Guide: Privacy Upgrade.

Updated 11 January 2024.

A list of easy-to-use software to preserve your online privacy:

Hard Drives: Self-Encrypting SSD Samsung 850 Evo Pro.
Why: To quickly enable BitLocker, use a compatible Self-Encrypting Drive (SED) that adheres to TCG Opal standards. Without this compliance, BitLocker won't function. Normally, encrypting a new drive takes about 3 days per TB, but with the right hardware, you can expedite this process. For instance, the Samsung 850 Pro, when configured in e-drive mode using Samsung Magician software, allows immediate activation of BitLocker, bypassing the lengthy encryption time.

OS for beginners: Windows 10 Pro.
Why: Upgrading is a simple three-click process, and BitLocker is ready for immediate activation on each drive and thumb drive. Activation of BitLocker is optional; if not activated, you will see a persistent overlay in the bottom right corner of your screen.

OS for advanced users: Kodachi (Linux).
Why: Best OS for privacy, free, based on Linux Ubuntu. Can encrypt the entire hard drive during installation.

Windows Antispy: WPD (Windows Privacy Dashboard).
Why: Auto update, free, easy to use, IP-based firewall rules, App uninstaller, no need to install it on your computer.

Firewall: Glasswire (paid version).
Why: The "*Ask to Block*" functionality gives you absolute one-click control over your traffic. Note: it uses Windows firewall so the paid version isn’t compatible with antiviruses having their own firewalls like Bitdefender.

Email: Tutanota (freemium)
Why: Read our article: Tutanota vs Protonmail. Alternatively: Protonmail.

VPN: ExpressVPN.
Why: Fast and runs from RAM so it doesn't keep logs. Can also be used with DDWRT routers so that your entire home's traffic is protected.

Primary Browser: Firefox, Waterfox, Opera GX.
Why: You can enable DNS-over-HTTPS.

Password manager: Zoho Vault (freemium).
Why: Read our article: 13 password managers.

Messaging, Voice and video calls: Threema (freemium).
Why: open source end-to-end, zero-knowledge encryption, resistant to state-sponsored criminals, based in Switzerland (Wire and Wickr are great but now based in the US). Read our article: Threema pros and cons.

SMS: Don’t. If you have no choice, use Silence on Android (free).
Why: encryption over GSM network.

File sharing through links (think Dropbox): sync.com (free).
Why: end-to-end, zero-knowledge encryption. Granular control with the paid version.

File Synchronization between devices: Resilio Home (freemium).
Why: supports encrypted read-write folders for untrusted devices, so you can synchronize with your home server or off-site servers, your data are all encrypted.

Disk Cleaning: Bleachit.
Why: works on Windows and Linux. Alternatively: Privazer (free), but for Windows only.
Why: One click to clean your entire system in depth.

Anonymous Browser: TOR (free).
Why: should be your primary browser.

Anonymous Chat App: Briar (Android only).
Why: Everything goes through the TOR network. Can host a forum and a Blog.

Useful Links:

https://prism-break.org/en/

https://privacytoolsio.github.io/privacytools.io/

CIA tools released by Wikileaks: https://wikileaks.org/vault7/

NSA tools released by Shadowbroker: https://github.com/misterch0c/shadowbroker

Scanning Service against NSA’s Doublepulsar malware: https://doublepulsar.below0day.com/