Digital Security 2025

Advice for Activists, Journalists, and the rest of us

version 1.02, March 2025

WARNING: This is not legal advice. The authors are not responsible for your security or for the efficacy of the tools mentioned herein.

Please make sure you are using the most recent version of this guide. If it's more than about a year old, check for updates.

Want to jump straight to the recommended tools? Quick list is on the first inside page.

↓↓↓ this space reserved for your mailing information ↓↓↓

Digital Security 2025

Advice for Activists, Journalists, and the rest of us

version 1.02, March 2025

WARNING: This is not legal advice. The authors are not responsible for your security or for the efficacy of the tools mentioned herein.

NOTE: Please make sure you are using the most recent version of this guide. If it's more than about a year old, check for updates.

Want to jump straight to the recommended tools? There's a list on the first inside page.

ADDITIONAL RESOURCES

- The WIRED Guide to Digital Security: `www.wired.com/2017/12/digital-security-guide/`
- Freedom of the Press Foundation, Digital Security Education: `freedom.press/digisec/`
- The Electronic Frontier Foundation, Surveillance Self-Defense: `ssd.eff.org/`
- Activist Checklist, Security Essentials: `activistchecklist.org/essentials/`
- Privacy Guides, The Protesters' Guide to Smartphone Security: `www.privacyguides.org/articles/2025/01/23/activists-guide-securing-your-smartphone/`
- Reply All, What Kind Of Idiot Gets Phished?: `https://dcs-spotify.megaphone.fm/GLT9749789991.mp3`
- For an in-depth but accessible introduction to threat modeling, try the "Threat Modeling" and "Threat Modeling on Behalf of Sources" modules from the Freedom of the Press Fdn (freedom.press).

These links and more available at `protectedmode.pages.dev`

QUICK TIPS & QUALITY TOOLS

Start here for our top tips. OUTLINED tools are our favorites.

EMAIL. Gmail is extremely popular, and Google takes pains to protect your data from everyone... except themselves. Gmail is encrypted against everyone ***except*** Google (and anyone they might share with, or be hacked by). In fact, Google scans your email for keywords so that they can (helpfully) remind you about a meeting, or (less helpfully) target advertising to your interests.

END-TO-END encrypted email services are far more secure. PROTONMAIL is popular; it has very strong encryption and solid privacy practices. Others (like Tutamail) are at least as secure, or more so; sadly, they don't usually share encryption protocols, so messages from Proton to Tuta or Gmail are not (by default) encrypted.

PASSWORDS. Our #1 piece of advice: **Use a password manager** like BITWARDEN, and use the passwords and passphrases it suggests.

TWO-FACTOR AUTH. Use anywhere you can. Text (SMS) is easiest but least secure.

MESSAGING. SIGNAL gets the highest recommendation, since it is end-to-end encrypted, based in Switzerland (so other countries' courts can't get to it), & extremely secure. However, Signal may be blocked or even illegal in some places, and in other areas the government may assume that anyone using Signal is doing something illegal; be careful. WhatsApp is a good second choice; it's far more popular than Signal, and is also end-to-end secured, but it tracks a lot more info about you. WhatsApp is owned by Meta/Facebook, a company most security experts do not consider trustworthy.

Try not to use regular text messages (SMS/MMS), since they are not encrypted, and are easy to intercept. Both cell phone and landline phone calls are also insecure.

SEARCH. Instead of Google, try using privacy-focused tools like DUCKDUCKGO.

VPNs and TOR. These tools encrypt or anonymize your internet connection; see p10. If you think you might be targeted, you should be using one or the other. Again, however, some governments will assume that anyone using Tor (especially) is doing something illegal or suspicious.

NOTE: All of these tools are legal (at time of writing) in the USA. However, use of encryption-based tools may flag you as an activist, or otherwise lead to increased surveillance and risk. Proceed with caution. **Outside of the USA,** some of these tools, including Signal, Tor, and other encryption-based tools, may not be legal in your country; in other countries, they may be technically legal but may flag you as a problem, subjecting you to further scrutiny. Investigate the legal consequences of these tools before using them, especially if you are in an oppressive country.

