Self Defense in a Hostile Digital World

This document presents a grab bag of actions you might consider to improve your personal digital security.

It's a long (and incomplete) list, reflecting complicated times. Remember though, you're striking a balance between convenience and security. The goal is to gain awareness and build "good enough" defenses, not to end up in a steel encased bunker wearing a tin foil hat.

If nothing else, strongly consider implementing the highlighted actions below.

Hardening Your Accounts

Here are some steps you can take to ensure your data isn't easily accessed or modified by attackers.

Password Protect Your Devices

All devices you use (PCs, laptops, tablets, phones) should require a password or PIN. For those that use a password, consider using a nonsensical phrase of words ("pass phrase") like "hybridllamasareFishy", something you can remember but that is not easily guessable (the longer the better, but convenient).

For PIN devices like phones, use a minimum of 6 digits, 8 if you're doing very sensitive work.

Biometrics (fingerprints, Face ID) may be used as well, since you can quickly force your device back to requiring a PIN (described later).

Install Device Updates Diligently

Software security vulnerabilities are inevitable. Once discovered, they're added to the menu of automated hacker scripts that are tirelessly looking for victims.

It's a never ending game of cat and mouse – platform providers like Apple, Google, and Microsoft are constantly finding and fixing these. But in order to benefit from their work, you must turn on automatic updates, and pay heed to those "red circles". Sometimes automatic updates fail to install, so if you continue to see an indicator for a day or two, update manually from your system settings app.

Practice Digital Hygiene

In addition to the system vulnerabilities platform providers are constantly patching, apps can be have issues too, especially those managing complex documents that run code. When they do, attackers can gain control of your device simply by getting you to open a wickedly designed document (e.g. Adobe's PDF, Microsoft's Word and Excel, etc.). This is why emails and texts containing attachments can be dangerous to open. Beware - attackers have become adept at creating plausible reasons for you to open attachments. When you receive an unprompted document, **always** take a beat and ask yourself, can I get this directly from a trusted source?

Uninvited links are even more concerning. In addition to possibly luring you to a compromised web page, attackers also may invite you to what appears to be a service you use, then have you unknowingly provide compromising information. They are getting ever more clever at representing commonly used services like iCloud, FedEx, or Charles Schwab, at times you might expect to receive a notice, with very plausible requests. Always treat incoming links as suspicious. If they are from a service you know, don't click the link, go directly to the service and look up the request.

This includes QR codes (the square images made up of dots that you scan with your phone), as they are just links in disguise.

By the way, this also includes incoming phone calls – you should be wary of unsolicited calls that ask you for personal information. When they do, get their contact information, and call the trusted source they supposedly represent.

Avoid Dark Alleys

It's common sense but worth emphasizing: as with the physical world, stay in the light. Ads that inform you your computer is infected, or provide too good to be true offers, free trials, crypto/gambling ads, porn, illegal activities, etc. – your best move is to turn around and walk away. These may well result in a costly, embarrassing, and stressful visit to the Geek Squad.

Be Wary of "Antivirus Software"

If you suspect your machine is compromised, seek a professional. Valid useful tools do exist, but you won't be able to discern whether they're legitimate, and they will require full access to your machine in order to do their work. If antivirus was provided directly with your operating system, it might be worth using. Otherwise, it's hard for even the most knowledgeable users to verify – code is just too complex.

Use a Password Manager

When you share a password across accounts, they all become vulnerable together, especially if they also share a username. Using a service-specific variation in your passwords ("123google", "123schwab") is also no longer a secure approach.

And sadly, we as humans are demonstrably poor at generating secure passwords.

Instead: install a password manager, and have it generate and remember unique passwords for each of your accounts. **Important: this will be protected by its own master password, which is now a single point of failure for all your passwords** – it is *critical* this password be memorable to you, but very difficult to crack. A pass phrase is again your best bet here.

