PGP encryption: PGP (“pretty good privacy”) can be used to encrypt emails and files. This article has some basic information about what PGP is, how it works, and some advantages and disadvantages. *varonis.com/blog/pgp-encryption*

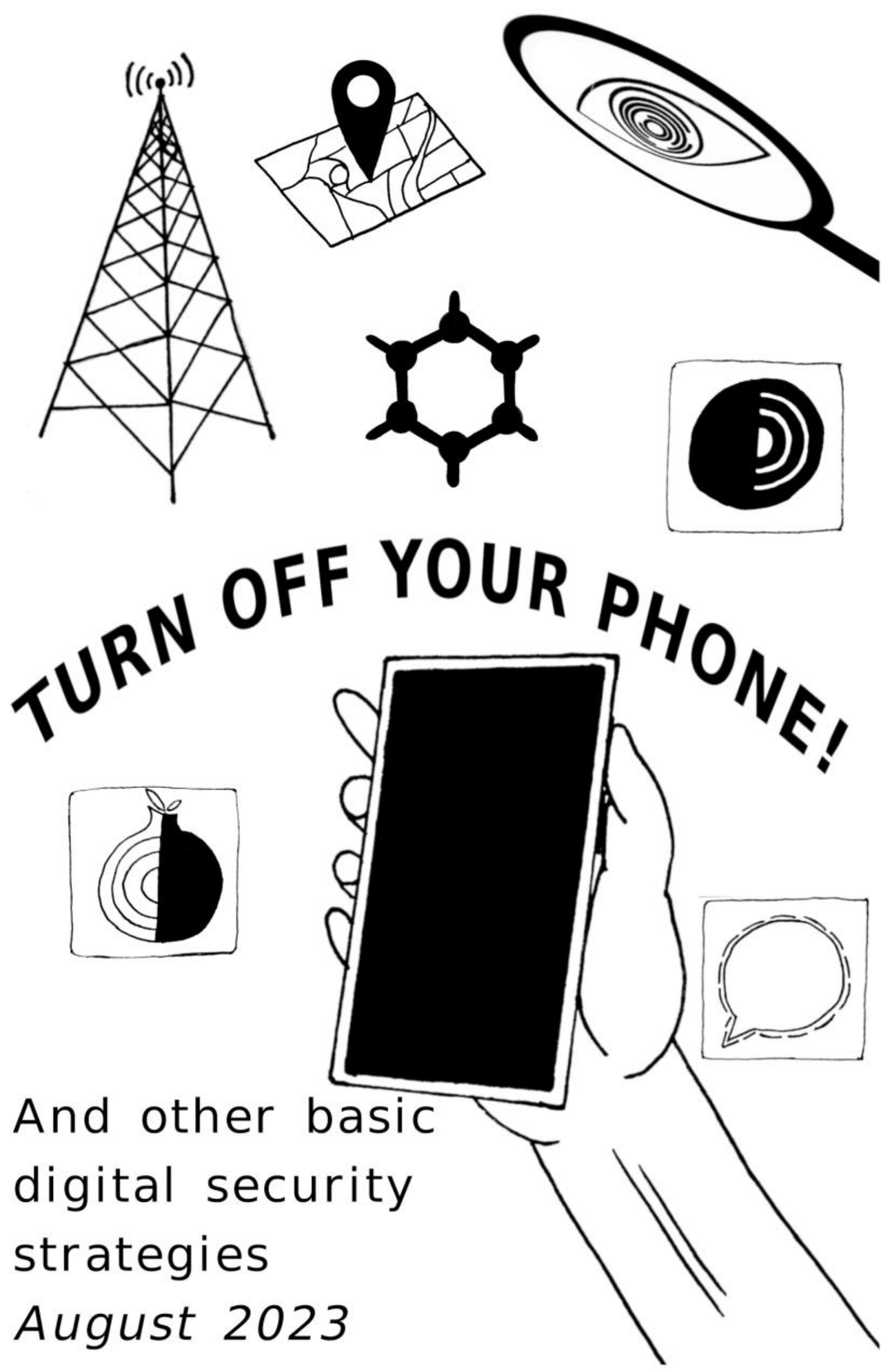
Rebel Alliance Tech Manual: A book-length document about electronic security for activists and political dissidents. Includes case examples from political struggles around the world. *github.com/rebel-tech/Rebel-Alliance-Tech-Manual*