"BIOMETRIC" UNLOCKING (face or fingerprint) is convenient, but be cautious. In the USA, authorities (like the police and the Transportation Security Administration, TSA) cannot (in most cases) legally require you enter your password. However, they ***can*** hold your phone up to your face, or press your finger to the fingerprint reader, to unlock it. Consider turning your phone off entirely while traveling; you may also want to disable Bluetooth and AirDrop.

Be cautious about **APPEARING TO GIVE CONSENT** by giving your phone to anyone (like TSA or the police). Handing over your phone or computer for even a limited purpose— for example, to show your plane ticket—**could be construed as giving access,** and you may have consented to their taking and copying all your data.

Sometimes you don't have a choice. Immigration officials have been known to require travelers to hand over and unlock their phones; you may be able to say no only at the cost of being sent home (or worse). An activist, journalist, or a lawyer in such a situation could be putting themselves or others in grave danger. Protecting your data against someone who has physical access to your phone or computer is a very difficult and complex issue, far beyond what this guide can cover.

Not carrying sensitive data is always the best defense.

For extra-high security, consider these travel tips:

- Log out of your email accounts before going through security—on your computer ***and*** on your phone. Web-based email like Gmail or ProtonMail should leave little local footprint once you've deleted your browser history and cleared your cache.
- Consider what data you can give up, and what you must keep safe: A regularly-used Gmail account might serve as a good decoy if you keep the most sensitive data in ProtonMail.
- If you store your work in the cloud, consider deleting it entirely from your computer while traveling, and reconnecting when you've arrived. For Google fans, a Chromebook, which can easily be reset to factory conditions, could be a good travel computer.
- As an alternative to the cloud, you might consider carrying data only on a portable external drive (SSD) or USB thumb drive. VERACRYPT is an excellent tool for storing encrypted data, and even supports multiple layers of encryption so that one layer remains entirely secret, and "deniable", even after you've given up passwords to the rest.
- Don't get too clever with the cloak-and-dagger stuff. If anyone, whether a hacker or a government, knows that you have data they want access to, it's only a matter of time and effort before they get to it. Remember, n**ot having sensitive data with you at all is the best way to protect it.**

access to everything you type, even on an otherwise secure platform like Signal.

Your computer & phone should both be password-protected; this is pretty weak security, but it will at least slow a hacker down.

Setting up **system drive encryption** will prevent hackers from reading data on your computer, even if they gain direct physical access. (Your phone will usually take care of this on its own.) MacOS's Advanced Data Protection will also encrypt your iCloud data and backups, but you have to turn it on yourself. Since ADP uses strong encryption, even Apple won't have access to your data once you enable it – nor will they be able to help if you lose your key.

MORE TIPS FOR SAFE BROWSING

When you're using the Web, remember that **your browser knows everything you're doing.** If you're using **browser extensions**, those may have insider access too. If you're vulnerable, or paranoid, research your browser choices carefully. Brave (which includes a good secure search tool) is one security-oriented choice; Chrome is famous for its hunger to track as much of your data as possible; Microsoft's Edge is surprisingly strong in many security tests; and Firefox, previously a leader in security and privacy, has recently been making conflicting statements that have raised concerns among security experts.

In **incognito mode,** your browser will not record your browsing history, cache copies of web pages, or save cookies or login information. Incognito mode is a great way to avoid leaving traces on on a public computer (like at a library).

It's easier to be sure who you're communicating with if you initiate the connection yourself. A call or an email from a bank or credit card could be a phishing scam. You can always call back at a phone number you are sure about—for example, dialing the number on the back of your credit card is a good way to ensure you're really talking to your credit card company. Similarly, it's better to type a web address yourself instead of clicking one that might be misleading, since there are many ways a hacker can misdirect your click. For example, the URL "www.loca1bank.com" looks ok, but that second "L" is actually the number "1". If you don't notice the difference, you could easily land somewhere you didn't intend.

TRAVEL AND PROTEST

If you're **ATTENDING A PROTEST,** special security concerns apply to your phone: It can be a serious liability, and may even be a way to track you. For example, it's easy for the phone company to see which cell tower you're connected to, thereby getting your location (even if your GPS is off). **Memorize a few numbers just in case**, get an old pocket-sized digital camera, and consider leaving the phone at home.

