UBINODES

GUIDE: PRIVACY UPGRADE

Guide: Privacy Upgrade.

Updated 07 January 2021.

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

Hard Drives: The Self-Encrypting SSD Samsung 850 Evo Pro is selected to enable Bitlocker instantly, since traditional encryption takes about three days per terabyte to encrypt a new drive. It is important to know that a Self-Encrypting Drive (SED) must be TCG Opal compliant to work with Bitlocker. Additionally, specific software is needed, and only the 850 Pro, when set up with Samsung Magician in e-drive mode, allows for the immediate activation of Bitlocker right out of the box.

OS for beginners: Windows 10 Pro is selected for its easy accessibility; it can be upgraded with just three clicks. It includes Bitlocker, which is ready to be activated for both drives and thumb drives. While activation is not required to use Bitlocker, an overlay may appear at the bottom right of the screen until activation is completed.

OS for advanced users: Kodachi (Linux) is chosen as the best operating system for privacy. It is free and based on Linux Ubuntu, and it can encrypt the entire hard drive during installation.

Windows Antispy: WPD (Windows Privacy Dashboard) is chosen for its automatic updates, user-friendly interface, and IP-based firewall rules. It is a free tool that includes an app uninstaller and does not need to be installed on your computer.

Firewall: GlassWire (paid version) is chosen for its "Ask to Block" feature, which provides simple one-click control over your traffic. Note that it uses the Windows firewall, and the paid version may not be compatible with antivirus programs that have their own firewalls, such as Bitdefender.

Email: Tutanota (freemium) is chosen. For more information, read our article: "Tutanota vs Protonmail." Alternatively, you can consider Protonmail.

VPN: ExpressVPN is chosen for its speed and because it runs from RAM, ensuring no logs are kept. It can also be used with DD-WRT routers, protecting your entire home's internet traffic.

Primary Browser: Firefox, Waterfox, and Opera GX are chosen because they allow you to enable DNS-over-HTTPS for enhanced privacy and security.

Password manager: Zoho Vault (freemium) is chosen. For further details, please refer to our article: "13 Password Managers."

Messaging, Voice and video calls: Threema (freemium) is preferred for its open-source end-to-end, zero-knowledge encryption, resilience against state-sponsored criminals, and operations based in Switzerland (unlike alternatives such as Wire and Wickr, which are now based in the US). For a detailed comparison of Threema's pros and cons, please see our article.

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

File sharing: Through links, akin to Dropbox, Sync.com (free) is selected for its end-to-end, zero-knowledge encryption. The paid version offers granular control.

File Synchronization: Resilio Home (freemium) is selected for device-to-device synchronization. It supports encrypted read-write folders for untrusted devices, enabling synchronization with home servers or off-site servers while keeping all data encrypted.

Disk Cleaning: BleachIt is chosen for its compatibility with both Windows and Linux systems. Alternatively, Privazer (free) is recommended for Windows users, offering one-click deep cleaning for the entire system.

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/