This guide is for those of you realizing 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 it's not in your hands, then it can be used against you.

***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. **Use a Password Manager** – You need an encrypted way to record information and to generate strong, unique passwords for each account. Store other information such as credit card numbers, passport and driver license scans, backup phrases for cryptocurrency wallets, software licenses, secure notes, etc. Start with one account, then add accounts as you gain confidence using a password manager.

   BitWarden – *Free/Paid* – Secure cloud-based password manager

   LastPass – *Free/Paid* – Secure cloud-based password manager (Free is not as good as before)

   KeePassXC – *Free* – Secure offline computer-based password manager (for advanced users)

2. **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 one-time code from an Authenticator App (better), or a physical device like a YubiKey (best) greatly increases your account security. Google purchased a YubiKey for each of their employees to increase security.

   Authy – *Free* – Cloud based Software Authenticator with backup

   BitWarden Authenticator – *Paid* – Part of BitWarden and is backed up with it

   LastPass Authenticator – *Free* – Software Authenticator that Is backed up with LastPass

   YubiKey – *Paid* – Hardware based 2FA device

3. **Purchase 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 or CMRA address on your driver's license. See RV Nomad Status for more information.

4. **Implement a Credit Freeze for Every Member of Your Household** – A Credit Freeze is now free for all adults and children. Identity theft of minors is a growing problem because it can take years to discover a problem. Get the free *Intel Techniques Credit Freeze Workbook* on how to do this.

5. **Lockdown Your Social Media** – It's not as private as you think! Delete old content and comments. Reduce the amount you share. Consider deleting all content. Google, Facebook, and Instagram are the worst three. Use the FB containers plugin for Firefox, or open a private browser window.

   ~~Social Book Post Manager (SBPM) plugin – A Chrome plugin (use with the Brave Browser) to bulk delete Facebook content~~

   Firefox Multi-Account Containers plugin – 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.

Some links are affiliate links of services I use.

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.

7. **Do a Digital Account Review, Cleanup, and Then Migration to Encrypted Platforms** – Delete unneeded data for accounts that you do not need anymore, randomize account information, then delete. Move from less secure and less private services (Yahoo, Hotmail, One Drive, Evernote, etc.) to encrypted and privacy-focused services. Look for ones that are "*Zero Knowledge*".

   Proton – *Free/Paid* – Encrypted email and cloud storage at rest, and to other Proton accounts.

   Tutanota – *Free/Paid* – Encrypted email at rest and to other Tutanota accounts.

   Sync – Free/*Paid* – Encrypted cloud storage (replaces Dropbox/One Drive/Google Drive)

   Tresorit – *Paid* - Encrypted cloud storage. Free large file transfer to others.

   Standard Notes – *Free/Paid* – Encrypted notes with cross-platform sync (like OneNote, Evernote)

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

   Google Voice – *Free/Paid* – Allows Virtual Numbers to forward to your mobile number. Can pay to transfer your old phone numbers to Google Voice.

   MySudo – *Paid* – Use one, three, or nine virtual phone numbers on your mobile device.

   Linphone – *Free* – Voice over IP client for use with an inexpensive VoIP phone service like Twilio.

9. **Protect Your Email Address** - Do not give out your real email address; give out a unique disposable email alias to mailing lists, or more secure alias for important email (Bank, Doctors, Insurance, Bills)

   Protonmail, Tutanota – *Paid* – have configurable email aliases for important email

   Abine Blur – *Free/Paid* – Create masked emails forwarded to your real email. It will mask your email even on the reply. They are adding more privacy services and will be rebranding to IronVest.

   33mail – *Free/Paid* – Create unlimited disposable email addresses

   Anonaddy – *Free/Paid* – Create anonymous email forwarding

   SimpleLogin – *Free/Paid* – Create different identities for each website. Open source.

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.

    Privacy.com – *Free* – One time use or limited Debit cards locked to the Vendor. If the card number is stolen then it can't be used anywhere else. They get paid by the seller, so it's free for you.

    Abine Blur – *Paid* – Masked Credit Cards

    MySudo – *Paid* – Masked Credit Cards

11. **Secure Your "Data in Motion"** – Internet browsing, SMS texting, and phone call metadata are all visible to your ISP or phone provider. This information is sold. Use encrypted communications and use a recommended VPN provider on your devices and your home router.

    ProtonVPN – *Free/Paid* – a Virtual Private Network that secures your internet traffic
    Mullvad – *Paid* – a Virtual Private Network
    Signal – *Free* – Encrypted replacement for SMS messages and phone calls between Signal users.
    Wire – *Free/Paid* – An audited encrypted conferencing system for video and voice.
    Element/Matrix – *Free/Paid* – An encrypted voice/video/message system, which bridges with other messaging apps.
    Threema – *Paid* – An encrypted text/voice messenger
    MySudo – *Free/Paid* – Encrypted messaging and voice calls between MySudo users.
    Mint – *Paid* – Prepaid cellular where service can be in an alias.

12. **Lock Down All Your Mobile Devices** – Make sure your devices have all the necessary security updates. Remove Apps you do not need or haven't used in a long time. Be suspicions of Applications because there are a number (especially free Apps) with spyware capabilities. Lock down privacy settings and review access permissions after OS updates. Use the device encryption.