WARNING: This is not legal advice. The authors are not responsible for your security, or for the efficacy or correct performance of the tools mentioned herein.

NOTE: Please make sure you are using the most recent version of this guide. If it's more than about a year old, check for updates.

The internet gives you access to the world — but it also gives the world access to you. There are lots of dangers out there, from "script kiddies" messing around for fun, to semi-pro hackers trying to get your money or your data, to governments that just want to keep an eye on you—or who are actively targeting you. This guide will show you a few simple ways you can make your communications both safer and more secure.

THE OPEN INTERNET

The internet is open and anarchic by design. Your data is passed from one computer to the next in little hops, until it reaches its destination – which might be on the other side of the world – milliseconds later. Not too many years ago, this data was passed along unencrypted, in "plain text", and any one of those computers might take a peek at what you were sending. Emails were like postcards, there to be read by anyone along the way. Logging into your bank posed the risk that someone might be watching over your virtual shoulder.

As the net has become more critical to our lives and work, we've started to rein in this openness. Much of the data that gets passed along is encrypted now at least some of the time, preventing the people in between from reading it – or so we hope. But as we'll see, there are many different types of information, and many ways of getting access.

This guide by protected.mode, and is in the public domain (CC0).
Please share and reproduce. Many thanks to our generous reviewers.
Links and more available at protectedmode.pages.dev
Comments / tips / corrections? protected.mode.info@pm.me

THREAT MODELING

The most important aspect of security is to understand what types of attacks and attackers you might be concerned about; then you can adjust your defenses accordingly. This is **THREAT MODELING**. First, let's think about types of hacks.

RAMDOM HACKS. People and bots around the world are constantly pinging your computer and your phone, or poking at your network's security, or sending you lame phishing attempts. Your computer might turn away thousands of these attacks every day. These attackers probably just want your money, and don't know or care about you; most of their attacks are quick and easy, and if they don't work, they'll move on. After all, most of us, with little money or power, are not particularly attractive targets.

TARGETED HACKS. Of course, some people do have money or power, or the keys to a Bitcoin wallet, or critical business information, or the launch codes for a nuclear missile. These are much more valuable targets, and the attacks on them will be more sophisticated, more subtle, and much more persistent.

The motivation isn't always money. If you're an environmental or human rights activist, you might be targeted by companies who want to discredit you, or even kill you. Journalists investigating corporate or political actors are frequently targeted in attempts to intimidate them or prevent them from publishing. Attacks might come from corporations, or from governments or government-linked groups (like North Korea's Lazarus Project), or from independent groups of hackers (like the Anonymous collective or the Conti ransomware group). Defending against attacks by professional or semi-professional hackers requires a great deal of expertise and caution, especially when the consequences can be so grave. This guide can only be a beginning; see the resources list (front cover) for more.

SURVEILLANCE. It's no surprise that companies try to learn as much as they can about us, usually just to target their ads more precisely. To do so, they use a complex array of cookies, trackers, etc. These can be extremely accurate.

> Retail businesses pay a great deal of attention to your purchases. In a famous case in 2011, a marketing computer analyzing purchases at the US retail giant Target concluded that one regular customer – a teenage girl in Minnesota – was pregnant. Target began to send her pregnancy-related ads and coupons, enraging her father, who learned only weeks later that Target was correct. In fact, marketing computers can usually estimate an accurate due date based *only* on purchasing information.

SOCIAL ENGINEERING

We usually think of digital security as being a technical issue, but in the real world, many (or even most) "hacks" happen through **social engineering**: By tricking you into clicking on something, or revealing something, that gives the hacker access.

Phishing is an extremely common form of attack that attempts to extract valuable information (passwords, bank accounts, etc) by impersonating a trusted source (like your bank). Phishing is very common in email, but can also occur in text messages, or even QR codes. Similarly, the endless Facebook "quizzes" in which you enter your middle name, or the name of your first pet, to reveal your "stripper name"—these are just collecting data on you. Avoid them.

