Open Source and Private Alternatives

A compact guide to privacy conscious tools you can actually use. Each entry is an alternative focused on open source, privacy, or both. This version excludes federated or moderated services. Pick the level of effort you want and replace default, telemetry heavy services with options that give you more control and fewer surprises.

Network Privacy

Mullvad VPN - a privacy first VPN that accepts anonymous payment methods. Simple apps, strong privacy policy, and clear logging rules. Use Mullvad as your network privacy layer instead of default ISP routing.

Email Alternatives

ProtonMail - end to end encrypted email with a strong privacy record. Tutanota - another privacy focused email provider with built in encryption and lower price tiers. Both are better choices than standard webmail for sensitive messages.

Notes and Knowledge

Obsidian - a local first note taking app that stores notes as plain text files. Plugins add power while your data stays on your disk. Joplin - open source alternative that can sync encrypted notes to cloud storage you control. Both prioritize local control and portability over centralized moderation or federation.

Operating Systems

Linux Mint - beginner friendly, stable, and easy to install. A good first step away from Windows. Qubes OS - advanced compartmentalization for threat modelers who need strong isolation. Higher learning curve.

Browsers and Search

Librewolf - privacy hardened Firefox fork that resists fingerprinting. Brave - user friendly with built in ad blocking and privacy features. Search engines: DuckDuckGo for general private search. Use local Searx instances only if you control them.

Messaging

Signal - simple, widely recommended end to end encrypted messenger for texts and calls. For private, one to one chats Signal is the standard recommendation. Avoid services that rely on federation or external moderation if you want a single-provider model.

Password Management and 2FA

KeePassXC - open source, stores databases locally and works offline. Bitwarden - open source, offers hosted service or self host option; use the hosted service only if you trust the provider. Two factor: use hardware keys like YubiKey for strong second factor. Avoid SMS based 2FA when possible.

Cloud Storage and Sync

Sync.com - privacy focused commercial option with zero knowledge encryption. Use commercial zero knowledge services rather than federated or moderated platforms if you want a consistent provider model.

Privacy Tools and Network Hygiene

uBlock Origin - robust ad and script blocker for browsers. NextDNS - customizable DNS with privacy filters and logging controls. Tor Browser - for high anonymity browsing sessions. Verify official downloads and use with care.

Device Security Basics

Full disk encryption - use the built in options on Linux distributions, or VeraCrypt for containers. UFW - uncomplicated firewall for Linux to restrict incoming connections. Keep software updated and install only from trusted repositories or official project pages.

How to Pick Tools for Your Threat Model

Match tools to your needs. If you want fewer trackers, replace the browser and search engine. If you handle sensitive data, use end to end encrypted email, hardware 2FA, and consider Qubes OS or air gapped workflows. Always verify downloads and read project documentation. Avoid federated services and any platform that requires external moderation if your goal is a single-provider, controlled model.

Further Reading and Resources

Project websites and official docs are the best source of truth. Check: Mullvad, ProtonMail, Tutanota, Obsidian, KeePassXC, Sync.com, Librewolf, Signal, Tor Project, Qubes OS.

This compact reference excludes federated and moderated services. Replace default services step by step and test each change. If you want a longer handbook with install notes, verification steps, and recommended settings for a chosen distro, tell me which distro and I will build it.