Five Moves to Block Spies, Trackers, and Data Brokers

Digital privacy can be challenging, but there are steps you can take to dramatically reduce your digital footprint and protect your personal information from marketers, profilers, stalkers, and hackers. Follow these five practical tips to safeguard your data today.

★ Get Privacy-Focused Comms

Your phone is a powerful tracking device. Calls and messages carry data that many trackers seek. And your enemies covet most. Locking them down isn't easy, but it is possible.

- **Select a Phone with Privacy in Mind**
  - **See our analysis of options:** We have analyzed most of the privacy phones currency available, and looked at them based on their privacy, anonymity and security profiles.
    - **OIQ GUIDANCE: Privacy Phones**

- **Avoid linking your real identity during phone setup:** Don't tie the phone to your true identity if at all possible.
- **Consider a de-Googled phone:** Use GrapheneOS for maximum privacy.
- **Consider a secondary phone:** A dedicated phone for sensitive tasks (e.g., banking) limits exposure.
- **Watch out for SIM tracking:** Some privacy-conscious users rotate SIMs or use eSIMs. You can even get an **encrypted SIM**.

○ Select a Secure Messaging App

- **See our analysis of options:** Encrypted messaging apps make your texts impossible to read - the tech is good and there are no other issues. Unfortunately, it's not just about the encryption. For instance, if there is no anonymity an App may leak the fact that you are communicating daily with someone and that fact might be just as problematic.
    - **OIQ GUIDANCE: Private Messaging Apps**
- **Signal was our top choice…:** But maybe Session is where you should be looking if you need maximum protection. Get both and start pushing your connections toward Session.

Why? Even with the best digital hygiene, a standard smartphone still exposes location data, app usage, and device activity to Google, Apple, carriers, and third-party trackers.

★ Protect Your Data, Especially Financial

Prioritize your financial accounts. Secure them first, as financial data is critical and often harder to recover if compromised. Other things are easier to fix. Freeze your credit and use a separate clean device for your financial transactions. That's it.

○ Freeze Your Credit

- **Prevention:** Prevent identity theft by freezing your credit so no one can open accounts in your name.
- **How to do it:** Visit **FrozenPII.com** for simple, step-by-step instructions on freezing your credit.
- **Ancillary Freezes**
    - **Bank Security Freeze**: a **ChexSystems freeze** on your consumer report, which prohibits consumer reporting agencies from releasing any information in your consumer file without your expressed authorization.
    - **Utilities Security Freeze**: a NCTUE **freeze** prevents the information in your **NCTUE** data file from being reported to service providers and other companies.
    - **Employment Data Freeze**: a **freeze** that keeps **Equifax Workforce Solutions**, e.g. The Work Number, from sending out your work history.

Why? Freezing your credit makes it harder for criminals to use your personal information if they manage to get hold of it. And it's easy to unfreeze - you can do it in

minutes if you need to make a large purchase.

Credit monitoring and **identity theft insurance** services are not worthless, but their value is suspect. Credit monitoring tells about problems after the fact. And once the free service runs out, they try to sell you on premium plans that are rarely worth it. While identity theft insurance sounds good in theory, we do not know of any person who has ever had it pay off. Don't pay for this stuff, just freeze your credit.

○ Shield Your Financial Info

- Access bank accounts and other financial accounts using a **separate, secure device**.
    - Buy a cheap laptop, chromebook, or ipad just for accessing your bank and money. Do nothing else on this machine. No email. No web surfing. No apps.
    - Keep the passwords for this device and money accounts separate.
    - Be sure to run a VPN, antivirus/anti-malware, privacy browser, adblockers like you should do on your main device(s).
    - **Recommended tools:**
        - **Hardware:** Lenovo IdeaPad 1 *(as cheap as $100!)*, HP Stream, iPad (9th gen or better), iPad Mini (5th gen), Acer Chromebook 314
- Access your money with **Virtual Credit Cards**
    - Use disposable or virtual credit cards when shopping online to prevent exposing your real card details and to limit the amount to credit available.
    - **Recommended tools:**
        - **Virtual cards:** **Privacy.com**, American Express Virtual Pay, Capital One Eno

Why? Freezing your credit is the single most important thing you can do to protect yourself from identity fraud. Credit bureaus require you to take proactive measures. Freeze your credit and use virtual cards to protect your information.

Virtual cards, on the other hand, ensure your credit card info isn't compromised if a website or vendor is hacked.

○ Strengthen Passwords & Use Two-Factor Authentication

- Use a password manager to generate and store strong, unique passwords for each account. You want long passwords of at least 20 or 30 characters; we recommend you use passphrases.
- Enable two-factor authentication (2FA) for extra security.

OIQ GUIDANCE: Password Managers

- **Recommended tools:**
    - **Password Managers:** **BitWarden**, **1Password**
    - **2FA:** Google Authenticator, **YubiKey** for hardware-based 2FA

Why? Using a password manager reduces the risk of weak passwords.Utilize a password manager to create and store strong, unique passwords. These tools help manage multiple email aliases effectively. 2FA ensures that even if your password is compromised, your account remains protected. You should have 2FA on every important account. People without 2FA get hacked.

