ISSUE 007 UNREDACTEDMAGAZINE.COM SEP 2024

UNREDACTED

FIGHTING BACK AFTER BEING SCAMMED:

Using state resources to force action

THREE MONTHS OF CLOAKED:

Masking emails, phones, addresses, and payments

REVENGE AGAINST SPAMMERS:

Forcing spammers to attack each other

UNREDACTED
ISSUE 007

IN THIS ISSUE

Cover Design by Anonymous Reader and layout by Astropost. Special thanks to everyone who helped make this happen. You know who you are.

FROM THE EDITOR

By Michael Bazzell

It has been just seven months since the previous issue of UNREDACTED Magazine. That is better than the full year it took to obtain content for issue 006. Hopefully things are moving in the right direction. As previously stated, the magazine is a community-driven product. Without the community driving it, it will go nowhere. If you would like to submit an article, please email it to staff@unredactedmagazine.com. If enough content is received, I will happily publish the next issue. Without content, there is nothing to publish.

With this issue, we have tried something new. Cloaked has offered to sponsor the entire issue. In past issues, several sponsors paid a small fee to serve a single advertisement. This time, Cloaked is picking up the entire tab. I had already planned on writing an updated article about my experiences using Cloaked over the past three months, so this sponsorship made sense on both ends. I sincerely thank them, and all of the past sponsors who keep this product free to all readers.

I also thank all of the content contributors for this issue. The theme is "fighting back", and I think we present an amazing lineup. My favorite part about putting this magazine together is when I read an article that makes me smirk in excitement. This happened several times within this issue. I still believe that a long-form publication such as this beats the onslaught of blog posts, clickbait headlines, and social media snippets bombarding us every day. I continue to be impressed with the submissions.

Please note that we try to edit these articles as little as possible. I always want to preserve the author's words, tone, and overall vibe. It is not our place to abbreviate their content or correct their writing patterns. If you have objections to someone's grammar or prose, take it up with them. Better yet, acknowledge that we are all unique and just keep reading the free content without the need to judge others. We received a record number of "grammar police" complaints from the last issue, but I still refuse to modify someone else's thoughts.

I sincerely thank you for the interest in this concept. I hope to meet back here very soon. I now present issue 007 of UNREDACTED Magazine.

MB

Image: jeshoots

FIGHTING BACK AFTER BEING SPAMMED

By Anonymous

Spam emails seems to be worse lately. I am sure we all get the occasional unsolicited vacation offer or Chinese gadget promotion. I accept those as a price of using email. I am more frustrated at the direct marketing messages which never stop. Several of my email addresses somehow found themselves within marketing databases being sold to spammers. Every day, I receive countless messages asking me if I want to have my website redesigned, if I need a business loan, if I want to buy marketing databases to spam other people, or if I need a mobile app created. This is nothing new and probably a common annoyance with most readers. The difference lately is the persistence. Instead of sending an email blast and hoping for a few bites, the same people are sending me reminder messages every day wondering why I haven't responded to their spam. They never give up so I decided to fight back.

Some spam emails have an unsubscribe link to be removed from their list. If the sender is a reputable company, I click them. That seems to work for a while. If the email is shady, I never click the unsubscribe link. It just confirms that you read the message and encourages them to continue the attack.

Some email providers allow you to report spam to a third-party service. They report emails marked as spam to the company with which they analyze incoming messages. If enough people report that sender as a spammer, then multiple email providers will start marking the messages as spam. This helps a little, but spammers switch domains and addresses often.

My solution is to waste their time. I give every spammer a pass for the first message. When I see a message which is a "reminder" or "bump" to get in my inbox, I place it in a designated folder. When I receive a third message from them, annoyed that I never responded to their spam, I attack.

I first look for any footer details which include a telephone number. These are VoIP burner numbers but they are monitored for sales leads. I copy the phone number from one spam email and reply to a different spam message asking them to call me at that number. I then let the two spammers try to figure out who is selling trash to the other. For some reason this brings me joy. Here is an example I sent to a company offering me a loan:

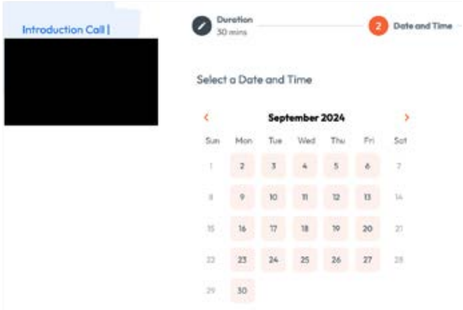
That sounds great! Can you call me at REDACTED? I don't like to discuss business over email.

I provided the number included in the footer of a spam message about real estate.

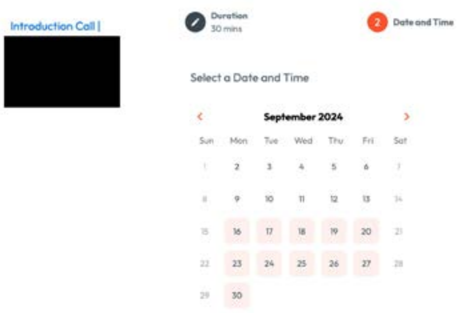
Next, I look for spammers who include a URL to their calendar. These allow anyone to schedule a call with them. Here is a true example with only one letter missing from the URL:

"If you have software development needs you would like to discuss with us, feel free to use this link to choose any open time when you're ready. http://schedulintool.bairesdev.com/brandon-oconnor/default"

These are my favorite. I send this URL to every spam message in my folder, asking them to set up a time for a call about their service. Now several spammers are excited that someone wants to talk with them, and I waste their time like they have wasted mine. Here is this actual calendar for next month before I sent the email blast to all other spammers.


[redacted]

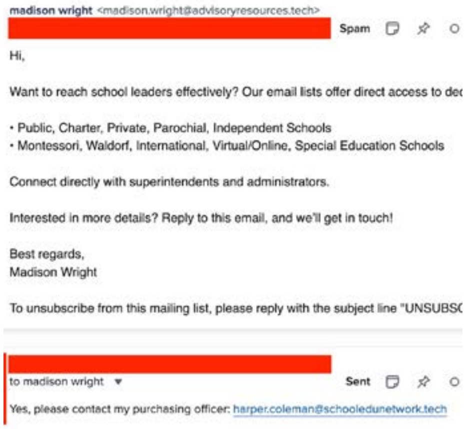
Here is the same calendar four hours after the blast.


[redacted]

Oh I wish I could sit in on those calls. If I am truly bored, I will go ahead and register a few spammers on the calendar myself. This will generate email verifications from one spammer to the other which may distract them from hassling me.

If there is no phone number or calendar URL, I just ask them to email my "assistant" all of the details. I then copy a random spammer email address and let the two of them figure it out. Of course I send this from a masked email so they cannot trace it back to my real address.

As I wrapped up this article I checked my email. I saw two similar spammers communicating back and forth while copying my masked address in each message. They are both confused but still eager to sell the other their trash. The more time they spend on that the less time they come after us. I find it funny when they both think they are convincing the other to buy something from them. Here is how I started the conversation with each.



madison wright <madison.wright@advisoryresources.tech>

[redacted] Spam

Hi,

Want to reach school leaders effectively? Our email lists offer direct access to dec

• Public, Charter, Private, Parochial, Independent Schools
• Montessori, Waldorf, International, Virtual/Online, Special Education Schools

Connect directly with superintendents and administrators.

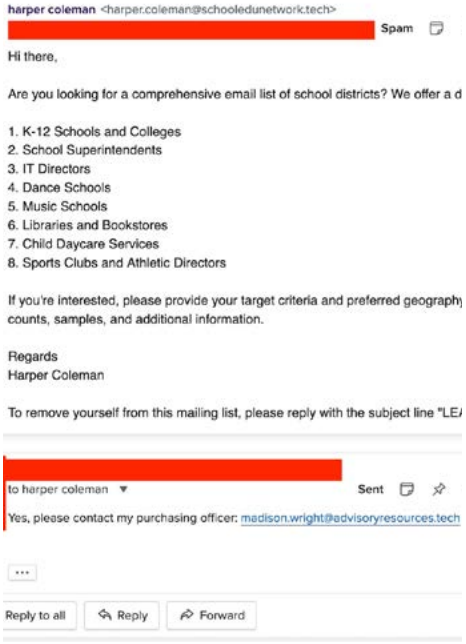
Interested in more details? Reply to this email, and we'll get in touch!

Best regards,
Madison Wright

To unsubscribe from this mailing list, please reply with the subject line "UNSUBSC

[redacted]
to madison wright ▾ Sent

Yes, please contact my purchasing officer: harper.coleman@schooledunetwork.tech



harper coleman <harper.coleman@schooledunetwork.tech>

[redacted] Spam

Hi there,

Are you looking for a comprehensive email list of school districts? We offer a d

1. K-12 Schools and Colleges
2. School Superintendents
3. IT Directors
4. Dance Schools
5. Music Schools
6. Libraries and Bookstores
7. Child Daycare Services
8. Sports Clubs and Athletic Directors

If you're interested, please provide your target criteria and preferred geography
counts, samples, and additional information.

Regards
Harper Coleman

To remove yourself from this mailing list, please reply with the subject line "LE/

[redacted]
to harper coleman ▾ Sent

Yes, please contact my purchasing officer: madison.wright@advisoryresources.tech

From there they began trying to sell the other person their data. The confusion was thick as they each tried to explain that THEY were selling data not buying data. I just hung out and watched. Eventually they figured out what is going on.

Every now and then one of the spammers emails me to blame me for wasting their time. I want it known that I only do this when the unsolicited spam is coming from a company which obviously bought a sales leads sheet. I would not waste my time trying to convince Facebook or other large mass mailings to take any action. This works best on small startups sending bulk messages hoping for a bite.

Does any of this make a difference? Probably not. I am just one person. But what if we all did it? What if we all harassed the spammers which won't take no (or silence) for an answer? I think we could influence these worst offenders and make them think about that next email campaign. ■

FIGHTING BACK AFTER BEING SCAMMED

By Michael Bazzell

While responding to questions in the upcoming Q & A section, I noticed the following entry awaiting a response:

"I was one of the many people scammed by Purism. I purchased the Librem Linux phone from them over six years ago and they still refuse to give me a refund after never sending the device. I sent several emails to support but they stopped responding. What else can I do?"

My response became quite lengthy, so I turned it into this full article. I also played off of the title of the previous article. Hopefully, some of my thoughts help others in similar situations (or other people scammed by Purism).

First, you should make every attempt through the official channels. In your case, you have already done that. You requested a refund for a product which was intentionally never delivered, and they refused. I know many people in your shoes. Fortunately for me, I demanded a refund from Purism in the early days when I could tell they would never deliver on their promises. Shortly after my refund, they stopped providing refunds on non-delivered products.

Next, you should file a dispute with your credit card company if two conditions are met. First, the purchase must be within that credit card company's dispute time frame. This could be 30 days to a year. Since you are likely out of that range, that might not help. Second, heed my warnings about filing too many disputes later in this article. Only do this if you are not concerned about being flagged as one who abuses the dispute process. In your case, I would still contact your credit card and make sure they cannot assist with such a large purchase.

When I do not receive any solutions from a company, my next action is to contact the CEO or other executives directly. I was recently suspended from my Telnyx account (again), so I reached out to the CEO via LinkedIn. Surprisingly, he responded and said he would look into it. I have contacted many executives through LinkedIn in the past few years. I would estimate that only 10% of them respond in any way. When that doesn't work, I move to the next option.

If a person does not respond to my LinkedIn message, I identify their LinkedIn user ID number (explained in my book OSINT Techniques). I then query this number through all of my LinkedIn breach data to identify a personal or business email address. I then repeat my message to them via this direct channel and hope for a response. This usually picks up another 25% chance of a response.

If I am unable to contact anyone at a company to resolve an issue, I move to more aggressive and official techniques. I could post a complaint to the Better Business Bureau using an alias name, but that could pose problems. I would never use my real name with them because they publish details of the complaints online. If that does not bother you, then you might receive a response from the offending company when a complaint is posted. I doubt Purism would respond.

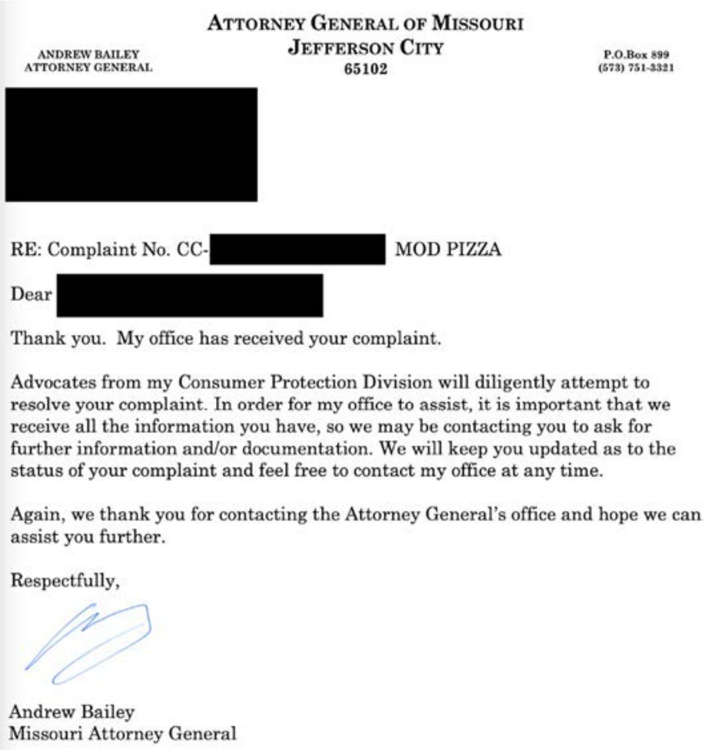
I prefer to involve my state's consumer protection division. Every state has their own office which handles consumer complaints. These may be titled something different than this, but most usually fall under the authority of the State Attorney General. I will offer a true example of one incident where this helped.

My team and I had just landed for a quick job. It was late and we were all hungry. The small airport was basically shut-down and all restaurants we saw were also closed. The only place open was a MOD Pizza establishment, and it was quite busy. We ordered a bunch of personal pizzas to go and waited. After about 20 minutes, I asked about the delay. They stated that they had accidentally given our pizzas to another customer, and we would need to get back in line and re-order. We had no interest in starting over, so I told the manager to refund the card and we would find something else. He assured me it would be taken care of the following day.

After the trip, I combined all of the receipts for our bookkeeper and noticed that the purchase was never refunded from my card. I called the restaurant and spoke to the manager. He stated he had no way to offer a refund, even though the products were never delivered. He encouraged me to contact their corporate office. The entire refund was less than $200, but I was determined to hold them accountable.

I called the corporate office a few times, left messages, and sent emails. A week later, there was still no response. I didn't want to dispute the charge on my credit card just yet because I like to reserve that for larger purchases. If you dispute too many transactions, your account gets flagged for review. I thought about dropping it and eating the loss, but I couldn't let it go out of principle.

I contacted my state’s consumer protection office and filed an official complaint. I was honest and detailed. I confirmed that no one from the offending company had returned any communication and that I was still out money. The state sent an official letter of the complaint to MOD Pizza and sent me a copy. I repeated this process with the state in which the event occurred. Both states demanded a response from MOD Pizza. I received the following from the second state (the location of the restaurant) the next day.



ATTORNEY GENERAL OF MISSOURI
JEFFERSON CITY
65102

ANDREW BAILEY
ATTORNEY GENERAL

P.O.Box 899
(573) 751-3321

[redacted]

RE: Complaint No. CC-[redacted] MOD PIZZA

Dear [redacted]

Thank you. My office has received your complaint.

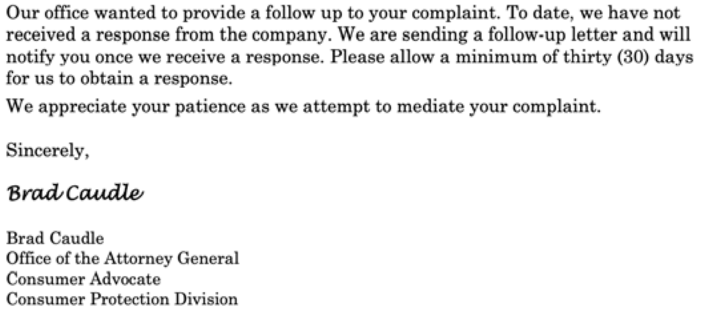
Advocates from my Consumer Protection Division will diligently attempt to resolve your complaint. In order for my office to assist, it is important that we receive all the information you have, so we may be contacting you to ask for further information and/or documentation. We will keep you updated as to the status of your complaint and feel free to contact my office at any time.

Again, we thank you for contacting the Attorney General’s office and hope we can assist you further.

Respectfully,

Andrew Bailey
Missouri Attorney General

It was a canned letter, but promising. Two weeks later, I received the following from the state.



Our office wanted to provide a follow up to your complaint. To date, we have not received a response from the company. We are sending a follow-up letter and will notify you once we receive a response. Please allow a minimum of thirty (30) days for us to obtain a response.

We appreciate your patience as we attempt to mediate your complaint.

Sincerely,

Brad Caudle

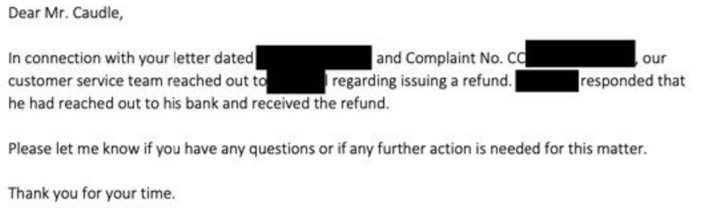
Brad Caudle
Office of the Attorney General
Consumer Advocate
Consumer Protection Division

I was shocked they were taking this seriously, and even more shocked that MOD Pizza ignored them. Within four days of receiving this notice via email, an executive with MOD Pizza called me offering to resolve the issue. It worked!

Let’s have a reality check about what is happening here. The state will never sue the company on my behalf or take any other action to help me. The letter they sent with my complaint looks concerning but there is no threat of further action. It is basically a note from the state saying “Knock it off and give this guy his money back”. However, these letters tend to receive responses, especially when they keep coming. No company wants to challenge a state over $200 and hope they don’t lose licenses or get sued.

The executive from MOD Pizza refunded the purchase to my card, but refused to apologize for the issue. They only wanted me to acknowledge that the issue had been resolved to the state. The state would not close the investigation until I confirmed the resolution, and MOD Pizza was eager to close the books.

