This guide is for those that have realized our privacy has been purposefully eroded the last few decades. It covers the basic steps that everyone should consider. It's better to build your digital safe haven now, before you lose control of private data. If data is not in your hands, then it can be used against you.

Threat Assessment – Most people are vulnerable in the following areas – Digital Accounts (especially from Email Phishing), Mobile Phones, Laptops, Web Browsers, Home Wi-Fi Routers, and Credit Reports.

Digital Privacy and Security is a life-long marathon, not a sprint, so start now! If you have an active threat, are a journalist or public person, then you will need professional help to secure your family.

Pro Tip – It is not illegal to use an alias or hide your information for non-criminal purposes. However, never give false information to Banks, Law Enforcement, or Government.

1. **Implement a Credit Freeze for Every Member of Your Household** – A Credit Freeze (not a Credit Lock) is now free for all adults and children. Identity theft of minors is a growing problem because it can take years to discover. Get the free *Intel Techniques Credit Freeze Workbook* on how to do this.
2. **Rent a PO Box (Post Office) or CMRA Box (Commercial Mail Receiving Agency)** – Do not associate your name with your home address. Start sending mail and packages to these services. Some PO Boxes allow you to use the Post Office street address for deliveries. Try to get that PO Box, UPS Box, or CMRA address on your driver's license. Search RV Nomad Status for more information.
3. **Lock down Your Social Media** – Regularly review your privacy settings. Delete old content and comments. Reduce the amount you share. Consider deleting all content while keeping the account active for future use (see #16). Google, Facebook, and Instagram are the worst three privacy invaders. Remove or don't allow GPS information in shared pictures. Don't run social media apps on your mobile devices, instead run it within a secured Web Browser. Use the FB Containers or the Multi-containers plugin for Firefox, or open a private browser window in Firefox or Brave.
4. **Use a Password Manager** – You need an encrypted way to create and store strong, unique passwords and random usernames for each account. Also, securely store information such as credit card numbers, passport and driver license scans, software licenses, secure notes, etc. Make sure you have setup emergency access for your family. Start with one account within your Password Manager, then add accounts as you gain confidence. Look for audited and open-source software.

   BitWarden**,** Proton Pass, 1Password – *Free/Paid* – Audited cloud-based password vaults.
   KeePassXC – *Free* – Secure offline computer-based password manager (for advanced users).

   There are other private and safe Password Managers available. *LastPass* is not one of them.

5. **Implement Two-factor Authentication (2FA) on All Accounts** – SMS codes to verify your login are much better than nothing, but are still vulnerable to "Sim Swapping". A generated TOTP code from an Authenticator App (*Better*), or a physical device like a YubiKey (*Best*) greatly increases your account security. Make sure hardware devices are FIDO2 for future compatibility.

   Ente Auth, Bitwarden Authenticator – *Free* – Cross platform authenticators.
   Aegis Authenticator – *Free* – Open-source, Android-only authenticator.
   YubiKey – *Paid* – Hardware based 2FA and FIDO2 device.

6. **Opt Out of All Data Collection** – Remove online records where you can. Your data is collected and then resold many times over, so you have to be prudent and search for your data several times a year. Get the free *Intel Techniques Data Removal Workbook* on how to do this. Or use a data removal service to do this, like Incgoni, DeleteMe, Optery, or EasyOptOuts.
7. **Do a Digital Account Review, Cleanup, and Then Migration to Encrypted Platforms** – Delete unneeded data for accounts that you do not need anymore. Move from less secure and less private services (Yahoo, Hotmail, One Drive, Evernote, etc.) to encrypted and privacy-focused services that can't see your data (Zero Knowledge*)*. Look for free services that also have a paid account option. Consider self-hosting your own secure "cloud" server using a NAS, purchased, or spare computer as a home server, that is running free/paid home server software (Start9, Umbrel, OpenMediaVault, CasaOS, etc.). Contact me or see my Sovereign Computing document for more options.

   ProtonMail, Tuta – *Free/Paid* – Encrypted email storage at rest and to other accounts.
   Sync, Proton Drive – *Free/Paid* – Encrypted cloud storage (replace Dropbox/One Drive/Google Drive)
   Tresorit – *Paid* – Encrypted cloud storage. Free large file transfer to others.
   Standard Notes , Notesnook– *Free/Paid* – Encrypted cross-platform synced (like OneNote, Evernote)

8. **Protect Your Phone Number** – Sim-swapping is on the rise, so do not give out your real phone number and instead use Virtual Numbers. Use a different Virtual Number for Family, Friends, Work, and other situations. Companies use your mobile number to legally track and uniquely identify you.