★ Protect Your Browsing Habits

Adtech is invasive. Everything you do online leaves traces unless you actively block it. The best thing you can do is stop using the Chrome browser, add some ad blocking tools, and turn on a legitimate VPN service with a no-logging policy.

- ### Use a Privacy-First Browser and Ad Blocker
  - Switch to browsers that protect your privacy and install ad blockers to prevent being tracked by marketers. **Stop using Chrome.**
    - **OIQ GUIDANCE: Browser Privacy**
  - **Recommended tools:**
    - **Privacy Browsers: Brave, DuckDuckGo, Mullvad**
    - **Ad Blockers: uBlock Origin, Privacy Badger, Ghostery**
    - **Network-based Ad Blockers: AdGuard on Raspberry Pi Device**

- ### Use a VPN to Hide Your Online Activity
  - Use a VPN (Virtual Private Network) with a no-log policy to ensure that your internet provider, apps, or third parties can't track your browsing.
    - A VPN masks your IP address by routing your connection through an encrypted server, making it harder for websites and advertisers to determine your real location. This prevents Ad Tech from using your IP to track your movements across sites and target you with location-based ads.
    - Additionally, by regularly switching server locations and encrypting traffic, a VPN makes digital fingerprinting more difficult, reducing the ability of trackers to build a unique profile based on your device, browser settings, and network characteristics.
  - **Recommended tools:**
    - **VPN Services: NordVPN, Surfshark, ExpressVPN, ProtonVPN**

- ### Use Secure DNS
  - Secure DNS prevents ISPs, attackers, or other intermediaries from tracking the websites you visit. It mitigates threats like DNS spoofing or cache poisoning, which can redirect users to malicious websites.
  - **Recommended services:**
    - **VPN Services: Control D** (Premium), **NextDNS** (Premium), **Quad9** (non-profit), **Cloudflare**, **Google**

Why? These browsers and blockers prevent websites from collecting and sharing data about your browsing habits. It's smart to do everything you can to stop invasive adtech. If you are unwilling to give up Chrome or Safari, at least install a good ad blocker. For every ad served to you, 20 companies get your information. Many of them are just building profiles.

Network-based ad blocking can be great, but requires tech savvy (or money) to install and keep up to date and running smoothly.

A VPN encrypts your internet traffic, adding a layer of security and privacy to your online activities.Secure DNS encrypts and protects internet activity from tracking, tampering, and malicious threats, ensuring greater privacy and security online. It's generally free, so be concerned about that in general.

★ Manage What You Let Services See

Every time you sign up for a service, you reveal personal information that can be tracked, linked, or sold. Reduce what you expose.

- **Manage Your Permissions**
  - Review and regularly update your device's privacy settings. Turn off location services, limit microphone access, and remove unnecessary apps.
  - **Key settings to adjust:**
    - **Personalization:** Turn off personalized ads. **Apple** **Google**
    - **Location:** Turn off unless necessary. **Be Location Safe**
    - **Permissions:**
      - Audit mobile app permissions and disable access to sensitive data.
      - Audit Social Media permissions and make them as strict as possible. If your business relies on you being social, you will have tradeoffs to make. Consider **sock puppet accounts**.
        - For help managing privacy on Social Media, we highly recommend the **Block Party** app.

Why? Most apps and SAAS services collect far more information than they need. Limiting permissions can drastically reduce what data is shared about you.

★ Become Harder to Track

This is the hardest change to make, and also the one that can have the most impact.

Data brokers track you by linking your accounts together in a lot of different ways. When you use the same email addresses, the same phone numbers, and the same

user names, it's easy to connect you across accounts and across devices. They don't even have to try. Bad actors can do this too.

Changing your identity across accounts may be cumbersome, but it greatly enhances your privacy. It is possible to do this with email aliases and a good password manager.

- **Use Unique Names and Emails for Different Accounts**
  - Avoid using your real name for online profiles whenever possible.
  - Use unique usernames for **each** account where you can
  - Compartmentalize your online activities by creating different email accounts for sign-ups and purchases.

OIQ GUIDANCE: Anonymous Email Services

- **Recommended tools:**
  - **Dip your toe in with a new email primary account:**
    - **ProtonMail** or **TutaNota** for secure, encrypted email accounts
    - **SimpleLogin** for email aliases
  - **Add more sophistications with burner emails:**
    - **10MinuteMail**, **GuerrillaMail**
  - **Go all-in with a full identity management solution**
    - **MySudo** or **Cloaked** offer an advanced approach by creating compartmentalized digital identities (usernames, emails, and phone numbers). These services help ensure that when you sign up for new services, your real personal data isn't exposed or linked across platforms. Cloaked is a startup. ($120/yr) The service is powerful but still needs some finetuning. It provides protection against both service tracking and data broker aggregation. MySudo has been around longer. ($10 to $150/yr) It offers a similar approach, allowing you to generate and manage multiple phone numbers, email addresses, and even virtual payment options.

Why? Reusing the same name or email across multiple platforms makes it easier for data trackers to link your accounts and build a detailed profile of your online activities.

You can have all of the different email addresses forward to one main address so that you can view them all easily.