I intentionally refused to acknowledge these requests for two weeks, much like they ignored me for two weeks. I wanted them to understand how it felt to be ignored when they needed something. I eventually notified the state consumer office that the issue had been resolved, and the case was closed on their end. I was then copied on the following.



Dear Mr. Caudle,

In connection with your letter dated [redacted] and Complaint No. CC[redacted], our customer service team reached out to [redacted] regarding issuing a refund. [redacted] responded that he had reached out to his bank and received the refund.

Please let me know if you have any questions or if any further action is needed for this matter.

Thank you for your time.

I have found this to be the best course of action. Back to the original question. If I were you, I would file a complaint with your state against Purism and see if that gets any traction. I would repeat the complaint to Purism’s state (California). If enough people who were ripped off by them do this, I think you could all see a response. California will not take kindly to being ignored.

If that fails, you could generate a small claims civil suit, but you may find that the jurisdiction falls in the location of Purism’s headquarters instead of your own county. You would need to look into that on your end. It would be cheaper for them to refund your purchase than to send an attorney to respond to the claim. Be warned that any lawsuit could expose you and ruin your privacy. Pick your battles wisely.

Leaving negative reviews online might get you a response, but not often. Purism has already received so much bad press about this, I don’t think they would care. I don’t like leaving online reviews because of privacy issues. I do not want a digital trail of the things I buy or the places I visit.

Overall, stand up for yourself. Any time a company takes your money and does not give you what you paid for, make a stink. Don’t stop until you receive a fair result. ■

Image: Steve Pancrate

NEXT-LEVEL DISINFORMATION

By Rambo

I read Michael Bazzell's book Extreme Privacy and applied his ideas about disinformation through cellular contracts. I was able to populate an inaccurate home address in my credit report but I was not content. I wanted to see what else would hit my report. This article tells my story. I am not a lawyer (IANAL). Don't do what I did.

My first attempt was through insurance. I wanted my previous address to be shown as my current home but it was nowhere on the report. I was only there a small time and it was a rental home. I asked for a quote from State Farm and Progressive and I gave them my true name, DOB, SSN, and the old address. They gave me quotes but all said that they do not do a credit pull as part of the process. I wanted that credit pull.

I then tried Lemonade. This is a new rental insurance provider and they target younger people willing to install apps for everything. I installed the app and applied. I provided the same details but they did not ask for a SSN. They did demand a DOB which would be enough for a credit pull. They offered me a quote for renter's insurance at $18 per month for my old place.

I pulled the trigger and accepted their deal. I insured the place for one month and then cancelled. I know they report this to various private insurance databases and I only suspect they conduct a soft credit pull based on name and DOB.

I then requested an auto quote from Zebra. I gave them my real name and DOB plus the rental address used in the last example. They demanded a bunch of personal information which could be easily fudged. I told them I was just looking and provided false vehicle details. They shared my information with Progressive, Gainsco, and four additional insurers. I did not select any policy.

Thirty days later, I requested all possible reports about me from the Data Requests portion of the book. On four of them they listed my false rental address as my current home. Two listed the VoIP number I provided in my applications. The LexisNexis report had all of the information I had provided. That was the goal. They believe I live somewhere I don't.

I'm not confident that this will help hide my real address in the long run, but for now it helps. It also allows companies to think they know me instead of showing a suspicious announcement of having no residence. ■

Image: Chris Yang

THREE MONTHS OF CLOAKED

By Michael Bazzell

In May of 2024, I posted a blog about my usage of Cloaked (https://inteltechniques.com/blog/2024/05/20/cloaked-detailed-review). It served as an introduction to the service and I added more details in my latest book Extreme Privacy 5th Edition. It has been over three months since the review and several people have asked if there is anything which needs updated. This article combines portions of my original review, updated usage from the book, and follow-up details about the techniques discussed within each.

> ***Disclosure:*** *Cloaked is the sponsor of this issue. Their sponsorship occurred after I had planned this updated article, but it would be irresponsible not to disclose the partnership. Cloaked had no input or editorial review of this piece. The opinions are my own. There are no Cloaked affiliate or referral links within this article (or entire issue). I receive no compensation if you decide to try their service.*

Several readers of my books have been asking about a newer service called Cloaked (cloaked.com). At first glance, I saw they offered some type of email masking and VoIP telephone service, and I delayed a full review toward the end of a long list of pending tasks. I finally got around to taking a deep dive, and there is much more there than I thought. There is a lot to discuss. Let's start with some basics.

On-Boarding: Creating an account is easy, and they accept a Proton Mail or Tuta email address. There seems to be no verification of identity and automated confirmation emails arrive immediately. I was issued a two-week free trial, which appears to still be offered and provides a full-functioning experience. That gave me plenty of time to play around without commitment.

Layout: The web layout is very polished and easy to navigate. Everything seems to function properly. The mobile app layout is also nicely done. I have no complaints, and everything seems professional and smooth.

Email: Nothing too exciting here. It works fine. Create an identity and get an auto-generated email address at a Cloaked domain. You can choose whether you want incoming messages to stay within the Cloaked portal or be forwarded to your registered email address. I chose to leave them within Cloaked. It seemed I could create unlimited Identities, each with their own masked email address and optional usernames and passwords. We have more masked email choices than ever, but I like that this provides an option to receive the messages right in the portal. This is more than an email forwarding service. This is true two-way email communication within the service.

VoIP: This is where things get interesting. I had assumed they were offering true two-way unlimited-use VoIP telephone numbers. This was surprising since they claim to offer unlimited numbers for a flat membership fee, and that would be an absolute steal. I soon realized this was not the case. Cloaked does offer unlimited telephone numbers, but there are major restrictions.

1. You can only call numbers which have previously called or texted you first.

2. You can only text numbers which have previously called or texted you first.

3. All voice calls are routed through your own true cellular number (if connected via the app), but masked to display your VoIP number as the caller ID.

4. If you did not connect a cell number to the app, then incoming calls go to voicemail.

That is a lot to digest. Here is how it all works. You are in need of a telephone number to provide some type of service (healthcare, shopping, streaming, etc.). You generate a new "Identity" within Cloaked and ask to have a number generated. That VoIP number is assigned to you and it can be given to the service. If the service calls that number, it will forward to you. If anyone else calls that number, it will forward to you. If you did not associate your true cellular number within the mobile app, the call goes to voicemail and you can listen to the message in your portal (web or app). If you associated your cellular number with the app, the call is received at Cloaked; forwarded to your true cellular number from their servers; presented to your mobile calling app as a random Cloaked number; and the call can be answered. If you choose to call the provider back (mobile app only), the call is routed through Cloaked servers and presented to the original caller as coming from the Cloaked number assigned to your Identity. Got all that?

This is actually not anything new. Online VoIP providers have been offering similar services for years. This is how Cloaked can afford to issue you unlimited numbers for every purpose. If needed, you could have 30 Identities for 30 services, with 30 unique numbers. Again, this presents a serious limitation. You cannot call any receiving number from a Cloaked number until that receiving number calls you. Same for SMS text. If you want to call a restaurant to confirm a reservation, but they have never called you, you cannot do that. Traditional VoIP providers allow this, but you pay a premium monthly fee for every number you possess, plus the minutes you use.

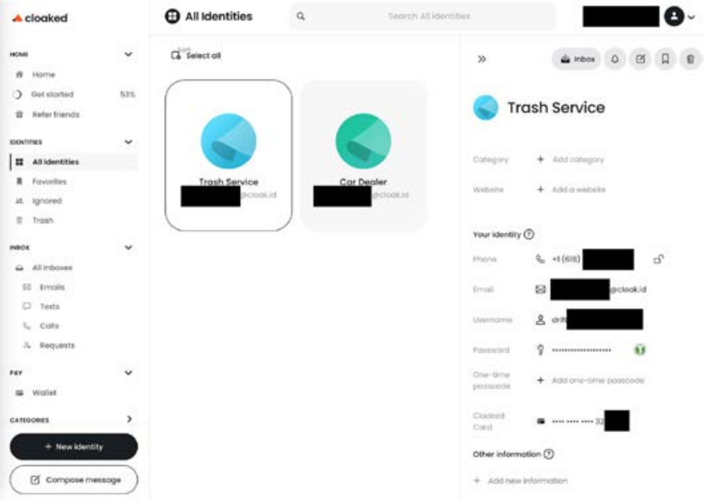
If you receive no calls or text messages into a number issued by Cloaked within 60 days, they reclaim that number and recycle it to another user. This is concerning, but they have an option to "Lock" the number for permanent use. Once you do this, no other incoming calls or messages can be received, but any numbers which have connected to you are locked in.

If you give your doctor's office a Cloaked number, they call it and you are now connected to them. If you lock the number, then that office (from the number which has already called you) will forever be forwarded to your account without expiration. However, if they call from a different number, it will not go through. I worry about "collisions" with this method, but I may just need more time to digest it. If I lock a number which has received a call from my doctor, and that number is re-issued to another Cloaked user for all other purposes, and he has the same doctor as me, would I receive the call intended for him? I do not have the answer, but I am working on some tests.

Personally, I do not connect my true cellular number to my account. I never use that number for any purpose. Also, if you forward calls and text messages through your true number, even though you are masking that number from anyone on the other end, you are creating a lot of metadata with your cellular provider. All of those calls are now documented by your ISP, but they would all show you were calling Cloaked servers. All of your voice calls use your own cellular minutes on your cellular network. I prefer to simply receive a voicemail which I can listen to through the web or app. I can also send and receive SMS messages directly through web or app once I am connected to another number. I like that all of my Cloaked communications just stay within the app.

Pricing: During your trial, you will likely receive an offer to upgrade to the full version at a discounted rate ($4x annually). If you plan to upgrade, take this offer. Once my trial was over, I could only renew at the upgrade rate ($5x-$6x annually). Their website lists $96 as the full-price annual rate. If you will be using this as a way to connect to services under your true name, I see no reason to hide your identity. I used my AMEX to make the purchase.

Documentation: Cloaked offers plenty of fields to name your identities and provide data such as the company, website, password, notes, etc. I do not use much of this, but it is well done. The following is a screen capture for desktop.



Trash Service

[redacted]@cloak.id

Car Dealer

[redacted]@cloak.id

Trash Service

Category + Add category

Website + Add a website

Your identity

Phone +1 (618) [redacted]

Email [redacted]@cloak.id

Username dri[redacted]

Password ••••••••••••••••••

One-time passcode + Add one-time passcode

Cloaked Card •••• •••• •••• 32[redacted]

Other information

+ Add new information

Wallet: This was the most interesting part for me. I rely heavily on Privacy.com and want a redundant option for masked payments. I requested to join the Cloaked beta program for masked payments and was accepted. I had to provide my true name, DOB, and SSN for financial verification. This will upset some, but should be no surprise. US laws require financial institutions to verify their customers. I was excited that I was confirmed on the first try.

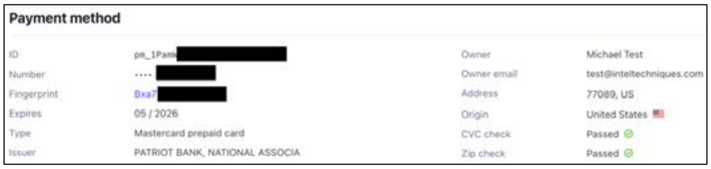
From there, you must connect a source of payment. You can connect a bank account, debit card, or credit card. I chose my business AMEX credit card and it connected through a third-party processor called Stripe. I have no objection to any of that association. There is no such thing as a completely anonymous US financial account. I could then generate new cards and select the available dollar amount and limits (day/week/month/one-time/fixed).

Cloaked placed an authorization on my credit card for the amount I approved on the card. This issued me a MasterCard for use online. I tested this by making a payment for my trash service. Everything worked as expected, and very similar to Privacy.com. My AMEX showed a charge from Cloaked, but not the merchant. The merchant saw my alias and Cloaked card number, but not my AMEX. Unlike Privacy.com, I did not have to associate any bank account or provide account credentials for verification. Stripe made the connection to my credit card with minimal details. I never had to disclose any account passwords.

I saw no fees from this transaction, but we should not expect that to last forever. During my testing, the Wallet service was in beta and did not appear to include any usage fees. I talked with the CEO of Cloaked, and he stated that the program will eventually be part of a tier which requires a low monthly fee. By the time this article is published, you may see this program out of beta with monthly dues. Be sure to check the current pricing structure before creating too many cards.

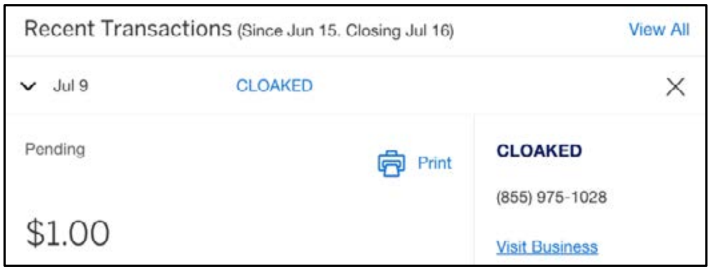
I decided to test this further. From my computer, I created a $1.00 payment link through my company's Stripe account. I then navigated to that page from my mobile device and completed the purchase with a Cloaked card. I used a random name and zip code, and returned to my Stripe dashboard to see exactly what a merchant would see about the purchase. I was pleasantly surprised with the results. The random name and zip code passed validation from Cloaked, which would assure the merchant that the card was verified to the user. I could also see that Cloaked was using Patriot Bank and my credit card statement displayed Cloaked as the merchant.

I am now confident in the ability for this service to protect my privacy. My bank and credit card only see that I made a purchase through Cloaked. They do not see where I actually spent the money. I can use any name and location desired for the cardholder. When these card numbers are breached through the vendors, they cannot be used elsewhere. The following images display the purchase through my Stripe portal and on my credit card statement.



Payment method

ID	pm_1Pa[redacted]	Owner	Michael Test
Number	•••• [redacted]	Owner email	test@inteltechniques.com
Fingerprint	Bxa7[redacted]	Address	77089, US
Expires	05 / 2026	Origin	United States 🇺🇸
Type	Mastercard prepaid card	CVC check	Passed ✓
Issuer	PATRIOT BANK, NATIONAL ASSOCIA	Zip check	Passed ✓



Recent Transactions (Since Jun 15. Closing Jul 16)

Jul 9 CLOAKED

Pending

$1.00

CLOAKED

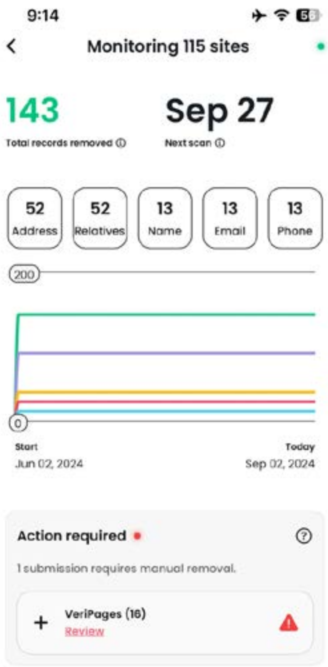
(855) 975-1028

Data Removal: Readers of my books know that I never recommend paying for online data removal, but I have no objection to the service if it is included for free with your plan. Cloaked now offers a data removal program within the main portal. You provide a telephone number which is already exposed and associated with your name, and they seem to use an API to confirm your identity.

I wanted to test this, but I am not a fair test. I have already removed any sensitive data about me and my home is not associated with my name at all. Therefore, I asked a client if she would like to try the service. She agreed.

First, I identified a cellular number which she had used publicly for a long time. I knew it was already exposed on several websites, so there was no harm in providing it to Cloaked. Cloaked immediately displayed her name and city as determined by their lookup service. I confirmed the accuracy and let the app get to work.

Over the next several days, the app displayed results of the types of data being removed, as seen in the following image.



9:14

Monitoring 115 sites

143 Total records removed

Sep 27 Next scan

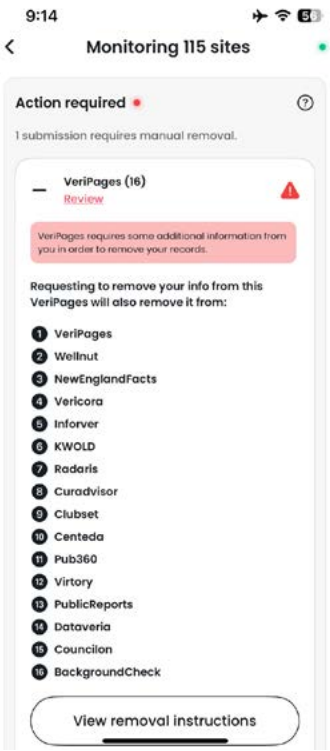
52 Address | 52 Relatives | 13 Name | 13 Email | 13 Phone

Action required

1 submission requires manual removal.

VeriPages (16)
Review

This is where several data removal services can be misleading. They like to show you the successes but do not disclose the failures. I was happy to see that Cloaked is addressing this. At the bottom of the previous message, you can see an alert about action being required. Clicking that section presented the following image.



9:14

Monitoring 115 sites

Action required

1 submission requires manual removal.

VeriPages (16)
Review

VeriPages requires some additional information from you in order to remove your records.

Requesting to remove your info from this VeriPages will also remove it from:

1. VeriPages
2. Wellnut
3. NewEnglandFacts
4. Vericora
5. Inforver
6. KWOLD
7. Radaris
8. Curadvisor
9. Clubset
10. Centeda
11. Pub360
12. Virtory
13. PublicReports
14. Dataveria
15. Councilon
16. BackgroundCheck

Cloaked confirmed that some of the services which display home address details about my client cannot be removed by them. Cloaked provides you instructions on how to complete the removal process through the service which refuses to remove the data based on a Cloaked automated request. Cloaked also tells you which third-party services will remove their data once you delete it from the parent service. This is a nice touch.

I want to state very clearly that no online data removal service will delete every piece of your information from the internet, including Cloaked. I look at this feature as a good way to get a head start. Allow Cloaked to do some heavy lifting, address the concerns they found which need manual action, and then scour the internet for any leftover services which need further action. Consider my free workbook to help you find the areas which are still exposing your details (https://inteltechniques.com/workbook.html).

Future: I had my office reach out to Cloaked about a few issues we were investigating, and the CEO confirmed they have many new features on the immediate horizon. I will not disclose them here, that is up to them. However, I believe the pricing will fluctuate upward once we start to see major new features. If you have a need for this type of service, I would join at the lowest rate you can get now, and hope to be grandfathered in.