Even more convincing is **spearphishing**, which uses targeted personal information. Any hacker in the world can get your address, find a picture of your house, & claim that they have lots of private info about you. (They do not.)

A **ransomware** attack encrypts your computer, and demands a large payment to give you your own data back. This is a good reason to have very good backups.

A **romance scammer** connects with their victim on a dating site (or elsewhere), and builds trust until that connection can be exploited. A similar scam, called **pig butchering**, pulls in its victim with proven investment advice, building trust over months or years until they can extract every possible cent.

SECURE YOUR PHONE AND COMPUTER

Many hacks start by gaining access to your phone or computer itself. From there, they can read just about anything. The best thing you can do is **keep your operating system up to date** with upgrades and patches. On Windows or Mac, you should leave "automatic updates" on. Don't procrastinate these. (Phones will usually update on their own.)

Both Windows and Mac come with strong built-in security (Microsoft Defender, XProtect). You shouldn't need additional virus/malware protection unless you have specific concerns. And although obvious, it bears repeating: Be extremely careful of shady websites.

In general, iPhones are considered far more secure than Android phones, which give both the user and the apps a lot more control. Apple also has a pretty good history of resisting direct court orders to release user data.

Apps are a real challenge to phone security. If you're really concerned with security, limit your apps as much as possible. Some apps can introduce surprising vulnerabilities: An app that lets you edit your keyboard shortcuts can have direct

governments (again, Telegram).

Email has almost always been unencrypted. On a web-based email system like Gmail, your computer's connection to Google's mail server is encrypted (using https). But once that message reaches Google's servers, your data is back "in the clear" and can be read by Google—and by anyone Google gives access to, and anyone who might have hacked into Google's system. For most people, most of the time, this is not a major worry, and Gmail (and similar systems) are secure enough. In fact, there are advantages to the fact that Google has access to your message text, since it can keep an eye out for calendar events, airline tickets, and other things it knows how to help you with.

For vulnerable activists and journalists, and for the paranoid crowd, you want **truly secure, end-to-end encrypted email**: Strong encryption of the message on your computer or phone that can only be decrypted by your correspondent. That way, no one in between—not Google, not your local cafe hacker, not the National Security Agency, not even the email provider itself—can read the encrypted text until the recipient decodes it.

The leading provider of end-to-end encrypted email is PROTONMAIL, which offers both free and paid accounts (as well as other useful tools). A message between ProtonMail users is end-to-end secure. However, these platforms are not usually compatible: A message between Proton and Gmail, or between a ProtonMail and a Tutamail user, is (by default) **not** secure.

For the tinkerer, consider using the PGP PROTOCOL. PGP ("Pretty Good Privacy") uses public-key cryptography to encrypt any data so it can be sent securely through email or almost any other channel; but your recipient will need to have PGP, too, and many people find it challenging to use. The GNU PRIVACY GUARD (GPG) is a good place to start. Other tools, like Mailvelope, encrypt messages with PGP so you can send them through insecure channels.

Search. Your searches say a lot about you. Instead of Google, use a secure, privacy-oriented search tool like DUCKDUCKGO or SwissCows.

Maps. Some maps (OsmAnd, Apple Maps), have better privacy protections.

Discord & Slack use secure connections, but they are not end-to-end secure, so you're trusting them with your data.

> In 2012, a well-known middle-aged British physicist ended up in an Argentine jail when he flew to Buenos Aires to meet his new internet girlfriend, world-famous bikini model Denise Milani, and was tricked into (unwittingly) bringing two kilograms of cocaine.

Sometimes the information about us becomes the product for sale, as when campaigns try to manipulate voters during an election, or when an insurance company decides to cancel coverage just before a claim is filed.

And then there's government. Local police justify their increasing use of surveillance and wiretaps by the need to track and catch their targets; national agencies like the CIA and NSA justify their far more comprehensive surveillance tools by the hunt for drug smugglers or terrorists. The result is an ongoing and extremely intrusive global surveillance system. The Five Eyes (FVEY) countries, who now number 14, use high-tech monitoring technologies to intercept, sift, and analyze a huge proportion of the world's phone and internet traffic – skimming for key words, or making global maps of who talks to whom. Though it sounds like a conspiracy theory, the evidence for these activities is incontrovertible. Many people see this as an intrusion on their basic rights of speech and privacy. For journalists, critics, and activists, it may represent a life-threatening risk.

