, although interesting, wasn't my preferred OS. The live CD was returned the next day, and I didn't think about Linux for another nine years. Amusingly, the Knoppix site looks like it hasn't changed in the past two decades, and that is no criticism.[2]

These nine years passed in a flurry of ones and zeroes. My computer interests shifted from the physical PC as an object of amazement to exploring the ever-expanding Internet. I embraced social media with Facebook before Myspace, due to having a .edu email address. The personal MP3 collection grew, while movies were more easily accessible through LimeWire and that greatest of file hosting sites, the late great Megaupload.[3] Then, in the summer of 2011 I had my next Linux experience. During those in-between years spent running Windows Vista and Windows 7, I missed a significant amount of drama in the FOSS world.

On June 7, 2008, Andy Wingo blogged that "The problem, as I see it, is that GNOME is in a state of decadence - we largely achieved what we set out to achieve, insofar as it was possible. Now our hands are full with dealing with entropic decay."[4] Dissatisfaction grew and GNOME 3.0 began to take shape.[5] Two years passed and the GNOME 2.x desktop environment was the default in many distributions, including SUSE Linux Enterprise, Red Hat Enterprise Linux, Fedora, Debian, Ubuntu, and Linux Mint. The timeline progressed:

- *April 29, 2010:* Ubuntu 10.04 LTS is released with GNOME 2.[6]
- *September 29, 2010:* GNOME 2.32 is released as the last major software version.[7]
- *October 10, 2010:* Ubuntu 10.10 is the last version released with GNOME 2.[8]
- *November 17, 2010:* GNOME 2.32.1 is released as the last iteration of the desktop environment.[9]
- *April 6, 2011:* GNOME 3.0 is released.[10]
- *April 28, 2011:* Ubuntu 11.04 is released with the Unity desktop environment.[11]

Why the emphasis on GNOME 2.x? That comes later. Why the emphasis on Ubuntu? I'll cover that now. In the summer of 2011, I bought a Cr-48 Chrome Notebook through Craigslist. This was Google's pilot experiment Chromebook, distributed in limited numbers to participants in the Chrome OS Pilot Program. The light minimalist "black slab" design, resembling the monolith from *2001: A Space Odyssey*, was attractive. It also seemed like a fun device for experimentation once I learned that conventional full-featured operating systems could replace the stock OS. Carefully following instructions, I successfully installed Ubuntu 11.04 Natty Narwhal.[12]

This was my first experience with Linux since trying Knoppix in college. I didn't know anything about the enormous variety of distributions other than Ubuntu, which happened to be the most popular search result. I was completely unaware of the GNOME 2.x/GNOME 3.0 controversy, and how new desktop environments sprang up in its wake. This was an entirely recreational and experimental project that lasted for roughly one month. MacOS never interested me, Windows was the "old reliable," Linux (Ubuntu) was something new. Unity didn't bother me, as I had nothing to compare it with inside the Linux DE ecosystem. It was fun while it lasted, but as before I soon returned to Windows 7.

As I was testing Ubuntu, a more significant project was underway. On June 18, Argentine programmer Germán "Perberos" Perugorría posted an announcement on the Arch Linux[13], Ubuntu[14], and Linux Mint[15] forums. Disappointed with the disestablishment of GNOME 2.x, he spent six months forking the project into a continuation called MATE. Named for the traditional South American drink, the project was described as "a non-intuitive and unattractive desktop for users, using a traditional computing desktop metaphor." Perberos described the project philosophy as a representation of mate drink preparation through its culture of sharing, simplicity, and efficiency.[16] It wasn't long before he was contacted by Clement "Clem" Lefebvre, of Linux Mint fame, who assisted with expanded development of the desktop environment. Clem posted the first blog entry on the project's home page on December 5, 2011.[17]

I returned to Linux in time for the release of Ubuntu 16.04 LTS and fell into a downward spiral of distro hopping. Ubuntu, Debian, CentOS, Fedora, Antergos, Mint, and even setting up Arch from scratch. Lots of flirting without commitment; I suffered from option paralysis. The only aspect I settled on was a preference for the MATE desktop. Since its inception, the DE had propagated to every distribution. I first experienced it through Ubuntu MATE. As Perberos described it years earlier, I was drawn to and appreciated the efficiency and simplicity. Windows 8.1 and 10 were tolerated, not enjoyed. When the Windows 11 beta was leaked, I took it for a test drive and decided 2021 would be my Year of the Linux Desktop.

Linux revitalized my perspective of the PC as an environment in itself, not simply a tool for accessing the Internet. It has been a wonderful journey, more fulfilling than the endurance tests of Win 8/10/11. It calls back to my mid-90s adventures with DOS and boot disks. The idea of community development, globally-shared hobbies, enthusiastic support and Free and Open Source Software is immensely appealing. In contrast to the cold monolithic *closed* world of Enterprise software, Linux is *open*, with all the vibrancy and chaos that includes.

I credit Ubuntu with bringing a popular marketing campaign to Linux, without which I may have never taken the plunge. I also credit Perberos with epitomizing the idea of a software passion project, by working hard to resurrect a dead desktop environment through skill and enjoyment. MATE, and GNOME 2.x by extension, symbolize the Linux experience for me. Function over form; "unattractive and unintuitive." That three-tier menu, Applications-Places-System, as iconic an element as NCC-1701. Spanning years of FOSS development; inspiring countless retired GTK2 themes across DeviantArt, and perhaps most perfectly realized with the Ambiance and Radiance themes of Ubuntu 10.04 LTS. GNU/Linux is how I want to experience the digital world - Free as in Freedom.

[1] foundation.gnome.org/2002/06/26/gnome-2-0-released-desktop-environment-boasts-simpler-user-interface-and-a-host-of-powerful-developer-tools/

[2] knoppix.net/

[3] arstechnica.com/tech-policy/2012/01/why-the-feds-smashed-megaupload/

[4] wingolog.org/archives/2008/06/07/gnome-in-the-age-of-decadence

[5] arstechnica.com/information-technology/2008/07/gnome-3-0-officially-announced-and-explained/

[6] arstechnica.com/information-technology/2010/05/lucid-dream-ars-reviews-ubuntu-1004/

[7] help.gnome.org/misc/release-notes/2.32/

[8] arstechnica.com/information-technology/2010/10/ars-reviews-ubuntu-1010-wip/

[9] mail.gnome.org/archives/gnome-announce-list/2010-November/msg00056.html

[10] foundation.gnome.org/2011/04/06/gnome-3-0-released-better-for-users-developers-3/

[11] arstechnica.com/information-technology/2011/05/riding-the-narwhal-ars-reviews-unity-in-ubuntu-1104/

[12] chromeos-cr48.blogspot.com/2011/04/ubuntu-1104-for-cr-48-is-ready.html

[13] bbs.archlinux.org/viewtopic.php?id=121162

[14] ubuntuforums.org/showthread.php?p=11333073

[15] forums.linuxmint.com/viewtopic.php?t=86481

[16] pclosmag.com/html/Issues/201703/page01.html

[17] mate-desktop.org/blog/2011-12-05-introducing-mate-desktop/

Dial-a-Word

by N1xis10t N1xis10t@protonmail.ch

This software is for finding words in phone numbers (like 888-EYES) that you see government agencies and others using. Now, I'm pretty sure that they just pay the telephone companies extra so that they get special phone numbers. The idea behind this software is to provide the user with the ability to acquire numbers like that without paying extra.

Functionality

When you are setting up a phone line with the telephone company, what they typically do is give you an option to choose a randomly selected phone number, or have them randomly select another one. When they present you with a number, feed it into this program with no dashes or special characters (like xxx5243373 where "xxx" is an area code) and it will search the number to see if it has any words in it. If it does, it will show you what the number is in the format "xxx5-CHEESE." If it doesn't find anything, or if you don't like what it did find, have them show you another number and then check it. Repeat this until you find one that you like, or until the technician gets fed up with you.

Dependencies

This software requires that the file "google-10000-english.txt" be in the same folder. This is a file that has the 10,000 most common English words in it, and can easily be found on the Internet. I have limited this program to such a small dictionary because the running time is simply too long to be practical when you try to use an exhaustive list of English words. Feel free to try to use a better dictionary.

Notes

This software cannot find words that are less than three characters long, as a side effect of having to filter out garbage words from the dictionary. This could be fixed by removing the filter and using a better dictionary.

This software is only 6.5 kilobytes in size (not including the dictionary), and would easily fit on a 5.25 inch floppy disk.

Copyright Notice

```
# Import the dictionary
dicti = open("./google-10000-english.txt")
Dictionary = dicti.read().replace("\n", " ").split()
DictLen = len(Dictionary)
dicti.close()

# Define what letters the numbers can be
letters = {"1":"1", "2":"A B C", "3":"D E F", "4":"G H I", "5":"J K L",
"6":"M N O", "7":"P Q R S", "8":"T U V", "9":"W X Y Z", "0":"0"}

number = ""

# Garbage word filter
i=1
while i <= len(Dictionary)-1:
if len(Dictionary[i]) < 3:
del Dictionary[i]
i-=1
i+=1

# Enter the main loop
print("Type 'exit' to quit.")
```

```
while True:
printnums = "\n"
number = input("Number: ")
if number == "exit":
break
modnumber = ""
printnumber = ""

# Start iterating through all the possible letter combinations for
the number
for i in range(0, len(letters[number[0]].split())):
modnumber += letters[number[0]].split()[i]
for i in range(0, len(letters[number[1]].split())):
modnumber += letters[number[1]].split()[i]
for i in range(0, len(letters[number[2]].split())):
modnumber += letters[number[2]].split()[i]
for i in range(0, len(letters[number[3]].split())):
modnumber += letters[number[3]].split()[i]
for i in range(0, len(letters[number[4]].split())):
modnumber += letters[number[4]].split()[i]
for i in range(0, len(letters[number[5]].split())):
modnumber += letters[number[5]].split()[i]
for i in range(0, len(letters[number[6]].split())):
modnumber += letters[number[6]].split()[i]
for i in range(0, len(letters[number[7]].split())):
modnumber += letters[number[7]].split()[i]
for i in range(0, len(letters[number[8]].split())):
modnumber += letters[number[8]].split()[i]
for i in range(0, len(letters[number[9]].split())):
modnumber += letters[number[9]].split()[i]

# Once the current iteration has been assembled, check to see if it
has any English words in it
for i in range(0, len(Dictionary)):
if Dictionary[i].upper() in modnumber:
# If it does, and it's unique, add it to the list of numbers to be
printed out
word = Dictionary[i].upper()
wordlocation = modnumber.find(word)
printnumber = ("^" + number[0:wordlocation] + "-" + word + "-" +
➥number[wordlocation + len(word):] + "^").replace("^-", "").
replace("-^", "").replace("^", "")
if not printnumber in printnums:
printnums += printnumber + "\n"

# Take away the last character so a new one can be tried
modnumber = modnumber[0:9]
modnumber = modnumber[0:8]
modnumber = modnumber[0:7]
modnumber = modnumber[0:6]
modnumber = modnumber[0:5]
modnumber = modnumber[0:4]
modnumber = modnumber[0:3]
modnumber = modnumber[0:2]
modnumber = modnumber[0:1]
modnumber = ""

# Print the results
if printnums == "\n":
print("\nNo words found\n")
else: print(printnums)

# Copyright (c) /05/09/2022 N1xis10t
```

The Hacker Perspective

by ZauxZaux

We're probably all writing these submissions from quarantine. We've had time to reflect. Time to fear. Time to have hope. If we're fortunate, we've had an easy adjustment to forced "work from home" since it was probably already a perk of our jobs. "What it means to be hacker." The first time I became interested in the term was in the 90s. I watched one of the infamous movies that involved such folk and became instantly fascinated. Coincidentally, it was also the same summer I got my first laptop. What a monstrosity. The worst battery life ever. Heavy as brick. Whirring fans and horrendous boot times. Oh how I loved it dearly.

After watching that movie, I was convinced that I, a fool, had been overlooking this whirring brick and not seeing it for what it truly was: a bastion of power, a futuristic piece of machinery that could enable me to traverse cyberspace and travel into places unknown. Or so I thought. The only command I learned how to run that summer was "dir", and I got as far as downloading Python and running some sample calculator program. But fuck if I knew what was really happening. I was defeated: code and programs and hacker stuff were the things of super geniuses and people going to fancy schools, not of small town folk like me, whose only computer class up to that point was typing, and some CAD class that I had no interest in. At the time, the would-be hacker dreams were snuffed out, I was resolved to AIM, Yahoo chat, online games, and whatever else kids of my age were getting into, and some of what they weren't.

Fast forward to 2015. I had made a proper disaster out of my life from high school to 2014, got a degree I would never use, a fair bit of debt to go with that silly degree, and not a clue as to what might be next. Fortunately, by 2015 I had managed to pull myself out of the hole I had dug and began making some sort of an actual "life," albeit very humble at the time. One thing I learned through all of it was that I was more capable than I gave myself credit for. With enough time, effort, and will, one could not only rectify what had since seemed a hopeless life, but could also do all sorts of things. Things like ride a bike 27 miles to work in the middle of a scorching summer because it was a choice between food and bike ride or gas and an empty belly.

That summer I delved back into Python again. It was just as inaccessible to me, but the amount of learning information online had since become abundant and I had plenty of time on my hands, seeing as I had started fresh in a new place and had minimal social contacts. I resolved to doing at least an hour a day on a common learning site. I tracked my progress in a notebook. I took notes. I wrote for loops on paper like some masochist. I dove into Linux. Perhaps, just like most things in life, with enough time, effort, and will I could learn this stuff.

Technology was again at the forefront of my mind for a bit; it resumed the same place of intrigue and curiosity that it had when I was a child. My fascination was nostalgic; I was no more a 20-something-year-old when I was delving into all this. I was a kid again, indulging to my mind's content for hours at a time, lost in the endless complexity while barely scratching the surface. What a time.

Fast forward another year. I found someone I loved. We began trying to plan our lives a little bit. At that point, I hadn't any better ideas than becoming a therapist. The other half said that was fine, but that we would both be broke. We laughed. That same summer, entertainment made another lasting impression on me. This time the theme was computer security. And I couldn't get enough of vigilante hackers. Down the rabbit hole I went, overloading my brain with all sorts of security information. "Did you know you could hack your own Wi-Fi?" "We got you this gift for your birthday, can you tell us what the heck even is a Raspberry Pi?" I was convinced that this was the way forward.

I ditched the therapist idea and was resolved to getting into the tech industry as fast as possible. It would be a two-pronged approach. First, everything runs on software, right? So software engineering seemed like a good approach, and in the spare time, I could continue to indulge my infosec obsession. I began going to meetups. I applied to internships left and right and was rejected. I began working at a cell phone/computer repair store. I met people in industry, some great, some not. I made a home of a local hackerspace, volunteering time to help others starting the same path I was on.

Before I knew it, I had landed a low-level analyst position at a service provider. My mom thought I literally guarded the computers - like mall security, but in front of a computer. Then onward to an internal security team for a bank. My first "real job" in industry. They told me seven times between interview to first day "you know we do a follicle test, right?" I don't know if it was my long hair that I had let grow for the past year for the first time in my life, or if that's how all banks were. Joke was on them though, I'd been clean for over two years. There I learned what a great team looks like and how it functions. What a good boss is. What a good CISO is. I also learned that even if you can't type well, you can still be a killer analyst. My favorite analyst can't type for crap, but damn is he smart and funny as hell too. I miss you, my Nigerian friend - you're right "we've got it too easy!"

To me, being a hacker has been about connecting with others. Whatever that may look like. It could be your BFF at a job, you know, the coworker you're just a little bit closer with than the rest. Or it could be someone from the meetup; you've never been to each other's houses, but damn if you don't greet each other with a hug and a smile and know a bunch of little oddities about the other's life. It might be a teen-aged hacker that joined your hackthebox crew that just laughs when you say "you're miles ahead of where I was at when I was your age." Maybe it's the super whiz you know, the one that used to do some grayhat shit back in the day, the one that's a staunch open source proponent, that drops little gems here and there about opsec, or wild ass stories from other places, that has a garage full of servers and doesn't have to work anymore because they're rich off of Bitcoin, but is working at some new place because a good friend is the boss, and they want to see that person succeed. Maybe it's the leader of the hackerspace, the loud rambunctious one, that will say what's on everyone's mind, and maybe be embarrassing at times, but that's also one of the most selfless people you know; the one that offered you money which you were always too proud to take when you were out of work; the one that always offered and paid for lunch because they knew times were tough, and they never expected anything in return. It's the person you only knew by their handle and not their real name, that is until a former client from a contract job called looking for help, and then you thought "I know who needs this work more than I do right now..." so you had to message them to get their name and info; and they trusted you enough and ended up making a bit of coin. It's the person that thinks *you're* the whiz, but they don't realize that the only reason you know what you do now is because you paid way too much for power over the summer running your own server, and learned a million ways to break an operating system, including but not limited to: recursively chowning a dir and not giving a fuck; being super 1337 and encrypting your disk, then forgetting the password; banning yourself from a VPS because you were hitting the wrong IP; running commands on files with * instead of using tab completion because you were too impatient to train your muscle memory; rsyncing without a dry run and copying dest to source instead of source to dest; breaking your LAN because you didn't understand default gateways and only learned enough networking to get by... the cup runneth over.

Being a hacker has become to me just as much about bits and bytes as it is about others. It's about staying curious and continuing to learn. The transition to being someone that RTFM, and grinning nostalgically at someone whose shoes you were once in getting frustrated and turning to you for an answer. More importantly, it's about being willing to give that answer. To extend the hand that was extended to you. Sometimes we go overboard. I do. I have to remind myself it's okay to say no sometimes. When I'm volunteering, I have to remind myself that I'm a volunteer, and a human first. If I'm not keeping myself sane and happy, then I'm damn sure not going to be pleasant or of much use to others. Being a hacker is about being humble. Being able to say "I don't know." Because, more often than not, I *don't* know. That's become more true in my new position. The first week I grasped the gravity of the situation and the fires we were putting out... the amount of change we were in. I had a sleepless night full of stress when it all sank in. "What have I done!? I gave up cushy cozy bank life for stress and a bit more coin.... *What a fool!*" Then a five minute meditation the next day before work put things back into perspective. I was amongst friends. Real friends, the same kind of friends I mentioned above. One of them gave me some solace: "You have to remember that a lot of this is screwed up, but also, it's not your fault that it's that way. Remember that." So when all is said and done, we'll either emerge, having managed to pull off the seemingly impossible, or we'll go on to other things - saner places with saner paces.

Being a hacker is about finding a way. Finding a way to get in. Going back over the port list; what service were we missing? Scouring through the commands again; what flag were we missing? Googling harder; what article was I missing where this was done the *right* way? Implementing logging in your scripts; if only someone had built a sane way to track the progression of your programs! Being obsessed with reverse engineering for three week chunks; hey, I solved it and know all these r2 commands... that will surely be gone the moment something else catches my curiosity. It's about people saying "you're always on your computer!" and then having enough sense to step back and take a break, cook something delicious, or watch something interesting. It's about not letting praise go to your head, not because you can't take a compliment, but because you are in tune with your place and you know when you have become a big fish in a small pond. It's about sending DMs to that super nice Twitter person, who selflessly had an open ear for your concerns career-wise and offered you whatever advice they could, and then subsequently congratulating you once things worked out in your favor but you forgot to tell them so you did it six months later. It's about empathy for another Twitter friend doing security work in your home state; their pictures of the landscape make you long for home, and as they're going through tough times you wonder what if life had been different and you had somehow stayed there and been able to befriend this person IRL.

It's about information warfare and your cognitive dissonance as bots flooded Twitter during a big election; how you knew, not exactly, what was going on and you watched the effects play out; how you debated whether or not it would be worth the time to try and discuss such events with your parents on Christmas break. Sometimes it's about getting a foreign language intel report, then tediously copy/pasting it into Google Translate and blasting the result on Twitter because people were looking for an English copy - only to have the team drop their appropriately translated version a day later.