   Mint – *Paid* – Prepaid cellular where service can be in an alias.
   Google Voice – *Free/Paid* – Allows Virtual Numbers to forward to your mobile number. Can pay to transfer your old phone numbers to Google Voice. Recommend you keep all your old numbers.
   MySudo – *Paid* – Use one, three, or nine virtual phone numbers on your mobile device.
   Above Suite, or Brax – Paid –JMP.chat & XMPP service or can freely setup (advanced).
   Linphone – *Free* – Voice over IP client for use with a paid VoIP phone service like Twilio or Telnyx.

9. **Protect Your Email Addresses** – You need at least four email accounts to compartmentalize your information (work, personal, social media, financial, etc.). Create unique email aliases for different online accounts, from mailing lists to online stores, or use other unique secure aliases for important email (banks, doctors, insurance, bills). Turn off email client remote images to reduce spam.

   Proton Mail, Tuta – *Free/Paid* – Create configurable and secure email aliases for important emails.
   SimpleLogin – *Free/Paid* – Create email aliases. Open-source. Now a part of Proton.
   Iron Vest , 33mail, Addy.io – *Free/Paid* – Create masked emails forwarded to your real email. It will mask your email even on the reply.

10. **Protect Your Credit and Debit Cards** – Do not give out your real Card information to companies. We have seen large data breaches in the last decade where customers information was stolen. Consider moving to Bitcoin/Lightning/Nostr as a censorship-resistant freedom payment platforms.

    Privacy.com – *Free/Paid* – One-time/limited use Debit cards. These cards are locked to a Vendor, so if the card number is stolen then it can't be used anywhere else. Can limit monthly spend amount.
    IronVest, MySudo – *Paid* – Masked Credit Cards.

11. **Protect Your "Data in Motion"** – SMS texting and phone call metadata are all visible to your phone provider so the FBI recommends secure messangers. Additionally, Internet browsing is kept forever and sold. Always use encrypted communications and use a recommended VPN provider for your devices and home router. Be careful of fake, free Wi-Fi hotspots in Airports and other locations.

    ProtonVPN – *Free/Paid* – a Virtual Private Network that secures your internet traffic.
    Mullvad / ExpressVPN – *Paid* – a Virtual Private Network that secures your internet traffic.
    Twin Gate/Zero Tier/Tail Scale – *Free/Paid* – Layered networking that connects various server/clients
    PiVPN / Wireguard – *Free* – Create your own VPNs (advanced).

    NextDNS / 1.1.1.1 / Quad9 – *Free/Paid* – If you can't use a VPN, then use a privacy DNS provider.
    Signal / Molly – *Free* – Encrypted replacement for SMS and phone calls between Signal users.
    Simplex Chat – *Free* – Next-generation distributed encrypted messaging using relays.
    Wire – *Free/Paid* – An audited encrypted conferencing system for video and voice.
    Element/Matrix – *Free/Paid* – An encrypted voice/video/message system.
    MySudo – *Free/Paid* – Free encrypted messaging and voice calls between MySudo users.
    OxChat – *Free* – A encrypted messenger using the NOSTR protocol.
    Keet – *Free* – A peer-to-peer encrypted messenger using the BitTorrent protocol.
    Briar – *Free* – A peer-to-peer encrypted messenger using the Onion network. Wi-Fi, or Bluetooth.
    Bitchat – *Free* – A peer-to-peer messaging application that operates over bluetooth mesh networks. This was used in Iran during the protests of 2025/2026 to bypass Internet restrictions.

12. **Lock Down All Your Mobile Devices** – Listen to now discontinued Privacy, Security, & OSINT Show – archived Episode 290 and archived Episode 291 on mobile settings. Keep devices and apps updated regularly. Uninstall unused apps to reduce vulnerabilities and improve performance. Be cautions of free apps; they may contain spyware. Disable Bluetooth and Wi-Fi in public places. Review and restrict app permissions and privacy settings. Enable device encryption. Use open-source and privacy-focused applications.

    Silent Pocket Camera Stickers – For covering your rear-facing camera.
    Mic-Lock Blocker (Lightning) – For physically disabling microphones in Apple devices.
    Anti-Tracking EMF-blocking Pouch – Designed and tested by Dr. Bradley (Disaster Preparer).