When thinking about the types of attacks you might be subject to, consider these categories. Who might attack your data or your communications, and why? Are they hoping to charge a new iPhone to your credit card, or do you have a million-Euro Bitcoin wallet that merits much more time and effort? Do you represent competition for a local business – or an existential threat for a global corporation? Have you spoken up against human rights abuses, or about government malfeasance?

You'll never have perfect security; fortunately, most of us don't need it. Most hacking is random, and most of us are not very lucrative targets. But if your opinions or your work put you at odds with large corporations or corrupt governments, you'll need to be far more cautious.

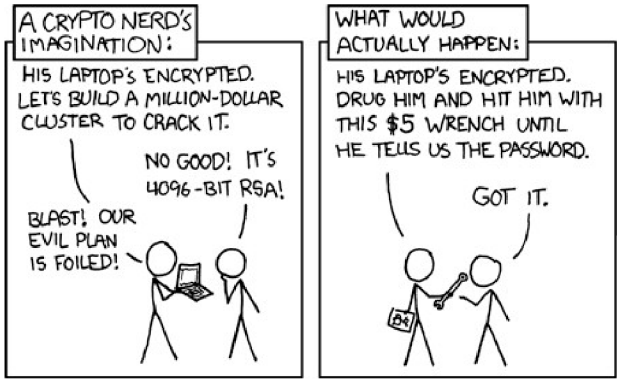
> There's an old joke about two hikers who run into a bear. The first hiker dumps their backpack and prepares to sprint away. "You can't outrun a bear!" the second hiker says with some puzzlement. "I don't need to outrun the bear", the first hiker replies, "I just need to outrun you." The same is true of digital security. Most of the time, you don't need to outrun the bear; you just need to be a little bit more difficult to hack than everyone else. If you're a journalist or an activist, of course, be ready – you may need to outrun that bear after all.

Your threat assessment will be different for different types of information. Your Sonic fanfic may not need much protection, but your bank account does; and a journalist's communication with a confidential source might be the most sensitive of all. What information can go into an email, and what should only be shared on

Signal? Is there anything that should not be written down at all? Consider also where and when you're vulnerable, and by what means. An unsecured Wi-Fi network in an airport terminal may not be the best place to do your banking. It might be ok to log into Instagram and scroll for a bit while you're waiting, but if someone else on the network grabs your Insta password, it had better not be the same as the one for your bank.

SECURE YOURSELF

Social engineering (see p13) is an extremely common way that people get hacked; but don't forget to consider your **physical security**, and the physical security of your devices. The best security tools won't do you any good if someone grabs your unlocked phone from your hands, or sits down in front of your unlocked computer. Lock your computer, or shut it down, when you're away from it. (The webcomic xkcd, an endless source of security tips, made this point vividly.)



An important lesson on practical threat modeling from xkcd.com .

In 2006, whistleblower and retired AT&T technician Mark Klein revealed that this unmarked door at a major AT&T internet facility in San Fracisco hid a roomful of internet surveillance equipment. The surveillance center, run by the National Security Agency, was attached directly to the network backbone, with AT&T's knowledge and consent. Klein and many others have alleged that similar sites exist around the country (see for example, "The Wiretap Rooms", *The Intercept*, 2018).

SECURE YOUR COMMUNICATIONS

Communications tools use many different protocols to carry data over the phone network or the internet. However, **some countries may prohibit or regulate the use of some of the following tools,** or may just find it suspicious if you use them. Know your local situation before adopting new tools.

Basic phone or text communications, whether over a landline or a cell phone, is laughably insecure. Assume that everyone is listening to your calls and reading your texts. (2024's huge SALT TYPHOON hack broke into US telecom providers using a "back door" that was originally created decades ago so that the US government could intercept phone traffic.)

Messaging. The gold standard of secure messaging is SIGNAL, a text-message-like tool which uses end-to-end encryption for all data (and nearly all metadata). Signal is based in Switzerland, so it can avoid court requests from most other countries. It's free, and also offers (secure) group chats as well as (secure) voice and video calls. If your country blocks Signal, you may still be able to use its built-in Censorship Circumvention and TLS Proxy tools.