Being a hacker means being able to go into the unknown of the technological realm as far as your curiosity will take you. Engaging in debates with others. Helping others. Learning from others. Staying up late. Drinking too much caffeine. Becoming wiser. Discovering your true self. Doing what you love. Being there for those that love you. Identifying with vigilante hackers. Begrudgingly going to vendor events. Disagreeing with friends. Lasting relationships, fading relationships. Excessive bandwidth. Cheap laptops with modded ram. Responding to inquisitive text messages with "download team viewer first." Sending a "Let me Google that for you" link when you're feeling like a turd. Learning to love a language, learning to hate a language. Upgrading shells to fully interactive TTYs. Mapping SMB shares. Loving operating systems, hating operating systems. Being a hacker is every bit as dualistic as anything else in life. Blackhats, whitehats, grayhats. Wherever you are, happy hacking. We can do it. It's not over. It's only just begun.

End of the Dream

by Sean Haas

As I'm sitting here in my office, the Russian invasion of Ukraine is ongoing. I'm half a world away, tucked in the fold of some undisclosed state. Despite that seeming isolation, I still have a connection to the conflict. I have a friend, a journalist we'll call K, who just got into Odessa. He's based out of eastern Europe and has been trying to get into Ukraine since the war started. He finally made it after a month and some change. K has been keeping up daily reporting about the war, his travels, and where he gets his information from. Since the conflict started, I've been noticing a pattern, something gnawing away at me. I think it's something I should have noticed earlier. The dream of the Internet is ending.

The biggest triumph of the Internet has been its ability to connect the world. Some locales may only have limited bandwidth, but there are few places the Internet hasn't at least touched. The free and rapid flow of information has fundamentally changed the state of the world. This hasn't been a slow change, or some shift in irrelevant policy. I'm talking about change that has occurred in our lifetime, change that affects most of us personally.

I remember struggling with a dial-up modem back in the day. I'd check my email every few days, maybe download a file or two overnight when no one was hogging the phone. Now I'm constantly connected to some networked something. Information flows right into my fingertips. Many of my friends I've never met face to face, but I can keep in touch with them as if they were sitting right here in my office.

The roots of the Internet are fundamentally militant and aggressive (look up Paul Baran's report on distributed networks if you want to feel some spook energy), but as the ARPANET matured it transmuted into something fundamentally different. The modern Internet is, by and large, a productive force that's made the world a smaller place. However, that may be approaching an end. What if the Internet no longer touched everywhere the sun shines? What if the free flow of information ran into a roadblock?

I don't think that you necessarily need to look at all sides equally when covering a conflict. People often lie, governments always have agendas, even something as mundane as the media that carries a message can color its content. Combat footage played over a radio show loses something in translation. However, I think it's always worth a few brain cells to look at what both sides are arguing. Sun Tzu said something to the effect of: "know your enemy and know yourself." Well, we mostly know ourselves, so information gathering is often an exercise in knowing the enemy. That includes knowing how the enemy presents itself to its citizens.

K and I are on the same page when it comes to this. The media lies, some media lies more than others, but it's still important to take a look. Know your enemy, know their lies, and know how they want to be seen. To that end, K often reports on Russian state media. It's all part of the blend that makes for good journalism. At the beginning of March, the European Commission announced moves to block content from Russia Today and Sputnik. Maybe that's a good move, maybe it's not - I'm not here to argue either way. But it makes it a little harder to know your enemy.

The EU is using interesting tools to restrict this flow of information. The Commission is working with large tech companies to stop the spread of selected Russian news sources within the EU. They are using a legal framework to pressure private entities. In most cases, these entities, mainly social networks, are based outside of Europe. These are American companies that happen to do business within the EU's borders. To keep operating in that locale, you have to play by the rules.

The Kremlin has started enforcing similar policies. In the same timeframe, sites such as Facebook and Twitter have been blocked within Russia. The tools used here are different than in the west. Reporting makes it sound like these sites are blocked lower down on the network stack. In Russia this was done via, once again, legal actions. The intent of the EU and the Kremlin here is in unison: they both seek to control the free flow of information.

This is only the surface level of the story. Russia is also being disconnected on the infrastructure level. At least Lumen and Cogent have severed connections to the country. Lumen specifically is a possibly dangerous case. They are a Tier 1 ISP; that's one of the components that people reference when they talk about the "backbone" of the Internet. A single Tier 1 pulling out of Russia will probably just mean worse bandwidth, annoying but not an immediate disaster. What happens if more providers follow suit? What if there is political pressure at home to cease dealings with Russia? What if new laws within that country make it either dangerous or no longer profitable to operate there?

We can complicate the picture. There are 15 Tier 1 providers. These providers are based out of the United States, the U.K., Sweden, Spain, Japan, Italy, India, Hong Kong, Germany, and France (note that most of these are NATO countries). The reason these providers matter is that their networks can access any IP address in the world, at least in theory. If you have a hook into one, then you are tied right into the information superhighway. Theoretically, if a regime were to alienate all those countries, then they could be totally isolated from the 'net.

We have yet to see a situation where a country is totally cut off from the Internet for an indefinite period of time. It seems that once the Internet arrives, it's there to stay. I'd guess the network is just too handy for governments to totally pull the plug, or it's proven too profitable to those who back regimes. That said, there are some nations that approach digital isolation.

The canonical example is always China and the so-called Great Firewall. It's well known that the Chinese government has gone to great lengths to restrict the flow of information in and out of the country. This ranges from censorship on government-regulated platforms to fully blocking certain services. All backed up by laws and regulations, of course. But even this firewall is surprisingly porous.

PCCW Global, a Tier 1 provider headquartered in Hong Kong, retains connections with mainland China. There's one backbone right there. Foreign operators can drop servers in China - it's just a bit of a process. About ten years ago, one of my coworkers spent a few months trying to get some servers colocated in China. They eventually gave up on the idea. At the time, it was just too expensive to justify, but it is possible. So while the Internet in China may look different, there is still a flow of information. There are broad swathes of the network that will still look the same.

Even a pariah state like North Korea is hooked into the World Wide Web, at least in theory. Access is severely restricted in-country, but they do have service providers that connect up to larger networks in China and Russia. Those, in turn, eventually find their way up to Tier 1 providers.

Practice is a different matter. North Korea actually offers a taste of where we might be headed. Internet access isn't just censored, it's hard to come by. Certain government agencies, schools, and research centers have a link to the outside world. For everyone else, there's Kwangmyong: North Korea's own intranet. This is a network isolated from the rest of the world. The technical details aren't entirely forthcoming, as one can imagine. It sounds like Kwangmyong is air gapped, or otherwise physically isolated from the good fiber of the wider world. It also appears to use the same protocols as the normal Internet. Everything is just in miniature, fully controlled by the North Korean government.

A network like this offers some distinct advantages to a regime. The reduction in scale makes censorship much easier. While systems like email and chat rooms supposedly exist inside this network, they operate on a smaller scale. Fewer users means fewer eyes are needed to track their movement. Total isolation ensures that your nice network can't be used as a vector for the wrong kind of ideas. No bad news comes in, no bad news goes out, and no international actors can compromise your network. Imagine the savings in security alone!

Someone connected to the Kwangmyong isn't just looking at some limited set of the overall Internet. They aren't connected to the Internet at all. Their networked world isn't made smaller, it just is small. So what happens if North Korea decides to invade South Korea? Let's say a journalist is trying to report on the conflict. How do you know your enemy if you can't even read their domestic news? How do you get sources on the ground if no one on the ground can shoot you an email? It's not that there's no information, there's just no flow.

We may be heading towards a wider adoption of the Kwangmyong approach. A nation wouldn't even have to be a pariah state to pull the plug on the Internet. North Korea has allocated IP addresses - they can route to the rest of the world. They've just chosen to isolate the vast majority of their network. This is, no doubt, partly due to internal political pressures and partly due to external pressures.

I think it's at least possible for a similar system to be implemented in any nation in the world. Cuba has a similar system in place; a connection to the Internet for a select few users, and government-controlled intranet for the balance. Myanmar has, at some points, maintained their own national intranet. In 2011, Iran announced their intention to develop a similar intranet.

We can also add Russia to this "maybe" list. In 2019, a slate of laws, sometimes called the Sovereign Internet laws, were passed. According to the State Duma these laws mandate the creation of a "national Internet traffic routing system" (`duma.gov.ru/news/44551/`). This system can serve as a centralized means of censorship and tracking. It can just as easily serve as a choke point to switch Russia from the Internet to its very own intranet.

At what point does the balance of financial and political pressure cause that switch to be flipped? I think we might find out soon.

Where does that leave the Internet? Maybe it sees a downgrade, maybe it drops the big I. The death of the Internet may be even closer than we think. PRISM and similar projects administered by the U.S. government are already able to track Internet traffic. That takes some serious hardware and some serious access. It takes arrangements similar to those set up in Russia. I'd argue that the feds already have the technical ability to cut America's network off from the wider world. Can we truly consider the Internet free if that ability exists? Can the dream of the Internet come true while political actors can control its fate? I, for one, am savoring each packet I receive.

Why Exploiters Should Optimize Their Code

by greg

As far as Internet "bad actors," or "exploit bots," or simply "assholes" running code that tries to exploit websites for "shits 'n giggles" (or whatever reason) - by which I mean those who are simply looking to disrupt and to "hack" sites that have WordPress installed to take over admin accounts or to delete content - I have some things to say.

First, and foremost, I am not discussing those who would want to remotely (or otherwise) install malware or ransomware, but those actors who regularly use Hypertext Transfer Protocol (RFC2616 et.al.) directly to try to exploit websites.

Like this:

```
GET /wp-includes/wlwmanifest.
➥xml HTTP/1.1
```

You should all know what I mean. (If not, keep reading *2600 Magazine*...)

If one *has* WordPress installed, that may be a legitimate request, but if one does *not* have a WordPress website (like my pathetic little static site), such a request *should not happen*.

Thing is, they do. They occur, literally, about one thousand times per month. That ain't the problem, per se, as my site don't care. To it, it's just a 404 - which I make the response just a few bytes directly by Apache's .htaccess file.

The thing is, multiply that by one billion websites and the entire Internets slow down.

Get it?

Obviously, WordPress is not the only code being exploited every second of every day over the entire Internets. I am using that as just one example. I am not mentioning the 2,000 or so other "CMS" software with exploits....

A few thousand, few byte, 404s per month? Yes, no big deal. But it's more than that.

1. Exploit code does not just try for that one file, they try for dozens of path variations.

2. Exploit code does not use a single IP address or User-Agent string.

3. Exploit code does not give up. Ever.

All this means is that one cannot block them easily. Deny by IP? Losing battle. Deny by request strings? Losing battle.

Again, I am thinking of just WordPress shit. (If you have WordPress, more on that later.)

The simplest blocking mechanism is this Apache configuration:

```
ErrorDocument 404 "FU"
RedirectMatch 404 "(?i:wp|wordpr
➥ess|admin|xmlrpc)"
```

That won't cover all, but it is the basic example to stop 90 percent of WordPress exploits upon first request before loading one's own massive 50MB+ CMS! (One can see how just a few more strings in the match list can help.)

Now, to the point of this article, an appeal to *exploit code authors*. Yes, that is exactly what I am doing.

This appeal is based on one simple little obvious fact: `GET / HTTP/1.1` and then look at the results and *see if any WordPress signature is there!* And there will be! For WordPress *informs everyone that it is a WordPress site!*

Therefore, to all Wordpress exploit coders, just check the root page and if WordPress is not indicated, *stop further requests and move on to your next target!*

Let me add here a log excerpt of an example of some WordPress exploit code. Instead of wasting *2600 Magazine's* valuable space, I will not excerpt the entire log blurb but the files requested - each request just one or less seconds apart:

```
/
/
/wp-includes/wlwmanifest.xml
/xmlrpc.php?rsd
/
/blog/wp-includes/wlwmanifest.xml
/web/wp-includes/wlwmanifest.xml
/wordpress/wp-includes/
➥wlwmanifest.xml
/website/wp-includes/wlwmanifest.
➥xml
/wp/wp-includes/wlwmanifest.xml
/news/wp-includes/wlwmanifest.xml
/2020/wp-includes/wlwmanifest.xml
/2019/wp-includes/wlwmanifest.xml
/shop/wp-includes/wlwmanifest.xml
/wp1/wp-includes/wlwmanifest.xml
/test/wp-includes/wlwmanifest.xml
/wp2/wp-includes/wlwmanifest.xml
/site/wp-includes/wlwmanifest.xml
/cms/wp-includes/wlwmanifest.xml
/sito/wp-includes/wlwmanifest.xml
```

Let me remind you that this happens thousands of times *per month* on just my no good, static website. But who cares, right?

You need some math: *billions of websites every second of every day.*

Ignoring *all other exploitable web code....*

Here is the crux of the title to this article:

I appeal to all WordPress exploit coders to please check the root page and, if WordPress is not indicated, move on to your next target!

My criticism is, are you coders or are you assholes?

Fine with your exploit coding! Just, please, for the sake of the world, *do it right!* Blind requests like the above example, is... *simply pissant amateur coding.*

None of you are hackers. None of you are doing anything but declaring, "I am an Idiot Script Kiddie." Grow up.

Hacking into the Past

by Curtis Vaughan

In my youth, I would take apart various electronic games, un-soldering and re-soldering them, and taking pride in the fact that that the successful operation on the device worked. However, with respect to my first computer - a TRS-80 - it would have been beyond all reason to vivisect such an investment. An old TV, a radio? Who cared? But my computer? No way.

Back then, computer magazines would advertise computers that you could assemble yourself. Although interesting, I did not have the confidence to build a computer, nor the resources.

Time jump to the late 20th century: then an adult without any technical training, I often fixed tower computers and even built a few. Jump again to today and the advancements in technology - most computers are single-board devices. Alas, there's nothing to assemble and little that can be repaired. Not that that has stopped me.

A few years ago while browsing the web, I discovered PDP kit replicas. Intrigued by the possibility of not only building, but operating, my own PDP-8, I took the bait. Thus began my new hobby into vintage computers.

Big time jump to the dawn of microcomputing, albeit through the lens of retro kits. Starting with the PiDP-8/1, I then went on to build a PiDP-112, an Altair 88003, an IMSAI 80804, and finally a KIM-15 - all computers that I had only read about were now at my fingertips.

Building them was only the beginning of the adventure. Although sometimes challenging, the real work was figuring out just how to operate the various systems. What could one do with them? What programs could be run? This is where things get really interesting or, depending on one's disposition, quite dull. You will have to dive into reams of documentation, which is often somewhat esoteric. In additional to technical documentation, the magazines of the era (most of which are available at archive.org) will also further one's submersion into the past.

With my curiosity piqued, I began to collect vintage computers: Kaypro 4, HP 54B, Poqet Pocket Computer, Heathkit M4100, and various TRS computers, including the TRS-80 Model 1 - back to my very first computer.

Perhaps because I'm a Linux user, I'm also something of a Luddite. As I often use terminal-based programs instead of perfectly reasonable GUI applications, it was natural to use various text-based programs and games on these computers. Of course, I've played my fair share of text adventure games, but there were terminal-based versions of *Lunar Lander*, *Pacman*, and *Donkey Kong*. Although I had used computers during the BBS age, I never had a modem, so it was an adventure for me to visit still existing BBSes from these systems.

To further challenge myself, I discovered Wordstar for the Kaypro. I vaguely recall knowing about Wordstar, but I had never used it. But now, there it was waiting to be "newly" exploited. As with vintage hardware, one will find another adventure into the past figuring out how to use vintage software. In this case, I decided to fully immerse myself and write part of this article on Wordstar. Due to the modern-day demands of the *2600* editorial staff, however, I could not submit this article in Wordstar format and had to deal with conversion issues. Again, learning! I was quite impressed by how capable Wordstar is and wondered whether we really need such complex word processing programs today?

Part of this article was also written in AlphaWorks on the extremely portable Poqet Computer. The major hurdle in this case was getting files off the proprietary PCMCIA memory cards used by the Poqet. Prior to using the Poqet to compose anything, I had to figure out how to access the PCMCIA cards from another computer. After days of trial and error, I finally found an old PC tower, onto which I was able to install Windows 95 and get a PCMCIA adapter to work with said cards. There were so many times when I was ready to give up, but success meant a much greater appreciation of this first-generation pocket computer.

I would encourage readers to invest in at least one of these vintage projects. Whether you have ever soldered before or not, you'll get the hang of it pretty quickly. I hadn't done any soldering in 40-odd years! As you solder away, imagine those early computer designers planning out the boards, circuits, etc. I have no idea how one does that.

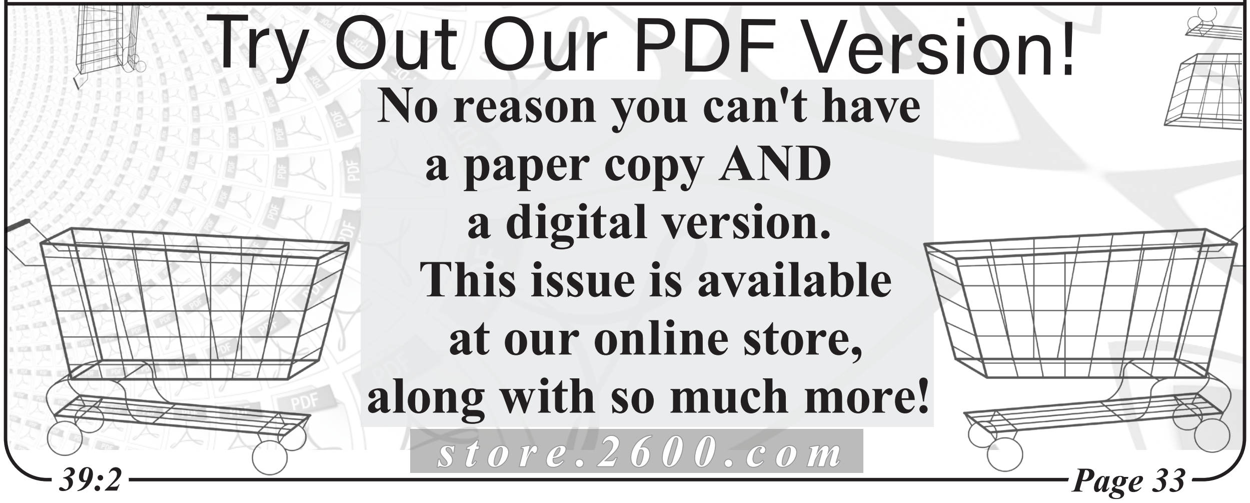
I know there are many out there who cannot understand why one needs the vintage hardware when one can simply run an emulator. Undoubtedly, I could never afford every bit of vintage hardware and have on many occasions run emulators. But if you are not sitting in front of a device that sounds like a prop airplane, ensconced in the smell of overly heated electronics, bathed in the strobing warmth of a CRT, then you will never puncture through the firmament holding you in the present. The past will remain an illusion.

Once you start down this journey, you will want to join in relevant user groups, as they provide a plethora of information and assistance. I was also amazed to discover that there are many enthusiasts who have gone through the trouble of developing accessories to these, dare I say, outmoded computers, making them very competent devices.

Needless to say, I do live in the present, but now I have the option to hop behind one of my time machines and venture back to the vintage computer days.

References

obsolescence.wixsite.com/
➥obsolescence/pidp-8
obsolescence.wixsite.com/
➥obsolescence/pidp-11
adwaterandstir.com/altair/
thehighnibble.com/imsai8080
www.tindie.com/products/tkoak/
➥pal-1-a-mos-6502-powered-
➥computer-kit/



Prognoses

Findings

Dear *2600*:

Anyone else have an email address that's too popular to use? I managed to get in on the early days of Gmail with a very common email address. I get so many emails for *other people* that I can't even use it. Today I got someone's Kenny Chesney tickets straight from Ticketmaster, no spam/scam.

