PROTECT YOURSELF CHECKLIST

How you protect your privacy is up to you, and you might not want to do all of these things. Items in **bold** are things that everyone should do, the others depend on how far you want to go with your privacy.

This document provides examples of specific companies and products. **No mention of a company or product constitutes an endorsement of that product**, nor does it indicate that the product has been thoroughly vetted.

GENERAL BEHAVIOR

- □ **Hang up on robocallers, or don't answer the phone if you do not recognize the numbers. Legitimate businesses will leave a voice mail.**
- □ Sign up for Scam alerts – be aware of common scams.
- □ Avoid bringing internet-connected devices (Internet of Things) into your home entirely, or use ones made by companies with a strong commitment to privacy and data security. Use strong passwords and keep the firmware updated.
- □ Don't sign up for business loyalty programs unless you are sure that your purchase history is not being shared.
- □ Never give your social security number to a business unless they convince you that they have a legitimate need for it.
- □ **Research businesses, websites, and products that you aren't certain about to make sure they're not scams and they're safe to use.**
- □ **Never throw mail with sensitive information (like bank, health, or insurance statements) in the trash. Get a shredder. Also shred credit cards when they expire.**
- □ **Never respond to a request to wire money or to pay using a gift card.**

AVOIDING IDENTITY THEFT

- □ **Freeze your credit reports with all the credit reporting agencies. You can thaw them when need a loan or a new credit cards.**
- □ **Monitor your credit reports.**
- □ **Monitor your credit card and mobile phone statements.**
- □ Sign up with a reputable ID Theft monitoring service.
- □ Get ID Theft insurance. If you think you have it, make sure it carries sufficient coverage.

ONLINE BEHAVIOR

- □ Limit the amount of information you share on social media.
- □ Create unique accounts on all websites and apps, instead of relying on Google or Facebook logins.
- □ Don’t use websites or apps that have a record of disrespecting privacy.
- □ **Be skeptical of anyone you don’t know who tries to connect with you directly through social media.**
- □ If service requires you to enter an email address, consider using a temporary email address from a site like 10minutemail.com.
- □ Cover your laptop’s webcam when you aren’t using it with tape or a sliding cover.
- □ If your bank supports it, use a “virtual” credit card number when one is requested online.

ONLINE SERVICES, BROWSERS AND APPS

- □ Do business with companies that have a good reputation for privacy and avoid companies that don’t.
- □ Be aware of what companies control what services. For example, Google owns YouTube, Nest, Android and Chrome. Facebook owns Instagram, WhatsApp, and Oculus.
- □ **Browser:** Use a web browser with a strong commitment to privacy like Firefox, Epic Privacy Browser or TOR.
- □ **Search Engine:** Use a search engine that doesn’t store your searches or mine them for data like DuckDuckGo. Change your browser’s default search as well.
- □ **Email:** Use an email service that doesn’t read your messages like ProtonMail.
- □ **Messaging:** Use a privacy-protecting, encrypted messaging app like Signal.
- □ Install privacy add-ons to your browser like Privacy Badger, Ghostery, HTTPS Everywhere, uBlock Origin, AdBlock Plus, or others.
- □ Browse the web using your browser’s “Incognito” or “Privacy” mode.

PASSWORDS

☐ Turn on two-factor authentication wherever it is available.

☐ Create strong, unique passwords on all websites that carry sensitive information:

- ○ Banking
- ○ Investments
- ○ Health Care
- ○ School & Work
- ○ Cloud Storage
- ○ Email
- ○ Shopping
- ○ Social Media

☐ Change your passwords annually.

☐ Use a password manager and consider an authenticator app for dual-factor authentication.

☐ Never:

- ○ share or write down your passwords
- ○ store your passwords on a text file on your computer or phone
- ○ enter your password on a public computer (like at the library)
- ○ enter your password on a site that doesn't use HTTPS

DATA SECURITY

☐ Install anti-malware/anti-spyware software and make sure it is being updated.

