Awesome Privacy

*A curated list of privacy & security-focused apps, software, and providers *

Skip to Content

Intro



Large data-hungry corporations dominate the digital world but with little, or no respect for your privacy. Migrating to open-source applications with a strong emphasis on security will help stop corporations, governments, and hackers from logging, storing or selling your personal data.

Note: Remember that no software is perfect, and it is important to follow good security practices.

A Codeberg mirror is available here.

Categories

- **Essentials**
  - Password Managers
  - 2-Factor Authentication
  - File Encryption
  - Private Browsers
  - Non-Tracking Search Engines
- **Communication**
  - Encrypted Messaging
  - P2P Messaging
  - Encrypted Email
  - Email Clients
  - Anonymous Mail Forwarding
  - Email Security Tools
  - VOIP Clients
  - Virtual Phone Numbers
  - Team Collaboration Platforms
- **Security Tools**
  - Browser Extensions
  - Mobile Apps
  - Online Tools
- **Networking**
  - Virtual Private Networks
  - Self-Hosted Network Security
  - Mix Networks

    - Proxies
    - DNS Providers
    - DNS Clients
    - Firewalls
    - Ad Blockers
    - Host Block Lists
    - Router Firmware
    - Network Analysis
    - Cloud Hosting
    - Domain Registrars
    - DNS Hosting
    - Pre-Configured Mail-Servers
- **Productivity**
    - Digital Notes
    - Cloud Productivity Suites
    - Backup and Sync
    - Encrypted Cloud Storage
    - File Drop
    - Browser Sync
    - Secure Conference Calls
- **Utilities**
    - Virtual Machines
    - PGP Managers
    - Metadata Removal
    - Data Erasers
- **Social**
    - Social Networks
    - Video Platforms
    - Blogging Platforms
    - News Readers
    - Proxy Sites
- **Operating Systems**
    - Mobile Operating Systems
    - Desktop Operating Systems
    - Linux Defences
    - Windows Defences
    - Mac OS Defences
    - Anti-Malware
- **Development**
    - Code Hosting
- **Home/ IoT**

    - Home Automation
    - Voice Assistants
- **Finance**
    - Cryptocurrencies
    - Crypto Wallets
    - Crypto Exchanges
    - Virtual Credit Cards
    - Other Payment Methods
    - Secure Budgeting
- **Bonus**
    - Alternatives to Google
    - Open Source Media Applications
    - Self-Hosted Services
    - Self-Hosted Sys-Admin
    - Self-Hosted Dev Tools
    - Security Testing Tools
    - Raspberry Pi Security Projects

See Also

- Personal Security Checklist

Password Managers

Provider	Description
Bitwarden	Fully-featured, open source password manager with cloud-sync. Bitwarden is easy-to-use with a clean UI and client apps for desktop, web and mobile. See also Vaultwarden, a self-hosted, Rust implementation of the Bitwarden server and compatible with upstream Bitwarden clients.
KeePass	Hardened, secure and offline password manager. Does not have cloud-sync baked in, deemed to be gold standard for secure password managers. KeePass clients: Strongbox *(Mac & iOS)*, KeePassDX *(Android)*, KeeWeb *(Web-based/ self-hosted)*, KeePassXC *(Windows, Mac & Linux)*, see more KeePass clients and extensions at awesome-keepass by @lgg.
LessPass *(Self-Hosted)*	LessPass is a little different, since it generates your passwords using a hash of the website name, your username and a single main-passphrase that you reuse. It omits the need for you to ever need to store or sync your passwords. They have apps for all the common platforms and a CLI, but you can also self-host it.
Padloc	A modern, open source password manager for individuals and teams. Beautiful, intuitive and dead simple to use. Apps available for all platforms and you can self-host it as well.