Carl

This is yet another problem Gmail has. Way too many people assume they have email addresses that they don't actually have and the scenario you describe repeats itself over and over. We've been experimenting with this for quite some time and often get all sorts of personal information, as well as inside corporate and government details that we really shouldn't be seeing. With Gmail, it comes to you without your even asking because everyone somehow assumes they have the address they want. We never noticed this issue with Yahoo, Hotmail, or any of the other email services of the past.

Dear *2600*:

My wife's email address is very similar to someone else's, and she's frequently on email chains involving the same cluster of people (a random community in Alaska). She has tried politely several times to get removed from these chains, but the folks using them are seemingly very un-tech-savvy and misunderstand, re-include her later, and the cycle continues. My wife has taken to just ignoring it and amusing herself by passively reading the communication. So my question is, if it were you, what would you do to mess with them? It's a group of five to ten people who do things like plan lunch outings. The main person who misuses my wife's address is the intended correspondent's wife. She often forwards things like utility bills and "honey do" sort of reminders.

J

As these people seem mostly harmless, we don't advise anything that would really mess with them. This kind of cluelessness is extremely common. To have some fun, we suggest becoming part of the conversation until they realize that they actually don't know who it is they're talking to. Actually showing up to one of their lunch outings would sure be fun, but the trip to Alaska might be a bit much. If you really didn't like them, including them in a different mail chain would probably get them running off the net in a hurry. The possibilities are really quite endless. We'd like to hear more ideas.

Dear *2600*:

Ever since the war in Ukraine started, Russia Today's website rt.com is offline every now and then. They've even installed a DDoS checker.

Peter

It's been rather interesting to see the evolution of this. RT was a channel seen on many cable and satellite systems through Europe and North America. As Russia's unfortunate actions progressed, the channel began to be taken off of these outlets. Then it became only available via YouTube. Then they were kicked off that platform and were only reachable through their own website. Then that site was attacked and taken offline, as well as blocked by various providers. We're currently able to reach it fairly easily, but that can change at any moment. Creative types can almost always find a way around the blocks, as people have been doing inside Russia when trying to reach many Western sites that are blocked there. We believe all of these sites should be accessible to everyone, but there's absolutely no obligation on the part of any cable, satellite, or Internet service to amplify their messages. We believe individuals are usually smart enough to be able to distinguish truth from fiction on their own. In groups, not so much.

Dear *2600*:

I've had Verizon Fios for 14 years now and it has *never* gone down!

Jesse

We're not sure what prompted this proclamation, but we just know you're going to regret saying that.

Dear *2600*:

So yesterday I experienced my first automated fast food order at a McDonald's drive thru. In true form, it totally f'd up my order and I had to repeat myself several times. Eventually a human came on and asked if I needed help. Is this the future? Ordering with Alexa?

Brad

It probably is. But if this dystopian hell has to exist anywhere, it may as well be at McDonald's. And we can always count on people to do what it takes to clog up the works.

Dear *2600*:

So evidently Irish cellphone provider Eir has screwed up its clock, and is resetting cell phones to a very wrong time. I don't know how they can screw something like this up so badly. It takes real talent.

Robert

We prefer to think of it as a test to see if people are paying attention. And maybe a reminder to never believe anything you see on your phone without question.

Dear *2600*:

I have been reading *2600* since the early 1990s and have been involved in hacktivism my entire life. I don't know if you all have noticed it yet, but there is something "wrong" with the world right now. They are taking over the planet. I don't know if they are aliens, fallen angels, cyborgs, etc., but I know this. In 2019 I stood face to face with some sort of 14-foot-tall, white skin giant that spoke directly into my mind and said, "this is the only time we will see each other face to face." I don't know what the literal fuck it was, but I have a few theories. Since this happened, I started looking heavily into freemasonry, Nazism, and both of their connections to the Ashkenazi Jewish people - who aren't even "Jews" but some steppe people from the Caucasus Mountain region. The Nazis never "lost" World War Two. They just changed strategies. They are trying to enslave all of us right now. The 5G system and the vaccine are *not* what they are telling people. The vax contains nano particles of graphene oxide. GO will vibrate rapidly when 26ghz microwave radiation is applied to it. The 5G system can produce 26ghz radiation. It is a fucking remote control killswitch. There are literally *billions* of people with some fucking nanocyte death system inside of their body right now. I began talking about this on my YouTube channel that had close to 30,000 subs and my account was *banned* within 20 minutes of uploading the video after having had it for ten years. I don't know if you all are infiltrated like Anonymous has been (they are a CIA psy op at this point), but unless you want to be fucking enslaved, I need help. I have a plan to stop this, but I cannot do it on my own.

Jason

There are plenty of letters that we don't print, but occasionally we feel compelled to share one so readers can see the type of content that pours into our offices. There's a lot going on here, none of which we're going to touch, not because we're part of the conspiracy (which, of course, we are), but because there simply isn't enough time in any of our lives. Much of this is being spoon fed to people everywhere and accepted as gospel by those who lack the ability to question things that don't make any sense. The people who are the real problem are those who take advantage of this for their own selfish purposes. That's a conspiracy that's quite real.

Dear *2600*:

Hey real quick, Computerphile has great videos on Unix and the history of Bell Labs.

Zach

Too quick. We were able to figure out that you were referring to a channel on YouTube, but others might not have. There's no need to rush. That said, yes, there are all kinds of cool videos there.

Dear *2600*:

I never thought of myself as a hacker. Maybe if I had acquired hacker credentials from *2600,* I would have. But there have been times....

Like the time I received a list from an organization including names, addresses, zip codes, and another identifier (that I can't go into). Several million records in a PDF file. No other format such as text, CSV, or Excel. I only wanted the cross reference between the zip code and the other identifier that the organization obviously must have. So I contacted them and asked, but was rebuffed, told that their contract with the post office in this country didn't allow the cross-reference information to be released. But I had it already in a giant haystack; I just needed to find the needles. There were millions of records over thousands of pages, based on this cross reference. But how to obtain just the tiny fraction that I needed? Any manual process would obviously take too long.

Luckily I remembered that Adobe Acrobat contains an implementation of JavaScript. With this I was able to go to each page and sequentially ask for each line. This, unfortunately, returned header and footer lines and other junk, but the lines I wanted had a very consistent format, so I could throw away every line that didn't match the data format. For each data line, the script would extract the ZIP and other identifier, look it up in the smaller list I was generating and, if it was a new pair, add it to my list.

So, after several hours of crunching PDF pages, I had exactly what the organization refused to give me.

I wish I could give more details, but I'm sure you don't want me serving time....

D1vr0c

It doesn't really sound like you'd be in any trouble for revealing what this list was all about if you were able to contact an organization that had a contract with the post office concerning this same data. But lists of millions is hardly enough these days to even make it onto the news. Remember, Equifax let data for over 100 million people get out. Yahoo lost private info for over three billion! You know we're in bad shape when leaks can't keep up with what the companies lose on their own.

Recommendations

Dear *2600*:

My daughter is going to her first concert with a friend and she is 15. I will be dropping her off and picking her up. With her consent, is there some sort of tracking device we can install on her iPhone so I can know her location from my Android phone? I realize it sounds creepy, and I may be over protective. But I assure you it would just be for this concert and maybe others.

Max

You really don't need our approval to do this. It's quite common, actually, although the potential for abuse is huge. "Find My iPhone" is just one of *these apps - there are many. But we can't mention such an app without also telling people how to detect them on their phones (which shouldn't be a problem in your case if you did in fact get consent). In most cases, the tracker would need to have physical access to your phone at some point and would also need to know your Apple ID and password. Changing the latter can help to stop tracking from continuing. If you're using a feature known as "family sharing," you can be tracked by other members even without knowledge of your password. Checking what apps are installed and running is usually the best way to find something like this. There are numerous other methods for compromising your phone, such as iCloud or admin access to local routers. We hope to see a detailed article on the various abuses out there.*

Dear *2600*:

I'm a big fan of the magazine for a long time, and a subscriber since 2008. Congrats for the fantastic work you have been doing for the hacker community.

Although I've never written any letters, I wanted to share the way I'm storing my physical magazines, as it was suggested by *2600* in one of the past editions (don't recall which one).

I'm using "photograph" sleeves (8"x9") from BCW, and storing them on small boxes (same as those used to store standard comic books). I'm also fastening the back of the sleeves with standard Scotch tape so as to maintain them perfectly closed.

It's a perfect fit for me as the "digest" sleeve format also from BCW is larger than the *2600* mag and the "comic book" sleeves are too small.

Hope this helps hackers/collectors to store the mags throughout the ages!

Keep up the great work.

sl33p

Thanks for that helpful suggestion. We'd love to see pictures of this and other methods people have devised.

Dear *2600*:

I am writing to see if you can help me. I am looking for two things. I am looking for a secure private chat service and a secure private payment service to pay people with. Venmo is just too open for me.

Sean

There are tons of so-called private chat services, but there's always someone who will tell you they're not as private as they claim or that they're run by some evil entity. You need to simply use a service that employs encryption and connects you to the people you want to communicate with. Then take the usual precautions since there isn't a system anywhere that can't be compromised in one form or another. As for private payments, paying by cash remains at the top of the list. Disposable credit cards and gift cards are probably the most anonymous methods of payment, but they require a bit of coordination. Otherwise, there are plenty of semi-anonymous options, each of which has its own unique weaknesses.

Dear *2600*:

We all know that Mastodon and the fediverse exist and should be using that instead of Twitter anyway, right?

Chris

While such decentralized outlets are far preferable and don't run the risks of abuse that the mainstream social media companies do, let's not kid ourselves that there won't also be negativity and abuse on these platforms. As long as we don't believe this will solve everything, any disappointment won't be crippling. (We're also looking for a good comprehensive article on this.)

Memory Lane

Dear *2600*:

I was wondering if anyone might be able to fill in some gaps in my memory. I recall using a chat system of sorts at the University of Alaska Fairbanks in 1989-90. I recall I was able to talk to users at the other two campuses pretty easily (one on one, it wasn't a chat room). I was also able to get out and talk to other people at other universities - several U.S. schools and some of the European ones, some cool guys at the University of Helsinki (I think?). I just remember one of the admins for that system went by the user purplehaze and was a super nice guy. Does anyone know what program(s) they probably were? I want to say the university system at the time was IBM A/S 400 if that helps at all.

Bill

While we can't steer you to any of the specific systems or people, we can confirm that it was indeed once possible and common for users of one university system to be able to chat with users of other systems using programs with names like "talk" or "ytalk." Some of this software can still be found on many Unix-based systems, but we don't believe it's still in use between systems anywhere as the security holes this opens up are just too great. Most of this predated instant messaging, the web, and even SMS.

Dear *2600*:

How many people still get on Usenet? The alt.2600 thread made me think back to what was once a thriving community on the Internet. Agent Newsreader was my go-to choice to get on... that and my WWIV BBS.

Miles

We would love to know how many people still are on Usenet and what they are reading. We have fond memories of alt.2600, but like much else on Usenet, it turned into a real shitshow of spam and abuse.

Dear *2600*:

Hello, I'm clearing out a magnetic media HD here, and found something I wrote that I never sent you. I think it's pretty amusing! Had forgotten about this. Do what you want.

"How to Steal Things Part 2 (25 or so years later) by J.J. Styles aka 0ptiKal i1usioN aka Zot the Avenger

"Okay, this article is completely despicable, it completely undermines the capitalist system that holds our society together. But, this is a *2600* article and I've been reading this magazine ever since the How to Steal Things article. So here it goes. Go to any store, buy two items, return later, and say that you got double charged and that you didn't realize it. They will refund you for one of the two items. Then return later with the same receipt and return the first item. You will have the second item completely free. Getting double charged is a simple mistake. It could happen to anyone at any store. You know they're scanning the barcode and it beeps but they don't hear it, so then they scan it again and they hear the beep and they're like okay everything's good but it's not, cuz you got double-charged! If this technique works for you, I don't want to hear about it. This right here is a reason to use the self-checkout because I never get double charged when I use the self-checkout because I pay attention and I only scan the barcode once. Don't be a criminal! Fix the system! Goodbye."

JJ

Yes, this is outright theft as you correctly conclude. The original article you refer to was indeed printed back in our Winter 1996-1997 issue and wound up pissing off a lot of people, which was our intent, as too much of the hacker world seemed to be veering into common criminal behavior at that point in time. We're all about the theory and the technical explanations, but stealing has always been stealing.

Dear *2600*:

Back in the 1970s and 1980s, you could call a number - xxx-xxx-0046 - and hear a strangle tone that just went up and maybe down. Was told by a phone tech that it was a special number for testing something or another. Anywho, told our female friends and for years they'd give out that number at clubs. We called it the acid line. Sadly, since analog has left the scene, so has the acid line. Can anyone confirm this?

S

It sounds like you're referring to a sweep tone that used to be operated by the phone company. In New York, they could be found on numbers ending in 9979 and were used to test frequencies on a phone line, but for some reason only in analog switch areas. It was definitely a good number to give out to people you wanted to annoy, as was the always-busy extension of 9970. Believe it or not, some of these test numbers are still in operation, but it's a real challenge to find them. Our recent series on phone switches shared a few of these numbers. We will certainly print more when we find out about them.

Dear *2600*:

A couple of my earliest "hacking" experiences: In middle school (1994 or 1995), we had a "computers" class that was really just a typing class. For some reason, the word processor we used had an option buried in a menu that dropped you to a DOS prompt. I couldn't (or didn't) do much, but I could explore the network drives and see some cool stuff. That got me yelled at by the teacher. Another one: In that same class, our usernames were algorithmic (it's been nearly 30 years so I don't remember the exact formula but think something like "smithj" for "John Smith") and our passwords were our student ID numbers. Pretty secure for a bunch of 14-year-olds who didn't even know their own student IDs before this class. This teacher also posted our grades on the wall. To anonymize them, she posted them by student ID instead of name. So it wasn't hard to match them up to usernames, and soon I had all my friends' usernames and passwords. We used to get into their accounts and mess with their assignments and stuff.

Eddie

In many places, this would be enough to get you labeled as both a computer genius and a massive threat to the entire school. While the technology has changed over the years, the attitudes haven't. And, in many cases, neither has the security.

Dear *2600*:

Many decades ago, I taught "Introduction to Teleproceasing" at a college in New York City. The first time I created an exam, it was an accident.

The first day of class, I told the kids that I would call my final exam "20 Questions" as my personal rebellion to the Education System. After I printed out the two page exam, I noticed a mistake. At the bottom of Page 1 was Question 19, and at the top of Page 2 was another Question 19.

I then recalled a friend lecturing me on Exam Panic Syndrome, and made a decision. I explained about the two Question 19s as I placed the exams face down before each student at every desk, and said that as a consequence of my mistake (and having promised them 20 questions and not 21), they would be granted one free wrong answer. The collective sigh of relief in the room was palpable. I kept the two Question 19s in the exam in subsequent semesters. Only those who got all 21 questions correct got an A+ on the exam.

Cheshire Catalyst

What we really want to know is what kind of material was taught in "teleprocessing" back then.

Offerings

Dear *2600*:

We would like to place the article on your site.

Do you allow the guest posts with do-follow links on your website? If yes, can you tell the price for that? Thanks a lot!

Daniel

This shit again. What if we just say it costs a million dollars? Would that make it stop? Or would it make us rich?

Dear *2600*:

Hi there. At this point, you may be thinking "Wow, this person has been bothering me for weeks, what a tremendous heart! Is this person going to summit Mt. Kilimanjaro next?"

All jokes aside, the reason for my persistence is I believe our Shopify agency can help you deliver a seamlessly interactive, innovative, and scalable e-commerce solution so you can attract more customers, untap bigger ROI, and grow your business into the future.

Are you the right person to be having this conversation with? I'd appreciate any reference.

Lisa Hudson
Business Development, PureLogics

No, Lisa, we are not the right person. We are the letters department and what we were thinking had nothing to do with Mt. Kilimanjaro, but now that we've thought about it, we would like to suggest that you relocate there and be sure not to bring a computer or communications device.

Spam has gotten so conversational in recent years. Soon we will be having spirited debates and fights with AIs and, once they interface with robots, actual battles will commence. We are already planning ways of sabotaging this dark and dangerous future.

Dear *2600*:

I am the Project Manager working with Middle Island Country Club in Middle Island, NY. We are creating the brand new scorecards to be used by the golfers that will be highlighting a few local businesses around the scoring grid. The course has invited your business to be featured for 12 months in front of all golfers as the industry exclusive.

Jude

This goes on for quite a bit about what a great opportunity this is. It makes us ponder what kind of message we might have for local golfers and how simply having a post office box in a particular community is enough to get pulled into this world. Had they done even the tiniest bit of research, they would have quickly realized that giving us a mouthpiece to their clientele would end badly in every possible scenario. It almost makes us want to try.

Dear *2600*:

Hello concentrationcamps.us
Hope you are doing well.

I was examining your website and saw you have a good design and it looks great. But it was not ranking on any search engines for most of the keywords.

[...]

Note: We are not spammers and are against spamming of any kind. If forwarding this email has made an offense to you or to your company, then we apologize for the same. In order to stop receiving such emails from us, simple type "NO" in the subject line.

Warm Regards,
Maveric Miller
Digital Marketing Executive

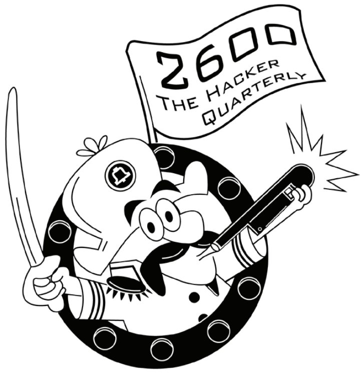
NO.

You wrote to concentrationcamps.us with this unsolicited cheery message and a pitch to do some kind of search engine business. How could we possibly be offended? You are the very definition of what spam is, from the cluelessness of your initial contact to telling us that the only way to stop hearing from you is to respond to you. Does this approach ever actually work?

Dear *2600*:

Hey there *2600* - people sure do want some new swag. I couldn't sleep last night, so here's my contribution for a possible new design. Are there potential copyright issues? Possibly. But it's your design now. Do with it what you will. Love ya.

Moose



Well, we sure don't want any trouble with the Quaker Oats people. But this was too good a design not to share. Thanks for thinking of us.

Thoughts on Meetings

Dear *2600*:

I live in Miami and have always wondered why there was never a meeting here in the biggest (and most well known) city of Florida. And it's not just because of COVID-19; there hasn't been as long as I can remember (which means decades).

I find it impossible to believe I'm the only person in Miami with the *2600* "hacker" mindset. In fact, I know several people/friends that would be joining if one was created (assuming I had your blessing, of course).

What is required to start a *2600* meeting (if you don't mind my asking)? I'd like it to be an official *2600* meeting and have it published in your future editions (only to draw in the most amount of people). And yes, I fully agree with everyone having to be vaccinated and will do everything in my power to state that requirement. What are the requirements as for where it's held?

Also, is there a certain part of the city where it would have to be held? I only ask because Miami is quite a large (and spread out) city with a lot of traffic and essentially no real (practical at least) public transportation. Especially Friday at 5 pm (which is peak rush hour) - that could easily take three or four hours to go from one end of the city to another. Again, assuming it's OK with you guys, I'd much prefer making it slightly later in the day (only because of what I said above). I'd say 8 pm would be the best time if being totally honest, but even 7 pm or 7:30 pm would make it much better than 5 pm (in my humble opinion).

Not that I'd think I was some kind of "leader" of that meeting by the way. I have zero such ambitions, I promise. I just want to link like-minded people together (for everyone's sake, including my own as well).