Signal Configuration and Hardening Guide: A detailed guide to Signal settings which improve your security, on both Android and iOS. Includes suggestions like automatic disappearing messages, disabling link previews, and changing notifications to show minimal information. Also recommends Molly and Molly-FOSS (mentioned above). *blog.privacyguides.org/2022/07/07/signal-configuration-and-hardening*

Signal Fails: A zine calling out the limits of digital organizing, and encouraging us to organize more in person. s*proutdistro.com/catalog/zines/security/signal-fails*

Tails: An operating system that runs off a flash drive and leaves no digital evidence on your computer. Comes with privacy-focused software like Tor Browser, Metadata Cleaner, and others. Can also have an encrypted “persistent volume” on the same flash drive as Tails, which makes the files only accessible while using Tails. *tails.boum.org*

Tor Project: Created and maintains Tor Browser, a safer way to browse the internet that anonymizes your online traffic. *torproject.org*



And other basic digital security strategies

August 2023

TABLE OF CONTENTS

PEOPLE....2
BuT WhAt AbOuT DiGiTaL SeCuRiTy??....3
SO... WHAT DO I DO?....3
ENCRYPTION....5
PASSWORDS....5
APPS....6
SIGNAL....8
SOCIAL MEDIA....10
VPN (Virtual Private Network)....10
TOR (The Onion Router)....11
ORBOT....12
LOCATION DATA....13
PHYSICAL ACCESS....14
SUMMARY....15
ADDITIONAL READING & RESOURCES....16

And here's the summary, right up front:

- Turn your phone OFF, especially if a law enforcement interaction or arrest is likely
- Use long alphanumeric (14+ random characters) or diceware (7+ random words) passwords—NOT 4 digit pin
- Use a password manager, with backups
- Social media is hostile—delete your accounts
- Stick to encrypted, open source, recently updated everything, as much as possible
- Use a VPN, Tor browser, and Orbot for phones
- Likely physical compromise? Get a new device!

Have questions about any of these? Unsure what some of the words or acronyms mean? Maybe you should read the zine...

Faraday Bag: Blocks electromagnetic signals like cell service, WiFi, Bluetooth, and RFID. Test that signals are actually blocked prior to trusting a specific bag with your security. *howtogeek.com/791386/what-is-a-faraday-bag-and-should-you-use-one*

F-Droid: An app store that prioritizes privacy-minded apps. Prior to installation of any app, you are informed of "anti-features" like paywalls and surveillance of your activity. *f-droid.org*

Graphene: A privacy-focused operating system that is currently only compatible with Google Pixel devices. Extremely helpful to "de-Google" (remove all Google products and services) from your phone. *grapheneos.org*

How to Set Up a Burner Phone: A zine detailing how to set up a burner phone, from acquiring the phone to installing specific privacy-focused apps without ever needing a Google account. *libgen.is/book/index.php?md5=D5868F96785B0DEDFE305A1CDDC5D2A6*

Molly: A version ("fork") of Signal for Android which provides additional security and anti-forensic features. Molly is identical to Signal with security enhancements, while Molly-FOSS is the fully open source version without Google's proprietary code. A comparison of the two versions, as well as more info and install instructions are available on the project website. *Molly.im*

The P.E.T. Guide: A zine comparing and contrasting Signal with **P**eer-to-Peer **E**ncrypted over **T**or alternatives Briar and Cwtch. *itsgoingdown.org/the-guide-to-peer-to-peer-encryption-and-tor-new-communication-infrastructure-for-anarchists*

ADDITIONAL READING & RESOURCES

If digital security is an area of interest for you, or you have specific security needs beyond the basics, there is so much more you can do. Here are some places to start, many of which are also interspersed as footnotes throughout this zine:

Confidence, Courage, Connection, Trust: A zine about developing a security culture based on trust and connection. *itsgoingdown.org/confidence-courage-robust-security*

Counter-Surveillance Resource Center: A database of surveillance techniques, their uses, and how to protect against them. Helpful for threat modeling or learning more about security, digital and otherwise. c*src.link*