Who is this good for? I think it is a great option if you need many phone numbers and only want to use each for a single purpose. Get them connected, lock them in, and forget about them. It may be an option for people who are unable to use traditional VoIP 2-way providers. However, it may not be a good fit for people who ONLY need a fully-functioning two-way telephone number. If you make many outgoing calls from only one number, this may not be enough for you. This is an option to mask mostly INCOMING connections, which has value.

How do I use this? This is my isolated portal for incoming connections which I do not want associated with any sensitive phone numbers or email address. I create many one-time VoIP numbers and email aliases through the Cloaked app or web interface for use with the everyday bombardments for personal information. I receive only voicemails and text messages through the service with no forwarding whatsoever. It is perfect for loyalty cards, hotels, airlines, restaurants, etc. It provides a truly compartmentalized environment which does not escape into my personal life. The masked payments for all of these things also stay within this bubble (and I still get credit card points). It feels like a true "burner" style of phone number usage and I can throw them away when I am done. I am not committing to a set of specific phone numbers which I must pay extra for as long as I have them. I now find that my pre-existing two-way VoIP numbers represent my "clean" identities while Cloaked can take care of all the junk which has less priority. Cloaked does the dirty work for me.

I have seen reports from users that creating hundreds of phone numbers will get your account locked, which I respect. Don't abuse the service. I currently possess 32 numbers and everything just works. I will lock in numbers in order to prevent them from disappearing when appropriate. I will continue to test the payment options.

Overall, I like this service for what it is. It is a great incoming communication portal with masked payment option. I will still maintain other VoIP solutions for true two-way unlimited usage, but redundancy is vital. I believe we will see continuous changing and evolving from Cloaked. Once new features arise, I will update this review here. ■

cloaked

Find, remove and disguise your personal data today

Enjoy the internet—safely. Cloaked protects personal information from public, private, and shady organizations.

Get started with Cloaked:

Call Toll Free

☎ +1 (855) 75-CLOAK

1. See if your data is compromised

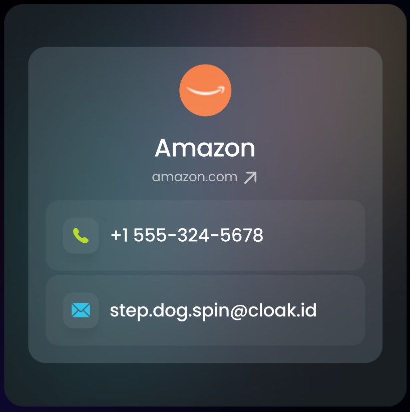
Fri Jun 24, 2024

107 records removed

- 🟩 15 full name
- 🟪 26 email addresses
- 🟨 51 addresses
- 🟥 12 phone numbers
- 🟦 0 relatives

Today
Oct 24, 2024

2. Remove your sensitive data


Amazon

amazon.com ↗

☎ +1 555-324-5678

✉ step.dog.spin@cloak.id

3. Create new aliases in place of your data

Discover more at **Cloaked.com/Bazzell**

For 20% off at checkout use code: **Bazzell**

Available on

App Store Play Store Extension Desktop

Cloaked's security and encryption protocols have been independently audited and verified.

DIGGING IN TO THE NATIONAL PUBLIC DATA LEAK

By bradm

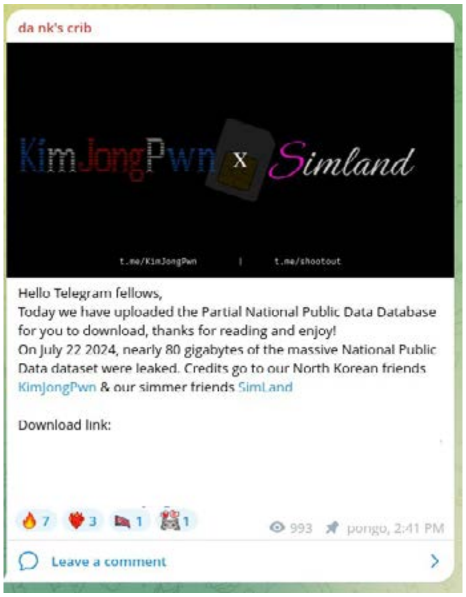
I've had some time to go through the monster National Public Data leak. The leak of the NationalPublicData database is definitely the most significant release of confidential sensitive personal information to have happened in the United States. The conditions that appeared to create this leak have been simmering for years, as similarly large SSN database have been trading among the private investigations and public data communities for decades, at a fraction of the $3.5mn that was sought for the NationalPublicData database.

A history of the NationalPublicData breach

For background, in early 2024, the threat actor 'USDoD' announced on BreachForums that he was selling a complete copy of the National Public Data database, allegedly containing 2.9 billion records. USDoD released two teaser files to drum up interest in this leak– one file contained records later leaked in the 2.6bn SSN database posted in August, the other contained records consisted with the separate "people_data" files later released on the 'da nk's crib' Telegram channel. This breach reportedly came from a Florida-based vendor operating the websites NationalPublicData.com and RecordsChecknet, which offered API access to public records including various credit header databases. In August 2024, a user named Fenice, working with USDoD, leaked 2,695,681,506 records in two files: ssn.txt and ssn2.txt. The fields for this database included twenty columns with the following header: ID, firstname, lastname, middlename, name_stuff, dob, address, city, county_name, st, zip, phone1, aka1fullname, aka2fullname, aka3fullname, StartDat, alt1DOB, alt2DOB, alt3DOB, ssn.

Early on, there were signs that this massive database was going to be publicly leaked. On June 1, 2024, a threat intelligence researcher using the Twitter handle 'vxunderground' was given a sample of the database, apparently from the SSN portion. [^1] On Telegram, numerous actors appeared to have the database, with teaser leaks accelerating in July and August 2024.

Before these records were released by Fenice, users on the "deanonymize" telegram channel posted a screenshot showing that they were uploading the National Public Data breach to their private database search project. On July 22nd, telegram user 'pongo' posted a partial archive of the NationalPublicData database on the telegram channel "Da NK's Crib:"

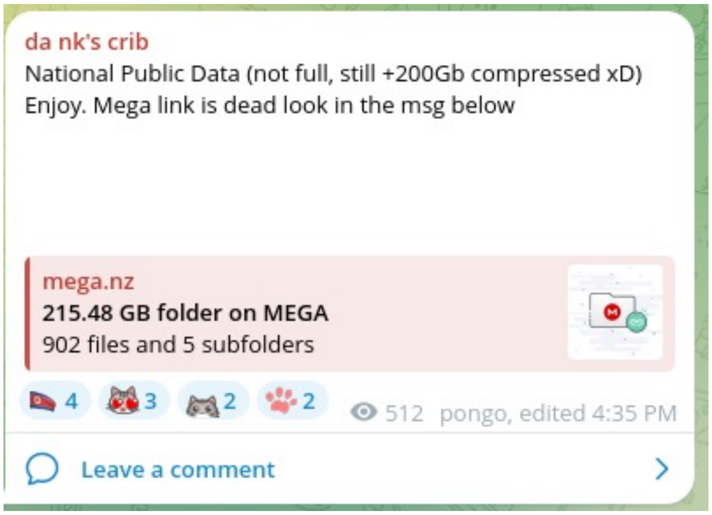


Hello Telegram fellows,
Today we have uploaded the Partial National Public Data Database for you to download, thanks for reading and enjoy!
On July 22 2024, nearly 80 gigabytes of the massive National Public Data dataset were leaked. Credits go to our North Korean friends KimJongPwn & our simmer friends SimLand

Download link:

Uncompressing this archive, the Partial_National_Public_Data.zip contained multiple csv files with twenty-seven columns. The most interesting of these files, which began "people_data" did not contain AKA names or variant DOBs, but did contain "first seen" and "last seen" records common in credit header databases. The roughly 300mn records in these release contained names, DOBs, SSNs, address information, phones and emails.

On August 1st, pongo would release the ssn.txt and ssn2.txt files on the Telegram channel 'da nk's crib' before announcing his retirement later that day. By August 4th, the mega.nz folder on the Telegram channel would be reported and the data would no longer be accessible.



da nk's crib

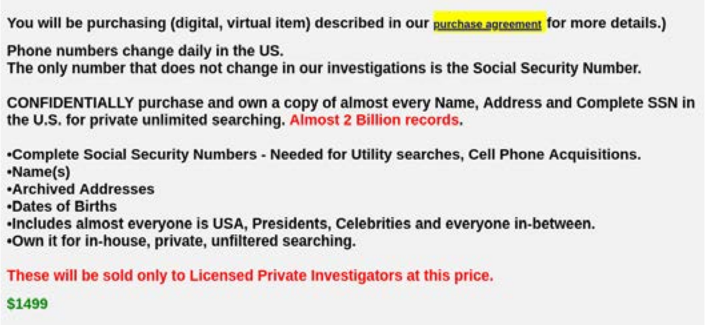
National Public Data (not full, still +200Gb compressed xD)
Enjoy. Mega link is dead look in the msg below

mega.nz
215.48 GB folder on MEGA
902 files and 5 subfolders

On August 6th, BreachForums user Fenice released the database for free, using two download links on the usdod.io server operated by the threat actor USDoD.

The leak of this kind of data was inevitable

While the leak apparently stems from the theft of records rather than the purchase of large SSN databases, the fact that pre-GLBA data has been circulating in large files was likely the reason that NationalPublicData had this dataset to begin with. The National Public Data file appears to be consist of credit header records from before the passage of the Gramm-Leach-Bliley Act (GLBA) in 1999. A similar database containing 1.9bn records was widely sold to private investigators in the early 2000s, at a price as low as $1500. I purchased a copy years ago, and the similarity in data between the two databases is undeniable. The pre-GLBA database is titled TUCS, a likely initialism for Trans Union Credit Systems, though the specific provenance of the data was not explained by sellers. The ad below is from a 2014 website offering the data for sale:



You will be purchasing (digital, virtual item) described in our purchase agreement for more details.)

Phone numbers change daily in the US.
The only number that does not change in our investigations is the Social Security Number.

CONFIDENTIALLY purchase and own a copy of almost every Name, Address and Complete SSN in the U.S. for private unlimited searching. Almost 2 Billion records.

•Complete Social Security Numbers - Needed for Utility searches, Cell Phone Acquisitions.
•Name(s)
•Archived Addresses
•Dates of Births
•Includes almost everyone is USA, Presidents, Celebrities and everyone in-between.
•Own it for in-house, private, unfiltered searching.

These will be sold only to Licensed Private Investigators at this price.

$1499

The TUCS database contains a very similar layout. The fields include three sets of AKA names, an incrementing numerical ID (similar to the NationalPublicData file), SSN, DOB, phone, a field indicating when the record was created, and fields associated with names and home addresses. Much of the data appears to be very similar, though the NationalPublicData file has more records than the TUCS database.

While the NationalPublicData database is distinct from the TUCS database that was previously circulating, I believe the NPD is mostly "aged header" from before the enactment of the GLBA. For the uninitiated, prior to the passage of the GLBA, credit ratings agencies could license their data to any buyer. This included "credit header" data– the top portion of the credit report which shows the address history, name, DOB, and SSN of the consumer. Beginning July 1, 2001, the GLBA placed credit header data into the category of "non public personal information" and required a permissible use to access this data. Until the introduction of bank header in recent years, credit header was the most comprehensive set of address history available to investigators. Credit header is still the foundational data used to produce the comprehensive reports used by commercial data vendors like TLO, CLEAR, and Accurint.

I've spot checked a bunch of records and searched a handful of younger individuals– people born after 1990 who would not have had their credit header data exposed after the passage of the GLBA. While I have just begun this process, I do not believe the 2.6bn record database released in August 2024 contains many, if any, individuals from before the GLBA took affect. This strongly suggests that the file is largely comprised of pre-GLBA data (and possibly entirely comprised of pre-GLBA data). If true, individuals not of credit age by the year 2001 should be less concerned that their data could have been compromised in the NationalPublicData leak.

Numerous other files from a larger dataset, allegedly belonging to NationalPublicData, were leaked before this latest SSN leak. These files were CSVs (rather than the two .txt files leaked by Fenice) and began with "people-data" before containing serialized ranges of their unique IDs. These files also contained emails and cell phone data for the individuals present. Notably, these files had individuals who were younger than those in the ssn.txt and ssn2.txt files leaked by Fenice.

[^1]: https://x.com/vxunderground/status/1797047998481854512 ■

(BY)PASS THE AUX!

By: up

My first vehicle had an AM/FM radio with a cassette deck which later could be used to play CD's with the now iconic 3.5mm to Cassette adapter. Of course connected to a portable CD player sliding around the passenger seat. The sound was terrible and any bump in the road caused a skip, but I was able to escape the limitations of the audio head unit to play from an external source.

Next vehicles began to incorporate a 3.5mm jack standard so the passengers could easily play any device that could get a signal into this port, commonly known as the AUX (short for Auxiliary Input). I'm sure everyone reading this has "Passed the AUX" cable to someone in their car because they didn't care for your music choices.

I recently purchased a new vehicle, and honestly the entertainment system was not one of the determining factors of my purchase. They all look the same to me from afar. Yes some have different features and interfaces, but the large screen in the center of the dash is now ubiquitous across the automotive space. This is not something I need or even wanted, but they are present in all new vehicles, generally speaking.

Once I took possession of my new vehicle I took a moment to look at settings and features of the audio head unit and the admittedly very nice touch screen. I could see several audio source options (USB 1, USB 2, Bluetooth, SiriusXM, AM, FM). The one thing I did not see was AUX. I looked around and even inside the glove box, no AUX. I got a flashlight and crawled on my back looking behind the dash for a possible connection port on the back of the audio head unit that could be used for additional inputs, no AUX. I figured maybe I couldn't see the back clearly, so using an old trick I looked for my model of head unit on eBay. I found a head unit for sale that had been removed (I'm sure legally) from a vehicle similar to mine with a very clear image of the back. Still no AUX visible. Hmmm...

I spent a lot of time and money purchasing this vehicle as privately as I could. The last thing I wanted to do was directly connect my phone to the USB ports or via Bluetooth. This would create a record of my phone being linked to my vehicle. Possibly even unintentionally sharing contacts stored on my device. Possibly some other sensitive information shared by mistake or not recognizing what a vaguely worded permission setting truly means. Maybe I should just pay for a SiriusXM subscription once the complementary new car trial period ends. Maybe I should live a simple life and only listen to AM radio. Maybe I should just... connect my phone.

Everyday these USB ports, which would so easily solve my problem, stared at me. They are the physical manifestation of everything I despise about modern data collection efforts. These companies aren't happy with my money anymore, they want to know about me. They want to build a profile about me. They want ME to provide the data plan they use to send data about ME back to them. All so they can attempt to sell me more stuff and simultaneously sell MY information to other businesses. I decline.

But how? How can I beat this? Let's discuss what I have to work with.

My phone: Google Pixel 6a with GrapheneOS installed - USB-C Female (output)

My Vehicle: USB-C Female & USB-A Female (inputs)

I purchased a 3.5mm Male to USB-C Male cable. I also had a FiiO USB-C Male to 3.5mm Female DAC (Digital to Analog Converter) laying around.

Plan #1: Connect in series - Phone > DAC > 3.5mm Male to USB-C Male cable > Vehicle

I felt this was a great option. Using this pathway, in theory, the only data that would make it from my phone to the vehicle would be the audio that is output from the phone. Data wouldn't have a way to be transmitted over a 3.5mm port. I smugly connected everything and plugged it into the USB-C port on the Vehicle. "USB Device not recognized". Hmmm...

Plan #1 failed. After researching it turns out that modern head units need to 'play' the digital audio files on the head unit. This is not how a DAC would output an audio signal as it's a Digital to Analog Converter. If you would like a better explanation of this concept related to modern cars, please read this article.

https://www.lifewire.com/usb-to-aux-cable-in-car-audio-3986249

Plan #2: I purchased an FM transmitter that I could connect my phone to via Bluetooth, then using my head unit's FM tuner listen to the broadcast from my phone by way of the FM transmitter. The sound was as expected terrible. Plan #2 was also a failure. It works but I rather listen to music on my phone's speaker instead.

Plan #3: At this point I still do not want to give in and connect my phone to the vehicle directly by USB or Bluetooth just to play music. But since the head unit can play digital audio files, perhaps I can load these on a digital storage device and play them directly (as noted in article above)?

The answer here is YES, this can be done but with limitations. I can play .mp3 & .flac but I can't load Terabytes of music on a hard-drive and plug that in. I am limited to 8,000 files. There are some additional limitations with folder structures & file systems. So yes, this would play audio but with a limited experience. I could have multiple USB drives for different genres of music, but the truth is I don't want to play a personal collection of music. I do respect those with the patience to curate a collection of audio, video or other media. What I want is a way to stream music. I don't always want to be so intentional with what I listen to. The beauty of the internet to me is being exposed to things I would never have experienced otherwise. Streaming services offer this, to an extent.

So, how can I stream music without using my phone?

We can fight, hack and resist all we want. Ultimately the easier thing to do in many cases is simply give them what they want. In this case they want access to my phone because they assume I will use the same phone that I use for my daily activities, which is full of data that could be collected. Wrong! I'm the type of person who will buy a new phone specifically for the purpose of creating a streaming audio device that can connect to this dumb USB port and block any nonsense the car wants to send back to the mothership.

Plan #4: Rather than using GrapheneOS as I do on my personal phone loaded with secure communications apps, I will use it for a secure digital media streaming device that works fully with my cars head unit. Let's get started.

If you haven't yet, I recommend picking up IntelTechniques' Mobile Devices PDF. I wasn't asked to promote that here. I genuinely think it's a great guide. I'm borrowing heavily upon the concepts in that guide, so it makes sense to reference it. The fundamental setup is the same. If you want to replicate my setup very closely, use that guide from chapters 1-6, then skip to chapters 11-13. We don't need any secure communications or data service on this device.

I purchased a Google Pixel 6, because it was very cheap and for my needs the audio output will be no different than a more expensive model. If this phone is ruined by leaving it in a hot car, stolen or lost, oh well. I will refer to this as my GOS Media Device from now on. This is not to be confused with my Google Pixel 6a which is my personal phone used for actual communications.

After initial device setup was complete I have a device with GrapheneOS, NextDNS, F-Droid & Aurora store installed, and in my case Proton VPN & VLC. One thing I have NOT installed is a SIM Card or eSIM. This device will not connect to a cellular network (directly) for data. Rather I will use my personal phone as a hotspot & supply it with data via WIFI. I see this as a minimal risk to my personal phone. Be sure your personal phone's data plan can accommodate this hotspot data usage as many plans have tethering limits.