    Zapstore.dev – *Free* – Android app store that curates recommended apps from release pages.
    Obtainium – *Free* – Android app to install and update apps directly from release pages.
    F-Droid – *Free* – Android app store to download open-source apps.

    NextDNS – *Free/Paid* – Secure DNS for iPhone/Android with ability to block ads and trackers.
    NetGuard Firewall – *Free* – For Android to block ads and trackers.

    Apple iPhones are more secure than Android, but just as privacy stealing. Consider getting an unlocked GrapheneOS mobile device from Affordable Privacy Phones. If you already have a Pixel phone, then let us install GrapheneOS on it, then provide you with training on how to use it

    GrapheneOS – *Recommended* – Secure Mobile OS based on Android. Only Google Pixels supported.
    CalyxOS – Another de-Googled Android OS for Pixels that focuses on usability over security.
    LineageOS – Mobile device OS. Only some phones and tablets are supported.

13. **Lock Down Your Desktop/Laptop** – Windows 10/11 is horrible on privacy and getting worse. Consider a Macintosh (somewhat better on privacy), or a Linux (best) computer with Intel management disabled for your next laptop or desktop. Consider replacing the BIOS with Coreboot (Advanced). Freshly reinstall the operating system and use whole-disk encryption.

    Run as a regular user (not as Administrator) for virus/trojan protection. Do the recommended security updates on a monthly basis or better have them automatically applied. Remove all unnecessary Apps. Update the applications you use (especially Adobe products).

    Linux Mint, ZorinOS, PopOS!, or Ubuntu – *Free/Paid* – Linux operating systems geared for beginners.

    Tails – A privacy-oriented Linux Desktop that only boots off USB drive. Has encrypted storage.
    Coreboot – An Open-Source Firmware for your computer.
    System 76, Privacy Computers, PineBook, Raspberry Pi 400 – Purchase Linux PCs with Coreboot.

    KnockKnock – *Free* – Mac Utility to block Malware.
    Little Snitch – *Paid* – Mac Firewall to block unknown outgoing connections.
    LuLu – *Free* – Mac Firewall to block unknown outgoing connections.

    MacUpdater – *Free/Paid* – Mac Utility to scan and update Mac applications.

    Bitlocker – *Free* – Windows 7/8/10/11 Disk Encryption.
    VeraCrypt – *Free* – Creates Encrypted partitions or drives on Windows/MacOS/Linux computers.

    Spybot Anti-Beacon – *Free/Paid* – Blocks Windows software from calling home.
    Glasswire – *Free* – Windows/Android Firewall to block unknown outgoing connections.

    NextDNS – *Free/Paid* – Secure DNS for Windows/Mac with the ability to block ads and trackers.

    Run the following Windows software on a monthly basis.
    O&O ShutUp10 – *Free/Paid* – Corrects Windows 10/11 privacy settings.
    O&O AppBuster – *Free/Paid* – Lists and deletes all the extra software on your computer.

    BleachBit – *Free/Donation* – Cleans up your Windows computer of old files, cookies, etc.

    Spybot Search & Destroy – *Free/Donation/Paid* – Scans your Windows computer for Malware.
    Malwarebytes Anti-Malware – *Free/Paid* – MBAM scans your Windows computer for malware.

    UCheck – *Free/Paid* – Easy updater for Windows applications.

14. **Lock Down Your Home Network** – There are a number of detailed steps, so I recommend following the short and full task lists from routersecurity.org.

    The ISP router given to you is cheaply made and insecure. Most home's Wi-Fi routers use out of date firmware, so make sure it's recent (within 6-8 months), if not, then you need to upgrade.

    If you just have basic needs, then I recommend a router with OpenWRT pre-installed.

    Consider moving to a "Prosumer" level router like the Ubiquiti or Protectli, and networking/Wi-Fi systems like Ubiquiti which gets regular updates and has many security features.

    Use a *free/paid* DNS filtering service (DNS Blackhole/Sinkhole) like NextDNS, Cloudflare Family DNS or others (easy) or self-host the *free* Pi-hole or AdGuard Home (intermediate/advanced).

15. **Use Open-Source and Privacy-Oriented Software** – Remove unused apps. Run any suspicious or problematic software inside a virtual machine or software sandbox.

    Only Office / LibreOffice – *Free/Paid* – Full featured open-source office applications.
    Jitsi Meet – Open-source Zoom replacement that you can self-host.

    SumatraPDF – Open-source Adobe Acrobat Reader replacement.