Cover Your Tracks: A website from the EFF that shows you what information your browser and most websites can see about you and your device. *coveryourtracks.eff.org*

Electronic Freedom Foundation (EFF): An organization dedicated to digital freedom and privacy for everyone. Has many online resources about digital security, both simple and complex. *eff.org*

Elle on Threat Modeling: A podcast episode discussing an overview of threat modeling. From Live Like the World is Dying, hosted by Margaret Killjoy. *live-like-the-world-is-dying.pinecast.co/165a27f6/elle-on-threat-modeling*

Extreme Privacy: What it Takes to Disappear, Chapters 1 & 2 (4th edition): A book from a private investigator about privacy in many areas of life. Chapter 1 is about computers; chapter 2 focuses on mobile devices. Includes information comparing and contrasting privacy of different operating systems. *inteltechniques.com/book7.html (or LibGen, PirateBay...)*

Phone and tech security is often the least important part of a plan... until it isn't. If you or your device(s) are under criminal investigation, this stuff really matters. And if you haven't thought about any form of digital security until you are arrested... Uh oh.

Disclaimer: This zine is written by anarchists for people who face legal investigation or repression in the United States. However, it may be helpful for anyone who wants to reduce the data that cops or companies have about them. It should also be considered a 101-level document; the tips in this guide are the most basic steps you can take to protect yourself and your data. If your enemies are very powerful or potential consequences are very high, spend some time threat modeling[1] and create a security plan for your specific needs.

Phones and digital surveillance are unlikely to be the thing that gets you in legal trouble. However, once you are already known to law enforcement or other enemies, or the cops know a crime has taken place, digital data is one of the first places they will look for evidence. If your data can be accessed retroactively, it may be used in a legal case against you or people connected to you. And, if user data is easy to access (as is the case for location data obtained through geofence warrants[2] and hyper-specific internet searches), it may be used to narrow the suspect pool.

The best way to ensure your internet history, location data, cell phone use, saved files, and other digital activities cannot be used against you is to make the data inaccessible to your enemies. Even better, make sure the evidence never exists in the first place. Think of the steps that go into planning and executing an action:

- Have an idea
- Do research
- Talk with friends/form an affinity group
- Acquire materials

1 Threat modeling: evaluating what threats exist, their likelihood, and potential consequences. Here's a podcast episode (with transcript) about it: live-like-the-world-is-dying.pinecast.co/165a27f6/elle-on-threat-modeling

2 wikipedia.org/wiki/geo-fence_warrant

- Transportation to and from location
- Publish communique (if desired)

You can minimize or eliminate tech use for all of these! The most secure form of communication is face to face in an unmonitored area. Learning materials may be available as hard copies. When obtaining supplies, pay in cash or don't pay at all. Make sure any cars you use don't have GPS tracking from the manufacturer—or don't use cars. Publishing a communique is one step where tech use may be needed, but can be done safely using Tails[3] and Tor[4].

PEOPLE

Why does a zine about digital security have a section about people? Statistically, your biggest threat BY FAR is people: bragging after an action, suggestive not-really-hypotheticals shared with strangers, suspicions from uninvolved friends/partners/family, intentional cooperation with law enforcement, etc. And, before you jump to tech security next, consider many threats like cameras at the scene, license plate readers on surrounding roads, whether your physical features are covered or disguised, and forensic evidence like hair/DNA/fingerprints that have nothing to do with tech use.

The best security measures you can take? Genuine, lasting relationships where everyone feels safety, care, and trust. And shared norms[5] that include refusal to cooperate with law enforcement. Carefully consider how and why you trust certain people in specific ways, then act accordingly.

3 An operating system that leaves no digital evidence on your computer. Learn more and install at tails.boum.org

4 More on this later

5 Sometimes called "security culture"; read more on any anarchist website or zine catalog. For example: itsgoingdown.org/confidence-courage-robust-security

If your device is returned after a serious felony arrest, especially after a long period of holding by law enforcement, trash it. It could have new additions like a keylogger which tracks every key you press, constant audio recording, or other malware. Seriously. Get a new phone or computer.