Let's discuss why this is not perfect. My vehicle has an IMEI# (no service activated however), My personal phone has an IMEI#, My GOS Media Device has an IMEI#. In theory each of these devices could be discovered to be traveling alongside each other constantly pinging towers. While I don't like that, this is well beyond my threat level. My vehicle purchase, while not perfect, is as private as I can make it. My personal phone uses only VoIP #'s & Secure comms for communication (not the true SIM #), and the GOS Media Device doesn't even have a SIM. All of this purchased with cash. It would be difficult to find a starting point to begin an attack on me with this setup. Another weak point, my personal device will be broadcasting a WIFI network everywhere I drive. Use your best judgment here for your scenario. You and I will be much more likely tracked by the never ending supply of ALPRs on the roads with much more accuracy than cell towers provide. I also realize there could be some contradictory points with the rest of my setup. I have made what I feel is be 'Lesser of the Evils' decision at each fork in the road. It can be convoluted and contradictory using Google Play Services and apps which are notorious for abusing our data. Trust me, I get it. The common thread regarding privacy in all aspects is compartmentalization. In each realm we create a secure box to put things inside of. In this case we have a segmented phone which will store 'dirty' apps. Let's move on.

I recommend at this point downloading a media file you can store on your device. I found an .mp3 file and stored that in my Downloads folder. Since I will not have any internet access initially I want to determine which setting will allow me to play audio with this device first. I performed my initial setup on my home router which is well protect with a VPN, but you could do this part on public WIFI as well.

The next step was visit my NextDNS portal. I then navigated to SECURITY > BLOCK TOP-LEVEL DOMAINS (TLDs) > ADD A TLD > Select all likely options (.com/.net/.org/.edu/.us etc).

The logic here is I don't have any clue what is going to attempt to reach out once I give this head unit a way to connect with the internet. If I block ALL TLDs then no traffic can escape to the mothership. This will be reversed later, but for now I can 'catch' anything trying to reach out.

The time has arrived. I connected the GOS Media Device to the USB port of my vehicle and once again "USB Device not recognized". As I began to throw this phone in the trash, I remembered seeing ANDROID AUTO in the list of apps in the native APPS menu within GrapheneOS. After some research I decided to move forward with installing Android Auto on my new GOS Media Device. Keep in mind, using this option DOES require installing Google Play Services on the device. This may be a stopping point for many, but I recommend you research what is really at risk by enabling this option. Personally, I was willing to move forward. I won't list each setting but I will leave you with this advice.

1) Turn EVERYTHING OFF & work towards functionality.

At the system level for Android Auto, I have at this point only enable Nearby Devices & Notifications. Network permission is NOT needed at any time, leave it DISABLED. Within the Android Auto app itself, I have disable everything with the exception of

START ANDROID AUTO WHILE LOCKED

2) Enable Developer Mode for Android Auto

Within the Android Auto App - Settings > Apps > See All Apps > Android Auto > Additional settings in the app > Scroll to bottom & Tap Version 10x > Scroll to top and tap 3 dots top right > Developer Settings > Tick UNKNOWN SOURCES & Un-Tick all other options

This feature will allow open source apps from F-Droid to appear on your vehicles screen. Once again I connect the GOS Media Device to the USB port on my vehicle.

Success! The GOS Media Device will now connect to the head unit and our test.mp3 file will play using an app like VLC. Next I checked the DNS logs on NextDNS via web-browser. To my surprise there were no vehicle manufacture specific queries being made. I was very surprised by this so I waited. There were several attempts by Google to communicate but given Google Play Service and Android Auto, I was not surprised. After blocking a few items I wanted to prevent I then UNBLOCKED ALL TLDs previously mentioned in NextDNS. This would restore internet connectivity to the GOS Media Device for the next step.

It's now time for streaming apps. Via F-Droid I installed Antenna Pod, New Pipe, Harmony Music, Spotube, Transistor and the previously mentioned VLC. Via Aurora Store I installed iHeartRadio, Pandora, SoundCloud, & Spotify. I also have the native Vanadium web browser as well should I wish to visit more unique services online.

Using this mixture of audio sources, I can access most of the music, podcast and other audio files I have interest in. For the most part these also display on the vehicle's touch screen allowing me controls while driving. Of the apps listed Pandora provides the closest experience to what I envisioned from the beginning. In Pandora, I can create a 'Station' which includes 6 artist. I use this to narrow in on specific genres of music. Let's say I want a 60's Classic Rock experience. Choosing The Beatles, Rolling Stones, Led Zeppelin, The Doors, Pink Floyd & The Who will then force the Pandora algorithm to play those artist and 'suggest' related music from this genre. According to this forum post, a free account can generate up to 250 Stations, the same as a paid account.

https://community.pandora.com/t5/My-Collection/Station-limit/td-p/8984

I would like to give a recommendation for Harmony Music as well. This is an app available on F-Droid and based on the version history appears relatively new at the time of this writing (First release July 2023). This app sources music from YouTube and the user experience is fantastic! The interface is very clean and minimal but displays album art and plays music as well as any mainstream service. Streaming music here is much better than via NewPipe and light years ahead of the native YouTube app which is so bogged down with pop ups it's unusable. Keep in mind I am speaking from an AUDIO experience, not video.

This gives me all the variety I need without being so intentional when I press the play button. One unexpected behavior of using NextDNS is ads are automatically blocked at the DNS level. While playing on screen a grayed out advertisement box will pop up, and immediately disappear skipping to the next song in the queue. I tried to find a solution to get those long drawn out ads back, but was unsuccessful. I suppose I will have to live with this unintended behavior for now.

The last recommendation I have is to generate 'burner' accounts for each of the streaming apps which require a log in as opposed to using an old account you may have for one of these services. Don't do all of this work and connect it to an old profile. I would recommend making these accounts directly from the app on the GOS Media Device. I've found making them in a browser first leads to the account being locked more frequently. If using the app to create the account, being on VPN and using email masking services seem to work with no issues.

Since I had this device setup for Audio, I also installed some Video streaming apps such as Netflix and Tubi. While my primary use is to stream audio in my vehicle, it's reasonable to use this for watching movies on the go or at hotels. The Pixel is not the best device for this given output limitations via USB but perhaps there will be another write up in the future if there is interest. Don't allow technology to compromise your privacy, but also don't let privacy limit your enjoyment of technology. ■

Image: Daniel Thomas

NAVIGATING GOVERNMENT
BACKED LOANS, HOME OWNERSHIP, AND TRUSTS

By Toj91

Using a government backed loan such as an FHA or a VA loan to purchase your new anonymous home and achieve your privacy goals may seem counter-intuitive to living a privacy-oriented life. During our early to mid-career years, unless you've been living a frugal lifestyle and stuffing away mass quantities of cash, it's not always feasible for us to put down a sizable down payment for a conventional loan. Not to mention closing costs, attorney fees, and the inevitable home repairs. If you're moving, your time to house hunt will be rushed and you'll have very limited time to get your affairs in order while still working your day job. In late 2021 to early 2022, the seller's market did not work in everyone's favor especially if you put in multiple offers, which were sometimes thousands of dollars over the asking price. Not to mention that the highly scrutinizing appraisals that were a complete turnoff to many sellers when considering accepting your offer (or at the advice of their real estate agents).

The good news is you absolutely can close on your home in a trust while using an FHA or VA loan. My number one disclaimer here is that this will not be an easy process and you will definitely have to make some extreme privacy compromises along the way in order to make the stars align for closing. If you're still following along hopefully my experience and lessons learned will make your experience a little less stressful and a lot more encouraging.

Start Planning Immediately:

I'm sure many know the drill on getting your dedicated VOIP number and e-mail established.

Have your PMB for the trust set up and ready to go. Keep in mind the USPS 1583 form mandated for opening a PMB only allows one business name per box. Setting this up immediately will help prevent any trust mail/correspondence from being kicked back or sent to your new home later.

Your passport card is likely going to be your best choice when your lender demands a copy of your photo ID. As a backup if demanded, if your state allows it, get your PMB on your drivers license.

It will be your decision to create your new trust on your own or with the help on an attorney is up to you, but keep in mind that many government backed loans will require you to work with an attorney if closing in a trust. You'll need your trust to open your trust checking account, which will be used for all expenses directly related to your home. If I could do it over again, I would include minimal additional trustees and beneficiaries and as little PII as possible. The bank where you establish your checking account may accept a certificate of trust only, but I can almost guarantee your future lender will demand a full unredacted copy of your trust document. Once established, ask your bank to issue a debit card in the name of the trust without your name. This can be good for emergency home related purchases if you have insufficient cash on hand.

Being more privacy minded than I was a few years ago has taught me to do more thorough research and read the fine print. I'm not perfect and I have rushed things. However, when it comes to picking your real estate agent, lender, and title company, ask all the up front questions Michael suggests. Verify their responses by requesting any supporting documentation from each entity regarding FHA or VA loans and trusts or by researching any available information on the website. If their answers don't meet your standards, there is nothing wrong with looking at other options.

It may not hurt to ask what guarantees you have that your loan underwriter will allow you to close in a trust so long as certain conditions are met. Generally, a higher credit score will increase the likelihood. Unfortunately, as I'll mention later, you will never see nor hear from the loan underwriters and you'll have to deal with the loan coordinator(s) directly. Getting an honest answer that they'll 100% allow you to close in a trust is not guaranteed. Ask a lot of questions in advance, get several opinions, and document the responses you get so you can make the best informed decision on which lender to go with.

Whenever you set up any account (financial, insurance, utilities, etc) during the process, always remember to opt out of the sale of personal information. Although it's never bullet proof, this should still be muscle memory to minimize exposure later.

Keep the Privacy Topic on a "Need to Know" Basis

Personally, I lucked out when I found my realtor. They were very helpful and patient the whole time and even respected my privacy wishes. Your mileage may vary. Disclose details that you feel comfortable with and deem necessary.

I was open with my attorney about my goals of keeping my name off public record to the maximum extent as your attorney will be a major lifeline during the home buying process.

Your lender should know that you intend to close in a trust for "estate planning purposes." Statements like "I'm trying to stay off public record" or "I'm a highly targeted individual" will probably open your file up to more scrutiny no matter what you do for a living. Overall, to be fair, the lender wants to make sure you aren't going to default on your loan. However, the very well hidden team of underwriters and attorneys won't show you any more mercy than the other highly targeted individual that attempting to close in a trust.

I would be open, honest, and patient with your partner, spouse, etc. especially if they are a cosigner. The reality is privacy is a lifestyle change and only you can find the best way to compartmentalize it with your family relationships and communicate "how this all works" to minimize exposure during and after the process.

Plan For the Unexpected and Expect Resistance

During the home buying process I ran into several unexpected road blocks. I share these because there is a good possibility that one or more of these will happen especially when using an FHA or VA loan.

I sent in my certificate of trust to the lender. My loan coordinator called and said the underwriter needs the full trust document. I resisted and heard nothing back. Later on closer to closing they continued to push for the full trust document. Yes, this is a privacy invasion. However, this is why I'd recommend again to keep your trustees and beneficiaries to a minimum on your base trust document initially and file a local amendment after closing. Once my attorney created the first amendment to the trust, the attorney stamped it as "confidential" and added a disclaimer that it is not to be disclosed to any third parties without consent of the borrower. Is this a bullet proof solution to preventing leakage? Nope. Sometimes we have to compromise and this is the middle ground we came up with.

The lender also required my attorney provide an opinion letter to ensure the trust was legally binding and not fictitious. I would ask the lender well in advance if they require this as some lenders openly make this a requirement while others may not mention it until an underwriter suddenly demands one.

Your realtor will have you sign a lot of paperwork along the way, usually through Docusign or another platform. Keep in mind that although you are the borrower for the loan, the buyer is actually the trust. Within about a week of closing we identified this issue as I was signing all documents as if I was closing using my name. Your attorney will probably need to submit an addendum with language saying that the "contract is attached to the trust" to close the gap. Raise this point sooner than later to prevent a last minute roadblock.

I was under contract initially and when the appraisal came in, the lender demanded that the seller fix certain items. The seller refused and I had to back out of that first contract and reset. I say this because it could be hard to gauge when to pull the trigger on your homeowners insurance, utilities, and internet. Passing the appraisal stage is more than likely a green light that you will eventually close. However, depending on when it's finalized, this could leave a smaller window to get everything else set prior to closing. Insurance I believe deserves a separate article. If you can pull off the utilities using the trust name and prepayment, I commend your negotiation skills. If not, an EIN as sole proprietor to appease the utility company can make things easier and cleaner. Prepaid internet if available in your area is my recommendation without the need to use the EIN or your true name.

Once we found a new promising home, the seller insisted we use their title company. The seller, was a major real estate company and the title company was closely affiliated with them. I pushed back and went back to the original title company after several requests to upload my IDs. I didn't get this far to fall into that trap. Let's move on...

You may or may not be able to sign remotely and have to appear in person for closing per VA and lender requirements (so they said). The lender did not seem to care if was on official travel, I would need an immediate family member as my "attorney-in-fact" to sign on my behalf in person along with my attorney. Since this is my first experience, I couldn't say if using a different "mom and pop" lender would have allowed me to avoid appearing at closing. If you have no other choice but to appear and present ID, the passport card is probably the lesser of the evils.

The lender pushed my closing date back a week since this scenario wasn't a common thing they deal with and their underwriters continuously scrutinized my file. Several loan coordinators asked if I would agree to closing in my name and I kept a firm stance on closing in the trust. To be blunt, I was exhausted and I had to come to terms that the lender may demand closing in my true name and then transferring to the trust. My objection and backing out would put me at substantial risk of losing my $10,000 earnest money deposit. This wasn't worth it and I almost had to concede knowing the home titled in my name for one day would leave a forever recorded public facing document tying me to the home. You are the most familiar with your own financial situation so my point here is to never execute any strategy without fully comprehending the potential consequences if things go sideways.

Fortunately the lender and title company worked it out. I later learned that realtors will sometimes use the loss of earnest money scenario to keep you focused to get to closing, but I still wouldn't rule out the possibility of that happening. At closing, I learned the lender required my name to be listed on the deed as the borrower. Fortunately it was buried several pages in and not on the first page of the document . This was still not ideal for me. Again, a compromise I had to make as we were at the 11th hour and my attorney also gets paid by the hour while sitting at the settlement table.

You Closed! Maintain What You've Achieved

As I had mentioned before with privacy being a lifestyle change, the work and attention to detail to prevent exposure never really ends. Although we are outside of the home buying process now, here's a few things I considered after the fact:

Emergency services: If your life is in danger and you need the police, fire, or medics, a all to 911 from your true cell phone may be your only option unless you have a VOIP configuration that supports this. Your life and safety is much more important than a publicly recorded police report. If you see something in progress that is not extremely time sensitive, I keep my local police department non-emergency numbers in my contact list and provide them with a VOIP contact number only if follow up is needed. Unless required by law I have no need to provide my name or other identifying information.

As mentioned you may initially receive some mail in your name usually from the title company, insurance, or lender. Prevent what you can with the initial PMB setup, but keep reaching out to make sure it all goes to your PMB and go paperless.

Home repairs are inevitable as well as dreaded calls to the insurance company. I had a repair within days of moving in I needed fixed immediately but was not worth my insurance deductible. My insurance company provided me with a list of applicable repair companies. I called three. One of them blasted my phone number and I was getting spam calls almost every hour on the hour. Fortunately I did not give them my name and only my dedicated VOIP was exposed. If you have an emergency repair that requires the insurance step in I would deal with it promptly as a delay in reporting may jeopardize your coverage. If not, remember your trust account, cash, and privacy.com options to combat home service companies abusing your information.

Finally, once you get moved in (anonymously) and settle, bring yourself back down to earth and reflect on your accomplishments. My most satisfying moments are when I saw my trust appear online followed by junk mail in my attorney's name and the trust name. If you're doing this all on your own for the first time, it may not go as flawlessly as you'd like. Instead of dwelling on the exposures or the lack of respect for your privacy, remember that your small victories put you exponentially ahead in the privacy game. ■

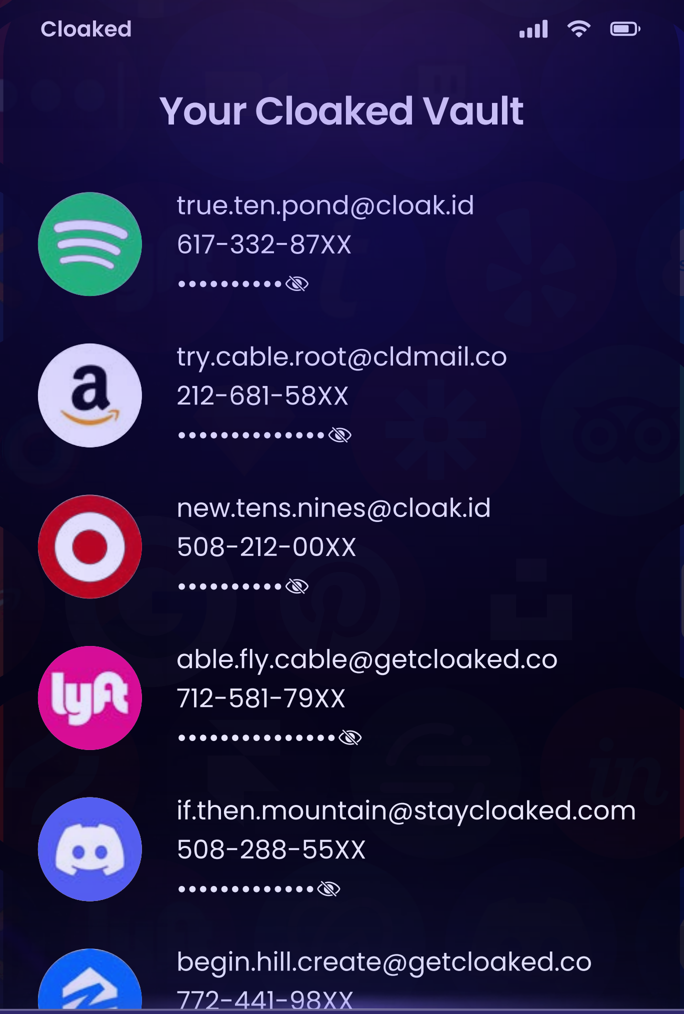


Image: Dan Dimmock

THE OSINT CORNER

By Jason Edison

Jason instructs live and online open-source intelligence courses for IntelTechniques in addition to working as a cyber-crime detective for a large U.S. police department. Each issue will feature an OSINT tactic from the IntelTechniques online training.