    Thunderbird, Betterbird – Open-source email client (Win/Mac/Linux/Android).
    eM Client / Canary Mail – *Free/Paid* email clients (Win/iOS/Mac/Android).

    Firefox Web Browser / Brave Web Browser (Chrome based) – *Free/Donation* – for many platforms. Do not install any "toolbars" and disable PDF viewing in the browser. Use minimal extensions to minimize your browser fingerprint and threat exposure. Many extensions can spy on you.
    Tor Browser – *Free/Donation* – Uses the Onion network. Based on Firefox.

    Ublock Origin – *Free* – This is a Brave/Firefox/Tor plugin. Blocks many known trackers and advertisement platforms (better than Adblock Plus) (Be aware of fakes). Configurable per website.
    Firefox Multi-Account Containers – *Free* – A Firefox Plugin which provides the ability to contain website data within a containerized tab and prevents websites from seeing other website cookies in different containers. This prevents cross-tracking of your web browsing habits.
    Privacy Badger – *Free* – Blocks many known trackers and advertisement platforms.

    Brave Search, Presearch, Duck Duck Go, StartPage.com – Privacy oriented search engines. Use instead of Google, Bing, Yahoo, etc. DDG Search doesn't have the DDG Browser issues.

    Run software in a virtual machine – *Free/Paid* – For advanced Windows/Mac/Linux users.

16. **Plant Your Flag** – Consider opening online accounts with healthcare portals, social media, and government agencies (e.g. SSA, Unemployment, etc.) even if you don't need them. Save the passwords in your Password Manager.

    If you already have an account, then others can't open it to impersonate you. Think Twitter/X usernames like @RealMikeTyson (Real) vs @MikeTyson (Fake). There was unemployment fraud in 2020 due to thieves opening accounts in other people's names. Medical ID theft is growing where they open a Health Care System account in your name and either steal sensitive information or bill expensive health care to you.

17. **Protect Your "Data at Rest"** – We generate more documents, photos, and videos than we realize and often leave them unprotected. To safeguard your data, use encrypted storage (See #7). It is now recommended to use software encryption like Bitlocker or Veracrypt instead of hardware encryption, as its more portable and can be updated to protect against new vulnerabilities.

    Additionally, we should also create a system of regular encrypted backups for our data. The backup rule is "Three -Two - One - Zero": maintain at least three backups on two different media (e.g. cloud storage, portable hard drive, USB drive), with one copy offsite (e.g. cloud service, safety deposit box, or with a nearby family member). Finally, it's crucial to test the backup to see if it restores correctly. Businesses have lost millions of dollars and some have closed because they didn't verify if their backups could be restored.

Privacy Resources

Big Tech Threat

- Glenn Greenwald – Why Privacy Matters https://www.ted.com/talks/glenn_greenwald_why_privacy_matters
- Naomi Brockwell - They're not SELLING your data. It's MUCH worse https://odysee.com/@NaomiBrockwell:4/google-selling-data:8
- https://googlestriplethreat.com (PDF download)

Explainers, Recommendations and Privacy Guides

- **Michael Bazzell** (https://inteltechniques.com) – Books, Resources, Recommended Virtual Private Networks, Protectli Vault (Home Firewall) Configuration, and Redacted Magazine. He no longer sells his individual ebooks due to piracy.
- **Naomi Brockwell** (https://www.nbtv.media) – Odysee, Rumble, and YouTube,
- **All things Secured** (https://www.allthingssecured.com) – Odysee, Rumble, YouTube
- **Techlore** (https://www.techlore.tech/resources) – Odysee, PeerTube, YouTube
- https://privacyacademy.com – free/paid Privacy Training.
- Lists of Privacy and Security sites (2023) – https://medium.com/@techmindxperts/the-ultimate-privacy-guide-tools-and-resources-for-online-security-4c2ab25f6a89
- https://www.privacytools.io
- https://www.secretsofprivacy.com/p/our-personal-privacy-stack
- https://prism-break.org/en/
- https://anonymousplanet.org/guide.html
- https://restoreprivacy.com/simple-privacy-guide
- https://cyberinsider.com/privacy-tools/
- https://ssd.eff.org/en
- https://securityplanner.consumerreports.org
- https://www.privacyguides.org/en/
- https://lifehacker.com/tech/privacy
- https://lifehacker.com/tech/security

Feel free to email me with questions, corrections, updates, and additions at:
ejfb4e267y4h@opayq.com (This is an email alias)

Online Version of this document is at https://affordableprivacyphones.com/resources/