SUMMARY

- Turn your phone OFF, especially if a law enforcement interaction or arrest is likely
- Use long alphanumeric (14+ random characters) or diceware (7+ random words) passwords—NOT 4 digit pin
- Use a password manager, with backups
- Social media is hostile—delete your accounts
- Stick to encrypted, open source, recently updated everything, as much as possible
- Use a VPN, Tor browser, and Orbot for phones
- Likely physical compromise? Get a new device!

Do these few simple things and you greatly reduce the risk of your data being used against you or your friends. Remove the low hanging fruit. Seriously. It's easy and takes maybe a couple hours. And the ongoing habits are worth getting used to now.

Imagine the relief when you are arrested and you know your phone is secure. Or in court when the prosecutor says there was no relevant data obtained from your computer or internet history. It's totally possible, and in most cases extremely easy. Do it now.

Besides the actual location setting, your location can also be surveilled through your internet connection. Accessing the internet without a VPN or Tor means your internet service provider and any website you visit can know your location.[31]

PHYSICAL ACCESS

Physical access, in this context, means that your phone or computer has been taken and held for some time by law enforcement.

This is probably unlikely to be an issue if you were arrested for something minor and "apolitical" (misdemeanors like shoplifting, trespassing, drug possession, etc.) and your device is returned to you when you are released within a couple days.

However, if you are arrested for political reasons, or on suspicion of a higher level crime (felony/ies), cops have more interest in your data. This is especially true if they believe you are part of "organized crime" or some kind of political leader. It could also come up if your criminal record includes charges like those, no matter what the most recent arrest is for. Known association with anarchists or suspicion of “radical” political beliefs may also make your data more interesting to them.

Phones and computers may be sent to digital forensic labs for months or longer, and can be kept indefinitely by local, state, or federal agencies.

30 Note that public computers may have spyware for administrators to monitor activity, live or retroactively. Make sure not to enter sensitive or identifying information in the same session as anything you want anonymous!

31 Check out iplocation.io to see if your IP location is visible and accurate. Also coveryourtracks.eff.org or webkay.robinlinus.com to see what information websites can see about you and your device.

Next? Make solid action plans that minimize or eliminate tech use, forensic evidence, and potential exposure of anyone's identity.

BuT WhAt AbOuT DiGiTaL SeCuRiTy??

Ugh, fine. That's what the zine is about, I suppose.

Another important security measure is having basic tech security norms, for yourself and your friends. Have a conversation—or several—about digital security practices and desired norms with friends and comrades. Maybe show them this zine.

Also remember you cannot control other people's security measures or lack thereof. However, you can (and should!) have boundaries about your interactions, digitally and in real life.

Especially in the context of large groupchats, or organizing that includes online components, people often have very different backgrounds and security concerns. In order to reduce information that other people could share about you, intentionally or unintentionally, YOU need to balance what info is available to them versus what is critical to communicate.

SO... WHAT DO I DO?

This zine suggests some basic steps you can take to greatly minimize risk to yourself and comrades when interacting with technology. There’s almost no limit to how deep the security rabbit hole goes, but most additional security measures come with some degree of inconvenience. The balance of these factors that feels worth it for you is a decision you have to make. But it should be an informed decision, and a conscious one.

It may help to think of each security improvement as reducing the likelihood that your digital footprint[6] could be used against you or your friends. Could you get to 0%? Sure, if you never use a phone or computer for anything and only associate with others doing the same. But that's not realistic or desirable for most of us.

It's better to use some safety precautions than none, but addressing all the obvious sources of risk makes you much safer overall. The following sections are an overview of low-bar security measures that make it MUCH harder for your data to be accessed. Even if you don’t adopt all these habits right away, any improvement you make is a good one! Just be honest with yourself and others about what risks are likely and make plans accordingly.

Here's an analogy for the climbey-wimbey firstie types: if you routinely go climbing with frayed ropes, no safety, and broken carabiners, eventually someone will get hurt.

If you follow all the recommendations in this guide, whichever cop is assigned to look at your phone or computer data will have a bad day. Maybe they'll quit their job... we can hope.

The reasoning behind most of these recommendations and specific information on how to execute them is outside the scope of this zine. But there are footnotes throughout and additional resources listed at the end. If you are unsure how to do something or want more info, look it up or ask a friend!

6 Digital footprint: All the digital information available about you, including internet presence and activity

Browser (especially in conjunction with a secure operating system like Tails[28]) is still the most secure way to use Tor.