Add 2 Factor Authentication to Critical Accounts

Passwords are a first line of defense, but they can be compromised. Like adding a deadbolt to your front door, you should add a second lock ("authentication factor") to critical online accounts. This is often referred to 2FA. Common options offered by your services include:

Type	**Available Products**	**Security Quality**
Physical Key Fob	Yubi, Google Titan, NitroKey	Best
Authorization Apps	2FAS, Google Auth, Microsoft Auth, Ente Auth *Note: Authy is no longer recommended*	Very Good
SMS		OK – vulnerable to SMS spoofing
Email		Poor – vulnerable to email spoofing

Banking/retirement accounts are of course critical, but be sure also to secure your email provider, your phone carrier, and large data services like iCloud or Google. These gateway accounts, once compromised, can themselves be used to access the rest of your data.

Encrypt Your Disks

If someone gains physical access to your device, your data is vulnerable. Encrypting it makes it much harder for attackers to actually view.

Most phones and tablets are encrypted by default. Modern PCs and laptops offer this as an option. Note that external disks, like backups, or phone external storage SD cards may not be encrypted!

Secure Your Cloud Data

Be aware that your device may be quietly syncing data with a cloud service provider, for your benefit. Microsoft, Google, and Apple all sync calendars, photos, drives, etc. Of these, Apple and Proton are the only ones that allow you to encrypt your data such that they can't access it.

Much of Apple's data is encrypted in the cloud, but there's a catch – if you back your devices up, the backup is vulnerable, unless you enable a feature called Advanced Data Protection that allows you manage your own encryption keys for most of your data. Warning: this is not without risk – if you do this, and lose your encryption keys, **you lose access to your digital data!**

Freeze Your Credit

To thwart attackers seeking to take out credit in your name, you can freeze your credit with the credit agencies Equifax, Experian, and TransUnion. This prevents banks, credit card companies, etc. from opening accounts in your name.

It does require that you remember to unfreeze it whenever you seek credit of some kind.

Minimizing Your Digital Footprint

We all expose considerable data publicly as well, sometimes intentionally, often unknowingly. It can be useful and important to make your voice heard, but minimizing unnecessary exposure is good digital defense.

Sobering but true: when connected to the internet, you are constantly under surveillance from multiple parties. It may be the app you're using (Apple News, Spotify, NY Times Games, Chrome), the service providing internet access (AT&T, Comcast), or indirectly, using analytics installed in the data sent back to you (Google, Meta). This data is tirelessly logged and mined. To be clear, much of this is not with nefarious intent, but it does leave a trail. While to some extent inescapable, there are steps you can take to minimize it.

Consider the Business Model

For any service or app you use, consider how they make their money. Google and Meta, for example, are mostly free in exchange for learning as much as they can about you, whereas Apple advertises themselves as up front expensive but privacy oriented. Microsoft is a bit of both.

Also, many say they're privacy friendly, but only those taking serious measures to ensure it (Apple, Proton, Brave) can be relied upon. Your data is only a hack or subpoena away from being public.

Apps

Apps can quietly harvest and forward whatever information their host operating system allows them to acquire. This is why it's important to only install reputable apps, and minimize the permissions they are granted (e.g. access to location, photos, contacts, calendar, etc.).

Also, consider the data you consciously provide to them as vulnerable. Dating apps, therapy apps, AI chatbots, fitness apps… your private information is only a subpoena or hack away from being public, as the users of Ashley Madison (cheater dating) and uMobix (stalkerware) are now acutely aware!

The Web Browser

The browser (Chrome, Safari, Edge, Brave, Firefox) is more private than apps. Given the choice between going to a web page or installing an app, if the web experience is acceptable to you, prefer it.

It's still not private though – some browsers (Chrome, for example) are not privacy oriented, and may share information directly. Further, identifying breadcrumbs called cookies can be used to track you across pages. Worse yet, even if you disable cookies, your device can be "fingerprinted" like a typewriter to uniquely identify you. If you are signed into Meta or Google, and go to a completely different website even from a different tab, it's entirely likely they'll know, since injected ads can contain their code.

