7 Steps to Reduce Your Digital Dust by 90%

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

1. Lock Down Your Data with Smart Account Choices

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.
- **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
  - **Dive deep with a solution like Cloaked.com**
    - It's effectively an enhanced “password manager” that helps you create identities (usernames, emails, phone numbers unconnected to your existing ones) so that signing up for new services does not spread your personal data. At $120/yr, Cloaked is not cheap, but it offers more privacy, such that 1) those services you use are not tracking you, and 2) data brokers can’t connect that data to you.

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.

2. 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.

Why? This 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.

---

3. Shield Your Financial Info

- Access it 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 it with Virtual Credit Cards
    - Use disposable or virtual credit cards when shopping online to prevent exposing your real card details.
    - **Recommended tools:**
        - **Virtual cards:** **Privacy.com**, American Express Virtual Pay, Capital One Eno

Why? Virtual cards ensure your main credit card info isn't compromised if a website is hacked.

---

4. 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.**
- **Recommended tools:**
  - **Privacy Browsers:** Brave, Firefox, Opera, DuckDuckGo
  - **Ad Blockers:** uBlock Origin, Privacy Badger, Ghostery
  - **Network-based Ad Blockers:** AdGuard on Raspberry Pi Device

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.

---

5. 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.
- **Recommended tools:**
  - **VPN Services:** NordVPN, Surfshark, ExpressVPN, ProtonVPN

Why? A VPN encrypts your internet traffic, adding a layer of security and privacy to your online activities.

---

6. 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 collect far more information than they need. Limiting permissions can drastically reduce what data is shared about you.

---

7. 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.
- **Recommended tools:**
    - **Password Managers:** **BitWarden**, **1Password**, **Cloaked**
    - **2FA:** Google Authenticator, **YubiKey** for hardware-based 2FA

Why? Using a password manager reduces the risk of weak passwords. I will help you remember longer and more complicated passwords and usernames too! 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.