How do I build a career in OSINT? This is a question that I am asked often and one which always causes me to inhale deeply before answering. This is because the answer is never as simple or satisfying as the person asking would like. The truth is that so much depends on who you are, what your background is, and which industry you intend to work in. So, while there is no one-size-fits-all path to a rewarding intelligence career, I will do my best to share some insights, based on both my own career and the extensive opportunities that I have working with various intelligence teams.

OSINT is a skillset not a job. This is one of the first things I like to point out to new practitioners. While we are starting to see some defined "OSINT analyst" positions pop up here and there, it is better to think of OSINT as a tool that any analyst, investigator, or operator should have in their belt. Do not expect to focus solely on open source intelligence and leverage that into a career. We need to layer multiple disciplines and skills into our repertoire if we want to be marketable and attractive to potential employers.

You must be able to write and speak well. I can't think of a single intelligence profession that does not involve generating a work product. We are almost always providing assessments and briefings either in a written or verbal form. From initial interview and on to your first assignment, you must be able to speak and write concisely and intelligently. Communication is probably the most important yet underrated skill.

Pick a lane. As mentioned, OSINT is a great set of skills which can complement a wide variety of professions and specialties. If you are not already in an industry such as government intelligence or information security, do some research into what types of public and private sector agencies are looking for an OSINT background. Although you could certainly study OSINT in general, it would be more effective to specialize in the tools and skills that apply most directly to the industry where you plan to make your mark. For example, if pursuing an infosec career you may want to focus on gaining experience digging up threat intelligence or investigating infrastructure.

Experience: the chicken and the egg. When asked what the most difficult obstacle is in building a career in the intelligence industry, the answer is always the same: every employer only wants people with experience, so how can you get your first job to build that experience? In short, networking and controlling expectations. You will have a much better chance of earning a position which builds experience if you are willing to work for free. Not all organizations take on unpaid interns or volunteers but nothing ventured, nothing gained. Study companies and/or agencies with intelligence teams, and consider offering up your services as a volunteer. It is always a long shot, but I have known this to pay off. The key is to get a foot in the door, acquire some documentable experience, and start building a network of colleagues in the intelligence field.

Research is your superpower. Your OSINT skills are growing and yet you are having trouble finding or landing a job. This can be very frustrating, but I like to remind folks that we are all specialists at conducting research, and we should use that special skill to bolster career hunting. Use the research skills and tools from your training to dig into and monitor the companies and individuals you would like to work for and with. Looking at their job descriptions/requirements can be very helpful in planning out your training and resume goals.

You probably do not need a certification. Certifications are a bonus on any resume, but they require time and expense to earn and maintain. For most people, earning certifications is a bonus, nice to have on a resume, but not essential. This will of course vary based on industry. For example, the information security field tends to emphasize certifications heavily when evaluating candidates, and those of us in law enforcement benefit from the credibility a certification adds to our court testimony. Certifications do establish some foundational proficiency, but there is no replacement for true on the job experience.

Slow and steady wins the race. Although it may seem like your peers are moving, shaking, and making all sorts of exciting things happen, I am a firm believer in steady and reliable. I have seen so many flash-in-the-pan, loud and proud, personalities try to force their way into prominence within the intelligence community, and they tend to crash and burn before too long. When I am looking for teammates or candidates, I want someone interested, honest, and reliable. I want the person who is hungry to learn from others and willing to put the work in over the long haul. Although slow and deliberate may be frustrating in the short term, long term you will build a network of people who respect your work ethic, and eventually, you will become a sought after commodity. Reputation is everything in our business, so avoid shortcuts, and put the work in.

Editor's Note: The last section about being slow and steady resonates the most with me. If you are browsing sites such as LinkedIn, it seems like everyone there is saving the world and doing huge things. That is not the reality. Don't let a feed of self-congratulatory posts get you down or dismiss your own progress. Several years ago, I noticed Jason at all of my trainings in his area. He was quietly absorbing everything he could and taking it to his job as actionable tradecraft. He craved all things OSINT and slowly crafted his own skills. He was meticulous and took the time to do things right. Today he runs the entire IntelTechniques program. Deliberate and calculated moves are always better than trying to be the best or loudest voice on the internet. ■

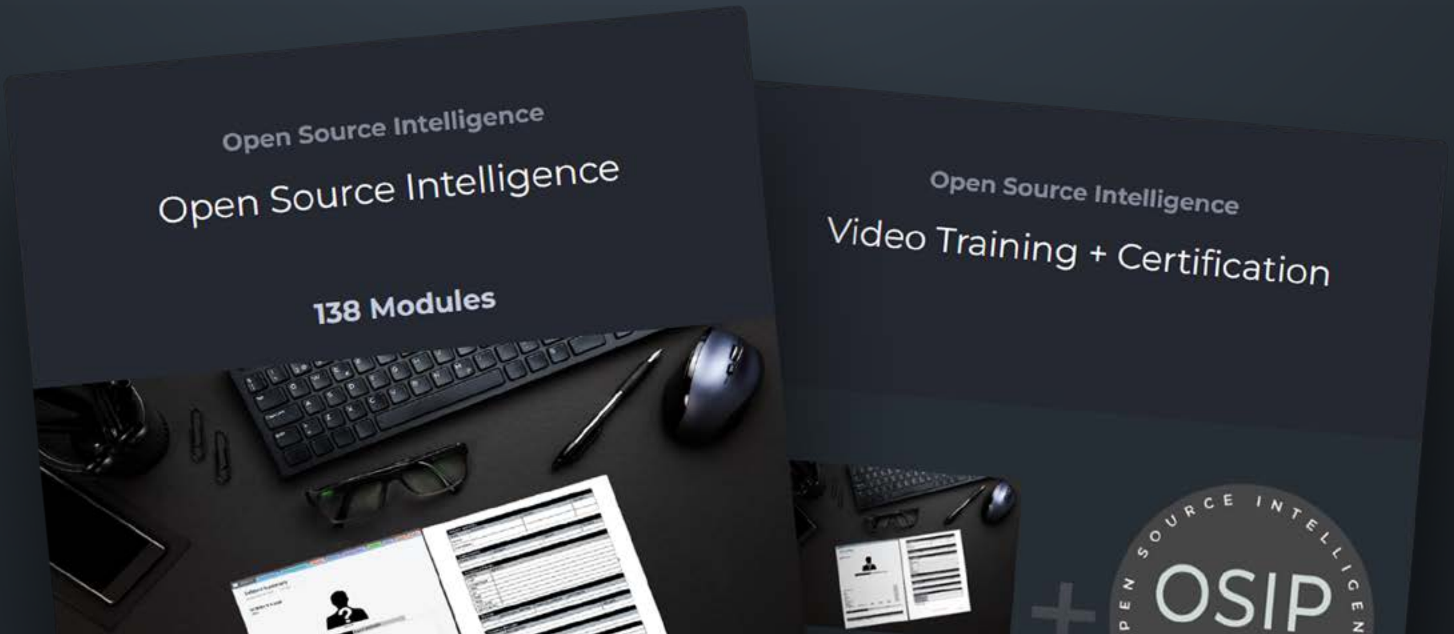


Image: GeoJango Maps

BUILDING A CRIME MAP
WITH POLICE SCANNER AUDIO

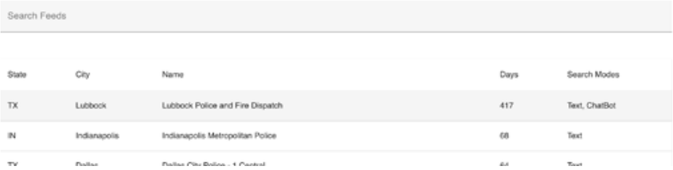
By NotJoeMartinez

In the third edition of Unredacted Magazine Michael Bazzell discussed the utility of police scanners monitoring neighborhood activity. I believe he also mentioned their utility for OSINT investigations on a podcast episode sometime around 2021. It gave me the idea at the time to start transcribing police scanner audio with one of Google Text To Speech APIs. I was trying to see if I could build a historical transcript database and cross-reference incidents with my university's campus crime logs and mug shots from the county jail. I gave up on the project because speech-to-text was too expensive in 2021.

I had enough free time this summer to finish the project, https://copcrawler.com. It's a police scanner transcript full text and semantic search engine. The audio archives are scraped from broadcastify.com, and I'm transcribing them with Whisper on a couple of old laptops. A concerning amount of police departments still share phone numbers, driver's license numbers, addresses, license plates, vehicle descriptions, crossroads, and a bunch of other uniquely identifiable information on unencrypted radio.

Because of the low quality of most radio audio feeds, the transcripts are not that accurate, but good enough to find common police phrases like "shots fired", "vehicle accident", or a well-spoken street name. The use cases for this will vary depending on what specific information you are seeking and none of this will work if the department encrypts their radio. I'm going to focus on something most of us would find useful, crime maps. You don't have to use copcrawler to do this and can use this command line tool (https://github.com/NotJoeMartinez/broadcastify-cli) to download and transcribe the audio to any broadcastify feed, but you will need a premium account and have to build out your text search solution.

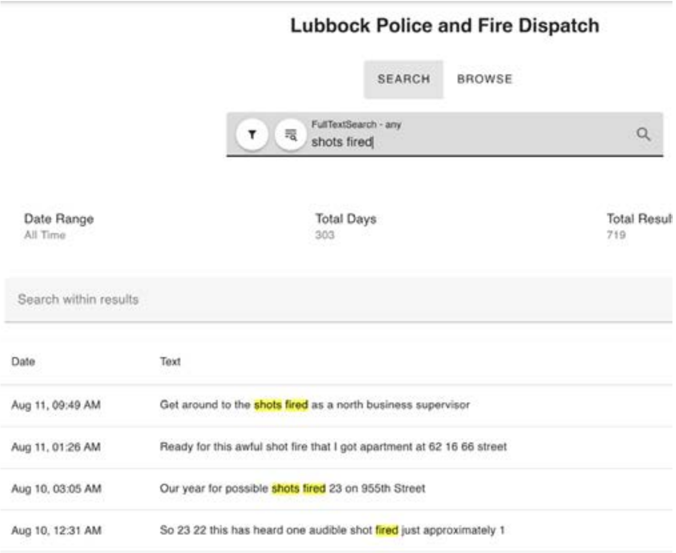
While I'm only choosing to make a crime map for demonstration purposes, I should note companies like LexisNexis offer publicly available crime maps however they tend to exclude small cities and rely on agency reporting for the dataset. One of those excluded cities is my former college town, Lubbock Texas.



Search Feeds

State	City	Name	Days	Search Modes
TX	Lubbock	Lubbock Police and Fire Dispatch	417	Text, ChatBot
IN	Indianapolis	Indianapolis Metropolitan Police	68	Text
TX	Dallas	Dallas City Police - 1 Central	44	Text

As you'll see in a bit it helps to be familiar with the street names of the area you are researching. Depending on the feed you are searching the transcripts are split up into 4-10-second segments and the recordings are usually 30 minutes. The short text segments mean keyword searches are more effective. The keywords we will map out are: "Shots Fired" and "Burglary".



Lubbock Police and Fire Dispatch

FullTextSearch - any
shots fired

Date Range
All Time

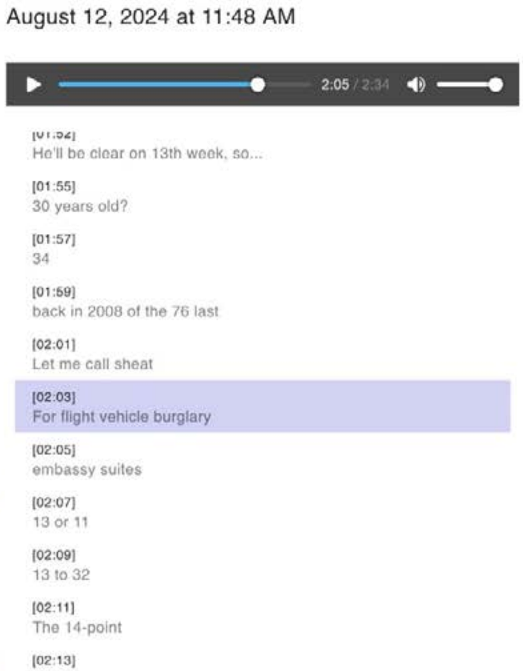
Total Days
303

Total Resul
719

Search within results

Date	Text
Aug 11, 09:49 AM	Get around to the shots fired as a north business supervisor
Aug 11, 01:26 AM	Ready for this awful shot fire that I got apartment at 62 16 66 street
Aug 10, 03:05 AM	Our year for possible shots fired 23 on 955th Street
Aug 10, 12:31 AM	So 23 22 this has heard one audible shot fired just approximately 1

When you click on one of these rows it will launch an audio player with the full transcript of the 30-minute segment at the time stamp where the keyword matched.



August 12, 2024 at 11:48 AM

[01:52]
He'll be clear on 13th week, so...

[01:55]
30 years old?

[01:57]
34

[01:59]
back in 2008 of the 76 last

[02:01]
Let me call sheat

[02:03]
For flight vehicle burglary

[02:05]
embassy suites

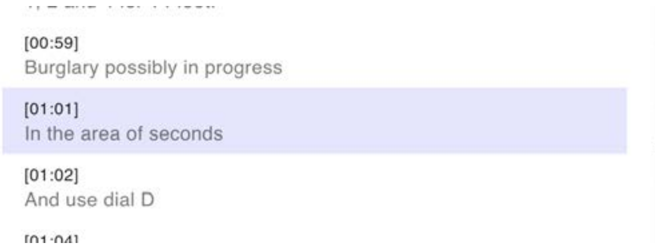
[02:07]
13 or 11

[02:09]
13 to 32

[02:11]
The 14-point

[02:13]

Whenever the dispatcher announces a crime over the radio they usually give an address or crossroad with a brief description.



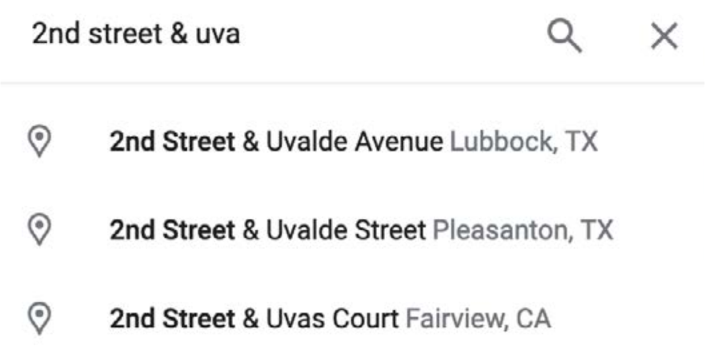
[00:59]
Burglary possibly in progress

[01:01]
In the area of seconds

[01:02]
And use dial D

[01:04]

As I explained earlier, Whisper is only good enough to get the important keywords, the correct transcription of the above is "Burglary possibly in progress in the area of 2nd and Uvalde". We can use the Google maps autocomplete feature to complete the address.



2nd street & uva

2nd Street & Uvalde Avenue Lubbock, TX

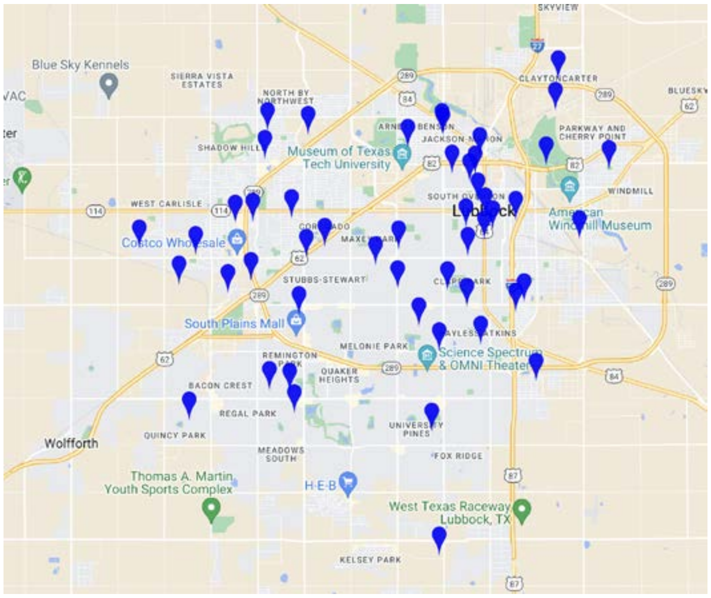
2nd Street & Uvalde Street Pleasanton, TX

2nd Street & Uvas Court Fairview, CA

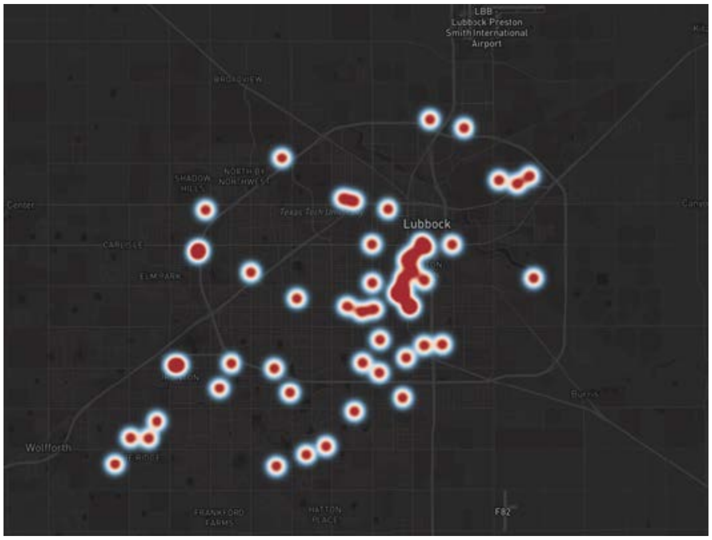
The operators often use landmarks like restaurant and apartment names with the address of the incident and you can use these to verify what you heard. After you have verified the address grab the coordinates with a right click then paste that data into a spreadsheet.