LOCATION DATA

First and most obviously, consider if you really need to bring a phone wherever you're going. If you don’t need it, don’t bring it!

Turning your phone’s location on means that your precise GPS coordinates are tracked by your cell service provider. Having location off, but with cellular data, provides an approximate location due to communication with nearby cell towers.

It is debated whether airplane mode turns off the cellular radio—the part that communicates with nearby cell towers—on most phones. The only ways to be absolutely sure it is not transmitting this data are to have the phone off with the battery removed, or in a sealed Faraday bag[29].

Some suggestions for getting around without your phone:

- For navigation, look up directions before you leave. Write them down if there are many steps.
- If you go somewhere often, memorize the route. (Plus you avoid creating metadata about your routines!)
- Plan specific places and times to meet, then stick to them.
- If you’re in a public place and need to call someone or look something up, ask to borrow a stranger's phone. Write down or memorize important phone numbers.
- Use hard copy maps and public info like bus schedules.
- Use public computers, for example in a library or hotel business center.[30]

28 See footnote 3, or additional resource Tails: tails.boum.org

29 A Faraday bag (or cage) blocks electromagnetic signals like cell service, WiFi, Bluetooth, and RFID. More info: howtogeek.com/791386/what-is-a-faraday-bag-and-should-you-use-one/

Tor is safer when more people use it, and through public WiFi.[26] If you're in a public place, check for cameras that could see you, your keyboard, and the computer screen.

The most secure method is to connect to Tor using the Tails operating system[27] on a public computer (or public WiFi, on a secure personal computer) in an area without surveillance cameras, far from your regular location. Do not enter any identifying information, log in to personal accounts, or visit websites linked to you. Visit only the sites you need.

While websites might not see your personal data on Tor, they may know you are using Tor. Some sites won't allow access at all, or some features may not work. And if you enter personal data into a website, that website may record the data you enter regardless of what browser you're using.

ORBOT

Orbot is an app that routes all of your internet traffic through Tor, instead of just websites that you open in Tor Browser. This means all apps that access the internet, not just the browser, will do so through Tor. You can also select specific apps to include/exclude in the Orbot app.

Orbot can also be set as "always on VPN" in settings so you don't accidentally connect to the internet un-anonymized.

However, just like when using Tor browser, some features or apps may not work with Orbot. This issue seems rare, but may be an instance where you switch to a VPN instead. Additionally, keep in mind that while Orbot is a great tool, the desktop version of Tor

26 For an illustrative story about someone who was de-anonymized despite using Tor: forbes.com/sites/runasandvik/2013/12/18/harvard-student-receives-f-for-tor-failure-while-sending-anonymous-bomb-threat

27 See footnote 3, or additional resource Tails: tails.boum.org

ENCRYPTION

Encryption is complicated math equations that turn data from useful info into scrambled nonsense (and the opposite, decryption).

Data stored on a modern smartphone is encrypted when the phone is OFF, and before you enter your password for the first time after turning it on. Putting your phone in "sleep" mode (turning off the screen) is NOT the same and does not re-encrypt your data. If you think you might be arrested, turn your phone off. If you have been arrested and your phone is elsewhere, make arrangements for someone else to turn it off (in case there is a warrant to find and seize it).

On computers, you can encrypt the hard drive, in full or divided into partitions—this is very good to do. Same idea for flash drives, external hard drives, and anywhere else you store digital data. Even for content you think is innocuous, it still could be used against you or your friends. And why make the cops' job any easier?

Suggested programs: VeraCrypt for Mac and Windows, LUKS for Linux (default, not compatible with Mac or Windows)

PASSWORDS

Passwords should be 14+ random alphanumeric characters (upper- and lowercase letters, and numbers)[7], or 7+ random words (also called diceware, or a passphrase)[8]. Randomness, also called entropy, is part of why these are so secure; a 7-word phrase or 14 characters with patterns or meaning are not equivalent in terms of security.[9]

7 bitwarden.com/blog/how-long-should-my-password-be/

8 theworld.com/~reinhold/dicewarefaq.html

9 Suggestions for making passphrases: random word generator, a physical word list with dice (eff.org/dice), random numbers for pages and entries in a dictionary, or the "passphrase" option in your password manager.