Some steps you can take:

Use a privacy oriented browser	Consider using Brave, or in the Apple ecosystem, Safari with ad blockers. Both of these are hard at work trying to minimize fingerprinting.
Use private ("incognito") tabs	Using these **does not** hide your activity from the sites you contact or from your internet service provider, but they do prevent history from being accumulated on your device, and by clearing cookies, they also create a new web "identity" for you each time a tab is created. (Note they do not prevent fingerprinting)
Use a VPN	A VPN allows you to hide all your internet traffic from any potential prying eyes, be they someone on a shared sharing Wi-Fi network or your cable company. It also prevents the service on the other end from acquiring your actual IP address, and thus your rough location. It does this by sending all traffic encrypted through a middleman (the VPN provider), which in turn forwards it to and from the actual destination. The good news is that this is an effective, well supported, and commonplace technology. The bad is that if the middleman is nefarious, you are actually **less** secure than if you hadn't used one, since they can see all your traffic. If you must use one, do your due diligence first. Some people also use VPNs to fool a destination service regarding their location (e.g. to watch a football game outside your region)
Private Relay	If you pay for iCloud services, you can enable Apple's Internet Private Relay. This acts effectively like a VPN for web traffic, automatically.

Web Searching

When we search in the browser, we are engaging with a service that is likely logging and accumulating that information. You can minimize that by using a privacy oriented search engine:

Search Engine	Cost	Data Source
StartPage	Free	Google
DuckDuckGo	Free	Bing, DuckDuckGo
Swisscows	Free	Bing, Swisscows
Kagi	Paid	Kagi, highly focused

AI Chatbots

The enticing power of chatbots like Gemini, ChatGPT, and Claude can easily lull one into sharing extensive personal information. The companies behind these do offer "incognito mode" sessions, which they assert to mean your conversations are not used for training, and are not associated with your account. While it is less convenient (you can easily lose long useful discussions), you might also consider using private tabs for each session, and closing them when done.

Social Networks

While useful and compelling time sinks, social networks can expose considerable personal information:

- For photos of sensitive locations like your home, you should consider location "metadata". Some services hide this information publicly (Facebook, Instagram), but keep it themselves. Others (Google, iCloud Photos, email) leave it in. Signal strips it automatically. Note most phones have a Remove Location on the share sheet these days.
- Watch out for sharing time sensitive data, like your plans/snapshots when on a trip. If an empty house will be vulnerable, wait until you get home.
- Beware sharing personal data in public. Often this knowledge can be used to gain trust either directly with you or others.
- Sharing images of yourself or others exposes them to facial recognition. Consider that machines are learning who we are, where we go, and who we are interconnected with. And they won't ever forget.

Use Aliased Email Addresses

An email address is unique like a social security number, so it can be used as a way to identify you in a Google search. If you use the same email address across multiple accounts, the accounts can be associated with each other, allowing attackers to build a profile of you.

In addition, if a service is hacked, and you share passwords, the hacker can simply try using the hacked email address with its password on various services until it finds a match. (Of course, you don't share passwords across accounts anymore, right?)

To avoid these issues, there are various services that allow you to generate a unique email address for each account, forwarding them to a hidden actual email address.

As a bonus, these provide a kill switch – you can silence any spam you might end up receiving. It can also be entertaining to track where your email address is being shared. Some options:

Apple Hide My Email	Requires paid iCloud services and iCloud.com email account
Google Shielded Email	Free, works with Gmail
DuckDuckGo Email Protection	Platform agnostic
SimpleLogin	Owned by Proton (Swiss privacy company)

Communicating with Others

When considering communicating sensitive information, four things should be considered:

- Can someone intercept this while it's in transit?
- If someone gets my device, can they read my copy?
- If someone gets one of the recipient's devices, can they read their copy?
- Even if they can't read it, can they see who I'm writing to ("metadata")?