> ```csv
>
> Date, Address, Lat Lon
>
> "August 12, 2024 at 09:40 PM",6320 19th St,"33.5785, -101.9539"
>
> "August 12, 2024 at 11:48 AM",5215 S Loop 289,"33.5349, -101.9249"
>
> "August 12, 2024 at 12:19 AM",4702 86th St,"33.5163, -101.9132"
>
> ```

Continue this for as many days as you like, it will depend on the frequency of the incidents and the size of the city. For a small town like Lubbock, I felt 50 shots fired calls between August and May was enough to get a picture of where the hot spots were. There a several free sites to plot coordinates on a map but I recommend this one (https://mobisoftinfotech.com/tools/plot-multiple-points-on-map/), you'll need to remove all spaces from the CSV and add `,blue,marker` to each row before pasting it into the box and you should get something like this back.



I did a little extra and added the shots fired data into MapBox with a HeatMap (https://github.com/NotJoeMartinez/lubbock-scanner-heatmap).



With only a month of audio data we were able to discover something anyone who's spent a day in Lubbock could tell you: stay away from Avenue Q. ■

HOW TO USE USENET FOR
RESEARCH AND OSINT INVESTIGATIONS

By Jason Evans

OSINT, especially the SOCMINT (Social Media Intelligence) specialty, is often focused on widely used social media platforms like Twitter/X, Facebook, etc. However, there are lesser-known alternatives, such as Usenet, that can be a goldmine for OSINT investigations.

This article is not only for OSINT practitioners but also for researchers and internet historians who want to understand the specific ins and outs of Usenet research. This is just a very brief introduction to a very dense topic. However, Usenet is very well documented and more information on any of the topics found here is only a Google search away.

What is Usenet?

Before diving into how to use Usenet for OSINT, let's briefly cover what it is. Usenet, also previously known as "NetNews," is a decentralized network of servers that provide access to Usenet network. Usenet is not a product; much like email or IRC, it is an open internet standard (NNTP) that anyone can use. In many ways, you can think of it as the message board cousin to email.

Usenet has been operating non-stop since 1979, before the Internet and before the institutions that started it (UNC and Duke University) even had access to the ARPAnet. Since Usenet articles (Usenet refers to messages or posts as "articles") are plain text, archives from that time until today still exist and are available. From the 1980s through the early 2000s, Usenet served as the primary online forum for the Internet.

How Does It Work and How Is It Organized?

Each server sends and receives articles in a standard plain text format not unlike email. Each message is then categorized into one of hundreds of hierarchies, which are then broken down into individual discussion groups called newsgroups. Currently, there are over 40,000 newsgroups on Usenet. Within these newsgroups, you'll find thousands of topics, each focused on a particular subject. Users post articles, questions, or files to these groups, and anyone with access to a Usenet server can read or reply.

Many hierarchies are location-based, such as `tor.*` (Toronto) or `uk.*` (United Kingdom), while others are more topical, such as `comp.*` (computing), `sci.*` (science), `rec.*` (recreation), and `alt.*` (alternative topics). Within these categories, you'll find thousands of newsgroups, each focused on particular subjects.

Unlike federated services like Mastodon or Lemmy, every Usenet server receives every message unless they specifically request not to receive articles for some newsgroups (more about that later). This means that if you join or set up a news server, you will have access to all incoming articles from every newsgroup on Usenet that can be shared with you.

Anatomy of a Usenet Article

> *From -5182564358058015669*
>
> *Path: gmdzi!unido!fauern!ira.uka.de!sol.ctr.columbia.edu!zaphod.mps.ohio-state.edu!wupost!uunet!mcsun!news.funet.fi!hydra!klaava!torvalds*
>
> *From: torvalds@klaava.Helsinki.FI (Linus Benedict Torvalds)*
>
> *Newsgroups: comp.os.minix*
>
> *Subject: What would you like to see most in minix?*
>
> *Summary: small poll for my new operating system*
>
> *Keywords: 386, preferences*
>
> *Message-ID: <1991Aug25.205708.9541@klaava.Helsinki.FI>*
>
> *Date: 25 Aug 91 20:57:08 GMT*
>
> *Organization: University of Helsinki*
>
> *Lines: 20*
>
> *Hello everybody out there using minix -*

> *I'm doing a (free) operating system (just a hobby, won't be big and professional like gnu) for 386(486) AT clones. This has been brewing since april, and is starting to get ready. I'd like any feedback on things people like/dislike in minix, as my OS resembles it somewhat (same physical layout of the file-system (due to practical reasons) among other things).*
>
> *I've currently ported bash(1.08) and gcc(1.40), and things seem to work. This implies that I'll get something practical within a few months, and I'd like to know what features most people would want. Any suggestions are welcome, but I won't promise I'll implement them :-)*
>
> *- Linus (torvalds@kruuna.helsinki.fi)*
>
> *PS. Yes - it's free of any minix code, and it has a multi-threaded fs. It is NOT protable (uses 386 task switching etc), and it probably never will support anything other than AT-harddisks, as that's all I have :-(.*

This is a rather famous example of a Usenet article sent by Linus Torvalds, the creator of Linux, discussing his new operating system as a university student in 1991. Usenet hasn't changed greatly in how it functions since the early days, so we'll use this article as an example of what to look for.

The Header

> *From -5182564358058015669*
>
> *Path: gmdzi!unido!fauern!ira.uka.de!sol.ctr.columbia.edu!zaphod.mps.ohio-state.edu!wupost!uunet!mcsun!news.funet.fi!hydra!klaava!torvalds*
>
> *From: torvalds@klaava.Helsinki.FI (Linus Benedict Torvalds)*
>
> *Newsgroups: comp.os.minix*
>
> *Subject: What would you like to see most in minix?*
>
> *Summary: small poll for my new operating system*
>
> *Keywords: 386, preferences*
>
> *Message-ID: <1991Aug25.205708.9541@klaava.Helsinki.FI>*
>
> *Date: 25 Aug 91 20:57:08 GMT*
>
> *Organization: University of Helsinki*
>
> *Lines: 20*

The `Path` tells you which route the article took from Usenet server at the University of Helsinki to the server where this article was originally received. This may not be very useful for most people today, but if you were trying to generate a list of Usenet servers that were available at one time, you could use this information to start generating a map.

`From` is the email address and name of the sender. Traditionally, there has never been anything to force this information to be legitimate, with a few exceptions.

`Newsgroups` is a list of groups that the article was sent to. Cross-posting articles to multiple newsgroups used to be considered bad "netiquette" and could land you in hot water with your server administrator if someone complained. Today, such violations are rarely enforced.

`Message-ID` is the article's fingerprint. With this, you could theoretically find this article on any Usenet server that still had that article in storage. Because this is a rather famous article, if you Google, `1991Aug25.205708.9541@klaava.Helsinki.FI` you will find it republished on many different websites.

`Summary`, `Subject`, `Keywords`, `Date`, etc. are all pretty self-explanatory.

The Body

> *Hello everybody out there using minix -*
>
> *I'm doing a (free) operating system (just a hobby, won't be big and professional like gnu) for 386(486) AT clones. This has been brewing since april, and is starting to get ready. I'd like any feedback on things people like/dislike in minix, as my OS resembles it somewhat (same physical layout of the file-system (due to practical reasons) among other things).*

The body of the article is typically plain text, and prior to 2000, they were mostly just ASCII with a line width limited to 80 characters. Occasionally, when searching for non-English articles, you might encounter other typesetting formats. These can appear unusual if your system isn't equipped to handle non-ASCII characters and diacritical marks.

Binary Articles

Transitioning into the realm of filesharing, Usenet has also facilitated the sharing of binary data through a system known as yEnc. This method converts binary files like movies, images, PDFs, and entire computer programs into a format that can be distributed across multiple Usenet articles. Newsgroups starting with alt.binaries.* are particularly known for hosting such content, though they're not the only ones.

Today, the predominant use of Usenet has shifted towards the filesharing, mostly illicitly. Specialized software applications are employed for downloading movies and other media. These binary articles, unlike text-based discussions, are typically not archived for long-term access. Historically, this feature of Usenet has also been exploited for sharing illegal content, including CSAM, contributing to Usenet's decline in mainstream usage. At one point, access to Usenet was a standard offering with ISP packages, illustrating how integral it once was to online culture.

How Do I Get Access to Usenet Records?

Google Groups: In 2001, Google acquired DejaNews, the largest Usenet provider and archiver at that time. As of early 2024, Google stopped providing access to incoming Usenet articles and removed the ability to post directly to Usenet. The historical records are still available, but the search function is poor, and headers are missing except for the date, subject, and the sender's name.

Internet Archive: The Internet Archive holds nearly a terabyte (or more) of Usenet archives. These archives are usually organized by hierarchy and then by newsgroup. Each newsgroup is usually in `.mbox` format. `.mbox` is a text-only format that can be read with a text editor, searched using `grep`, or opened with email clients like Mozilla Thunderbird, with the aid of a plugin. The Internet Archive's collection typically covers content up to early 2013 and has limited coverage after that.

The UTZOO Tapes: These are archives of the earliest Usenet articles from 1981 to 1991. UTZOO was the name of one of Usenet servers used at the University of Toronto. They were once available on the Internet Archive but were removed at the request of a user. However, they can still be found on other websites with some searching.

Paid Usenet Providers: Paid providers often claim to have 10 years or more of article retention. However, this is usually not entirely accurate. It is an open secret that these providers primarily offer access to illicit materials in binary groups. Their retention of non-binary articles is limited, but some groups may still contain useful information.

Free Usenet Providers: Free services like eternal-september.org typically have archives spanning a few years. However, they do not carry binary newsgroups but are a great free source for monitoring existing newsgroups.

Why is Usenet useful for research and OSINT?

While it might seem outdated compared to modern social media platforms, Usenet has several features that make it a valuable resource for research:

Historical Data: Usenet has been around for decades, meaning it contains a wealth of historical discussions, opinions, and data. This is especially useful for investigations that require a long-term perspective or historical context.

Niche Communities: Many Usenet newsgroups are home to niche communities that discuss specialized topics in depth. These can include everything from software development to obscure hobbies, and even controversial subjects that might not be as openly discussed on mainstream platforms.

Anonymity: While not entirely anonymous, Usenet users often post under pseudonyms, making it a less censored space where people might share information more freely. This can be useful for gathering unfiltered opinions or uncovering discussions that might not happen on more public-facing platforms. Many Usenet providers, both paid and free, do not have the infrastructures in place to keep out users using Tor or VPNs. While Google required an actual Google account to post to Usenet, paid and free services do not require it. This makes Usenet ideal for anonymous discussions.

File Sharing: Today, Usenet is mostly known for illicit file-sharing, with users posting everything from software to documents. This can be a treasure trove for finding leaked data, rare documents, or software not easily accessible elsewhere.

How to Access Usenet

To use Usenet, you'll need access to a Usenet server and a newsreader, a program that allows you to browse and download content from newsgroups. Here's a quick overview of the steps:

Choose a Usenet Provider: Usenet access typically requires an account with a service that provides access to Usenet servers. Both paid and free providers are available. Paid providers usually sell access either monthly or by blocks of bandwidth. This is because they primarily sell access to pirated material rather than access to newsgroups for discussion.

Install a Newsreader: A newsreader is the software you'll use to browse Usenet. The most common option, available almost everywhere, is Mozilla Thunderbird. On Linux, Pan is fantastic. For those who prefer the command line, SLRN is another option.

Subscribe to Newsgroups: Once you're set up, you can start searching for relevant newsgroups. Most newsreaders allow you to search by keyword, making it easier to find discussions related to your investigation.

Types of Research Where Usenet Excels

With an understanding of how to access Usenet, it's essential to explore specific research scenarios where Usenet can be particularly advantageous:

Historical Research: Usenet's vast archives are a treasure trove for historical research. Whether you're delving into the early development of a particular technology, tracing the progression of a political movement, or investigating the roots of a conspiracy theory, Usenet offers unique historical perspectives that are often difficult to find elsewhere.

Technology and Software Development: Many Usenet newsgroups are rich in technical discussions, ranging from software development to cybersecurity and hacking. For researchers focused on cyber threats, software vulnerabilities, or the evolution of specific tools, Usenet provides in-depth discussions and access to original source code that may not be available on mainstream platforms.

Counter-Culture and Subversive Movements: Due to its decentralized nature and anonymity, Usenet has long been a gathering place for counter-culture and subversive movements. If your research involves exploring fringe communities, underground movements, or controversial topics, Usenet can reveal uncensored opinions and discussions that are often absent from more regulated platforms.

Intellectual Property and Copyright Infringement: Usenet hosts a variety of groups dedicated to sharing pirated software, music, movies, and other media. Monitoring these groups can provide crucial insights into distribution networks and the extent of intellectual property infringement, making Usenet a useful tool for those investigating these issues.

Things to be aware of

Usenet, at its core, is largely unmoderated. While moderated newsgroups do exist, it has long been assumed that users would manage "trolls" by employing software tools known as "killfiles".

Usenet is also riddled with spam. When Google took over Deja News in 2001, their only attempt at controlling spam was requiring users to have a Google account. They did not implement Captchas or other mechanisms to block bot accounts. This lack of spam prevention contributed heavily to Usenet's decline in the mainstream.

When researching Usenet, be prepared to encounter a high ratio of spam to legitimate messages, especially in articles posted after 2001. Spam did exist before this period, but not at the scale that followed.

The good news is that since Google no longer allows access to post to Usenet, the amount of spam has decreased dramatically, with the past six months being almost entirely spam-free in many newsgroups.

There has been a mild resurgence in Classic (non-file sharing) Usenet activity over the past few years. There has been renewed interest in many older technologies from retro video games to retro computers, leading many to rediscover Usenet. Real conversations are happening in newsgroups that have sat dormant for years.

Ror Researchers and OSINT analysts:

While Usenet may seem like a relic of the early internet, it remains a valuable resource for researchers and OSINT analysts. Its combination of historical depth, niche communities, and uncensored discussions makes it particularly useful for investigations that require more than just surface-level data. By understanding how to navigate Usenet effectively, OSINT analysts can unlock a wealth of information that might otherwise remain hidden.

Whether you're conducting historical research, exploring subversive movements, or analyzing technical discussions, Usenet has the potential to provide unique insights that can significantly enhance your research and intelligence efforts. ■

HOW I OBTAINED MY STATE
DRIVER'S LICENSE WITH AN ALTERNATE PHYSICAL ADDRESS

By Skeptical Sam II

I've had the opportunity, or misfortune, of moving many times in my life. I've lived at many addresses in the Midwest, New England and the Deep South and have always had my accurate physical address on every driver's license I've been issued. Then around 2015, I became interested in privacy due to certain life circumstances and started reading books on the topic. I immediately learned that one's home address is something that should be safeguarded and never to associate your name with your home address. I learned about trusts and LLC's and changed my mailing address to a P.O. Box. Then, due to other life circumstances, I had to move again. I seized the opportunity to implement significant privacy practices that can only be accomplished with relocation.

The first move was to an apartment complex in another town about 45 minutes away. I never place my house for sale until I have vacated it, so I needed a short term rental to move into while I sold my house and shopped for another one. I attempted to privately rent an apartment using an LLC instead of my personal name, but it wasn't possible. I ended up renting a townhouse and the lease and utilities were in my name. I continued using a PO Box for mail and was also using a CMRA for package delivery. My house sold after just a week on the market and I placed an offer on another home shortly thereafter. I created a revocable Trust and the home was titled in the name of a Trust, not my personal name.

I didn't change the address on my driver's license until I needed to provide a copy in order to obtain a Homestead Tax Exemption for my property taxes. The tax savings was significant and since the property was titled in the Trust name, I considered it worth the privacy intrusion. I later learned that anything provided to a County government regarding a property can and will be shared with anyone who requests it. I also learned that many states, including where I was living, sell the personal information contained in the DMV databases for profit to a number of entities willing to pay for it. This is infuriating and unacceptable to me, but the damage had been done. Then, due to more life circumstances, I had the opportunity to move again. A long distance move to another state. This was my opportunity to make more privacy upgrades.

I forwarded my mail to the address of a nearby relative in the new state. I rented a brand new apartment with garage, sight unseen, for a six month lease and made the 1000 mile move. My home was under contract in two days and I immediately began house hunting again. I found another home and again purchased it in the name of a Trust. My utilities are in the name of an LLC and my internet is in a fake name that I have adopted for use with the home. I continued using my out of state Driver's License for a few years, as it was still valid. I was finally forced to obtain a Driver's License in my new state, as the out of state one was nearing expiration. If I let it expire, I would need to take the full new driver's test again. Not happening.

This created a privacy challenge. Knowing that most states sell driver information for profit under the halo of "public record", how can I obtain a state ID with an address other than my home address? Post Office box and CMRA addresses are not allowed and proof of physical address is required in order to be compliant. This is why I had decided to not to close my checking account in the other state when I moved. I had learned that I was able to ask questions and get service through their secure messaging feature on the bank's website.

When I moved, I requested they update my mailing address to my new PO Box in the new state and they immediately made the change without any verification. I kept a small balance in the account and rarely use it, however, the real benefit has been the ability to change the address on my statements without any verification via email. I simply messaged the bank that I had moved and "wanted to update your records". I gave them the address of a relative and they made the change without any hassle. I was then able to obtain my new driver's license with the address of a relative using a copy of the bank statement showing that address, my Social Security card and US Passport card. Driver's licenses are no longer issued onsite and are instead mailed out. I provided my PO Box as my mailing address and my new credential was received within a week.

I've learned that privacy is a marathon and not a sprint. I'm not ready to become a NOMAD and may never go that extreme. But I enjoy testing new techniques and finding solutions to protect my privacy. I no longer claim a Homestead Exemption and use a PO Box on my tax returns. I'm not suggesting that anyone attempt this strategy, but instead explaining what worked for me in order to keep my home address off the internet.

Editor's Note (Disclaimer): *Make sure you understand any local, state, or federal laws before considering which address you will place on your license. I have had several successes convincing a county that a home in the name of a trust was used as a primary residence in order to access a homestead exemption discount without providing the resident name, but some counties demand it.* ■

EAST ASIA PRIVACY
AND AMERICAN EXPAT EXPERIENCE

By: Anonymous in Taiwan

I went to Japan to work in the early 1990's and later to Taiwan. What follows is simply some anecdotes (some funny and some scary) and observations, along with some experiences. I am not a privacy expert at all, but try to do what I can.

Sometimes it is easy, and sometimes there are major fails. I am probably too honest and that is how my IRA ended up being recently closed by an American brokerage house, forcing Federal withholdings and thus an indirect rollover and me having to supply the missing withholdings, though opening a new account is problematic because online verification is not friendly to American expats. One bank through a verification company wanted kyc/cip proof of address and required uploading of my local lease... in ENGLISH! Fail and declined! I am not in an English speaking country and any translation would look fake. Going to have to talk to a sympathetic human who doesn't rely on rigid computer software.