    Apple iPhones are easier to lockdown the privacy settings than locking down on Android devices, so consider purchasing one for your next mobile device. Even better, purchase a Linux phone or De-Google an Android Pixel phone.

    PinePhone – Linux based Mobile Devices

    LineageOS – *Free* – Mobile device OS based on Linux. Only some phones are supported.
    GrapheneOS – *Free* – Mobile device OS based on Linux. Only some phones are supported.

    NoAgendaPhone – Guide on how to install Graphene on Pixel devices, plus some recommendations.

    Silent Pocket Camera Stickers – For covering your rear-facing camera
    Mic-Lock Microphone Blocker (3.5mm) – For disabling microphone in device
    Mic-Lock Blocker (Lightning) – For disabling microphone in newer Apple products

    Anti-Tracking EMF-blocking Pouch – Designed and tested by Dr. Bradley
    Silent Pocket Faraday Bag – For stopping cellular tracking of your mobile device

    Lockdown Firewall – *Free* – For Mac and iPhone to block ads and trackers
    NetGuard Firewall – *Free* – For Android to block ads and trackers

13. **Lock Down Your Desktop/Laptop** – Windows 10 is horrible on privacy. Consider a Macintosh (better), or a Linux (best) computer with Intel management disabled for your next laptop or desktop. Freshly reinstall the operating system. Do whole-disk encryption. Run as a regular user (not as Administrator). Do recommended security updates on a weekly basis. Remove unneeded Apps.

    System 76, PineBook, Raspberry Pi 400 – Prebuilt Linux Laptops and Desktops

    Tails – a privacy-oriented Linux Desktop that boots off USB drive. Has encrypted persistent storage.
    PopOS!, Mint, or Ubuntu – Free – Linux Operating System geared for Beginners.

O&O ShutUp10 – *Free/Paid* – Corrects Windows 10 privacy settings
BleachBit – *Free/Donation* – Cleans up your Windows computer of old files, cookies, etc.
Spybot Search & Destroy – *Free/Donate/Paid* – Scans your Windows computer for Malware. Pair with Malwarebytes
Spybot Anti-Beacon – *Free/Paid* – Blocks Windows software from calling home
Glasswire – *Free* – Windows/Android Firewall to block unknown outgoing connections
Malwarebytes Anti-Malware – *Free/Paid* – MBAM scans your Windows computer for malware. Do the free trial and then disable premium. Pair with Spybot Search & Destroy
Patch My PC – *Free/Paid* – Easy automatic updater for Windows applications

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

VeraCrypt – *Free* – Creates Encrypted partitions or drives on Windows/macOS/Linux computers

14. **Lock Down Your Network** – Most home Wi-Fi routers use out of date or insecure firmware, so make sure it's updated or move to a "Prosumer" level Wi-Fi router like the Ubiquiti Dream Router which gets regular updates and has many security features. On your router turn off UPNP, which can let Malware open incoming ports on your network. Use a free DNS filtering service like Cloudflare Family DNS (easy) or use a Raspberry Pi or Docker server to run Pi-hole or AdGuard Home.

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

Firefox Focus Mobile Web browser – *Free* – For Apple and Android devices
Brave Mobile Web browser – *Free* – For Apple and Android devices

Firefox Web Browser – *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

Brave Web Browser – *Free* – for many platforms. Secure by default. Based on Chromium.
Tor Browser – *Free/Donation* – for many platforms. Uses the Onion network. Based on Firefox.

Firefox Multi-Account Containers – 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.
Ublock Origin – Firefox plugin. Blocks many known trackers and advertisement platforms
Privacy Badger – Blocks many known trackers and advertisement platforms
HTTPS Everywhere – Attempts to shifts HTTP traffic to secure HTTPS traffic
NoScript – Blocks webpage scripts from running. Over time you will train it to be less intrusive.

Brave Search, Presearch, Duck Duck Go, StartPage.com – Privacy oriented search engine. Use instead of Google, Bing, Yahoo, etc.

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

16. **Plant Your Flag** – Consider opening online accounts with Health Portals, Social Media, and Government Agencies, even if you don't need them. Save the passwords in your Password Manager. There was a lot of unemployment fraud in 2019/2020 due to thieves opening accounts in other people's names. Medical ID theft is a growing sector and if they open an account in your name, then they could potentially steal information or bill expensive health care to you.

## Privacy Resources

- Intel Techniques (Michael Bazzell) – Podcast (start with his Privacy Crash Course #174-178), Books, Resources, ~~Messaging Comparison~~, Recommended Virtual Private Networks, Protectli Vault (Home Firewall) Configuration

- PrepperNet Privacy Webinar (starts after 12m) (good for a different perspective)
- PrepperNet Privacy while Working from Home (starts after 13m)

- https://www.privacytools.io
- https://restoreprivacy.com/simple-privacy-guide
- https://ssd.eff.org/en
- https://securityplanner.consumerreports.org

Older but still has good information

- https://greycoder.com/all-my-recommendations
- https://www.ghacks.net/2015/12/28/the-ultimate-online-privacy-test-resource-list
- https://motherboard.vice.com/en_us/article/d3devm/motherboard-guide-to-not-getting-hacked-online-safety-guide
- https://medium.com/@re_53711/seven-simple-steps-toward-online-privacy-20dcbb9fa82
- https://lifehacker.com/how-to-make-your-entire-internet-life-more-secure-in-on-1348598911

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