☐ Install patches as they come out and keep your OS, software and app versions updated.

☐ Turn on automatic updates on your computer.

☐ Back up your computer regularly.

☐ Password protect your devices and set them to disable after a certain number of incorrect attempts, set your devices to lock automatically.

☐ Set a strong password on your home wifi

☐ Wipe your hard drive if you're going to sell your computer (or better, shred it).

☐ Check whether you have been the victim of a data breach at haveibeenpwned.com.

☐ Implement a firewall

☐ Never:

- ○ Submit sensitive data (including login credentials) through a website that doesn't have HTTPS:// in the web address.
- ○ Email sensitive data like passwords or social security numbers.
- ○ Send sensitive data or log into sensitive websites when using a public wifi network or on a public computer.
- ○ Click on links in email you didn't expect to receive.
- ○ Plug random USB drives into your computer.

AVOIDING BEING TRACKED

- □ Change your browser privacy settings to maximize your privacy
- □ Update privacy settings on apps and websites you use and decline the use of tracking cookies where possible
- □ Turn off location tracking on your smart phone for any apps that don't absolutely need it
- □ Implement a VPN
- □ Use the Tor Browser/Network
- □ Install privacy add-ons on your browser like Privacy Badger

OPTING OUT

- □ Turn off location tracking on all your devices, for any apps that don't absolutely need it. Set apps to only track your location while you are using them.
- □ Look at the privacy settings for every company you do business with, particularly banks and other financial institutions, and opt out of their ability to share your data where you can.
- □ Manage your privacy settings on social media sites (particularly Google & Facebook).
- □ Review your search and location tracking history on services that allow it, consider deleting it.
- □ Sign up for the national Do Not Call Registry to tell telemarketers not to call you.
- □ Sign up with Opt Out Prescreen to stop receiving unsolicited prescreened offers of credit.
- □ Opt out of certain advertising networks by clicking the green triangle on an online ad, or go to the AdChoices Opt Out page.
- □ If you receive unwanted, unsolicited email, unsubscribe from their mailing lists by finding the "unsubscribe" or "manage email options" link, usually located at the bottom of the email.
- □ Research Data Brokers and opt out of them sharing your data where possible by going to the Vermont or California Data Broker Registry.
- □ Sign up with a service that opts you out of data broker lists
- □ If you live in California, assert your CCPA rights to not have your data sold, or to delete your data (some companies like Microsoft have committed to implementing CCPA nationally)

COMMUNICATION

- □ Tell your friends and family what you know about privacy and data security, encourage them to adopt these practices.

  Your privacy is dependent on others. If someone you know has their email hacked, installs malware, or overshares their information, that can be used to scam you or hurt you other ways.

- □ If you know anyone who is particularly bad with technology, help them become more secure. For example, assist them in running a virus scan or make sure they haven't fallen for any scams.

- □ One reason our privacy is so threatened is because there are very few laws to stop companies from invading it. Contact your US Senators and Congresspeople, your state Representatives, your Governor and your Attorney General and let them know that you care about privacy.

- □ Privacy is a rapidly changing landscape. Stay up to speed. Here are a few helpful resources:

  Consumer News and Guides:

  - ○ Consumer Reports is always a good resource for privacy. This guide is frequently updated and has the latest news.
  - ○ Consumer Reports is also starting to test products for privacy concerns through their Digital Lab.
  - ○ Restore Privacy publishes a number of helpful guides, and also has news and reviews.
  - ○ The Mozilla IoT website rates the privacy of Internet of Things Devices

  Privacy News and Policy

  - ○ If you are interested in privacy policy and staying up to date on developments in the privacy world, check out the Electronic Privacy Information Center (EPIC) the Electronic Frontier Foundation (EFF), and the World Privacy Forum does a lot of great work in this area.
  - ○ The New York Times Privacy Project has been breaking a lot of news in this area.
  - ○ Reddit has a good forum on privacy news.