Anyways, thank you for your time. I appreciate it as always. And I'm almost done with my next article submission for you guys, by the way (actually I have several I'm working on).

Thanks again! Much love!

Doorman

We appreciate the support and we look forward to seeing more articles. To address your questions, it does indeed sound like starting at a later time might be best for your particular location. But you also want to make sure it remains open for those who can't stay out too late. It's a great question as to why there hasn't been a meeting in Miami in recent years, but usually the reason winds up being simply that nobody took it on. All it takes is one person to start the process. We prefer that meetings be held in easily accessible public spaces. That's something a native of the area is best off deciding. And, yes, you have it exactly right that setting up a meeting doesn't make you the "leader" of those who attend. We take great pride in nobody being in charge of our meetings. We wish you luck and hope to see something come out of your city soon.

Dear *2600*:

I was looking for *2600* meetings in Wisconsin and didn't see any on the list. Are there any groups (active or otherwise) in Wisconsin?

Nathaniel S

We're certain there are lots of people in Wisconsin who would be interested in meetings. The challenge is in reaching them and in getting one person to come up with a public place in which to start them. It's actually not that much of a challenge, but you'd be amazed at how we often convince ourselves that somebody else will step up. Every meeting we've ever had has started with the initiative of a single person which led to the flourishing of an entire group. There were meetings in Wisconsin before the pandemic, so we see no reason why there can't be meetings now.

Dear *2600*:

Hope all is well. I was curious what the startup plan is for the Toronto meeting?

Jeff

All it will take is someone from that meeting sending us an email (meetings@2600.com) or a DM on Twitter (@2600Meetings), letting us know where and when the meetings are. We will then help them spread the word. It really doesn't take much. We just suggest people choose a meeting location carefully so that it's easy to get to and in a public place.

Dear *2600*:

When is the next U.K. meeting?

Samir

Same as everywhere - the first Friday of the month. Check www.2600.com/meetings for specific locations or contact us to start a new one.

Dear *2600*:

Hi! I've read *2600* since I was a preteen. Now I'm in my 30s and, well, a "cloud engineer." I stay between Bali, Indonesia and Seattle, Washington, USA. I would love to host meetings for either or. I think there is an active Seattle *2600*, but I've never seen one for Bali. Could I get a listing in for May and future months?

Steven

Yes, but you have to tell us where you want those meetings to take place! Please send us the details. We also presume you'll be in Bali enough times to help the meetings take off.

Dear *2600*:

Was Petrozavodsk removed from the list because of the events in Ukraine?

***2600* Petrozavodsk**

Technically, yes, and we must apologize for that. We were contacted by a representative from another Russian meeting who requested that both meetings be delisted because of those events. We assumed they were speaking on your behalf, but clearly that wasn't the case. We've since restored your meetings to our listings. And we hope to see the other gatherings resume.

Dear *2600*:

Could you please give me the email address of the coordinators of LA2600? Thanks.

Queuemark

We don't give out personal info for anyone. What we can suggest is that you send a Direct Message on Twitter to @la2600 or visit www.2600.la, although it doesn't look like either of these outlets has been recently updated. Hopefully, we'll get an update in the near future. Failing that, anyone is free to restart them at a convenient location.

Random Bits

Dear *2600*:

If your computer is going slow, it might need more memory: DownloadMoreRam.com.

Alex

Who knew you could download RAM? We're sold.

Dear *2600*:

To find exposed FTP servers, use the following Google Dork: *intitle: "index of" inurl:ftp.*

Jim

There is an incredible amount of exposed content out there that's really easy to find and *that we often forget about. Thanks for this handy tip. (Although we should warn people that despite this being a simple command to access publicly available content, there are clueless people out there with a lot of power who will say you're committing a crime by doing this. You are not.)*

Dear *2600*:

Seems very strange that the far left are losing their minds because an African American bought a social media platform in order to promote an open and inclusive dialogue. What gives?

Lee

You think you're pretty clever, don't you?

Hello *2600*:

Please do not change the greeting line of this letter to read, "Dear *2600*". Thank you.

N1xis10t

That's the power of "please."

Security Issues

Dear *2600*:

So I brought up a problem with security in a group for Rove R2-4K dash cams. Why do they not allow you to change the default password? The password is 12345678. The responses I got from idiots in the group is amazing.

D

We don't doubt it (but please always share idiotic responses). Perhaps now that it's getting more attention, this "feature" might be added?

Dear *2600*:

Right now in America, a certain group of people are losing their mind over the idea that an app that tracks their period could be used against them if certain laws in states they do *not* live in are passed. And that "they" will know what is happening in their bodies. So what is stopping "them" from tracking you as you sit on the chair at a gynecologist, or any other doctor's office or service provider for two hours? Think of all the RFID tags ESN, IMEI, SIM, MSN (SN), and PIN identifiers that will connect to the apps on your cell phone that will tell "them" everyone around you, and which doctors and nurses are helping you. Not to mention the Wi-Fi networks your phone automatically handshakes and connects to, every minute of every day. If "they" really want to track you, "they" already are. One app is not the only thing holding "them" back or allowing "them" to do it. Ask Google to show where you have been in the last month. And if you really want to get scared, send Apple a legal demand letter for their location data of your Apple device for the last 120 days. What you get will be less surprising than how fast you get the data back.

Tim

You raise many good points, but you do so in an incredibly imbecilic manner. Do you think this is some sort of paranoid delusion? This shit is happening right now. The Supreme Court has taken away women's rights and there are backwards states in our country that have every intention of tracking pregnant women to make sure they don't try and get abortions, even by traveling to other states. There is currently a very real push to make this a nationwide restriction, which could become reality if people don't turn out en masse to the polls. It's a hell you'll likely never be able to imagine, but let us assure you that this is very, very real. Now the question becomes: how do we fight back and defeat this blatant intrusion into our privacy? We hope you become more supportive of this very real fight looming ahead as you seem to already be aware of the privacy implications.

Dear *2600*:

With the latest iOS, it's possible to locate your iPhone even if it's powered off. That's because even when the iPhone is turned off, certain wireless chips remain on, allowing the phone to still send signals that can help locate it. Now a group of researchers from the Technical University of Darmstadt in Germany has found that one of those chips, the one that enables Bluetooth, can be exploited and hacked to install malware on the phone even when it's turned off.

Ed

It's always nice to have something new to lose sleep over.

Questions

Dear *2600*:

Is *2600* a server attached to your magazine?

Brian

No, that's the name of the magazine that's attached to our server.

Dear *2600*:

Is there a proper hacker name registry? Just wanna make sure there are no well known hackers using MaxResDefault.

Dave

A hacker name registry... now there's an idea. Because we all just love to register our identities.

Dear *2600*:

Have you ever considered doing a "behind the scenes" article or video documentary about how the magazine is made? Or does one already exist? It would be really interesting, and potentially inspiring to anyone trying to start their own publication.

aestetix

It could also have the exact opposite effect. Plus, most of the action takes place on screens these days so it wouldn't exactly be a riveting documentary. Perhaps tuning up the 2600 *van might make for more compelling viewing.*

Dear *2600*:

I am sorry to ask. I have your digital subscription and I was searching for an email address to send the picture of a payphone I found here in Ohio but I just cannot find it and a web search is of no help. Is it payphones@2600.com?

Roland

You guessed right! We will work on improving *our visibility. It's harder than it seems.*

Dear *2600*:

What is *2600*'s opinion of copyleft sites like free2600pdfs.com?

John Hardy

What do we think of a site that takes our work and gives it away for free? Not much. If you support the magazine, then support it by helping it to stay alive. Ripping us off doesn't accomplish that. Is this really something we need to explain?

Dear *2600*:

Can you do a job with me?

J Wu

When will we develop the courage to just dive into one of these schemes?

Dear *2600*:

My friend had her car stolen. Toyota will not give her the GPS information and will only give it to law enforcement who are on holiday. Is there a way she can track down the GPS information on her car?

Josh

Law enforcement is on holiday? Look, we like to answer questions, but we don't like getting bullshitted. Clearly, there is something else going on here. Had you been up front about it, you might have been reading an answer in these lines instead of an admonition to try harder next time.

OK, we can't resist answering the question anyway. The system is called Toyota Safety Connect and it costs $80 a year. The "vehicle finder" feature will tell you exactly where your car is. If your car is stolen, then the cops get involved and use this technology to track it down as soon as the police report is filed, regardless of whether or not you subscribe to this service.

Dear *2600*:

I thought *2600* was not political - what is up with USA.WTF?

T G

Perhaps you should be running USA.WTF. WTF. But seriously, have you ever known us to not express an opinion on an almost constant basis? And if so, when exactly was that?

Dear *2600*:

I keep getting IG messages from hacked accounts, asking me to help them by "sending a code." How do I fuck with them?

Philip

Don't send them a code? Or... send them the wrong code. Or, finally, ask them for a code instead. This almost writes itself.

Dear *2600*:

how's the day going?

Hugoland

Is it wrong for us to assume this is some sort of scam? Maybe somebody genuinely wanted to know. Why can't we be more trusting?

Outrage

Dear *2600*:

Adobe is seizing control of my computer Again and Again and Again to insist that I delete my Adobe Flash Player! Isn't this harassment!? Where can I go to report this unethical and possibly illegal behavior!?! It is *mine*, not Adobe's. I bought and paid for the damned thing. I *don't want* to delete it - though that is more sentimentality than anything else. But I am damned tired of Adobe's "won't take 'no' for an answer" attitude. One of my pet peeves in life is people who will not take "no" for an answer. Whenever *anyone* obliges me to repeat "no" a second time, it is extraordinarily rude and orkish. *Another* pet peeve of mine is folks who will let people obtain their nefarious purposes by means of not taking "no" for an answer. And when you try to persuade someone who has already plainly told you "no," you have lowered yourself to the moral level of a pimp.

Robert

Clearly, Adobe knows how to push your buttons. And, we agree those reminders to uninstall their now-unsupported software can be super annoying and intrusive. Despite the fact that it's a security hazard that will only become less functional with time, it's still your right and your decision as to when or whether to disable it. We understand there's an option within Flash called EOLUninstallDisable which will disable these alerts. Good luck.

Dear *2600*:

I really don't understand why search engine companies insist on feeding me results that aren't even close to my search criteria. For example, I want to know how much aluminum cladding was used on the original World Trade Center buildings, especially the Towers. I would think this would be a simple request, an ideal question for the modern computer age to answer. *No!* You cannot find this answer within three pages of results by using any of the big name search engines! In fact, my random selections of the results did not contain any of the search terms that I said must be included in the results! Back 20 years ago, I would have gotten what I asked for. Today, AI and whatever algorithm hack exists has ruined search engines. Here's my search criteria: World Trade Center "aluminum cladding."

Richard

We have the answer but we're sworn to secrecy.

Dear *2600*:

Canceled subscription. Your Facebook page went political and the administrator was disrespectful. Twenty-five plus years of support gone.

Bobby

You do realize (which you can't since you canceled) that our Facebook page or group or whatever has nothing to do with what appears in the magazine? The various forums run in our name are done as public services for members of the community by other members of the community. They are all different. If they start *doing really evil things, we will disassociate, but disagreeing politically or someone being rude are things that simply don't rise to that level. We hope you don't judge everything like this or you'll be cutting yourself off from an awful lot of people.*

Dear *2600*:

What does it say about a security company who sends unsolicited marketing emails with no way to opt out? There's no subscription information in the body of the message or email headers. I had to contact them directly through chat to get them to unsubscribe me, and only after providing all my personal details and a confirmation code in my email to verify my identity. I then had to authorize them to unsubscribe me. This is completely unacceptable behavior for any security company, let alone one who says they're "protecting my privacy." I signed up for their service as part of a research effort, but their service is almost as invasive as the spam it is meant to block. How does anyone tolerate a constant onslaught of marketing and sales emails from this company? The application itself continually uses FUD (fear, uncertainty and doubt) to raise concern to strong-arm consumers into a hard sell of their other products. This isn't new for Norton - they have a reputation for the hard sell, even for products the consumer already has - constant pop-ups, email alerts, and alerts forcing people to renew.

Dave

For a moment, we were afraid you weren't going to mention the name of the company. But since you did, we can say that we've heard these complaints many times, not only about Norton, but a number of other anti-virus companies. It seems when fear is your main motivation in getting sales, it turns you into a bit of a jerk.

Dear *2600*:

I protest against moderators declining my posts as soon as "big brother" or "ministry of truth" is mentioned, while in the description of this group it is clearly mentioned that this group is also a place to speak out against increased digital surveillance and the limiting of free speech. That's what it says or doesn't it? If the moderators think that hacking is only about Cap'n Crunch whistles and script-kiddies, then they are wrong and acting against their own group policy. If moderators don't understand that politics (I hate it) can be left out of it, then they are wrong also. Yes, it shouldn't become a politics group, but censoring a member who posts a little about what currently is going on with the "ministries of truth" that they are trying to install everywhere is not OK.

Ronald

We really have no say in the particulars of any of our Facebook groups, but that's the precise reason why we have more than one. Moderators do an important job, but they're also human and will occasionally do things that you don't agree with. For most, the benefits seem to far outweigh the occasional conflicts.

Dear *2600*:

Attached is a copy of your classified advertisement from [redacted], a convicted child molester. He voluntarily entered into a nolo contendere plea and was convicted.

I do not appreciate a convicted child molester classified ad in *2600*.

I hope this magazine does not condone and support an imprisoned child molester. Please do not renew his ad. In my opinion, the ad is surveying for another victim.

From a paid in full subscriber

We understand your concerns and they are valid ones. But we are not going to do a background check on everyone who places an ad and we're not going to be the morality police and decide who is worthy and who isn't. What we will do is continue to advise people to be careful when contacting anyone they don't know. What we will also do is not run ads that appear to be encouraging illegal activity or looking for people to take advantage of. The ad in question didn't meet either of those conditions.

With people who are in prison, it's really simple to look them up and see what they're in for. They can't use handles. The knowledge that you get from finding out this information will then guide you into making a decision as to whether or not you want to contact them. And, despite what people may think, everyone still has the right to talk to other people, regardless of the crime they may have committed.

Keep in mind that the people who aren't incarcerated could be even more dangerous and able to hide their identities. That's why we always encourage vigilance. If we gave the impression that we were making things safer by weeding out certain people, that would only create a false sense of security. And, of course, it would also serve to dehumanize those individuals, something which we are not at all comfortable doing.

Dear *2600*:

See this man. [redacted], very politically connected, extremely wealthy. What if I told you this company was trying to buy my silence?

I'm not nearly as skilled like you guys. But I do know 1000 percent these fucks don't want it to be known child exploitation happened on their network, their servers, their dime, by their employees... or should I say taxpayer dime also (historic vehicle association)?

Anonymous

We're willing to investigate and reveal any such conspiracies, cover-ups, and/or misdeeds. But we need actual evidence in order to do this. We see a near-constant barrage of accusations but very little to back them up. Give us the data and we'll look into it. (We don't have time for long *conversations about any of this before getting to the point of actually having something of interest. We would still be stuck in 1986 if we returned all calls and answered all messages concerning these alleged injustices.)*

Feedback

Dear *2600*:

Your cover page supporting Ukraine just brought me to tears and took my breath away. Thank you *2600* team for everything you do!

Mike
Lifetime Member

We're glad it resonated. It was the least we could do.

Dear *2600*:

This letter is in response to duykham's article in 39:1, "How to Use Gmail to Send Emails From an SMTP Server That You Do Not Own." The article is correct. However, while the spoofed message could get sent and might get delivered, the chance of it making its way into someone's inbox is slim. There are three big anti-spam standards that should stop a spoofed message in its tracks:

SPF (Sender Policy Framework) is a DNS TXT record listing sender IP addresses, so if a domain doesn't list Google there, it would fail SPF.

DKIM (DomainKeys Identified Mail) puts a cryptographic hash on an outgoing email, like putting a stamp on a letter. Google would put their "stamp" on the message, and while it'd be a proper DKIM signature, it'd be for gmail.com rather than spoofeddomain.com, so a DKIM check would still fail. (Those guys at the IETF thought of everything!)

Finally, DMARC (Domain-based Message Authentication, Reporting and Conformance) would see that the From and Return-Path addresses on the email don't match, see that SPF and DKIM failed, and do whatever the spoofed domain's postmaster wants: deliver normally, deliver to quarantine, or flat-out reject it.

Assuming the message got this far, its last task is to get past spam filters such as SpamAssassin or Exchange Online Protection, who might give it more scrutiny.

The astute hackers out there might see one flaw in this plan: what if the other domain uses Google for email? On paper, that would pass SPF/DKIM/DMARC despite being a spoof. Did duykham discover a way to spoof Google Workspace users' emails? It's possible, but I'd bet some Google engineer put up a thin paper wall to prevent Gmail users from impersonating Google Workspace customers - you know, as opposed to fixing the actual problem.

PSA: SPF, DKIM, and DMARC are free and open standards that can stop phishers and spoofers in their tracks. Like flossing, setting these up is something you should do without being told, whether you outsource your email or you self-host (like Byeman espoused in another of 39:1's great articles). A how-to article would be out of scope for a hacker magazine, but there are plenty of resources online. This audience can figure it out.

Colin Cogle
Exchange Server Administrator

We have no doubt they can. Thanks for your feedback.

Dear *2600*:

Thank you for publishing my article and thank you for publishing Kevin Coombes' letter about it!

Discussion can only make the world a better place. Maybe one day the Internets will be secure! (Only *2600* readers can make it so!)

I say to all *2600* readers: Keep your thoughts not to yourself but to everyone! Write to *2600*! Letters are as good as articles. Write as if your life depends on it, because it does.

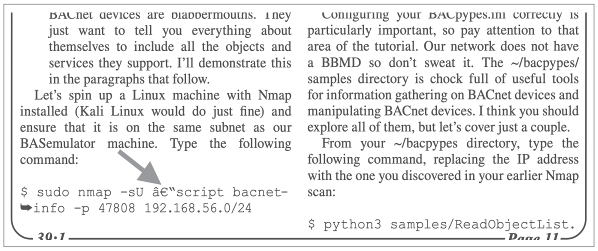
G.A.Jennings

That might be going a bit far. But we do value and encourage every last letter and article. Payphone pictures and back cover photos, too! The more the merrier.

Dear *2600*:

There was a typo in the Spring 2022 issue as shown.

Roman



BACnet devices are blabbermouths. They just want to tell you everything about themselves to include all the objects and services they support. I'll demonstrate this in the paragraphs that follow.

Let's spin up a Linux machine with Nmap installed (Kali Linux would do just fine) and ensure that it is on the same subnet as our BASemulator machine. Type the following command:

```
$ sudo nmap -sU â€"script bacnet-
➥info -p 47808 192.168.56.0/24
```

Configuring your BACpypes.ini correctly is particularly important, so pay attention to that area of the tutorial. Our network does not have a BBMD so don't sweat it. The ~/bacpypes/samples directory is chock full of useful tools for information gathering on BACnet devices and manipulating BACnet devices. I think you should explore all of them, but let's cover just a couple.

From your ~/bacpypes directory, type the following command, replacing the IP address with the one you discovered in your earlier Nmap scan:

```
$ python3 samples/ReadObjectList.
```

39:1 Page 11

We are ashamed and embarrassed. What happened was a bad translation of a file format that resulted in extraneous characters slipping by. We're very sorry and have come up with a better way of avoiding this.

Incidentally, the line should read:

```
$ sudo nmap -sU –script bacnet-
➥info -p 47808 192.168.56.0/24
```

Dear *2600*:

In the letters section of 39:1, you asked for suggestions of other hacker/phreaker movies from the 70s, 80s, 90s, and more. I have one that might be forgotten or overlooked. Not a hacker in the computer sense, but Gene Hackman really showed off his skill set in the 1974 movie *The Conversation*. The pacing is slow and deliberate. The ending is perfect. I think it's one of the best in this genre!

mheyes

We're inclined to agree. That was one of the most authentic films on the subject ever made. It is indeed slow, but that's what made it work. It's also aged quite well.

