A Completely Non-Exhaustive List of Digital Security Tips & Resources

Internet security is not a one and done task, nor is it one size fits all. Every person has different vulnerabilities, and those can change with every new software update, app, and device, as well as every identity, project, socio-economic bracket, and life stage.

Most security experts suggest you begin by conducting a risk assessment. Journalists, activists, and artists working against oppressive regimes have very different digital security needs than, say, a 60-year-old woman protecting her 401k or a twenty-something with a lot of creepy ex-Tinder dates. But everyone faces risks. It's a grueling task, but worth it. Think of it as **critical digital hygiene.**

In the short term, here are six things everyone can do:

1. **Get a password manager** that you can use *across devices* (not the default service on your laptop, tablet, or phone). Lastpass.com and Keepass.info are both free, and you can read about others here. Make strong, elaborate, diverse passwords for ***all*** of your online accounts. Sorry, 'cookiebear1993' isn't going to cut it anymore. Try EFF's Dice-generated Passphrase for creating strong randomized passwords instead. If you learn about a major cybersecurity breach that might involve your data, change your password immediately. And remember, passwords should be refreshed on a regular basis.

2. **Add a second layer to secure your account.** You can do this by activating **Two-Factor Authentication (2FA)** on your online accounts, such as email, banking apps, and social media. You can activate 2FA through your account security settings for many common services, including Google, Facebook, Twitter, most banks, and even ConEdison. There are four common types of authentication: mobile apps, physical keys, text messages, and biometric data (such as fingerprints). The most secure and convenient methods are mobile apps and physical keys. Is it time-consuming? Yes. Does it make your account *super hard* to hack? Also yes.

3. **Protect your personal contextual information by restricting access to your microphone, camera, contacts, location, and more on your phone or computer apps.** Most apps nowadays want access to your whereabouts, contacts, cameras, and mics to "ease your life." However, they can also monitor your behavior and profile in order to capitalize on your data. You, on the other hand, can defend yourself by actively restricting such access while still using the apps. For example, you can selectively deny an app access to your location, or elect to enable location services **only when required** for app use (for example, when using Google Maps). More time consuming? Yes. Safer? Also yes. Do you have apps that you never really use? If so, delete them. Disturbingly, many apps are engineered to harvest as much data as possible across your phone.

4. There are **browsers**, **messaging services**, and **other tools** that can help improve your privacy online. Want to watch porn and not be tracked? Maybe use **Tor browser** (which routes traffic through multiple servers, encrypting it each step of the way) or at the very least,

Firefox. Want to send end-to-end encrypted messages with your friends? **Signal** is pretty good. Use a lot of public Wi-Fi? Maybe it's time to get a **Virtual Private Network (VPN)**, which provides online privacy and anonymity by creating a private network via a public internet connection. VPN services establish secure and encrypted connections to provide greater privacy than secured Wi-Fi hotspots. Paid VPNs such as **AirVPN**, **TunnelBear**, **PIA** and **Vypr** work quickly and offer more security guarantees, but there are also free options, including **ProtonVPN**, **RiseupVPN**, **and** **BitMask** (as well as **TunnelBear** – free up to 500mb). We also recommend installing certain **web browser extensions**, such as **Privacy Badger**, **HTTPS Everywhere**, and **uBlock Origin**, to help keep people from snooping. Search engine **DuckDuckGo** also offers a browser extension designed to block cookies, pop-ups ads, and other annoying and invasive trackers.

5. **Defend yourself against phishing attempts**. Sometimes you will receive emails, text messages, or phone calls pretending to be from someone you know or containing information that might interest you in order to lure you into clicking a link or giving out personal information, like your phone number or account credentials. This is called a **phishing attack.** Beware of such clickbait: check twice before you click a link or download an attachment, and **always verify** a message's sender. FTC has this step-by-step guide to avoid phishing scams (only a 4-minute read!).

6. Finally, remember the old online adage: **if you're not paying for it, chances are *you're* the product :)**

How-To's & Further Reading

- Access Now's 'First Look at Digital Security'
- Access Now's 'Self-Doxing Guide'
- Crash Override's Interactive LockDown Tool
- EFF's Security Starter Pack
- Mozilla's Data Detox Kit
- A DIY Guide to Feminist Cybersecurity
- Martin Shelton has this megalist of online digital security guides (some of which are also included above). Check out his Medium blog too.

In Case of Emergency

- Access Now's 24/7 Digital Security Helpline
- Carrie Goldberg – badass lawyer for revenge porn & harassment cases
- Anita Sarkeesian's guide to surviving online harassment