Do NOT use a 4-digit PIN. Decryption tools and brute force guessing can decode shorter passwords in seconds to hours.

Once a phone is decrypted, common law enforcement tools like Cellebrite can download a full copy of all the data on it. There is plenty of data that can be downloaded from most devices without unlocking, but not nearly as much.[10] There are plenty of demo videos on YouTube showing the capabilities of Cellebrite and similar software.[11]

In order to keep track of many long, unique passwords (different ones for phone, computer, every account, etc.), use a password manager. This allows you to use a single password to open the file that contains all of your passwords. Many password managers can also generate passwords and passphrases for you when you add an entry. Needless to say, the password for your password manager file must be strong and needs to stay secret! Memorize it as soon as possible. If you keep a written hard copy, store it in a different location than the data it protects (and somewhere likely safe from police raids, seizure, or destruction). And make sure to keep backups of your password manager… or else you will be locked out of all your accounts.

Suggested password managers: KeePassXC on desktop, AuthPass or KeePassDX on Android

APPS

Having fewer apps is better; each app has its own potential security failures or exploits (or active data collection about you!). Instead of installing new apps for every service, consider if you can use a website in your browser. For the apps you do have, keep up with all software updates—these often address known security vulnerabilities.

10 youtube.com/watch?v=xBaIUvgrfro
11 youtube.com/watch?v=xLM19Y9QtXA

On a phone, you can enable "always on VPN" in settings to make sure all your internet traffic is routed through a VPN. This includes activity in a browser and also any app that connects to the internet. Helpfully, this also avoids your phone accidentally connecting to the internet when the VPN is off.

One downside of using a VPN is that it relies on trusting the VPN service provider. If they keep logs and sell your data, that's no good. Some VPNs free, some are donation-based, some are paid. Just make sure that the service isn’t free *because* the company stores and sells your data.

Suggested VPNs: RiseUp, Proton, Mulvad

TOR (The Onion Router)

Tor is a browser that anonymizes your internet traffic. It uses three layers to hide your data: entrance node, relay, and exit node. Tor browser is also available as an app for phones, though it is less secure than the desktop version.

Unlike a VPN, Tor doesn't rely on trusting a single service provider. And because there are many nodes around the world, it is extremely unlikely that one person or agency would control all three nodes that relay your internet traffic at any particular time.

Important note: Don’t use Tor and a VPN at the same time, unless you really know what you’re doing.[25]

25 Why? It’s complicated. But the Tor Project says so at support.torproject.org/faq/faq-5

SOCIAL MEDIA

Everything online, including on social media, is public and permanent. Companies like Meta (Facebook, Instagram), Apple, Alphabet (Google), Twitter (er...X?), etc. regularly comply with warrants about individuals' accounts. This means the company will hand over all your account data if any level of law enforcement asks them to.

If your profiles are public, literally anyone can look at whatever you post. This includes right wing fascist-types who want to dox you and your friends,[23] as well as cops and prosecutors. Unfortunately, many political and other organizations have a significant social media presence. Maybe this is a main way you get information about events or action camps, or find out about new campaigns. Tools like Nitter.net and ImgInn.com allow you to look at specific accounts on Twitter and Instagram without logging in (at least for now). On sites where you must have an account, you could have more anonymous access by making an account with minimal and random information, no connections with individuals or hyper-specific groups/pages, and only accessing it over Tor.

Overall, social media is generally very bad for security! Delete your social media accounts, especially ones where you voluntarily share photos of yourself and real information about your life.

VPN (Virtual Private Network)

A VPN gives you a new IP (“internet protocol”) address, which is the technical term for where your internet traffic appears to be coming from. It also encrypts your internet traffic so your internet service provider (ISP) can't see it.[24]

23 A zine on doxxing: crimethinc.com/zines/doxcare

24 Without a VPN, your ISP can see every site you access. This allows them to store and sell your data, report illegal activity (like piracy, downloading copyrighted items), and hand over this information to law enforcement.

Many phones, especially cheap smartphones, come with a dozen or more pre-installed apps. The assumption here is a tradeoff between cost and privacy; if something is cheaper, the collection and sale of your data makes up the difference in price. Uninstall all extra apps.