During my first months in Japan in the 1990's I had to wire money home every month incurring a $50 fee per wire. Later, when I had enough savings in both Japan and the US, I did not need to send the money immediately and so I asked the bank to cut a cashier's check, which had only a $25 fee. I took a bilingual colleague with me, and informed the clerk I wanted the check payable to me. She refused, as she said the US bank wouldn't cash it since I wouldn't be there in person...I explained the concept of "Deposit Only", but she still refused. I went back the next day without my too polite colleague and asked the same clerk again. She refused again.

I informed her the check should be payable to my "twin", who had the same first name and middle initial as me (but different middle name). She of course didn't believe me, but had no argument against it. Many months later a different clerk asked me about it, and I asked her if it was strange that I should have a twin. Oh, no, of course not! Fast forward a couple of years at the same bank. I went to make a cash withdrawal and forgot to write my pin number on the form. By this time I could speak Japanese, but this clerk assumed I couldn't and probably that I didn't know my pin. She went to a filing cabinet, fished out my original application, pointed to my pin, and told me to write that number down on the form. Great security! I never bothered getting an ATM card, as the ATMs were only in the bank and accessible during banking hours (3 pm close).

At that time I had no real concept of privacy nor opsec, but did understand redundancy. I had got myself a second bank account on the West Coast, as I believed they would have more Asian experience than my East Coast bank. I do not know if that's true or not. Probably not. Numbers are numbers.

At the same time, I had gotten a new credit card from the Bank of Baltimore. As I owed them money and payment was by mail, I changed the address to my Japanese address. Their computer system no doubt couldn't handle the foreign address, so they assigned me a "Bank of Baltimore PO Box" as my address, sent the bill to that address, and then someone received it, looked up my Japanese address, hand wrote it on an envelope, and placed the postmarked bill inside the new envelope with international postage. To this day Baltimore, MD is listed on my credit report as a place I have lived, though I have never been there.

Fast forward to about 2019 in Taiwan. A naive acquaintance I knew had the proposition that I could "earn" some money by going to China, setting up a bank account, and allowing someone there to "use it". And that I could make a lot of money (enough to "retire"). Oh yeah! Sounds like a great deal! And clearly some kind of organized crime money laundering scam. And how am I supposed to explain potentially millions of dollars passing through an account associated with me? "That's your problem my amerikanische Freund!" Oh, I would have to be single also and never married. I interpreted that as a reason to need my Social Security number for some kind of proof, and clearly leading to identity theft on a grand scale, while I am disappeared in China.

Now let me mention FATCA (Foreign Account Tax Compliance Act) passed in 2010 and now in full force. Every American with a foreign bank account must report it, as does the foreign bank. Thus, on any foreign bank account I have or get I must fill out and sign an IRS W-9 form and show my Social Security card. These are presumably kept on record and stored in some filing cabinet. (See above anecdotes) Bank clerks in Taiwan probably earn about $900 per month. But Americans are living everywhere all over the world. Well, Socials are not hard to get, but paired with signatures?

Must be worth something to someone... One more thing to worry about! Thanks Uncle Sammy!

A legal alias

When I started studying Chinese, my teacher assigned me a Chinese name. (I could have chosen my own.) As government forms here in Taiwan have a field for a Chinese name in addition to your actual name on your passport, I put my Chinese name down on a form and it is now my official Chinese name on government documents and ID (along with real name), and my bank even put it on a bank book. I once found a wallet and took it to a police station. I later received in the mail a form Thank You letter with my Chinese name on it and 20 others who had done similar deeds. Presumably the others got the same letters with my Chinese name on theirs. I may get a Taiwan credit card with that name on it. There are quite a few possibilities to use it for privacy.

In Taiwan people seem to be quite lax with documents in my opinion. That is to say a photo of my local ID is on quite a few employer phones within the Japanese LINE App that almost everyone uses exclusively. It actually is quite secure and has phone/video/text capabilities. In Taiwan there are a lot of in person protocols, which are quite feasible and convenient in Taiwan's urban high population density. I can pay my texted phone bill in person at any company store and they are everywhere! They also have my photo, and I have never heard of sim swapping here. There are no burner phones here. All sims are registered. Taiwanese (and us foreigners) use personal stamps [chops] on official documents along with signatures.

One fail I have seen involves the local city bike share platform I use. I had an issue once and went online to which they replied to me by email with my phone number/account number in the subject line thereby linking my number to that email for anyone who can snatch it out of the ether! I replied that wasn't a good idea and they forwarded the comment to IT. Previous to that I had once traveled through Beijing, China and stayed in a hotel. I was surprised to receive a text on my Taiwanese phone (in Chinese) offering various "adult services". They are watching and targeting everyone! Probably filming.

As for my latest phone, a Samsung, it has two sim slots so I have two numbers. One is a prepaid sim to which I must pay about $3 every four months plus anything beyond the maximum data or phone calls. The other sim is an unlimited data plan at $20/ month which I use almost exclusively for data.

The prepaid I got when my manager gave me a free smartphone they had received when renewing a phone contract but didn't want it as they used iphone. Said manager helped me get the sim and since the phone company would only accept a passport as ID from a foreigner (I didn't carry with me) the sim was put in said manager's name for about nine years until I finally got it switched to my name (again, with that person's help). I assume most calls to the primary sim are wrong numbers since I've never given that one out. I only answer the prepaid sim if it comes from a landline. If someone on a cell phone wants to talk, they'll first have to text me. I've never received a text, other than earthquake alerts or phone bill due, and police warnings about phone scams! Maybe I've missed a job offer? Their loss!

Convenience Stores

I'm not an expert on this subject, however in Taiwan they are VERY convenient. [See L.A. Times: Why are Taiwan's 7-Elevens so much better than ours?] You can buy train tickets, bus tickets, plane tickets, baseball game tickets...lots of things...pay in cash! Send a fax. Get a taxi! Renew your Driver's License!(It's not an ID in Taiwan and appears to be 1970's format: laminated paper -but don't fake that number!) You can also shop online and have goods delivered to a convenience store and also pay c.o.d.[Your little brother will not be opening your private mail!] You can send out (or receive) a DHL or Fedex envelope...or packages. You can pay any bills or parking tickets. They usually have ATMs inside. Many have tables and seating. They can microwave food. Some have beer on tap! Really! Yes, they have cameras everywhere! There are probably lots of bar codes scanned and probably no one is looking at your ID. Does the bar code match? OK. There are no doubt both privacy solutions and vulnerabilities.

Taiwan also has a cash touch card [Easy Card] that can be used for buses, trains, subways, bike share, and many stores. It can be anonymous, or you can link it to something. The bike share requires the card and a telephone number to register or an App and QR code. But the cards only cost about $3 and are of course reloadable at any convenience store. The train fare is 10 percent cheaper using the card or you can pay cash.

In the 1990's in Japan I was paid in cash and Taiwan too is still very much a cash economy, even with all the payment tech options, including Line Pay or Google Pay, etc...One can also use the ATM to transfer funds. Over the end of year holidays 2023 in the US I received a Visa gift card and made some online purchases. Some of them went through and then one was rejected by Amazon after first being accepted so they defaulted to my Amex on file. Luckily I noticed and so promptly canceled the order. Lesson learned. Don't keep a credit card on file unless it's a Privacy.com, but as I live abroad it is not available to me.

Well, that is about all of the privacy anecdotes I have. As for Americans owning any mutual funds while residing abroad, that is illegal and if banks find you are living abroad (or you tell them) they will possibly close your IRA or other account. There are banks that can work around that in some way, however I tried to use a next of kin address in the United States along with a South Dakota nomad residency id, but again the online verification didn't like that, even though all those addresses are on my credit report. I may really need a "twin" this time. ■

THE GROCERY STORE CARD

By Scarecrosint

Over the years I have seen more and more grocery stores rolling out "discount" cards in different forms. You sign up for a card and show it at checkout to get your discount each time you shop. The registration process varies but it usually requires handing over quite a lot of personal information which everyone in the audience has an aversion to. Who knows what is being done with your data on the backend. I don't know about you but it keeps me up at night thinking about someone selling my data, knowing where I shop, when I shop and what I purchase. Here are some of my findings.

Out the gate I will tell you the permutation that I cannot recommend but it worked for me and that was registering the card using a person's certain identifier that I knew was deceased and it worked to get a card. Karma will get me back no doubt but I found a hole in their system. At one store I even tried an ID that I have from another country but that did not work because the format was different. It was worth a try.

Where did these cards come in useful for me? For a sock puppet account. When I was creating my email address and social media accounts for one of my alter ego's I thought about how I could take it even one step further. So I registered a grocery store card in the sock puppets name and handed over everything I could in regards to cell number, email address and ticked all the marketing boxes for the first time ever in my life: yes, please add to me as many spam and marketing databases as you like, thank you. Why do this? If someone is ever suspicious of my sock puppet or hopefully some data is leaked pertaining to it, the account has a whole new level of authenticity. Oh and when I use the card, I always pay cash as to not tie the transaction to my actual bank card.

At one stage I registered a card partially in my name. I fed the registration process only partially correct information about myself. The reason I did this was that I used the card a few times to establish some patterns and from there on out I have swapped my card with several other people and have tried to entice them to do the same creating a chain of anomalous data in the marketing machine. I have no idea where my original card is these days but I have started sleeping better at night knowing that I have poisoned their data.

Finally here is my proof of concept in relation to these cards (well some of them because this will not work for all of them). This might catch the eye of any PI reading this out of interest as well as raise the worry level for the rest of us. I sat looking at the card thinking of permutations and it dawned upon me. For this particular card I could login into the stores portal using my cell number and view all my till slips. It then dawned on me "What if I registered a card to a cell number I have control of and swap it out with theirs somehow?". Well if I did any of this and left it for let's say a month to gather a decent corpus of data, I could login to the stores portal and view all the cards till slips. There I would be dumpster diving looking at what the person bought, where they bought it, what times they shop and so forth. If I did not know where that person lived before or worked, I might have a better idea now. From the purchases I could make educated guesses as to how many people are in the household and some details about their diet.

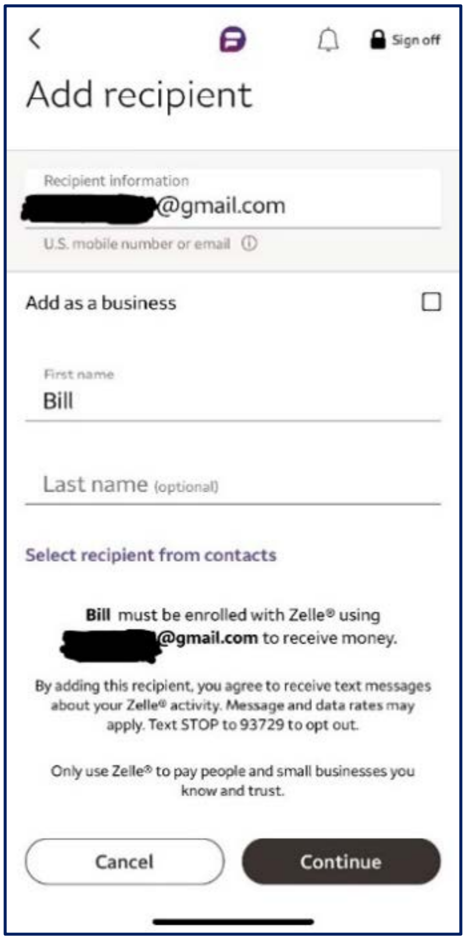
The store I go to now, I don't even have a "discount" card for. I gladly pay that tiny amount extra because I don't have one and wonder how many infinite loops in marketing databases I am guilty of causing. ■

EXPLOITING A PRIVACY VULNERABILITY IN ZELLE

By Dennis Lawrence

Zelle is a peer-to-peer money transfer app that allows users in the United States to move small amounts of funds from one party to another in near real-time and without fees. With over 120 million participating consumers, it represents a major payment platform that caters to roughly one third of the American population. Clients of many large financial institutions have ready access to Zelle enrollment which helps explain its large user base whose information is tied to banking records or debit card data. Since transactions are intended to be fast and user-friendly, a sender only needs the recipient's a) email address or phone number; and b) first name; to send them funds.

Zelle's functionality comes with a privacy vulnerability that can be exploited for the purposes of investigative research. If an individual is having trouble determining the owner of an email address or phone number, they can attempt to add the target as a Zelle recipient by entering the target's email or phone number along with an associated generic first name (i.e. "Bill"). If the target is an enrolled Zelle user, Zelle will reveal the actual first name (i.e. "James") of the email or phone number owner as seen in financial institution records regardless of what was self-entered when adding the recipient. In some cases, Zelle will also reveal the owner's last name. As another piece of good news, the target will not be notified if they are added as a Zelle contact. This simple tactic can provide useful leads when tracking down the owner of an email or phone number in the United States. [Note: This privacy vulnerability was found using Zelle via the Wells Fargo banking app. Results may vary depending upon how Zelle is accessed.]



Add recipient

Recipient information
[redacted]@gmail.com
U.S. mobile number or email

Add as a business □

First name
Bill

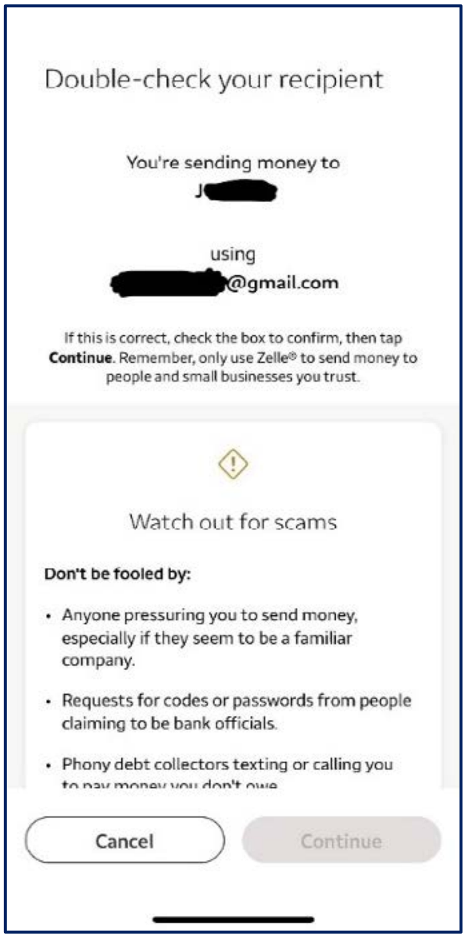
Last name (optional)

Select recipient from contacts

Bill must be enrolled with Zelle® using [redacted]**@gmail.com** to receive money.

By adding this recipient, you agree to receive text messages about your Zelle® activity. Message and data rates may apply. Text STOP to 93729 to opt out.

Only use Zelle® to pay people and small businesses you know and trust.



Double-check your recipient

You're sending money to
J[redacted]

using
[redacted]@gmail.com

If this is correct, check the box to confirm, then tap **Continue**. Remember, only use Zelle® to send money to people and small businesses you trust.

Watch out for scams

Don't be fooled by:

- Anyone pressuring you to send money, especially if they seem to be a familiar company.
- Requests for codes or passwords from people claiming to be bank officials.
- Phony debt collectors texting or calling you to pay money you don't owe

Left: When adding a recipient, enter the email address or phone number being investigated along with a generic first name. Right: If Zelle recognizes the email address or phone number as belonging to a valid user, the platform will display the user's real first name as seen in financial institution records. ■

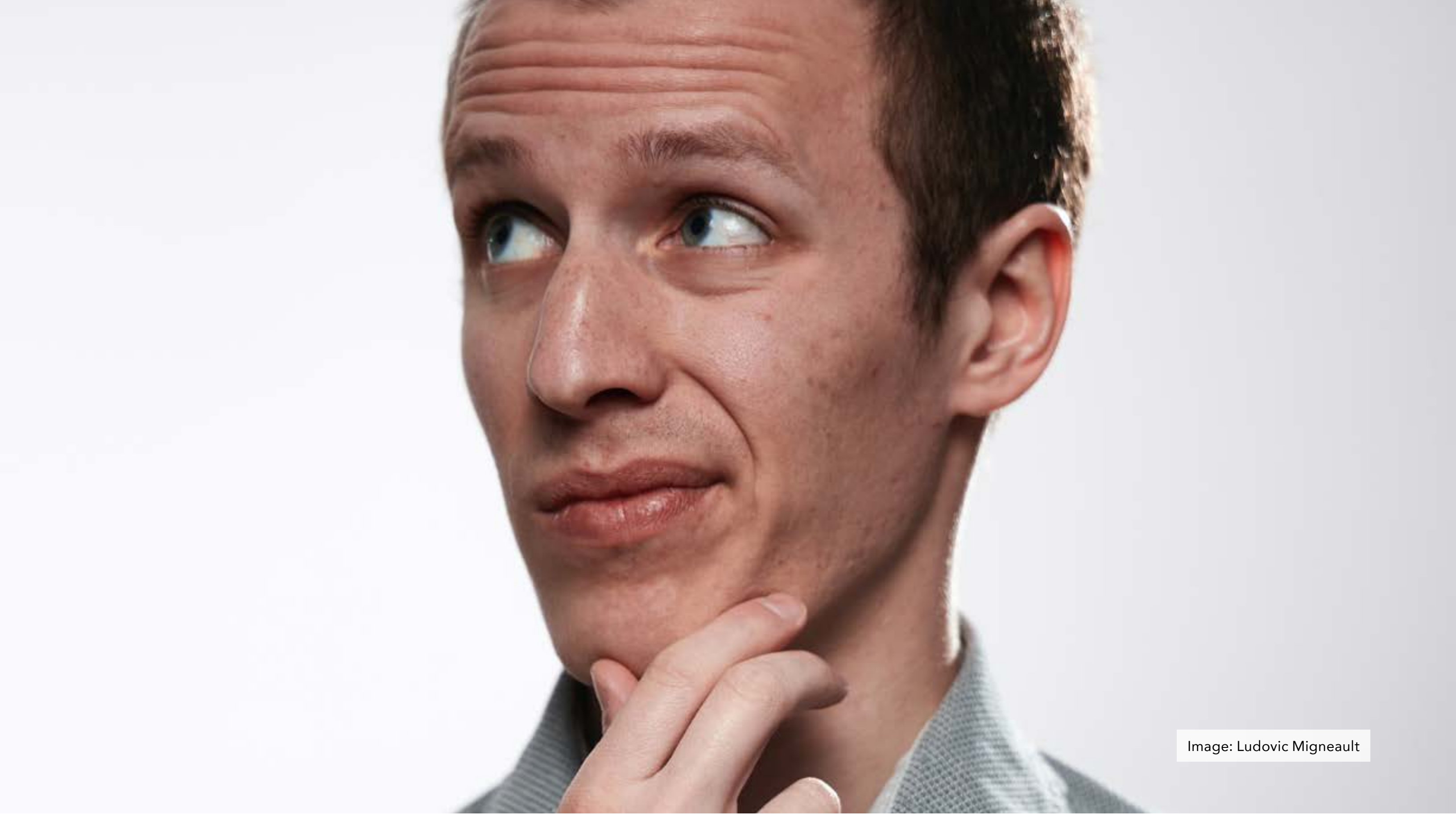


Image: Ludovic Migneault

READER Q&A

By Michael Bazzell

Q: Michael, I'm curious how you approach international travel, especially since you mentioned you spend a lot of time outside the United States. I don't think booking a hotel with an alias would work too well abroad as many countries, such as Japan, require you to have your passport on you at all times. If the hotel asks you for your ID, saying "I don't have it on me" isn't going to work out well. But maybe I'm wrong.