Dear *2600*:

The letters section in 38:4 contained a pleasant surprise for me with a reader's generally favorable comments on two articles I'd written about my Bitcoin experiences (35:1, 36:2). I really appreciate Ron's interest in a follow-up story and, in fact, I had been thinking the same thing!

A lot has been going on in the world of money, markets, and crypto. Bitcoin has been banned in several countries, enshrined in another, seen various scandals, has not reached the high prices that some predicted, yet it has not disappeared either. Inflation has returned at levels not seen in many decades.

I still think the evidence shows that Bitcoin is a decentralized hybrid of a pyramid scheme and a Ponzi scam. It is a con job wrapped in the appearance and language of investments. I believe it is not viable in the long term for many reasons, such as the extreme energy consumption of each transaction, which has real-world costs which must be paid. (Cash has no such fees, and credit card fees are low enough to usually be absorbed as a cost of doing business.) Bitcoin's system tends to give equal protection to good and bad actors, and provides little recourse for victims. (Credit cards skew towards protecting the good at the expense of the bad.) And some people see evidence of large crypto holders - "whales" - regularly influencing markets to their financial advantage. Certainly these kinds of problems also afflict other financial systems. There will always be those who seek ways to "get rich quick," others who will gamble at casinos believing they can beat the house, and some who will try to steal value rather than create it.

I have come to view cryptos as a legal (at present in the USA) scam in which nearly anyone can participate. When I saw prices continuing to go up, I bought into several different cryptos, sold some for profit, and continue to hold some in hope that "greater fools" will someday buy them for more than I paid. But I have not risked more than I can comfortably afford to lose.

All of this has led me to think a lot about the nature of money, wealth, and how they can serve as tools for those of us interested in using our abilities to create change for ourselves, and the world.

I'm writing more now, and plan to submit an article soon.

XtendedWhere

We look forward to this conversation continuing into all sorts of unexpected areas.

Gratitude

Dear *2600*:

I am already a lifetime print subscriber, so please do not initiate a second subscription for me! The purpose of this payment is simply to say "thank you" for the pleasure and enlightenment I receive from my current *2600* lifetime subscription. No doubt your costs of production and distribution are increasing, so please accept this contribution in the spirit in which it is offered.

Mark

We do appreciate your generosity, but always prefer to give something back when people make such donations. People tell us "just existing" is enough, but we think there should be something more. Thanks for the acknowledgment.

Dear *2600*:

For a while there, I was worried the final issue of my subscription (Winter 21-22) was lost forever, but it finally arrived mid-March at my state correctional facility! Whew! Close call.

After a brief consideration, I decided it is finally time to pull the trigger on a *2600* lifetime subscription. I've been an avid, dedicated reader for over 20 years now, but was always too frugal to splurge for anything beyond a one-year subscription.

Both my parents passed away in the past 15 months and my father specifically got me interested in hacking and computers at an early age. I remember being around 13 years old and him bringing me a boxed copy of Redhat Linux 5.2 to play around with. My father was a big fan of esoteric operating systems like OS/2 Warp, BeOS, QNX, and others. He spent most of his career working in IT and networking jobs. I miss him and my mother every day.

Their passing, however, has enabled me to be able to finally afford a *2600* lifetime subscription, and I know my father would find it a solid investment. I'm down to less than 20 months left on my sentence and look forward to getting back out in the world and learning about the latest exploits, technologies, etc.

It also seems like your magazine has really focused on hacking instead of politics over the past few issues and that too is refreshing to see. As a loyal and faithful reader, all I ask is that you continue to put out a quality product that questions the mainstream ideas in the world. People need to explore more, argue less, and not take their time in this world for granted.

I'll be having a third party subscribe for me on the street so future address changes aren't an issue. Thank you for this magazine - hack the planet and the universe!

Vincent

It was definitely a smart move to have that sent to a different address so your future issues won't wind up going to the wrong place. For people in a similar situation, we really appreciate the support, but please be sure you've taken care of yourself first. Most people reentering society will have their hands full finding places to live, employment, etc. Once all of those items are taken care of, subscribing to your favorite magazines can move higher up in the priority list. Thanks for your support!

Dear *2600*:

Readers:

Nice work on #OpRussia.

Respectfully
Anonomisiss

We're certain at least some of our readers were involved.

Dear *2600*:

Thank you for all the time and effort that goes into putting together and disseminating your publication.

I've just recently discovered *2600 Magazine*. I've read through the most recent issue and I thought it was really great. I learned about *2600* from reading Snowden's biography - a heroic and unfortunate story, I think.

I am a first-year graduate student at Illinois Institute of Technology studying software development. I never much studied anything related to computers or technology before this. In fact, sometime in my 20s, I convinced myself that I was "too dumb" to learn about computers or programming. A few years ago, I decided to give it a shot and see if I did have the mental capacity to learn. I started with studying for the CompTIA ITF+ cert and moved on to studying for the A+ exam. I did some cursory Python learning on the DataCamp website and read books, watched videos, etc. I took an Intro Java class at my school and then decided that these subjects can become complex and difficult quite quickly, but with time, effort, and sacrifice I was able to learn and understand the various concepts and how they come together. Now I've just completed my first semester of grad school. It was tough and I still have a lot of material to revisit from my Intermediate Java class, but I made it through and know more than I did before I started.

I am writing not to brag about these achievements, but to hopefully get some advice on how to proceed with growing into a competent and valuable developer, and also how I can get the most out of the upcoming HOPE conference. My particular interests are in learning about developing embedded systems/software and maybe even more specifically for hardware like cameras and sensors, etc. (machine vison types of things).

This will be my first participation in any conference/gathering/happening having anything to do with technology and I want to learn as much as I can, while not seeming uncool or unaware enough about this or that technology, social code, etc.

Any advice for a student that wants to show up, hang out, and be enlightened by the wisdom of those that come with lifetimes of experience?

All the best,
The PizzaOverlord

The best advice we can give you is to continue doing what you're doing. Setting challenges and meeting them is always the way to get on a good path forward. It's impossible to tell you which path is the best one to go down as the variables are always changing and everyone is different. The important thing is to be happy with your achievements on their own. You seem quite open to learning and, being in grad school, you should be able to surround yourself with a good deal of learning content, as well as people to share ideas and learn with. You tend to get more out of school by exploring subjects you weren't even aware of before. Too many people go into academic settings with very specific ideas of where they want to land in life. That's a wasted opportunity, as school is where you can discover whole new fields of interest that you never dreamed of pursuing. It doesn't always work out, but realizing that is a part of the process. Even failure is a learning experience and we know plenty of people who did badly in school, but learned much more than those who got straight As.

As for HOPE, it will have already happened by the time you read this. It's a similar scenario, all the more so this time, being set on a college campus. For people attending any conference that has a wide variety of subject matter, we suggest a similar agenda of exploration and learning about things you didn't know about before. And, as with any social setting, you will find many others doing the same thing. Just never assume that you or anyone else is "too dumb" to get something out of the vast array of knowledge that surrounds us every day. Good luck with the journey.

Dear *2600*:

Thank you all for being an outlet. The whole absence of solitude is fantastic. Seeing so much content from staff and subscribers and readers really enriches a niche that probably had other titles over the years. Labors of love are the most rewarding. Sure, you can solely commit to income and hoarding experiences as a revenue stream, but the transfer and enrichment of sharing is what I would dare say is a tenet of humanity over the ages. Maybe someday instead of thinking others know better than some, we can be more humane to more people?

Pic0o

We'll get there. It may be a bumpy ride.

WE WANT YOUR LETTERS!

Please send us your comments on articles, technology, privacy, or whatever else is on your mind. As you can see, we're open to a wide amount of opinions.

letters@2600.com or 2600 Letters, PO Box 99,
Middle Island, NY 11953 USA

EFFecting Digital Freedom

by Jason Kelley

Supreme Court Decision Overturning Abortion Rights Is a Privacy Wakeup Call

Fair and meaningful protections for data privacy are essential to independence and autonomy in the modern era. Everyone deserves to have strong controls over the collection and use of information they necessarily leave behind as they go about their normal activities, like using apps, search engine queries, posting on social media, texting friends, and so on. But after June's Supreme Court ruling in *Dobbs v. Jackson Women's Health Organization*, people are becoming more aware than ever before that those controls are sorely lacking.

Today, the concern is over abortion access - and for good reason: changing laws across the country now mean that those seeking, offering, or facilitating abortion access must assume that any data they provide online or offline could be sought by law enforcement. But tomorrow, the concern could be over something else. It is essential to remember that what is currently legal may not always be legal, and that who is in power can always shift, along with what laws are enforced, and how.

This isn't idle speculation - digital trails have already been ransacked in the service of questionable prosecution. After the "J20" protest over U.S. election results in 2017, Department of Justice prosecutors served a search warrant on the hosting provider of a site that was dedicated to organizing and planning the protest. The request would have required DreamHost to turn over the IP logs of all visitors to the site - anyone who visited, whether journalist, activist, or just interested reader - but it was later narrowed after pushback (though that later request was not without its flaws). By early July 2018, federal prosecutors dropped many of the charges against many of the defendants in the case, but even this sort of overbroad demand for digital data has a chilling effect on future protest organizers.

To ensure that digital data isn't misused by companies, courts, law enforcement, or the government, EFF supports data privacy for all. There are three main fronts in the fight to protect digital privacy and, whoever you are, you can help.

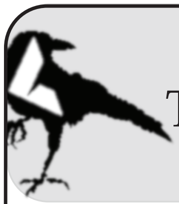
First, there are basic steps everyone can take to minimize data collection. EFF recommends a variety of methods in our Surveillance Self-Defense guides, available at `ssd.eff.org`, as well as other guides on `EFF.org`. We've got tips for protesters (for example: removing fingerprint unlock and FaceID on your phone, enabling full-disk encryption on your devices and using encrypted chat). We've got recommendations for those in the abortion access movement (keeping more sensitive activities separate from your day-to-day ones, carefully reviewing the privacy settings on each app and account you use). And we've got basic guides for anyone who wants to take their privacy into their own hands, while recognizing that there is no one-size-fits-all digital security solution.

But it should not be entirely up to individual people to take these elaborate steps to protect their own privacy. Because privacy is a fundamental human right, it should be protected in law and statutes. Digital privacy protections in the U.S. are generally weak, and we all must push our local, state, and federal representatives to do better. Perhaps the most important thing we can do to minimize data harms is to ban online behavioral advertising, which creates staggering profits for tech companies by targeting ads to us based on our online behavior. This incentivizes all online actors to collect as much of our behavioral information as possible, and then sell it to ad tech companies and the data brokers that service them. This pervasive online behavioral surveillance apparatus is what turns our online lives into open books. But there are also smaller bills that help fill the gaps: for example, Rep. Sara Jacobs' "My Body, My Data" Act will protect the privacy and safety of people seeking reproductive health care. Specifically, this bill would restrict businesses and non-governmental organizations from collecting, using, retaining, or disclosing reproductive health information that isn't essential to providing the service someone asks them for. Regardless of where you live in the U.S., or in other parts of the globe, you can visit EFF's Action Center at `act.eff.org` to find out how to speak up for better laws.

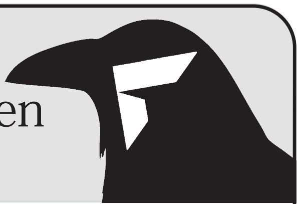
Lastly, we must demand that companies do better. There is a lot that companies - from ISPs to app developers to platforms and beyond - can do to protect privacy, and those steps will benefit all users. We must push companies to minimize the harm that can be done. In some cases, that means demanding better privacy options by default. In other cases, it means minimizing the use of "dark patterns" that push users to make choices harmful to their privacy. And generally, it means ensuring companies allow pseudonymous access, rethink data retention policies, encrypt what they can, don't share or sell their data, and make their tools interoperable with others, so we can have choices about how we use their products.

This is a tall order - we don't always have much say in what companies do, especially when it hits their bottom line - but you can start by making the switch to more privacy-protective apps where possible, and speaking up when a company whose service you use is negligent with their data protections. And if you're building your own tool or app, of course, you can make privacy a priority.

The Supreme Court decision to overturn abortion rights makes what was benign data now potentially criminal evidence. But it might not stop there. What we know from the past 30 years of work protecting digital rights is that if technology can be used to aid criminalization, it will be - and it might not matter whether the law appears just or not. As always, EFF will be fighting back in the courts, in the legislature, and online - and you can fight back too. It will take all of us, working together, to protect each other.



The Dark Side of DarkMatter: The Evil Hackers behind Project Raven



by Johnny Fusion =11811=

Scrolling through my social media feeds in the third week of September 2021, I came across a story about Project Raven. Three people - Marc Baier, Ryan Adams, and Daniel Gericke - who are either former intelligence operators or military from the United States were levied heavy fines by the Department of Justice and are forbidden to ever seek out a security clearance for life. This was a deal to avoid prosecution for their crimes. What were their crimes? They participated in the most unethical hacking I have ever heard about. Working for a company in the United Arab Emirates known as DarkMatter Group, they were an elite red team working on behalf of the Emirati government to spy on its own citizens, Emerati enemies, and even networks of the United States. But why is this the most unethical hacking in my opinion? Because of their hacking, human rights activists were tortured and imprisoned. Hacking does not exist in a vacuum. It is not just a challenge to test one's limits of their technical acumen. It has real effects on real people, and Project Raven led to real human suffering.

Set the Wayback Machine for the first years of the second decade of the 21st century. Cyber warfare was becoming the new battlefield for the 21st century, and countries all over the world were getting started in an arms race for not only defensive capabilities but offensive as well. Governments were using corporate contractors, often filled with former feds, Edward Snowden perhaps being the most well-known of these types of contractors. Before his whistleblowing, he worked for one such contractor, Booz Allen, that gave him access to all the secrets he was about to spill. Remember that name - it will come up again.

These contractors did not just work for the American government, but provided malware and attack vectors to other governments, equipping countries with cyberweapons sold to anyone who had the coin by those who could obtain a license to export technology and train foreign governments in cyber defense and policy. In September of 2012, one such company, CyberPoint, obtained a license to train the government of the United Arab Emirates in cyber defense - blue team sort of stuff. However, the UAE had other designs.

CyberPoint did not stick to blue team type defense such as firewalls, intrusion detection systems, or other defensive strategies. What is known, thanks to whistleblower Lori Stroud (who actually recruited Edward Snowden into Booz Allen's team contracted to the NSA, giving Snowden access to even more classified material - the perceived disgrace from this turn of events was the reason she left the NSA and went to work for Project Raven) is that this was the "unclassified cover story" for Project Raven to hide their red team style offensive exploits and penetration for the Emirati government. It was perhaps the UAE's desire to have more control and do things in-house that led to the Emirati company DarkMatter taking over the contracting for Project Raven in 2016, and the Cyberpoint contractors who wanted to keep their lucrative jobs in tax-free Dubai moving to DarkMatter. At the time, it was felt that DarkMatter had poached the United States talent working for Cyberpoint.

DarkMatter for all intents and purposes appeared to be an Emirati company, but in fact, they were part of the Emirati government, specifically The National Electronic Security Authority (NESA), the Emirati equivalent of the United States' NSA. These were state actors pretending to be a cybersecurity firm, and they were recruiting. They went to cybersecurity conferences such as RSA in San Francisco and Blackhat in Las Vegas looking for elite hackers to fill their roster by promising six-figure salaries, housing, and a tax-free lifestyle in Dubai. Maybe if you were at Blackhat, you came home with some DarkMatter swag. Many hackers took up DarkMatter on their offer, getting a major payday, but what was the cost?

To put it bluntly, the UAE wanted hackers to build and implement a surveillance state that could be described as "1984 on steroids." Blanketing the country with probes that could hijack cellular signals, do man-in-the-middle attacks, and inject malware, they would be able to intercept all cell phone communication in Abu Dhabi and Dubai, and with the press of a button pwn all the phones in a specific area like a shopping mall on the mere suspicion of a single suspected terrorist or dissident who might be there.

One may argue that every government

participates in some form of a surveillance state, including the United States. The difference is that even though DarkMatter told its hackers that they were fighting the very real threat of terrorism, they also were spying on what the UAE considers dissidents. It should be pointed out here that the UAE does not have freedom of speech. There are no First Amendment protections in the UAE and no exceptions for Americans working in their spy program. The watchers are definitely being watched. Criticism of the government is a punishable offense. Speaking for human rights protections could very well get you disappeared, tortured, secretly tried, and imprisoned. The hacking taking place under the aegis of Project Raven in fact did lead to these outcomes.

The tool that got the most press in early 2019 when Reuters broke the story is called Karma. It used an exploit in iMessage for iPhones that compromised a target phone just by sending a text message that didn't even have to be read or otherwise interacted with. This cyberweapon gave Project Raven hackers access to the device. It sounds a lot like the tool known as Pegasus that has also been in the news lately - and Apple recently pushed patches to fix it. However, in my research, I have not been able to determine if Karma and Pegasus are indeed the same tools, but the similarity of the exploit is uncanny. iMessage is such a desirable vector for exploits, as it is guaranteed to be on every Apple device out there. And because of Apple's closed system, Apple users cannot opt out of this application.

Hackers love freedom, often expressing this in free speech and free software. Many hackers believe in the sovereignty of their own lives and their choices. However, if we are going to exercise this freedom, we must temper it with the responsibility for the consequences of our actions. No matter how isolated or sandboxed you think your hacking is, none of us is an island. Our choices ripple out and affect those who we may not even realize or have the vision to see. People exist within our sphere of influence and beyond the horizon of what we can see. We must not remain ignorant of the impact of our hacking. What does our own freedom mean if we are taking away the freedom of others? Can we really say we are advocates of liberty if we do not work to ensure liberty for all instead of selfishly looking inward and thinking we got ours, and screw everyone else?

Hackers exist in a community of like-minded individuals with a diversity of opinions, skills, and goals. We form collectives to work together to achieve our goals, be it an open-source project, presenting at a conference, or writing for this magazine. We may see hackers as an in-group and those outside our community as "other," but in truth, we are all connected, every single one of us. Human beings create technology in order to be connected and interconnected with other human beings, especially in the realm of communication. From things like smoke signals, drumming across distances, running between cities with messages, postal systems, the telegraph, the telephone, radio, and television, and finally the Internet, humanity has increased our connection with one another to facilitate the sharing of information and understanding of one another.

But there is also a dark side. Human beings have used technology more and more to divide. To foment terrorism, spread misinformation, and facilitate fascism. The hackers of Project Raven were some of those individuals, under the aegis of the Emirati government, to squelch free speech, which is the lowest form of fascism - and facilitate torture of human rights activists, which is well into the realm of authoritarianism. Technology can facilitate freedom and technology can also enable tyranny. Even though some technology is utilized for good or ill, technology is not ethics neutral. There are some applications that are always unethical, immoral, and - I will say it - evil.

Some of the dark side hackers for DarkMatter were ex-feds. While giving lip service to the founding principles of the United States, they were more than willing to set these aside both in their work for the United States and Emirati governments in exchange for a big payday. We know Lori Stroud, the Project Raven whistleblower, was just fine with the NSA spying on everyone as Edward Snowden revealed while participating in it, but only drew the line when the Emirati equivalent, NESA spied on fellow Americans using Project Raven. She was already accustomed to facilitating the compromising of devices of journalists, human rights activists, and foreign governments around the world, and the torture of Emirati dissidents in exchange for six tax-free figures. Stroud knew she was a spy but thought she was a "good" intelligence officer. It was fine to do this to brown folks in the Middle East, to people who were "other," but when it came to Americans, her perceived in-group she suddenly found scruples for what she was doing. Her hacking had a real human cost.