Different apps work on different operating systems like (stock) Android, iOS, Graphene[12], etc. and there are multiple ways to get apps. Most commonly, Apple devices use the App Store and Android phones use the Google Play Store. However, these are not ideal because they are tied to a specific account. Some people download .apk files (the typical app filetype) directly from online or other sources. One alternative, the F-droid store,[13] contains a range of privacy-focused apps. It isn’t free of security concerns, but there aren’t currently better alternatives for phones using stock Android or iOS. For full access to more secure apps and ideal installation methods, you need a different operating system (like Graphene).[14]

One specific app to consider is your smartphone keyboard. If you use the pre-installed Apple Keyboard or Gboard, these can record everything you type and even actively learn about your typing patterns (“predictive text”). Disable settings that allow automatic learning. Even better, install a secure third-party keyboard app like Simple Keyboard.[15]

12 A privacy-focused operating system for Pixel phones. GrapheneOS.org

13 An app store that prioritizes privacy-minded apps and informs you of “anti-features” like paywalls and surveillance of your activity. F-droid.org

14 privacyguides.org/en/android/#obtaining-applications

15 Simple Keyboard by Tibor Kaputa, part of the Simple Suite: f-droid.org/en/packages/com.simplemobiletools.keyboard/

SIGNAL

The good news: Signal is overall pretty good! Its encryption is solid, minimal user data is stored (so warrants don't give much useful info), and the source code is public. Signal is an accessible, widely-adopted method of relatively secure communication.[16]

However, one big concern for many is that your account is tied to a phone number. Get around this by changing your number in the app or making a new account using anything other than a phone number tied to your legal name.

Some options:

- Get a phone with a pre-paid plan and use it only to verify your Signal account, then get rid of it[17]
- Use a Google Voice number for a burner Google account
- Test out different VoIP[18] number providers until you find one that is compatible with Signal verification
- Use an eSIM service that lets you rent a number for a week

There are many options at different levels of anonymity, difficulty, and expense. You may need to re-verify this number at some point in the future if someone else tries to register a Signal account with the same number, so there are risks to setting up your account with a number you do not control.[19] However, it may be worth taking this risk, especially if you have limited resources and are in group chats that are likely under surveillance—for example: from members being arrested, infiltrators, or cooperators aka snitches.

16 Though Signal itself is prevalent, Molly & Molly-FOSS are “hardened” (more secure) versions of Signal. Learn more and install at Molly.im

17 Or keep it and renew the plan to maintain exclusive access to the number. Just be sure use of the phone doesn’t compromise your anonymity.

18 Voice over IP, a phone number that works over the internet. Some common providers include TextNow, TextFree, and Google Voice.

19 blog.privacyguides.org/2022/11/10/signal-number-registration-update

There are also many Signal settings that allow you to enhance your security on the app. Suggested settings to enable[20]:

- Automatic disappearing messages, and disappearing messages set to appropriate times in individual chats (including direct messages)
- No notifications, or minimal info in notifications ("don't show name or message")
- Don’t allow screenshots of chats—it doesn’t matter how quickly the messages disappear if someone takes a screenshot!
- Screen lock: requires your phone password again to open the app

Think you or your device are imminently getting arrested? Turn off your phone!!! This (or factory reset) is the best way to keep the info in your Signal account from falling into the wrong hands.

Now the bad news: like any third party app, using Signal relies on trusting the service provider. While Signal collects minimal user data, it’s still not zero data. And any centralization of infrastructure presents an opportunity for significant disruptions: What if there is a digital attack that temporarily disables signal for all users? Or all the physical infrastructure is seized? What if the organization runs out of money and stops services that allow the app to function?

Let this be a reminder to form real, in-person relationships with people when possible. And maybe look into backup or alternative options, like Briar or Cwtch.[21] PGP encryption[22] is still solid too, even though the technology is over 30 years old!

20 For additional recommendations on Signal settings to increase security (“hardening”): blog.privacyguides.org/2022/07/07/signal-configuration-and-hardening

21 More info on these, plus comparing and contrasting with Signal at itsgoingdown.org/the-guide-to-peer-to-peer-encryption-and-tor-new-communication-infrastructure-for-anarchists

22 PGP stands for “pretty good privacy” and is used to encrypt content like emails and files; read more at varonis.com/blog/pgp-encryption