The table below shows the security of a digital message for various communication media. **Bottom line:** email and SMS are not secure at all, and **if your conversation is truly sensitive, use Signal. With disappearing messages unless it's inconvenient.**

	In Transit	My Copy	Their Copy	Envelope
Signal	Impossible (End-to-End Encrypted)	Safe If you reboot & use a PIN.	Safe If you use Disappearing Messages.	Private Signal stores nothing but your signup date.
iMessage (Apple to Apple)	Impossible	At Risk UNLESS you turn on Advanced Data Protection.	At Risk Unless they also have Advanced Data Protection.	Visible Apple logs who you contact and when.
iMessage (Mixed/Green Bubble)	Easy It usually falls back to SMS or basic RCS.	At Risk Standard device security applies.	At Risk They likely have no protection.	Total Carrier logs every single text.
SMS/Texting	Easy Carriers and "Stingrays" can read it.	Unsafe Usually stored unencrypted on the SIM or phone.	Unsafe Completely out of your control.	Total Your phone bill is a map of your life.
Email (Gmail/Outlook)	Possible Usually encrypted, but the provider has the key.	At Risk Usually stays in your "Sent" folder forever.	At Risk Stays in their "Inbox" forever.	Total Subjects, dates, and recipients are all logged.

In The Field

When you're in a politically sensitive environment like a rally or border crossing, consider the following additional measures for your phone:

Lock/Encrypt Your Device

Your device likely unlocks with biometrics. A strange legal quirk exists in the US that law enforcement may ask you to use biometrics to open it, but cannot ask you to open it with a PIN[1].

To this end, iPhones and Android devices now offer a "Go button", which automatically disables biometric unlock and prompts for your PIN. On iPhone, this requires holding the Power and Volume Down buttons together. On Android, it requires using the Lockdown button.

Ultimately, if you have 2 seconds to respond, use the Go Button. If you have 10, power the device down.

Prevent Location Tracking

There are tools available to DHS and law enforcement that allow for easy tracking of a phone's location. You essentially have four options to deal with this, in ascending order of effectiveness:

- Turn on Airplane mode and turn off Bluetooth (good)
- Power your phone off (better)
- Use a Faraday bag, a $20 pouch lined with a signal blocking mesh (even better)
- Leave your phone at home (best, though very inconvenient)

Map Searching

If you are navigating to sensitive locations within an area, you might consider using an offline maps app like OsmAnd Maps. It allows you download a region, then do your searches offline. This way the addresses you map will not be logged by a map service provider like Google or Apple.

[1] Within 100 miles of any US border (including oceans – that encompasses approximately 213M people!), you may still have your phone seized for forensic analysis. For this reason, rebooting or powering down your device without unlocking may be your best option.

Using Public Wi-Fi

Public Wi-Fi (e.g. coffee shops, airports) has been notorious in the past for snoops listening in on your traffic. This has improved some, as most web traffic and email syncing is now encrypted, but there are still risks.

Be aware that the hotspots you connect to may actually be provided by an attacker, who can use it to present fake web pages that look real but extract account information or download viruses. Be sure to verify you are using a hotspot provided by the locale.

Also, know that even on legitimate Wi-Fi networks, the web sites you visit (though not the full links) can be visible to snoops with the right tools. If you have the choice to use a cellular network like AT&T or Verizon instead, opt for that.

Using USB Charge Ports

When looking for a phone charge port in a public place, be aware that fake ports (“juice jackers”) exist that can be installed to infiltrate your phone. The best strategy is to either use an AC plug adapter of your own, or acquire a USB data blocker (“USB condom”).

Further Reading

The Electronic Frontier Foundation Surveillance Defense	https://www.eff.org/pages/surveillance-self-defense
50501 Digital Safety	https://www.fiftyfifty.one/digital-safety