A: It depends. A lot has changed over the past five years. If I am in the middle east, I use my true name everywhere and know I am being monitored. I do not want to be arrested for providing false information and jailed indefinitely. If I am in a populated city, such as London, it is the same. Social engineering attempts do not work like they did in previous years. I play by the rules. If I am escorting a sensitive client who demands anonymity, I use a local proxy. We have people in most major cities who will reserve the room in their true name, physically check-in at the front desk, provide their own credit card in their name for payment, obtain card access to the room, and then meet me in a pub to give me the card. I can then come and go with my client as needed without any personal details being provided. We pay the proxy all fees incurred, plus an additional fee for their efforts. The proxies never know the identity of the client.

Q: Can you give an example of when you were caught in a lie or bluff and what you did? Like if you entered a SSN starting with 666 or 9 and someone noticed and confronted you.

A: WAY too many failures to choose from.

Q: When using a Private Mailbox (PMB). How do you get big packages delivered (e.g. a treadmill)? Are the other sizes of PMBs worth it?

A: I never send anything large to a remote PMB. I rely on Amazon lockers or nearby CMRAs which accept large packages. In a worst-case scenario, I will order to my home in an alias, but that makes me nervous.

Q: Has anybody devised a way to buy a concert ticket anonymously? I don't want to install the Ticketmaster app on my phone, create a Ticketmaster account in my real name, etc. I just want to go to a concert of my choosing without having to get married to Ticketmaster and the like!

A: Most ticketing services will allow you to print the QR Code with the ticket, and allow that to be scanned at the gate. I have never installed any apps like that, and purchases through the website have always worked. You can also save the code as an image on your device and allow it to be scanned.

Q: I finished reading through the Unredacted issue #006 from Feb'24, and I have a question about how to contact one of the contributors/ authors. The article in question, was "It's not me, it's you: Breaking up with by cell phone number of 21 years." In that article, Alex Harris was talking about his privacy-loving MVNO that he uses. He says "Feel free to contact me if you want to learn more." Is there a process that I can follow to contact Alec to ask him some questions about this?

A: Several people had the same question. The author has agreed to provide the following masked email for any questions about the article: remindful.sardine133@mailer.me

Q: Would you change your preference of hardware based 2FA over software based 2FA for international travel considering that if the international travel is detained both the computer as well as the security key could be compromised.

A: Probably not. I have a very small YubiKey which I can hide well in my bag. It could even be sewn in somewhere. If someone has my computer, my YubiKey, my device login password, and my services passwords, I am screwed anyway.

Q: Ok, let's assume I succeed in anonymously building a new home (using an LLC or trust), getting mail at a PMB, and not registering to vote. If I meet a new neighbor on the street, perhaps I can use a pseudonym to avoid linking my true name to my address. BUT, if I ever want to invite over my grown children or old friends (who already know my true name), they'll need a physical address to know where to drive. But if I give them the physical address, they'll enter it into their contacts and it probably will be scooped up by Google and Facebook — if that occurs, its game over, right? So what do you do? Do you ever invite people to your home? How do you keep them from exposing your physical address? Can I have only have privacy OR houseguests, but not both?

A: My friends and family understand and respect my weirdness, so I don't have much concern. They stay off their phones while at my home and send any mail to me at a CMRA address. When someone wants to visit who has never been to my home, I meet them at a nearby shopping center and escort them in. If needed, I explain that GPS will take you the wrong way, so this is better for them.

Q: I recently applied for a mortgage with a lender, and within minutes of having my credit pulled I was receiving calls from other lenders. Even after being placed on the "do not call" list, I was getting calls and email. Is there a way to prevent these credit bureaus from selling our information, or is there a way to provide legal aliases?

A: You likely signed several documents which included a clause that they could share your information. There is not much you can do when that is the case. This is why a cash purchase is really the only way to achieve true privacy of the home.

Q: In the recent 5th edition of Extreme Privacy, a defense is made in favor of beginning a privacy-reboot with fresh devices. This position is defended well, in my opinion, however I have a minor problem. Before a privacy reboot, it is highly unlikely that one will possess the means to purchase online products with privacy. This means that in store purchases with cash would be the only "anonymous" purchasing format one has access too. This works well until one wishes to obtain a Linux laptop from System76, as recommended. Therefore, the question is this: Is it alright for someone new to privacy to purchase a System76 laptop in their name, and ship it to their own address? If not, how would someone new to privacy obtain a System76 laptop?

A: I think it is acceptable to purchase a Linux device in your true name, but never have any items shipped to your home address. There is no telemetry on the device attaching your name to System76 traffic like their is with an Apple serial number.

Q: What does Intel Techniques make of Starlink Internet? It appears on the surface to be essentially a cellular data plan on steroids. It has the unique benefit of providing a "VPN-Like" IP experience to end users (a single IP address is shared among numerous people), however has the downsides of being, well, mobile internet.

A: I would not classify Starlink as a "VPN-Like" experience. They absolutely know which user is connected, the location of the dish, and unique identifiers for your traffic. I have no objection to their service, but you would still need a VPN if you do not want them tracking everything you do. I think they are the same as any other satellite provider in terms of privacy, but their speeds are phenomenal.

Q: Many people wish that computers had dedicated WiFi/ Bluetooth kill switches which would hardware disable those radios. If one removed the WiFi/Bluetooth card from their computer, and replaced them with external USB WiFi/ Bluetooth adapters, wouldn't this be functionally the same?

A: Many Linux laptops have a standard M.2 slot which provides a Wi-Fi and Bluetooth card for connectivity. Most System76 laptops work this way. Removing that and relying on USB wireless devices is definitely an option if you do not trust the software disabling. I leave mine in but disconnected for convenience, but extreme needs could rely on this for protection. ■

UPDATES

By Michael Bazzell

The biggest update since the previous edition is the release of the 5th edition of my book Extreme Privacy. If you have the 4th edition of this book, you may want to know what has changed in this new edition. This is not a simple facelift, as I have drastically changed the flow, content, and goals for this edition, as follows.

First, I no longer present strategies which I believe are not optimal. In the previous edition, I delivered my recommendations, and then followed with alternative options for those who did not want to go the extreme route. With this book, I spend more time on the ideal solutions while trying to avoid compromises.

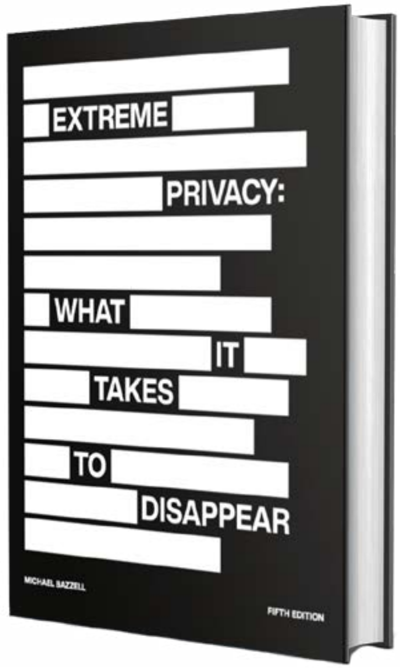
Second, I restructured chapters into sections, and isolated specific tasks for easier execution. In the previous edition, I presented huge chapters which covered a lot of ground. As one example, the mobile devices chapter was 77 pages and covered everything from selection and configuration of a mobile device all the way through DNS, VoIP options, and advanced applications. People were simply overwhelmed with the amount of information. In this book, I isolate each individual topic into its own "task". This allows readers to focus on one specific step, and may offer a feeling of accomplishment once the task is complete. In this example, the mobile devices section is now split into dozens of bite-size tasks which can each easily be completed in order.

Third, I offer a more chronological program. During a consult in late 2023, a client shared that she had read the previous edition twice, but was still very confused about the order of events ideal for her. Her voice was in my head while I wrote this updated work. In this edition, I have reorganized all tasks to flow in the most ideal order for most readers. This eliminates some of the confusion about finishing one task before starting another, or the need to wait for a service to be activated before proceeding with the next step. Every task in this guide is independent of the next, as long as they are followed in order.

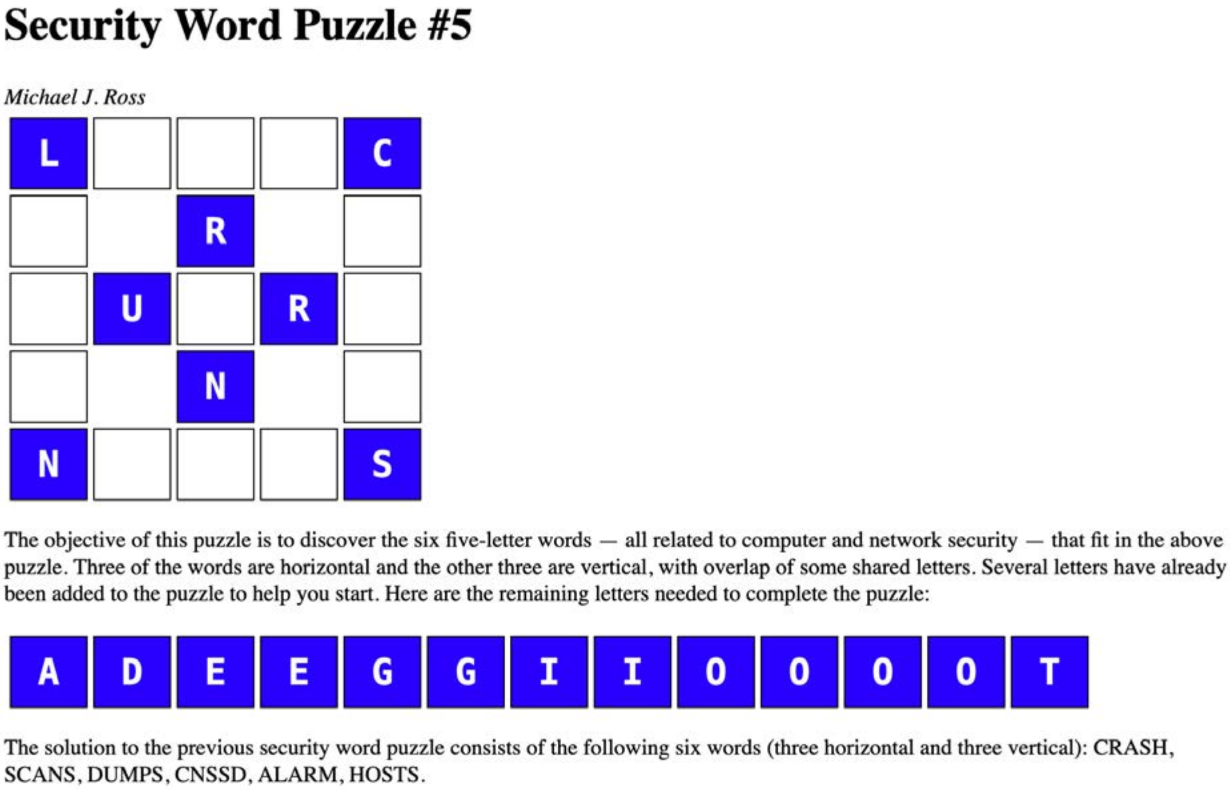
Finally, all expired and outdated resources were replaced with new methods throughout every chapter. Full details can be found at https://inteltechniques.com/book7.html.

We offer both print and digital versions of this book. We encourage most readers to consider the digital PDF version, as it is more affordable; your PDF will be issued immediately after your order; any minor updates which do not impact page count will be issued via email; an Amazon account is not required; and you can easily search, copy, and print content.

I sincerely thank all of the readers who keep supporting my research into these silly ideas. A detailed FAQ about updates and other issues is at https://inteltechniques.com/books.html#FAQ



PRIVACY-THEMED
PUZZLES



Security Word Puzzle #5

Michael J. Ross

L				C
		R		
	U		R	
		N		
N				S

The objective of this puzzle is to discover the six five-letter words — all related to computer and network security — that fit in the above puzzle. Three of the words are horizontal and the other three are vertical, with overlap of some shared letters. Several letters have already been added to the puzzle to help you start. Here are the remaining letters needed to complete the puzzle:

A	D	E	E	G	G	I	I	O	O	O	O	T

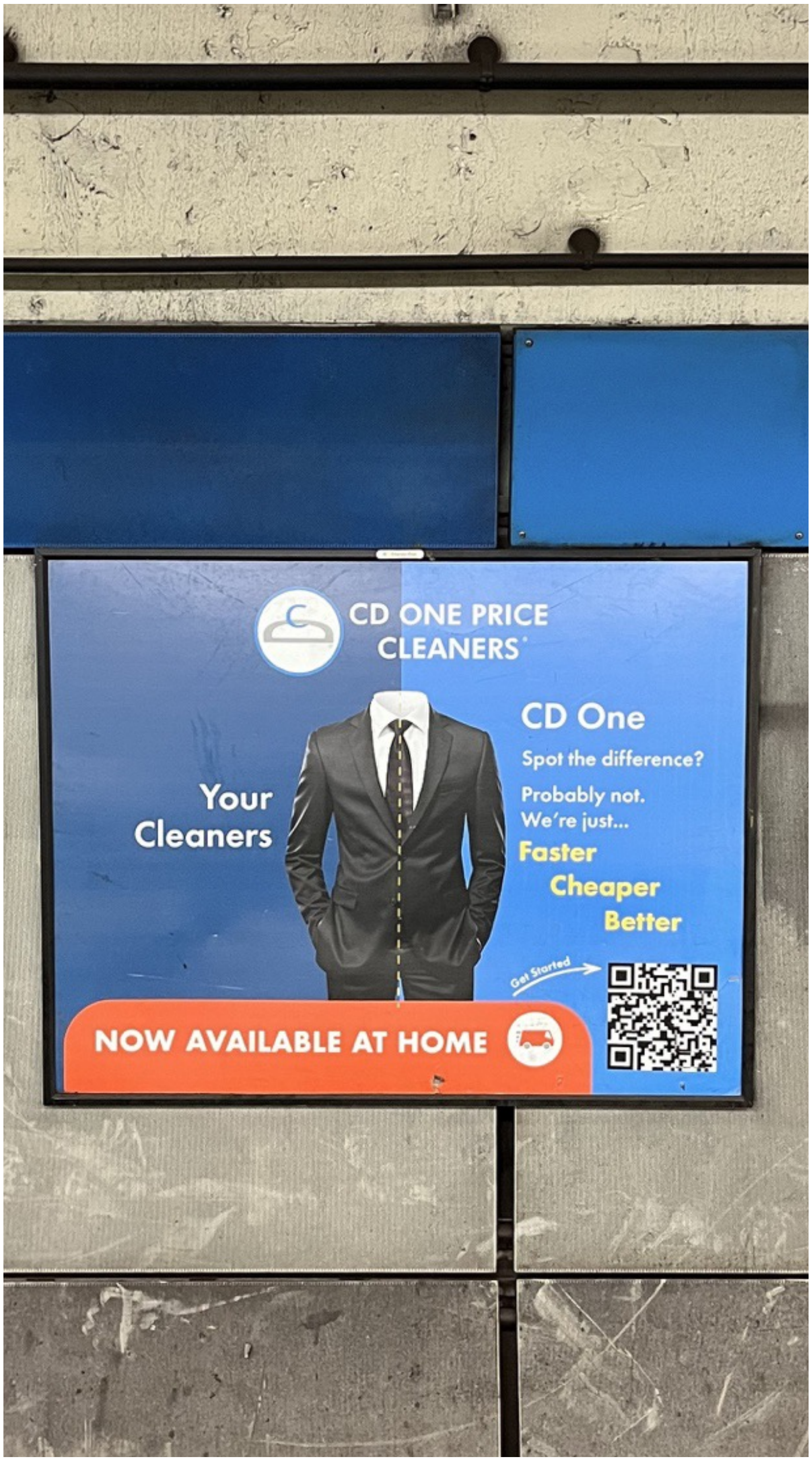
The solution to the previous security word puzzle consists of the following six words (three horizontal and three vertical): CRASH, SCANS, DUMPS, CNSSD, ALARM, HOSTS.

CHUCKLES

By heyczerny

The subway where I live has these new ads for a cleaning company. As you can probably guess, I do a double-take every time I see them because the clip-art it uses is identical to the profile pic stand-in that MB has used in the past (Amazon authors, LinkedIn, "Hiding From The Internet" 2e , etc). I don't wish to drag an innocent business into this fracas so I have mangled the QR code in the attached picture

Editor's Note: *I can confirm that is the exact image which I licensed for my series "Hiding Form The Internet".*



FINAL THOUGHTS

By Michael Bazzell

I hope that this resurgence of UNREDACTED sparks new interest from contributors. If enough content was available, we would publish every month. Now YOU decide when the next issue arrives. I can't wait to see what you write.

MB ■

AFFILIATE LINKS

If you would like to support this free publication, please consider using the following affiliate links. If you plan to purchase any of the items below, or other items from the vendor (such as Amazon), the following links provide a small financial contribution to us without costing you anything extra. We see nothing about you or your order.

Extreme Privacy Book (Amazon): https://amzn.to/4fFC2Ft
OSINT Book (Amazon): https://amzn.to/4dqbzcZ
Proton VPN Service: https://go.getproton.me/SH16Y
Proton Mail Encrypted Email: https://go.getproton.me/SH16Q
Silent Pocket: https://slnt.com/discount/IntelTechniques
Standard Notes: Coupon Code IntelTechniques20
VoIP.ms: https://voip.ms/en/code/IntelTechniques