But at least she eventually contacted the FBI about Project Raven, and Reuters did the initial investigative journalism that brought it all to light. Marc Baier, Ryan Adams, and Daniel Gericke cut a deal to pay a fine for breaking U.S. hacking laws and prohibitions for selling military technology to avoid prosecution. This does not undo the damage they have done. They used their technical acumen, access to high technology, and their ability as hackers to cause real harm - real human suffering because of their hacking.

It is a common story. Though I am merely a competent hacker and not a superstar, puttering around more as a hobbyist and technological idealist than an InfoSec worker (the closest being sysadmin jobs in Amsterdam, and California back in the nineties), I have often been approached to do something unethical when people find out I am a hacker, and I am sure many readers of this magazine have as well. What we decide to do matters. It would behoove us not to just hack code, but to have a moral code of what we are willing to do and not do. If we are going to cause harm, who are we causing harm to? Sometimes justice demands direct action, but if we are not careful, some company can wave a fat wad of cash under our noses and we compromise our values and, through our skills, become an agent of injustice. Or maybe we do something "just to see if it can be done."

We have all been there. Hackers are curious creatures. But we must not allow our curiosity to bring actual harm or suffering to other human beings unjustly. We must build an awareness of the influence hacking can have on individuals and organizations. We can use hacking for righteous causes or, like the hackers of Project Raven, for great evil. The choice is yours. Choose wisely.

I Don't Think I Was Supposed to See That

by lg0p89

Data security at times is underrated. Unauthorized persons viewing material is bad enough, however, when you add in the material being from senior management, you have a recipe for issues and people feeling badly. One area for this leakage has been with documents. At least two businesses I consulted with have been Microsoft shops. This gives the curious ample areas to peruse for fun.

One of these apps is Delve. If you happen to have a bit of spare time, for example a Friday after lunch when everyone is in a food coma, take a quick look around. Finding this, if you haven't already had the pleasure, is easy (open the Office app and you'll see Access, Calendar, Delve, Excel, etc.). Just check on that happy Delve icon. Here you'll see Home, Me, Favorites, and People. To get to the juicy bits, click on People. Here you'll see your command/management structure. Now the fun begins.

First, take a look at your documents. You'll see the documents you have emailed and worked on recently. Now, if you are brave enough, you can look at other people by clicking on the other people you work with to see what they have emailed, authored, or modified recently. (Warning: they may become irritated if/when they find out with the system.) That is an awfully large range of documents to let others simply have access to.

The first place I noticed this was at a manufacturing company. I was a little bored and began tooling around, seeing what I could see. In my adventure, I saw the CISO's name and thought it might be interesting to check out what was new. Yes, indeed there were a number of documents I probably should not have seen. These included budgets and other documents well above my pay grade.

Naturally being curious, this clicking activity was done at the next place. If it worked once, twice certainly should be the charm. Well, it worked again. This time, I was a bit more adventurous. I was able to see the documents for the CEO and COO, as well as human resources and other management members. Just by clicking a few items and not doing anything exciting or using mental gymnastics, I was seeing purchase orders, resumes for applicants and staff, research papers, bids, policies, incident responses, and many other items that should have been confidential, yet anyone could look at them. Fortunately for me, I was also able to see co-workers' documents.

The Delve disclaimer on the screen says that you, the user, can only see files/documents you have access to. This sounds very official and makes it seem as if there have been rules put into place to limit access based on the user's role, position, or work group. Not really. You tend to have access to most documents as the target doesn't know about limiting who has access to these or toggling this function to confidential. This may be the case in IT, but not with operations. It is likely their staff outside of IT are relatively clueless regarding the issue. To mitigate this involves more than clicking one button.

In my case, this was reported to IT as a potential problem. As a responsible researcher, this was appropriate. Was this fixed or at least mitigated in some fashion? No.

About Conversation, Thought, and Language

by Diana K

Some may wonder what conservation, thought, and language have to do with hacking in terms of expanding your knowledge of things and knowledge of your own perceptions. Let me answer this with a true account.

My alma mater was UW Parkside. I graduated in pre-med and computer science with a breadth of knowledge in art and history (actually, an academic minor at other universities) at a difficult time in the U.S. UW Parkside was established in 1968 at the most intense time of the Vietnam War as university protests were high at UW Madison and other universities.

However, UW Parkside was established with a different conversation. Many of the early professors were from UW Madison and did not wish to export the loss of conversation that had occurred at Madison. So, an idea was set up that although a topic may be loaded or charged, UW Parkside was supposed to be a thoughtful and academic space built to coincide with nature (actually, the campus still coincides with nature as it is part of a forest coexisting with the urban space outside of the university).

The first practice of this principle occurred in computer science and business programming classes. At that time in 1968, the university batched programs written in FORTRAN and COBOL to Madison to run and send results back. The first practice was that students, guests, and faculty were not allowed to mock the computer language that one used to solve a problem on a computer, sort of like a Constitutional amendment of language and thought freedom.

A second part of the practice stated that UW Parkside's library would obtain books from many sources and authors - and that professorial pull was not allowed to decide what books, magazines, and newspapers the library could obtain. The library was given complete independence from the administration and academic departments starting in 1968 and still continuing today. The advantage of this was that the library was able to obtain newspapers and magazines like *Le Monde*, *Der Spiegel*, *Paris Match*, European newspapers, as well as science journals like *Bioscience*, *Nature*, and *Biology* from the U.K. Outlier publications were also able to be obtained. The ability to gain access to various thoughts reflected the policy of UW Parkside, which was to trust the reader that they could make up their own mind and evaluate without blinders or without muffling (a concern I have had since the end of 2020 with regard to the shutting down of social media sites on the Internet and the muffling of voices not in chorus with the majority party).

As a result, my language comprehension included French, German, Spanish, Italian, and Russian. The comprehension included the ability to read, write, and speak - although my speaking fluency is reduced due to health issues. The important thing is that I saw that it was not about one language being better than another, but rather that language provides a perspective to evaluate or express an idea from a different perspective.

As my language comprehension increased, I began to see that FORTRAN, COBOL, and PL/1 (the language I programmed in as a programmer) were different ways to perceive or express an idea. So, I went from FORTRAN to BASIC to machine code (TI 58/59, SR-56, Z80, and PDP-11/20 assembly) to PASCAL and others.

One summer, as I was transitioning from ninth grade in junior high school to tenth grade in senior high school, I decided I wanted to learn PASCAL. My dad told me that Parkside had a liberal policy of allowing non-students to have a practice computer account. I went to the university computer center and asked for a non-student programming account to learn PASCAL. I filled out a form on green bar paper, about half a page, with information like name, address, phone number, and parent's name (for applicants under 18). I was then asked to read a simple typed double-spaced page with rules of use. After signing that, I was given a username, password, and assigned 128 blocks of storage.

"Blocks of storage" is an old term that is no longer used. It is similar to how much disk space you have to run or store programs on your hard drive. A block at that time was 512 bytes. So 128 blocks translated to 64 kilobytes of information. This amount may seem low, but you have to remember that in the mid 1970s, many hard drives used on minicomputers for business were only ten megabytes, which is one millionth of a ten-terabyte disk drive in common use today. Yet, that amount was sufficient to run many applications and programs back then.

The most important part of the open policy of non-student accounts then was that, compared to the security and rigor of today, it was a different time. People trusted each other and opening an account for the local community was not something to worry about - we all knew each other. With the environment that existed at UW Parkside, we did not have to worry about misuse of the account. There were safeguards installed to prevent misuse.

Some in other parts of the world - or even other parts of the U.S. - will say "you guys were very naïve and immature to put that much trust into non-students." Not really. One has to remember Wisconsin as it existed in the time of the mid to late 70s. Where UW Parkside was located, the area was a refuge for those escaping the race politics of the state of Milwaukee and those escaping the one-party political state of Chicago.

My family moved back to Kenosha from Wauwatosa in 1974. The race politics of Milwaukee had encroached upon Wauwatosa, and so we returned to my dad's home town. Then, it was an auto town that valued education and arts, and was also away from everyone in various political groups yelling at each other as they were doing in Milwaukee and Chicago at the time. Peaceful, quiet, and you could leave your violin in a music locker unlocked without fear of it being stolen.

Although the setting was safer than Milwaukee and Chicago at that time, we did have our discussions. Like many kids who were raised in the late 60s through early 70s, we would play war and have Mattel M-16 toy guns to simulate with.

When we moved to Kenosha, there were many veterans who had come back from Vietnam. One of them discussed an important issue that many of us in the neighborhood were not aware of. The toy M-16 guns we were playing with were the same size and made exactly the same sound as a real M-16. The veterans who talked with us didn't mention PTSD, but they did mention that the sound and sight of them caused flashbacks. So, as a neighborhood, we stopped playing war and instead focused on baseball.

During the 1970s in Kenosha, we were having the same discussions about national politics and what to do about those who were coming back from Vietnam. A thing to remember about Kenosha is that there were many military families. My grandfather's name is inscribed on the wall of the library of World War One veterans from Kenosha. Also, Kenosha was an auto town that greatly supported education and there were many who had questions and concerns. However, in that time of Vietnam, Watergate, and the Nixon resignation, we argued but never came to blows.

Also, everyone was encouraged to speak their own languages. Secondary languages included Polish, Italian, and German. No one was shut down unless someone was deliberately trying to start a riot. So, to me, when I learned various programming languages (up to 100 now from the early beginnings of the 70s) with FORTRAN, BASIC, machine code/assembly, and PASCAL, I think that even in a turbulent time like the 1970s, I did not feel like I do today. I felt freer to express my thoughts openly than I do today.

Part of the reason why I have concerns about expressing my thoughts today is that area of Kenosha/Racine which used to be a haven from the race politics of the state of Milwaukee and the one-party system state of Chicago is now absorbed into both.

What does this mean? I am a contrarian and I believe in reading and listening to multiple points of view. When we would visit my cousins in Madison, I would read different papers, such as the *Capital Times* (the liberal paper) and the *Wisconsin State Journal* (the conservative paper). At home, I'd read the *Chicago Tribune* (the conservative paper and I have been told I was reading "the Colonel's paper") and *Milwaukee Journal* (the liberal paper). Yet, today, when I try to share views and concerns about what I see happening worldwide, nationally, and locally, there is only a small circle of friends I can talk to. When I do try to reach out locally, as soon as I deviate from the majority party talking points, the listening stops and I am shut down in trying to share something important.

Today, I went to have tacos with a friend and I wore my *2600* t-shirt with the blue box schematic in front. Part of the reason I wore it is that I wanted to express being proud of the hacker culture that seeks to expand knowledge and insight. Also, I wanted to see what others would think at the bar I go to. I'm glad that I was surprised. Many were happy to see me wear it. Over a pitcher of beer, I discussed the components on the front of the shirt. Also, others who were retired looked and smiled at the fact that the spirit still exists.

by Alexander Urbelis

alex@urbel.is

Justice as a KPI

Sitting in my office in midtown Manhattan at the end of May, the sun was shining and, while in the midst of writing something on a short deadline and deep in thought, I was distracted, as always, by an Exchange notification of a new email. Though these new email notifications can often be disproportionate in their ability to be disruptive relative their temporality, this one was particularly so. In the two lines of text that popped into the lower right hand corner of the monitor, I saw something unusual: a notification that the Department of Justice had revised its prosecutorial guidelines for bringing charges under the Computer Fraud and Abuse Act (CFAA).

The notification was effective. My interest was piqued. I clicked the banner, opened the email, and was amazed to find the entirety of the email just as fascinating. I learned these new prosecutorial guidelines mandated that "good faith security research" would no longer be treated as a crime under the CFAA. This seemed like a victory for white hats, security researchers, pen testers, bounty hunters, etc., depending on how these new guidelines defined the contours of good faith security research. Too narrow and the change would have no effect; too broad and the statute itself would lose its meaning and force.

The CFAA is a famous and infamous statute: on the books since 1986, proposed by Congress in 1984, and drafted in direct response to the cult classic hacker flick *WarGames*. The new guidelines for prosecution under the CFAA coincidentally take their definition of "good faith security research" from another infamous statute in the hacker community, the Digital Millennium Copyright Act (DMCA), under which the Motion Picture of Association of America sued *2600 Magazine* just about 23 years ago. Because the DMCA deals in some respects with reverse engineering and security testing, it had a fairly broad definition of "good faith security research," i.e., "accessing a computer solely for purposes of good faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in a manner designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices, machines, or online services to which the accessed computer belongs, or those who use such devices, machines, or online services."

On the surface, this looks like rather expansive classes of activities that should not fall afoul of the CFAA. That said, there are many ways this definition can be interpreted and, for this reason, security researchers and prosecutors are likely to disagree on boundaries. As such, the CFAA will continue to exist as a nuanced law subject to multiple interpretations. These boundaries, by the time of publication of this article, will no doubt have already been addressed in a robust, respectful, and meaningful way at the HOPE panel I will have moderated.

But even now, on a gut level, the mere idea that good faith security research, that ethical hacking, is not outside the law but within it, should finally feel like the hacker community is seeing the policy changes it clamored for over the last three decades - that finally things are looking more just. Even though the law is not changed, the new guidelines are a public statement of what the DOJ believes is right and wrong, and of what is just and unjust to pursue as a prosecution.

Because of this shift towards justness, I began to ruminate, to re-think justice, the very elusive nature of that concept itself, with a particular focus on how to measure justice. Since this policy change would result in DOJ prosecuting fewer actions as crimes, would a lower number of CFAA prosecutions signal a greater amount of justice? How would the efficacy of this policy change be measured? What, if anything, can we make of differences in interpretation of these new guidelines between U.S. Attorneys' Offices? If there are fewer cases in New York brought under the CFAA but an increasing amount in, say, Kentucky, then what does that say about the result of the new guidelines? In short, can we measure justice like it's some kind of key performance indicator (KPI)?

It's certainly not how Aristotle thought of it. As an undergraduate, I was very fortunate to have the opportunity to attend Oxford University as a visiting student. While there, I studied Aristotle's *Nicomachean Ethics* with a truly great man, the Rev. Dr. Cyril Barrett. Cyril was an Irish Jesuit priest in the most irreverent, progressive, and controversial ways possible. I recall many fervent discussions during tutorials with Cyril about whether

Aristotle had it right or totally wrong, and a good deal of those discussions centered around the concept of justice.

Justice was a virtue to Aristotle; it was a standard of conduct to which humans should strive. Virtue, as Aristotle famously defined it, existed in the middle ground (i.e., the mean) between excess and defect. This concept makes sense for characteristics like temperance or moderation, because an excess of temperance would make one fussy and overly prudent, while on the other hand, a defect of moderation could lead to extreme or disproportionate behavior, like binge drinking. In the context of drinking, Aristotle would have neither approved of persons who were straight-edge nor persons who regularly drank too much - moderation was the key to virtue. Going too far in either direction from the mean, according to Aristotle, would lead to vice.

For Aristotle, justice was also a virtue - a rational mean between two extremes. While we can certainly envision there being a defect of justice or, in other words, too little justice, it does not necessarily make sense that there could be too much justice. Moving in the direction of ensuring a just result, viz. achieving justice, seems exactly like what a governmental agency that calls itself the Department of Justice should be doing.

On the defect of justice side in the specific context of the CFAA, we have an example from our community that will always make our hearts heavy: Aaron Swartz. Over a decade ago, based on what appears to be a now-rejected view of what the CFAA covers, the DOJ charged Aaron with eleven CFAA violations for systematically downloading academic journals from JSTOR. The U.S. Attorney's Office in Massachusetts intended to use Aaron's case to send a message. The State of Massachusetts, on the other hand, declined to bring any charges against Aaron for the same conduct. Nearly two years later, after DOJ rejected a plea arrangement, Aaron hanged himself in his Brooklyn apartment.

If ever there was a defect of justice, this case was it. To the contrary, did the decision of the State of Massachusetts to not view this conduct as criminal create an excess of justice? I say no: Aaron surely suffered and learned his lesson by the mere fact that both the State of Massachusetts and the U.S. Department of Justice were investigating his conduct. Viewed in the light of the new guidelines, even contemplating pursuing charges against Aaron's conduct could be seen as a defect of justice.

That raises the issue of whether the guidelines changes are too little too late. Overzealous pursuit of CFAA charges took a precious life from our community. The government moves slowly, arguably too slowly, but at least this is movement, and movement in the right direction.

I submit that, in Aristotelian terms, there may now be a way to measure the impact of the CFAA policy changes on whether the Department of Justice is pursuing just cases. The first metric would be to take the total number of cases where CFAA charges are contemplated, which we can call N. Subtract from N the total number of cases across the United States for which U.S. Attorneys' Offices have declined prosecution on account of new guidelines' carve-out for good faith security research. We can call that total D. Thus, the equation of (N-D) = the total number of cases actually pursued under the CFAA, which we can call C. Let P = the total number of CFAA cases pursued across the United States in previous years.

P should be greater than C. If C is greater than P, then it is likely that the new guidelines are not being implemented or there is a problem of inconsistent interpretation. C, therefore, could be further analyzed by jurisdiction. Unless there are a greater number of CFAA cases countrywide that fall outside of the new guidelines, C should decrease. The percentage of C's decrease can thus act as an Aristotelian marker as the spot that indicates the mean, or the middle ground, for justice.

Measurements such as these, though not actuarial in nature and certainly subject to some variance based on the facts and circumstances of individual cases, should also allow easier recognition of cases that would fall outside the mean of justice - cases like Aaron Swartz's. Those cases tend to be the ones that the government pursues to send a message, and which would deter future conduct. Those cases, therefore, are more likely to be inherently defective of justice, or more colloquially, those cases are simply less just. It is for this reason that I submit that U.S. Attorneys should be measured, not by their convictions, but by the use of sound discretion in declining to pursue certain cases.

Those declinations indicate an understanding of the need and place for good faith security research, a recognition of the policy errors of the past, and a commitment to prevent injustice going forward. This is an area where less can certainly be more as we, as a community and a country, continue to struggle with and strive for justice.

Brute-Forcing a Museum's Math Puzzle With Python

by Brenden Hyde

TL;DR: A seemingly simple math puzzle stumped me, so I brute-forced it with a Python program.

Background

During a visit to a museum called OMSI,[1] I noticed a puzzle that had a 3x3 grid and some wooden blocks labeled 1 through 9.

The grid looked like this:

```
[]  -  []  =  []
               x
[]  ÷  []  =  []
               =
[]  +  []  =  []
```

The puzzle was called "Four Equations," and the goal of it was to arrange the blocks to meet these constraints:

The top row was a difference (A - B = C).

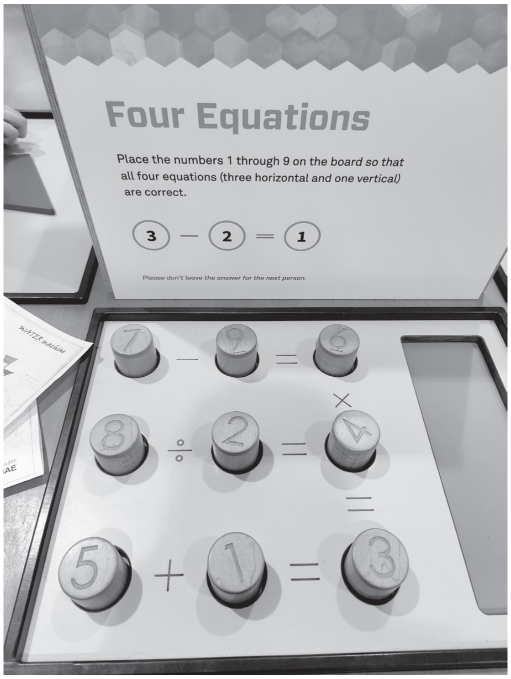
The middle row was a quotient (D ÷ E = F).

The bottom row was a sum (G + H = I).