> **Note: Signal does require a phone number to sign up,** but you can hide it after that. Once you've signed up, you can create a Signal username, and give that out to your contacts. At that point, you can change two settings: One will hide your phone number, and the other will prevent people from searching for you by phone number. If you can't risk letting even Signal know your number, you can sign up with a burner phone, or even with a virtual number like Google Voice. One resourceful reporter was even able to set up a Signal account using a pay phone. ("How I Got a Truly Anonymous Signal Account", *The Intercept*.)

> **Caution:** In some places, Signal may be prohibited or frowned upon, and simply having Signal installed on your phone might put you at increased risk. If that's the case in your area, consider using WhatsApp instead.

WhatsApp is an extremely popular end-to-end messaging system that also includes voice and video chat. It's based on the same encryption as Signal, but it stores much more information about you, and mayeven link you to your Facebook profile. WhatsApp is owned by Facebook/Meta, which security folks consider untrustworthy, and this makes them nervous. Use Signal if you can.

There are **many other messaging apps**, but we wouldn't recommend that you try any of them without a very good reason. Some have questionable technical security (e.g., Telegram), and some are very open about sharing data with

with a lot of information that could put you or others at risk. The same is true of Gmail or Google Docs: You're trusting Google with direct access to data, and you're also trusting that they won't share it, and that they'll never be hacked.

Several different types of tools can at least partially address these problems.

A **VPN (Virtual Private Network)** establishes a secure connection, sometimes called a "tunnel", to a computer somewhere else in the world, and channels all your traffic through that connection. This secures your data and metadata from your local ISP and other local observers. (It's also useful if you want to appear to be located in another country; for example, you need to access a site available only from a specific location.) There are many free VPNs, but paid ones will be faster (and probably more trustworthy). NordVPN and Surfshark are popular choices. A VPN is great for **privacy and security,** but notice that you are now putting a great deal of trust in your VPN provider. (You may find that you get odd problems with some websites when using a VPN; a few won't let you access them at all via VPN.)

The **Tor (or Onion) protocol,** by contrast, bounces your connection through a number of random, anonymous nodes, resulting in a (hopefully) untraceable connection. Tor is great for anonymity, since each computer knows about only one step in your data's journey, and unlike a VPN, you don't need to trust any one provider. (On the other hand, the multiple-hop design of Tor slows down your browsing considerably.) Tor is useful, for example, when connecting to the dark web, and may help you circumvent censorship or internet blackouts. (Unfortunately, many Tor network sites appear to be owned by the US National Security Agency.) To use Tor, download the (free) TOR BROWSER and stick carefully to its recommended settings. Tor is the best solution for true **anonymity** online.

Caution: Your internet service provider (and possibly other local observers) can tell when you're using a VPN or the Tor network. In some places, this may be suspicious or even illegal. Find out before you use these tools.

Lastly, there's **End-to-End Encryption (E2EE)**, the **only** reliable way of communicating without the need to trust any intermediaries. Your computer encrypts, the recipient decrypts, and no one in between can see your data at all. When you write a Gmail message, Google has direct access to what you've written; when you write a ProtonMail message, it's encrypted before it ever leaves your computer, and Proton cannot see it. Even if a court ordered Proton to turn over your information, Proton can't access your data, and can't break its own encryption. Similarly, Signal's E2EE ensures that even Signal itself can't access your data.

PASSWORDS and TWO-FACTOR AUTH

Most of us now have dozens of passwords for websites, accounts, and apps; many people reuse the same password across many sites. But sites are hacked every day, and those hacked passwords are shared that so even the most amateur hacker can try them out on other sites and accounts. Literally billions of cracked passwords are publicly available on the net.

We suggest a simple rule of thumb:

If you can remember your password, it's not secure enough.

Instead, **use a password manager,** a program that generates very strong passwords and remembers them for you. BITWARDEN, NordPass, & many other free or paid password managers are available. Of course, you'll need to remember at least one password – the one for your password manager! – and it had better be ***very*** strong.

