Data & Tech Privacy Resources

VPN

What is a VPN: A VPN, or Virtual Private Network, is a service that encrypts your data and masks your IP address to create a secure connection between your device and a remote server.

Why use a VPN: A VPN encrypts your data and masks your IP address to protect your privacy and security online. This allows you to browse the internet anonymously and safely, even on public networks.

Mullvad VPN

“A free and open society is a society where people have the right to privacy. That’s why we fight for a free internet. Free from mass surveillance and censorship. Free from personal data collection and business models where your online behavior is treated as commodity. Free from authorities mass monitoring entire populations. Free from big tech and data brokers mapping your life.”
https://mullvad.net/en

Proton VPN

Surfshark VPN

Do you own research to see what options are right for you.

Private Browsers

What is a browser: A web browser is an application for accessing websites.

Why use a private browser: Private browsers block trackers, remove tracking used to identify individual users from URLs, and add protections against advanced fingerprinting techniques.

duckduckgo

“The best way to protect your personal data is to stop it from being collected at all. Other companies try to hide it from hackers and scammers, which always comes at a risk. We don't track it to begin with and stop other companies from tracking it too..” **https://duckduckgo.com/**

Brave

Firefox

Do your own research to see what options are right for you.

Encrypted Messaging

What is encrypted messaging: Encrypted text messaging is a method of secure communication that converts your messages into code. This means that only the recipient with the correct decryption key can read it.

Why use it: It's a way to keep your conversations private from prying eyes, whether they're hackers, advertisers, or even government agencies.

Signal

“State-of-the-art end-to-end encryption (powered by the open source Signal Protocol) keeps your conversations secure. We can't read your messages or listen to your calls, and no one else can either. Privacy isn’t an optional mode — it’s just the way that Signal works. Every message, every call, every time.”
https://signal.org/

Do your own research to see what options are right for you.

Social Media Privacy

Meta, X, and other data farming social media companies

- **Privacy settings:** It's is important to make sure you're always up to date. It can be tedious and annoying, but it is important to check every nook and cranny.

- **Deleting the tech oligarch apps:** Deleting Meta is a great opportunity to protect yourself. However, *community is important*. If you can't delete these apps without affecting yourself financially or hurting your community connections, make sure to stay on top of your privacy settings and the content and photos you post.

- **Switching to decentralized social media:** Talk to your online community about switching to decentralized social media apps like **Mastodon** and **Bluesky**. Decentralized social networks operate on independently run servers, rather than on a centralized server owned by a business.

Tech Privacy

- **Stay informed:** Before deciding to use an app or service, carefully review its Terms of Use and privacy and data policies.

- **Adjust your privacy settings:** Pay close attention to the privacy settings on your accounts and devices.

- **Limit your data footprint:** Avoid oversharing personal information on social media.

- **Poison your data: "**Poisoning" your data is deliberately corrupting and confusing the training data and learning of a search engine, etc. You can manually poison you data footprint by searching up things and topics contrary to who you are and what you normally consume

- **Reproductive privacy:** Do not use period tracking apps or any app that collects data about your reproductive health. If you must log, manual pen and paper is the way to go.

- **AI:** Protect your creative property by not using AI tools like Chatgpt, etc, to edit your work. Turn off AI scraping on word processors. If you post your art online, use AI scraping protection like **Nightshade.** If you have an Phone 15 Pro or newer, Apple is using you to train their AI and collect data - you have to manually disable this feature in your settings and all individual apps.

The Police & Your Phone

Choosing a lock method on your phone

- Under the current law, the police have **the authority to demand unlocking if your phone has facial recognition or fingerprint identification**.

- However, they **cannot do so if you choose a pattern lock or a passcode/password**.

- **The Reason -** Unlocking with a passcode implies knowledge of that code, constituting a testimonial act protected by the Fifth Amendment. In contrast, using facial recognition or fingerprints is considered a nontestimonial act, revealing no explicit knowledge.

- While any form of lock on your cellphone might serve as a form of privacy, law enforcement's capabilities can challenge this. Therefore, **choosing a pattern lock or a passcode/password remains the safest choice.**