The right column was a product (C × F = I).

All four equations had to be solved at the same time, and you could use each number only once.

Here's a picture of the puzzle with its blocks jumbled:


Four Equations
Place the numbers 1 through 9 on the board so that all four equations (three horizontal and one vertical) are correct.
3 − 2 = 1
Please don't leave the answer for the next person.
7 − 9 = 6
×
8 ÷ 2 = 4
=
5 + 1 = 3

Motivation

As you might infer from the picture of the wooden blocks and simple, gigantic print on the sign, this was a puzzle for all ages including children, and yet I couldn't solve it in the five to ten minutes I tried.

Slightly annoyed, I gave up, sanitized my hands, and vowed I'd solve it later with a computer.

Number of Possible Solutions

The way to calculate the total number of possible block arrangements in this puzzle is with factorials.

There are nine starting blocks to choose from.

After you choose one, there are eight remaining blocks.

After you choose another, there are seven remaining, and so on until you run out.

That means that the number of possible arrangements is 9! or "nine factorial."

This can be written as:

```
9 x 8 x 7 x 6 x 5 x 4 x 3 x 2 x 1
```

The number 9! is equal to 362,880.

That's the number of naive guesses it would take to guarantee that you either get the answer or prove there isn't one. I say "naive" because not every permutation in our huge list is a potential solution.

The possibilities shrink when you consider the mathematical relationships among the numbers. For example, the second row is a division problem.

Because 2, 3, 5, and 7 are prime numbers, none of them can be the first number (dividend).

The ninth box is the product of two numbers, so none of the primes can go there either, as we don't have any duplicates, and a prime number only has two factors: one and the prime itself.

You could solve the Four Equations problem like a Sudoku, given that it has so many logical constraints to eliminate most solutions.

But, I have a computer, and I don't have the patience for that!

Solving It With Python

I chose the Python programming language to build my puzzle solver, since it's powerful and easy to use. If you don't care about the code, you can safely skip to the section entitled "Solving the Puzzle."

There are two main pieces to my Python program:

1. Get a list of all possible permutations of the numbers 1 through 9.
2. See if any of them solves the puzzle, and print it if so.

Getting All Possible Permutations

I want to find every way that the numbers 1 through 9 can be scrambled.

Rather than reinvent the wheel, I used the permutations function from Python's itertools module. This function returns all possible permutations of a list of numbers.

Here's some example code that achieves this:

```
from itertools import
```

```
➥permutations
one _ thru _ nine = list(range(1,
➥10))
all _ perms =
➥list(permutations(one _ thru _
➥nine))
```

In the above code, I first generate a list of all numbers 1 through 9 with Python's range function.

range takes two arguments here: the lower bound (starting number) and upper bound (ending number).

Confusingly, range is inclusive on the lower bound and exclusive on the upper bound. That means that if I run range(1, 5), it'll give me the numbers 1, 2, 3, and 4, but not 5. Therefore, I use range(1, 10) in the example to get 1 through 9.

After I get the list of numbers, I use permutations plus a built-in function called list to create the possible solutions.

Constraint Checking

Equipped with a list of possible solutions (and many erroneous ones), it's time to solve the puzzle.

To check if a permutation solves the puzzle, the code uses Python assertions. An assertion is just a statement that is either true or false. If the statement is true, Python does nothing and moves on to the next line of code. However, if the statement is false, Python raises an error to tell us this isn't a solution. This error is called an AssertionError.

Here's a snippet that uses an assertion to check if the difference between the first two elements equals the third element:

```
def check _ solution(p):
   try:
       assert p[0] - p[1] == p[2]
   except AssertionError:
       return False
   else:
       return True
```

In the above code, we make a function called check_solution that takes a list called p as an argument.

To grab an item out of a Python list, you refer to it by its index. An index is the numerical label that represents the item's place in the list. The first element has an index of 0, so if my list were [1,2,3], the number 1 would be at index 0, the number 2 would be at index 1, and 3 would be at index 2.

Our list is called p, so the first element in the list is called p[0], and the second one is p[1], etc.

In the code, we assert that p[0] - p[1] == p[2].

If this is true, as in the example case assert 6 - 4 == 2 then the function returns a value of True.

If that assertion is false, for example assert 4 - 2 == 7 then an AssertionError is raised by our function, and we handle it by returning False.

The above example only solves one of the four constraints, but we can test addition, division, and multiplication just like we did for subtraction.

Those assertions are included in the code, but I've omitted them here to stop the reader from falling asleep.

Solving the Puzzle

With all the math riff-raff out of the way, we can solve this puzzle.

Assuming you have Python 3.6 or greater installed, you can run my accompanying script from the CLI like so:

```
python3 grid _ puzzle.py
```

The answer will be rendered to the screen:

```
Solution found!
---------
9 - 5 = 4
       x
6 ÷ 3 = 2
       =
1 + 7 = 8
---------
Solution found!
---------
9 - 5 = 4
       x
6 ÷ 3 = 2
       =
7 + 1 = 8
---------
The total number of solutions is
2
```

Conclusion

To my surprise, there were two solutions to the problem.

My program started guessing with the number 1 in the first box, and the real solutions both started with a 9 in the first box, so it took a lot of attempts to get it right.

Specifically, it took 345,295 guesses to get the first solution and two more for the second!

It took about 45 minutes of coding and 50-70 lines of code to solve this problem. The actual execution of the program takes less than a second!

While I could have made paper cutouts and solved this by hand, I enjoyed doing it more with code, as it let me be sure there were only two answers.

The source code for grid_puzzle.py is in the penultimate section of this article after the conclusion and before the footnotes.

The code is licensed under the GNU General Public License, Version 3.[1]

If this article makes it to publication in *2600*, I will also make the Python source code to solve the “Four Equations” puzzle at the link in the footnotes.[2]

With my code now complete, I am finally armed with the computational power to brute-force a children’s puzzle. The next time someone asks me if I’m smarter than a fifth grader, I can respond more confidently than ever with a resounding, “probably!”

Source Code

```
from itertools import permutations

def render(l):
    """Render a 3x3 grid of a list `l`."""
    try:
        assert len(l) == 9
    except AssertionError:
        print(f"Expected list of length 9. Got length {len(l)}")

    first_row = f"{l[0]} - {l[1]} = {l[2]}"
    second_row = f"{l[3]} ÷ {l[4]} = {l[5]}"
    third_row = f"{l[6]} + {l[7]} = {l[8]}"
    leading_1 = " " * 8 + "x"
    leading_2 = " " * 8 + "="
    padding = '-' * len(first_row)

    rows = [padding, first_row, leading_1, second_row,
➥leading_2, third_row, padding]
    for row in rows:
        print(row)

def generate_lists():
    """Generate all permutations of range(1, 10)."""
    all_perms = list(permutations(range(1, 10)))

    return all_perms

def check_solution(p):
    """Given a permutation of range(1, 10), return True if p
➥solves the puzzle."""
    try:
        assert p[0] - p[1] == p[2]
    except AssertionError:
        return False

    try:
        assert p[3] / p[4] == p[5]
    except AssertionError:
        return False

    try:
        assert p[6] + p[7] == p[8]
    except AssertionError:
        return False

    try:
        assert p[2] * p[5] == p[8]
    except AssertionError:
        return False
    return True

def main():
    all_permutations = generate_lists()
    all_solutions = []
    for index, p in enumerate(all_permutations):
        solved = check_solution(p)
        # print(f'Trying permutation #{index + 1}...')
        if solved:
            print('Solution found! ')
            render(p)
            # print(f'Took {index + 1} guesses to solve.')
            all_solutions.append(p)

    print(f'The total number of solutions is {len(all_
➥solutions)}')

if __name__ == '__main__':
    main()
```

Footnotes

[1] www.gnu.org/licenses/gpl-3.0.en.html

[2] github.com/bxbrenden/four-equations-puzzle

Hacking and Politics: Why Talking About Both Matters

by Screaming Yellow Fish **sharky.yellowfish@gmail.com**

I've noticed a trend of late in what seems to be a louder chorus of voices who run the gamut from annoyed to royally pissed off at what is perceived to be the political tone of the magazine. It seems to me that this has always been the focus as part of the "voice" of *2600*, and as it has become louder, as well as the current political climate writ large, it has moved me to investigate and see for myself if I myself am biased and there is meat on this bone, or if the current climate is driving a deeper divide between us.

My original intent was to look at the editorial of the first magazine printed for each year. Since I have just completed a cross country move and could not locate my 8.5 x 11 copies of *2600* from 1984 to 1986, I chose to start from 1987 Volume 4, Number 1 and continue on through 2021, Volume 38, Number 1. Not unlike perusing YouTube or anything on the web, I became distracted by an article by none other than Cheshire Catalyst in the January 1987 issue ("TAP: The Legend is Dead.") Funny how I landed on that, as that article touches on many of the very points I have been pondering.

For those who don't have access to that article, allow me to synopsize. *YIPL* (Youth International Party Line) was created by a group of anarchists (Cheshire's term by the way, no letters please for "why did you use that term" blah blah). The "Party Line" part of the name was a reference to the term used when the phone company would connect parties in a networked call. You can Google "party line" and "selective ringing," or just purchase the back issues for the article - it's well worth it.

I should point out that I find it fascinating that my 27-year-old son who possesses half a dozen cell phones; has dozens of aliases online; and communicates via Facebook, Twitter, and TikTok would never imagine that before 1969 it was illegal to attach your own devices to a phone line, that calls were metered, that there was a concept of "long distance" vs. local, that calls were sometimes operator assisted, etc. He looks at a cell phone and asks "wait... you actually use that to make... phone calls?"

Back then, that was the impetus for exploring the phone network, as well as the seeds of the disdain for both the phone company and corporate America. This is not a new concept by any stretch.

In 1971, Abbie Hoffman and Al Bell got the idea to create the *YIPL* newsletter to share information with the members of this technical underground in the same way that the Bell System published information to its own members. It contained pretty random content, and contained anarcho-techno stuff (again, Cheshire's description) including lock picking, making pipe bombs, and other radical stuff.

Here's the kicker. In 1974, Al Bell said to himself (and I am quoting from the article) "What's all this political shit doing in what should have been a technical newsletter?" He left the Yippies, changed the name of the newsletter to *TAP*, and set up shop.

At this point, I read the rest of the article (the last time I read this was in 1987), and it started the wheels turning. My original intent when I started out was to demonstrate that *2600* has always been, and largely still is, a mix of both technical and political content. Imagine my surprise to find an article from 35 years ago from someone who I respect and admire greatly that actually offered up evidence that nope, this is not a new concept.

This got me thinking... what would I have said back then? What would be my advice now? I think it's often human nature when facing a problem to try and minimize options and to pare down the problem into nice neat packages. Thing is people are messy. We are not made of nice neat stuff. We talk at each other instead of to each other. We assume there is only option A or B instead of looking beyond to options C, D, etc.

Here's the thing. I am a tech head, nothing makes me happier than delving into the gritty details of cross site scripting, ARP table poisoning or NVM external memory access cycle times. Thing is, there is no such thing as a free ride.

Do you think the price of the magazine you are holding in your hand is the cost of a subscription, or picking up a copy of the magazine at your local Barnes and Noble? Try this scenario on for size. Texas lawmakers successfully managed to ban abortion in the state of Texas by end running the Constitution. Here's how they did it: The new law allows any private citizen to sue Texas abortion providers who violate the law, as well as anyone who "aids or abets" a woman getting the procedure.

Now let's suppose they decide to go after anyone who prints or publishes any "objectionable" content such as, say, *The Hacker Quarterly*. First Amendment: "Congress shall make no law... abridging the freedom of speech, or of the press." Texas lawmakers can't outright ban *2600*. They can enact a law that allows any private citizen to sue Texas bookstores, service providers, or anyone who violates the law, as well as anyone who "aids or abets" a "person" obtaining "*The Hacker Quarterly*."

Still think that politics doesn't apply to *everyone* who reads this magazine or surfs the site?

Ever since *2600* started publishing, I've read all kinds of attempts to define hackers or hacking or the hacker's ethic. Most more or less seem to hit it on the mark, some more than others. There have been some impressive articles published, including the continuing "Hacker Perspective" column. I would like to offer this:

Above all else, the hacker spirit, or ethos is more than just the exploration and sharing of knowledge... it is about being the voice for those who otherwise don't, can't, or wouldn't have a voice.

We all need to stay engaged, lest we lose the place to talk about and share in the things we love to do.

An Atavistic Freak Out, Episode Five

by Leon Manna

This story is a work of fiction.

Por eso soy andariego
Pa' olvidarme de pesares
Soy barco de cualquier puerto
No me le arrodillo a nadie
Me juego en cualquier gallera
Aquí o en otros lugares

- El Charrito Negro

I'm a coward and a fool! It seemed so simple in the moment, like such a sincere thought. Inner doubt, self loathing. It'll be my turn soon, here or in other places! God! We swam back to shore and started heading towards my apartment. Lenny coughed up seawater and looked at me. "Let me get a ride," he said.

"So you're living here now?"

He nodded. "Yeah dude. I got shot with a .22 like, four times in Miami. Four separate times! Can you believe that? Besides, you pay me to be your lawyer. You're the only person within a hundred mile radius who I can somewhat tolerate, and even then... You piss me off." He seemed to be in a good mood, I guess, despite the backhanded compliment.

"Just take my moped." He hopped on it and rode off. I watched him crank the brakes too hard and crash onto the sand. Then he got up like nothing happened, turned around, gave me the stink-eye, and rode off. About 15 feet later he did that whole thing again, and then disappeared on a bend in the road.

Lenny Cruz (right) and Leon (left)

I heard the dial tone. Then Ary picked up. "What do you want?"

"Uhh... Your stuff isn't at the apartment. I haven't seen you in a couple days. Are you okay?"

"No, I'm not okay. My *ex* boyfriend is a sociopath and I followed him across the country for no reason. I'm going home. I already bought a ticket."

"Wait, wait, wait I -"

"I don't want to hear it. I hate you."

I couldn't even say anything. Can I even be mad? No. Then she hung up, and that's where the Ary plotline ended, as well as any future I had with her. Once again, I felt guilty. It's my fault.

Across the U.S., a federal agent named Segev Bezalel, who we will refer to as Moe, gets a call about a strange guy. A strange guy who smokes crack in Best Buy. The strange guy has been doing unspeakable, despicable acts of cybercrime. Thousands upon thousands of dollars, missing, totally gone with no idea where it went. It's me. I'm the strange guy.

So the detective thinks to himself, "Piece of cake."

But the detective gets frustrated quickly because Leon Manna, who lived in Arizona, died pretty recently. What confuses him is that there's another Leon Manna in Utah. When he checks on that, it shows that he *also* died, but in 2013. Then he checks again, and sees a Leon Manna in California. And then he sees one in Nevada, and South Carolina, and then New York, until he's filled in all but 15 of the states in the U.S. Some are dead, some are alive. Each one has a vaguely similar description. I am everywhere and nowhere at the same time. I am more powerful than god.

This boggles his mind. How did he impersonate someone who's been dead since the last decade? How could it have happened? Moe has no clue what to do. He calls his boss, but it's three in the morning, so he doesn't pick up. He calls about ten other buffoons, none of which pick up either. He finally reaches his boss's boss, who "has no clue who the fuck he is and why the hell would he fucking call me at 3 AM, I mean who has the nerve. Your boss will be hearing about this."

But something didn't sit right with him. He listens to the tone on his phone while he waits for Leon to pick up. He's about to terminate the call when he hears a voice on the other end.

"Hello?"

Moe paused. "Is this Leon Manna?"

There was silence. Then, "Long time, no see. I miss you Moe."

"Segev, dumbass. Let's talk, please. You don't need to run."

"No, Moe. I do need to run."

"You don't. We gathered everything, Leon. I even see an armed robbery here. We're going to catch you eventually."

"No the fuck you will not. Also, that robbery wasn't me. It was a man named Nash Nashville. You'll find him in Memphis. I wouldn't bother looking in Nashville, though. If he's not there, I'd check your mother's house."

"Well, that's just disrespectful." But the call was terminated and there was nobody listening to hear him say that. When he called back, the number was disconnected. In the morning, he calls his boss. His boss decides to send him on a maniacal wild goose chase, investigating every single Leon Manna in the U.S.

So what now? Well, I have 15 states that need Leon Manna in them. A federal semi-turncoat is always won over with blackmail. They do nasty stuff, they really do, you just have to catch them. This is how we operated for a while. And then, we met this guy somewhere in a stack of papers. We knew he was from New Mexico, but we didn't know his name. I'll let you fill the rest in.

Moe sees this. Just like my shapeshifter act at Sawtooth, this actually did the opposite of what I thought it would. I was just trying to cause as much confusion and chaos as possible, there was basically no strategy past that. Moe isn't an idiot, and he realizes very quickly that I'm making all these fake identities in different states to confuse him. Why? Because if he would do it, I would. That's sorta how he caught us. They assigned my case to him after they did a profile on me. There was a reason it was him, but I simply can't tell you why just yet. There's more to say before. He calls his boss and after like, seven layers of bureaucracy or something, someone finally orders the Social Security Administration to check in on all of these Leon Manna clones. The SSA says they can't do that within the timeframe they needed because there were multiple real Leon Manna identities in some of those states. So after swearing profusely at the person from the SSA, the moron demands that they investigate every case of Leon Manna in any state ever, regardless of how long it takes. This was a huge waste of time because they can't seem to figure out which ones were real and which weren't. They couldn't go and check every single Leon in real life, they simply didn't have the resources, and I wasn't important enough for that.

So the Federal Pig calls the SSA back and says that they need to check to see which Leon Manna identities match up with each other in other states, for unknown reasons. I'm not sure what their tactic was there. But every single picture was a different person. I'm really good at photoshop.

...

What to do, what to do... I didn't know yet. I was thinking about it, waiting for 1.5 grams of phenibut hydrochloride to kick in when I heard a knock on my door. Déjà vu.

Again, Lenny, except normal this time. "I'm going to Cuba. We both have warrants."

"I know," I said. "I called the county office claiming to be an employer looking to hire us. I said I just needed to know if there was anything that should disqualify us. The list was pretty long, this isn't good."

"Well, let's go then."

I thought about it for a second. "What about a contingency plan?"

And so here's what happened: I sat back and did nothing. But one night, at 3 AM again, there was nobody in the office except for the security guard. The first thing that happened was somebody made it into the server that stored digital evidence of people Moe was investigating via the EternalBlue exploit. The intruder dropped a small executable file into a temporary folder, executed it, and then disconnected. This executable, which had been encrypted and then packed into another executable, remained unflagged by antivirus and looped through the entire filesystem until it had collected the paths of every SQL database file on the system. Then, the executable proceeded to overwrite that database with null bytes. Then it did that to the entire HDD. Then it destroyed the backups. Then wiped the MBR of the server.

The Master Boot Record (MBR) is the first 512 bytes in the first sector of your HDD that tells the computer where the OS is and then how to load it. If you overwrite the MBR with null bytes, the computer will not boot. If you overwrite it with your own code, the computer will run whatever you placed every single time it starts.

Long story short, the server says "fuck you" on boot, every single time. So did every computer in his office. Then, somehow, the intruder got control of the thermostat in the evidence room and then turned it up to a dangerously high temperature, making most or all of the physical evidence useless. At least the shit they had on me. Eventually the evidence room caught on fire due to the amount of paper documents inside. Needless to say, panic ensued.

But this wasn't me. The IP address they associated with the intrusion originated overseas. The executable had basically nothing in it of value, even though they spent a lot of time reverse engineering it. The IP they had came from a country where they had no jurisdiction, far far away. Somewhere in Europe I think... But I wouldn't know, I just sat on my couch and watched a movie.

What evidence? What are you talking about?

Oh God when will it stop on: An Atavistic Freakout*?*

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.** We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community.