Guides like this one usually spend a lot of time explaining ways to make sure your password is strong and secure. For example:

- **A good password** should be as random as possible, and as long as feasible. It must also be unguessable: Never use your dog's name or your kid's birthday, no matter how many random characters you add. It's best to use the highly random, nonsensical passwords suggested by your password manager, and let it remember them for you.
- Many experts now recommend **passphrases instead of passwords**. A passphrase is a set of random words, rather than the random characters of a password; there are so many different words available that a half-dozen word passphrase is utterly unguessable. (Never choose a phrase that appears elsewhere, like a favorite Taylor Swift lyric; even if you modify a common phrase – "2 B or not 2 B" – you're making it too easy for hackers.)

But wait! This **one weird trick** can replace all other password advice:

The human brain is exceptionally bad at thinking of "random" words (or numbers, or anything). Instead of trying to come up with something clever, **it's always best to use passwords and passphrases suggested by your password manager**—and then let it remember them for you.

TWO FACTOR AUTHENTICATION

Two factor authentication (2FA) is an extra step, after your password, during the login process. This ensures that even if a hacker gets your password, they won't be able to access your account. 2FA depends on **something you know**—your password—and **something you have**—your phone or security key. It comes in several flavors:

- A code sent by text (SMS) to your phone. This is the most common approach. It's better than nothing, but there are ways that a dedicated hacker can gain access to your texts, bypassing the 2FA. If you're vulnerable, exercise caution.
- An authenticator app on your phone, like GOOGLE AUTHENTICATOR or (with better privacy practices) 2FAS or Aegis. Authenticator apps generate one-time passcodes that you use to log in, instead of getting a code via text message. These are very secure, highly recommended options for the websites and apps that support them.
- A security key (e.g. from YUBICO). This is a small USB stick carrying a unique code that logs you in. Although it provides very high security, keeping track of the key may be a concern; if you lose it and don't have a backup, you could be locked out entirely.

Passkeys. Some websites, including Gmail, are now switching from passwords to passkeys. These use an encrypted virtual "key" that is securely stored on your device to log you in; it's very much like using an incredibly complex password, but there's no chance you can remember it, and no chance anyone else can guess it. If you decide to use passkeys, you can (and should) use your password manager to store them.

The ECHELON station at Menwith Hill, UK, one of several major facilities around the world used by the FVEY to intercept & read most internet traffic.

SECURE YOUR CONNECTION

Not long ago, most data was sent over the net unencrypted. Today, much of it is encrypted—encoded so that only those with the key can unlock it—but the complexity of the net means it's often encrypted for only part of the journey.

The first step is the connection between your computer and your router, which connects you to the internet; this is usually over Wi-Fi. If you're on your own Wi-Fi network, make sure it's password protected.* If you're on someone else's Wi-Fi, you have less control; you'll need to secure the internet connection itself by encrypting the link(s) between you and your destination.

** Note for real nerds: Use WPA2 or WPA3, not the much weaker WPA or WEP; and if at all possible, make sure your router's administrative interface itself has a good password.*

When visiting a website, ensure that your connection to the site is secure. A lock or a drop-down menu next to the address bar in your browser will confirm that the connection is securely encrypted from your computer to the website host. In 2025, most sites should be secure (**https://** instead of **http://**). For the average non-activist, non-journalist user, this might be an acceptable amount of security against simple snooping.

LEVELING UP

So far we've addressed only the most basic security measures to protect your Wi-Fi connection (the radio signal linking your computer to others physically nearby) and your internet connection (the virtual link, over any number of physical links, to a destination on the internet). Major insecurities remain.

- **Metadata.** Your data passes through numerous routers, switches, and other devices as it makes its way across the net. Even when your data is encrypted, these devices can usually see where it's coming from, where it's going, and more. This info, which is not your data but describes your data, is called **metadata**. For some people, metadata is not a major concern; but if you're working with a human rights activist in an oppressive country, and need to protect their identity, your metadata alone may put them at risk.
- **Trust.** Even when your connection is encrypted, your internet service provider (ISP) knows who and where you are, and probably has a good idea what type of data you are transferring and where it's going. Thus, you're trusting the ISP