Events are subject to change. Please be sure to follow all safety protocols that are put in place by these events and venues.

September 10-11
Vintage Computer Festival Midwest 17
Waterford Banquets
Elmhurst, Illinois
vcfmw.org

September 16-18
CircleCityCon 9.0
The Westin
Indianapolis, Indiana
circlecitycon.com

September 22-24
Texas Cyber Summit
Hyatt Regency
Austin, Texas
texascyber.com

September 23-25
Balkan Computer Congress
Congress Centre
Novi Sad, Serbia
2k22.balccon.org

October 13-14
GrrCON
DeVos Place
Grand Rapids, Michigan
grrcon.com

October 21-22
SecureWV 13
Charleston Coliseum and Convention Center
Charleston, West Virginia
www.securewv.org

December 27-30
Chaos Communication Congress
Hamburg Congress Center (CCH)
Hamburg, Germany
events.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

For Sale

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.

SECPOINT PORTABLE PENETRATOR. WPA WPA2 WPS WiFi Pen Testing Software. Vulnerability Scanning & Assessment. Customize reports with logo, name in PDF or HTML format. Coupon code 20% off: 2600. https://shop.secpoint.com/

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.

OPEN SOURCE HARDWARE: crowdfunded and in-stock on Crowd Supply (crowdsupply.com). Includes software-defined radios (SDRs), DIY computers, NASs, FPGA boards, open silicon (RISC-V), hardware encryption/security devices, pentest tools, health monitors, kite-balloons, workbench tools, optical decoders, and opportunities to help fight the DMCA (see bunnie huang's NeTV2 project).

SECUREMAC.COM is offering popular anti-malware app MacScan 3 to help protect Mac users from malware, spyware, and ransomware. Download a 30-day trial directly from SecureMac.com. Looking for a new podcast? Check out *The Checklist* by SecureMac on iTunes, Pandora, and Spotify.

GUIDEBOOK TO COMPUTER AND SMARTPHONE SECURITY by Brandon of Lipani Technologies LLC has been released. This new security book can be purchased at https://leanpub.com/techgeek. Brandon is a certified CompTIA Security+ professional helping users and companies secure their computers, networks, and smartphones across the country. He says, "The purpose of this book is to educate and teach computer and smartphone users about safety and security online."

Help Wanted

VIRTUAL ASSISTANT/PROGRAMMER NEEDED. I have various tasks I need done but I am incarcerated. I will need both a programmer and a general assistant. Tasks include: 1) Internet research, 2) product ordering, 3) printing and mailing of documents, 4) some light programming tasks. Requirements include 1) printer, 2) webcam, 3) U.S. phone number, 4) Internet. No experience needed for assistant position but good Internet research skills a plus. Please send resume and salary requirements and contact me via phone when sent snail mail: 360-295-4317. Timothy Bach, 901 Port Ave., St. Helens, OR 97051

JOIN THE HTTPS://CODEFOR.CASH community and earn money with freelance programming jobs. All hats welcome!

Announcements

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!

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.

THE MODERN TECHNOLOGY PODCAST NETWORK contains a growing selection of original audio programming by familiar voices from the hacker world and elsewhere. Our comedies, documentaries, audiobooks, cultural discussions, and more are totally free, completely independent, hacker-produced, CC-licensed, and utterly devoid of commercials. Feed your ears at https://modern.technology

DON'T JUST CELEBRATE TECHNOLOGY, question its broad-reaching effects. 78 Reasonable Questions to Ask About Any Technology - tinyurl.com/questiontech

DOC8643.COM: technical details of aircraft from International Civil Aviation Organization (ICAO) Doc8643. This is an educational and reference tool. Check it out at https://doc8643.com.

COVERTACTIONS.COM is the most comprehensive directory of encryption products anywhere. Search by type, hardware/software, country, open source, platform, and more. Now over 1036 products listed which include 221 VPN's, 192 messaging and 117 file encryption apps. These are just a few of the 28 categories available. There is no faster and easier way to find the encryption product that meets your requirements. Suggestions and feedback welcome. Now featuring news on important encryption issues.

Services

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.)

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.

DISCOUNT WEB HOSTING AND FREE WEB TRAINING. Squidix Web Hosting provides FREE WordPress training in Arlington, VA for Squidix customers. We provide fantastic web hosting for 1,000s of clients. We love our clients and they love us. Our ongoing *2600* promotion will give you 50% off any hosting service for the first year. This offer valid for any new accounts and includes a free CPanel transfer of one existing website. Sign up at www.squidix.com and use code 2600 on checkout.

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.

UNIX SHELL ACCOUNTS WITH MORE VHOSTS. If you like funny, relevant vhosts for IRC, get a JEAH shell. Also, use our vhost domains for email. Access new and classic *nix programs, compilers, and languages. JEAH.NET hosts bouncers, bots, IRCD, and websites. *2600* readers get free setup. BTW: Domains from FYNE.COM come with free DNS hosting and WHOIS privacy for $5.

DOUBLEHOP.ME VPN is actively searching for an acquisition partner that shares our vision (https://bit.ly/3a1bCuM). We're an edgy VPN startup aiming to rock the boat with double VPN hops and encrypted multi-datacenter interconnects. We enable clients to VPN to country A, and exit country B. Increase your privacy with multiple legal jurisdictions and leave your traditional VPN behind! We don't keep logs, so there's no way for us to cooperate with LEOs, even if we felt compelled to. We accept Bitcoin! Use promo code COSBYSWEATER2600 for 50 percent off. https://www.doublehop.me

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.

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

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.

HAVE YOU SEEN THE *2600* STORE? Plenty of features, hacker stuff, and all sorts of possibilities. We accept Bitcoin and Google Wallet, along with the usual credit cards and PayPal. EVERY YEAR of *2600* and EVERY HOPE TALK now available for digital download! Plus, we've lowered prices on much of our stock. Won't you pay us a visit? store.2600.com

Personals

HELLO PITTSBURGH & WESTERN PENNSYLVANIA. I'm looking for like-minded individuals to help relaunch monthly *2600* meetings in this area. I have access to a comfy conference room in a conveniently located suburban shopping center. Send me a letter with everything you think I should know: MARS, PO Box 27050, Pittsburgh, PA 15235. Confidentiality guaranteed.

DO YOU WANT TO BE A HACKER? I've had some write to me asking for tips on this or that, but based on what I read in the Letters, there are many of you out there who could use a bit of coaching. Long gone are the days when I billed out at $250/hr to save a datacenter's day or other such emergency. I'm in prison. You can look me up on the TDCJ website and see I'm no weirdo. I do have plenty of time on my hands. Lucky you! So, don't delay, write to me with your problems, questions, pithy comments, or exploits. The best way is to use the messaging app www.jpay.com. Looking forward to hearing from you. Ryan Sumstad, Ph.D., #01918058, Wynne Unit, 810 FM 2821 West, Huntsville, TX 77349.

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 your address label/envelope or a photocopy so we know you're a subscriber. If you're an electronic subscriber, please send us a copy of your subscription receipt. 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 next issue: 9/16/22.

HACKER PERSPECTIVE
submissions have closed again.

We will be opening them again in the future so write your submission now and have it ready to send!

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.

This is awkward.

Usually after a HOPE conference, we print an ad suggesting you get videos of all of the awesome talks that went on. But this year, because we're still catching up on our printing schedule due to the COVID crisis in 2020, this issue was put together right before the conference happened instead of well before - too late to promote HOPE but too early to say it was a success. So maybe we forgot to hit the record button and there are NO videos. It's unlikely but it's possible. We can't in good conscience put out an ad for something that doesn't yet exist. But by the time you read this, we will know one way or another. So check our website at www.2600.com or www.hope.net and see if there are videos from A New HOPE available on thumb drives or for download. If there are, we strongly suggest getting them.

And please spread the word!

"What about Facebook using the system to steer people? We know for a fact all the major Internets do that." - Wyoming State Senator Anthony Bouchard at a debate during his campaign for the U.S. House of Representatives

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
beave, koz, r0d3nt

Facebook Team
astrutt, Cryovato, Tina Rose, TechnoMage, danixdefcon5, ItsTehPope, LadyNikon, Osiris

Inspirational Music: Stevie Wonder, Cody ChesnuTT, Zdob si Zdub & Advahov Brothers, Charles Wright & the Watts 103rd Street Rhythm Band, Dramatik
Shout Outs: Stephen, Elena, Sonia, John
R.I.P.: John Drake

***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

BACK ISSUES:
Individual issues for 1988-2021 are $7.25 each when available. Shipping added to overseas orders. All back issues (1984-2021) available digitally as annual digests 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)

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

MEETINGS

2600 MEETINGS ARE RETURNING - SLOWLY BUT STEADILY. PLEASE CONTINUE TO TAKE PRECAUTIONS WHERE WARRANTED. KEEP CHECKING THE WEBSITE BELOW FOR MORE UPDATED LISTINGS AS WELL AS INFO ON HOW TO START YOUR OWN MEETING!

CANADA

Alberta

Calgary: Food court of the Eau Claire Market. 6 pm

IRELAND

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

RUSSIA

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

SWEDEN

Malmo (@2600Malmo): FooCafé, Carlsgatan 12A.

Stockholm (@2600Stockholm): Kungshallen food court, Kungsgatan 44.

UNITED KINGDOM

England

London (@London_2600): Angel Pub, 61 St Giles High St, outdoors at the red telephone box. 6 pm

Scotland

Glasgow (@Glasgow2600): Bon Accord, North St. 6 pm

UNITED STATES

Arizona

Phoenix (Tempe) (@PHX2600): University of Advancing Technology auditorium. 6 pm

Prescott: Merchant Coffee, 218 N Granite St.

California

San Francisco: 4 Embarcadero Center, ground level by info kiosk. 6 pm

Colorado

Denver (@denver2600): Denver Pavilions. 6 pm

Fort Collins: Starbucks, 4218 College Ave. 7 pm

Connecticut

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

Florida

Jacksonville (#Jax2600): Goozlepipe & Guttyworks, 910 King St.

Kansas

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

Maine

*** Portland (@Maine2600):** Open Bench Project, 971 Congress St. 6 pm

Massachusetts

Boston (Cambridge) (@2600boston): The Garage, Harvard Square, food court area. 7 pm

Hyannis: Barnes & Noble, Cape Cod Mall. 6:30 pm

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 Jersey

Somerville: Bliss Coffee Lounge, 14 E Main St.

New York

Albany: Starbucks, 1244 Western Ave. 6 pm

New York (@NYC2600): Citigroup Center, 53rd St and Lexington Ave, food court.

Rochester (@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.

Pennsylvania

Philadelphia (@philly2600): 30th St Station, food court outside Taco Bell. 6 pm

Texas

Austin (@atx2600): Central Market mezzanine level, 4001 N Lamar Blvd. 7 pm

Dallas: The Wild Turkey, 2470 Walnut Hill Ln #5627.

Houston (@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, Suite #B. 6 pm

Virginia

Arlington: Three Whistles, 2719 Wilson Blvd.

Reston: PH3AR/Nova Labs, 1930 Isaac Newton Sq W. 7 pm

Washington

Seattle: Cafe Allegro, 4214 University Way NE (alley entrance), upstairs. 6 pm

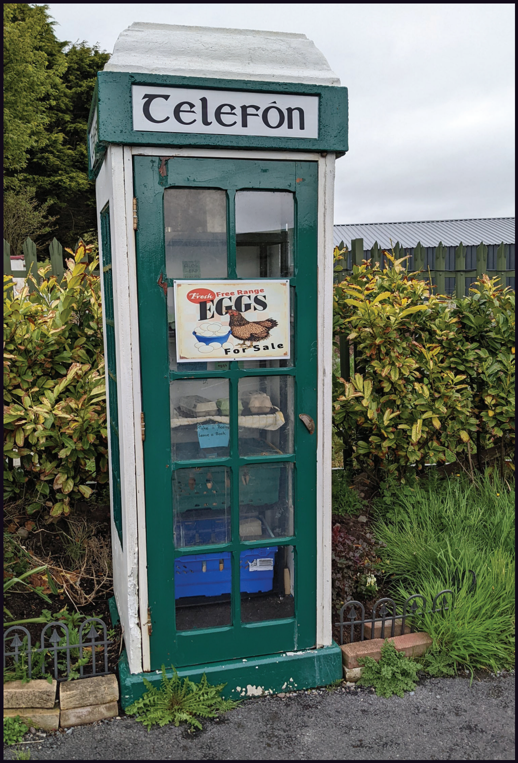
*** indicates Thursday meeting**

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 handle or hashtag 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.

NOTE: Please do not come to meetings if you're not vaccinated. This is for your own safety. Proof of vaccination is not required but we hope that common sense prevails.

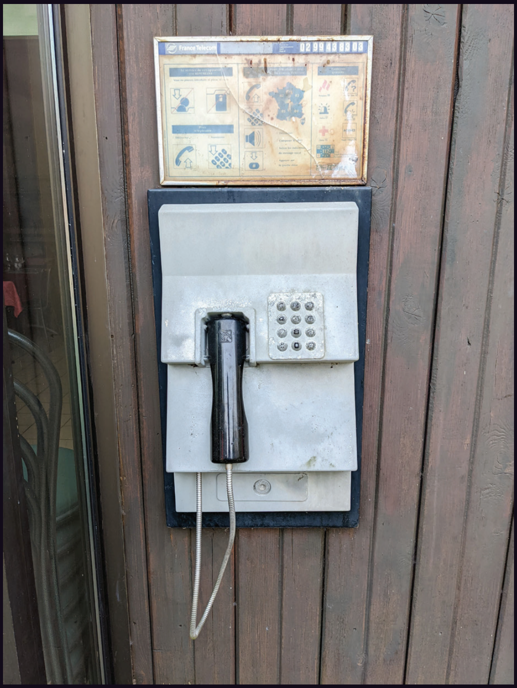
www.2600.com/meetings

Uncertain Payphones



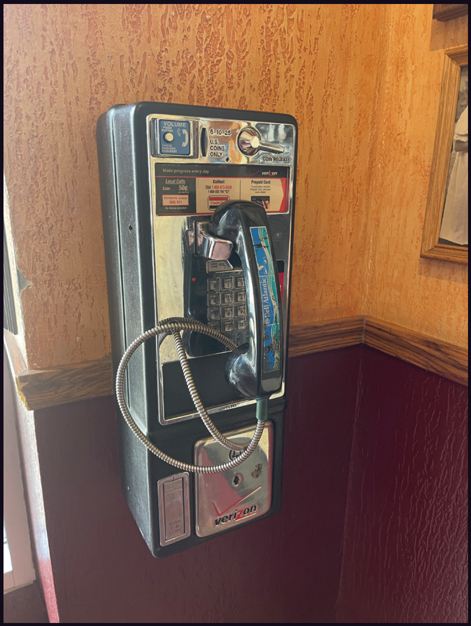
Ireland. We've seen phone booths converted to libraries but this is a first. Seen in Westport, this former phone box now sells eggs on the honor system. (And it's also a library.)

Photo by Daniel Cussen



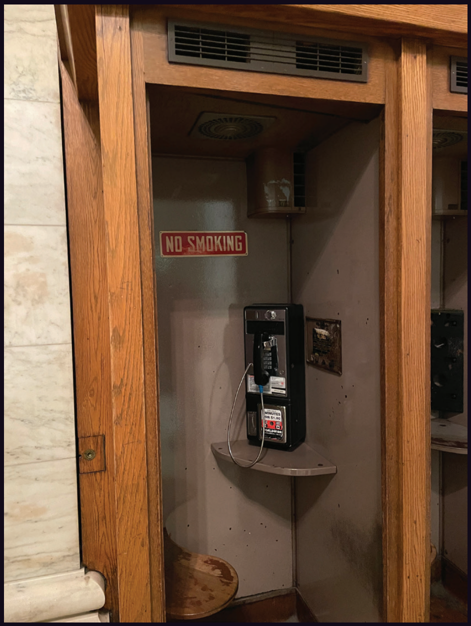
France. We honestly don't know what's going on here as most of this phone's features seem to be obscured by dust or sun or just fading into nothingness. Supposedly all payphones in the country were disappearing by 2018. Here's one they missed.

Photo by Nicolas RUFF



United States. Found at a Buca Di Beppo in Washington DC, this phone appears to defy the odds by even existing. The coin vault and instruction card were once updated, but nobody ever got around to replacing the handset sticker for Bell Atlantic, a company that hasn't existed for more than 22 years.

Photo by Byte Stealer

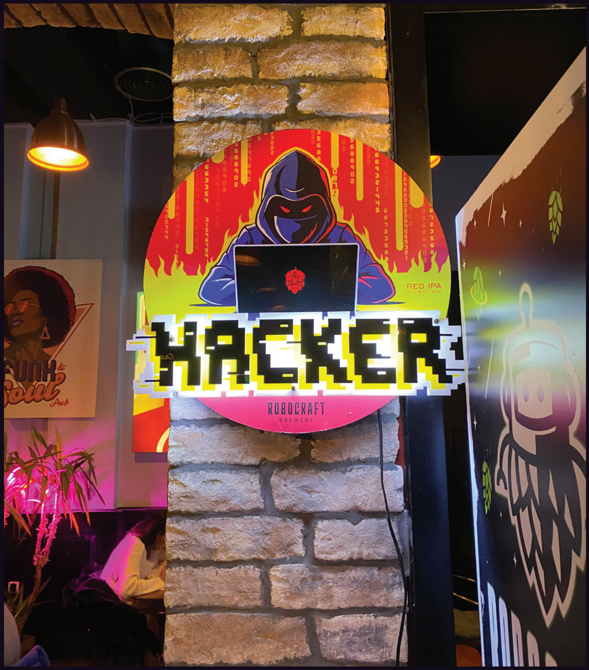


United States. Where else but inside the New York Public Library on Fifth Avenue in New York City would you expect to find a payphone in an old-fashioned wooden booth with chair, fan, and light? It's actually one of several. But you'll be disappointed if you expect any of them to work.

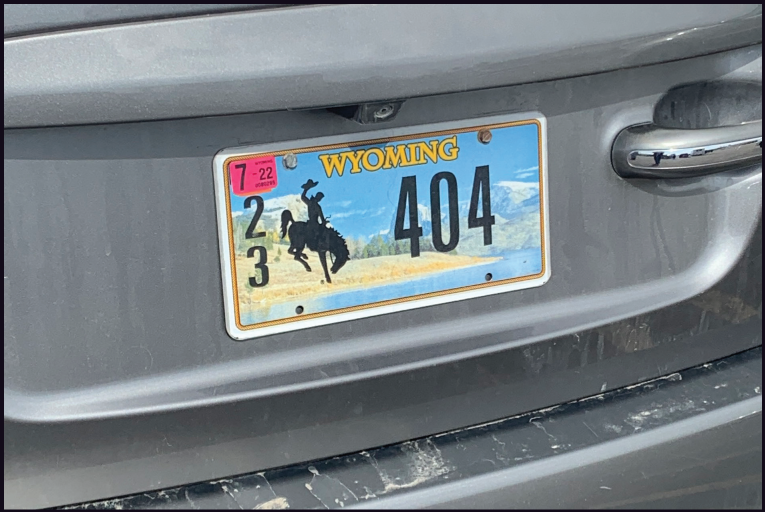
Photo by Anne Jackson

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



You'd think we would have heard of this by now, but there's actually a Hacker beer made in Belgrade, Serbia by Robocraft Brewery and discovered by **Sam Pursglove**. Their web has a description of the character the beer is named after which translates to: "Hacker is a developer who is tired of working for the big corporations that run our lives, and his mission is to decode the industrial matrix in brewing that we are bombarded with by the mass media." Maybe we'll get around to importing it



Observed somewhere in Wyoming by **Grace McNerney**, who theorizes that "maybe it's the Matrix trying to tell us Wyoming really doesn't exist." That's exactly what they'd want us to believe.

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.