Notable Mentions

Password Safe is an offline, open source password manager designed by Bruce Schneier, with native applications for Windows, Linux, MacOS, Android and iOS, and support for YubiKey. The UI is a little dated, and there is no official browser extension, making is slightly less convenient to use compared with other options

PassBolt is a good option for teams. It is free, open source, self-hosted, extensible and OpenPGP based. It is specifically good for development and DevOps useage, with integrations for the terminal, browser and chat, and can be easily extended for custom usage, and deployed quickly with Docker

1Password (proprietary) is a fully-featured cross-platform password manager with sync. Free for self-hosted data (or $3/ month hosted). Be aware that 1Password is not fully open source, but they do regularly publish results of their independent security audits, and they have a solid reputation for transparently disclosing and fixing vulnerabilities

Other Open Source PM: Buttercup, Clipperz, Pass, Padloc, TeamPass, PSONO, UPM, Gorilla, Seahorse (for GNOME), GNOME Keyring, KDE Wallet Manager.

If you are using a deprecated PM, you should migrate to something actively maintained. This includes: Firefox Lockwise, Encryptr, Mitro, Rattic, JPasswords, Passopolis, KYPS, Factotum.

See also Password Management Checklist

2-Factor Authentication

Provider	Description
Aegis (Android)	Free, secure and open source authenticator app for Android. Has a backup/ restore feature and a customisable UI with dark mode
Authenticator Pro (Android)	Free and open-source two factor authentication app for Android. It features encrypted backups, icons, categories and a high level of customisation. It also has a Wear OS companion app
Tofu (iOS)	An easy-to-use, open-source two-factor authentication app designed specifically for iOS
Authenticator (iOS)	Simple, native, open source 2-FA Client for iOS, which never connects to the internet - built by @mattrubin.me
Raivo OTP (iOS)	A native, lightweight and secure one-time-password (OTP) client built for iOS; Raivo OTP! - built by @tijme
WinAuth (Windows)	Portable, encrypted desktop authenticator app for Microsoft Windows. With useful features, like hotkeys and some additional security tools, WinAuth is a great companion authenticator for desktop power-users. It's open source and well-established (since mid-2010)
Authenticator (Linux)	Rust-based OTP authenticator. Has native With GNOME Shell integration. Also available through flathub.

Provider	Description
Authenticator (BrowserExtension)	Authenticator Extension is an in-browser One-Time Password (OTP) client, supports both Time-Based One-Time Password (TOTP, specified in RFC 6238 and HMAC-Based One-Time Password (HOTP, specified in RFC 4226.

Check which websites support multi-factor authentication: 2fa.directory

Notable Mentions

OTPClient *(Linux)*, gauth *(Self-Hosted, Web-based)*, Etopa *(Android)*

For KeePass users, TrayTop is a plugin for managing TOTP's - offline and compatible with Windows, Mac and Linux.

Authy (proprietary) is a popular option among new users, due to its ease of use and device sync capabilities. Cloud sync may be useful, but will also increase attack surface. Authy is not open source, and therefore can not recommended

See also 2FA Security Checklist

File Encryption

Provider	Description
VeraCrypt	VeraCrypt is open source cross-platform disk encryption software. You can use it to either encrypt a specific file or directory, or an entire disk or partition. VeraCrypt is incredibly feature-rich, with comprehensive encryption options, yet the GUI makes it easy to use. It has a CLI version, and a portable edition. VeraCrypt is the successor of (the now deprecated) TrueCrypt.
Cryptomator	Open source client-side encryption for cloud files - Cryptomator is geared towards using alongside cloud-backup solutions, and hence preserves individual file structure, so that they can be uploaded. It too is easy to use, but has fewer technical customizations for how the data is encrypted, compared with VeraCrypt. Cryptomator works on Windows, Linux and Mac - but also has excellent mobile apps.
age	`age` is a simple, modern and secure CLI file encryption tool and Go library. It features small explicit keys, no config options, and UNIX-style composability

Notable Mentions

AES Crypt is a light-weight and easy file encryption utility. It includes applications for Windows, Mac OS, BSD and Linux, all of which can be interacted with either through the GUI, CLI or programatically though an API (available for Java, C, C# and Python). Although it is well established, with an overall positive reputation, there have been some security issues raised recently.

CryptSetup is a convenient layer for use on top of dm-crypt. EncFS is a cross-platform file-based encryption module, for use within user local directories. geli is a disk encryption subsystem included with FreeBSD.

PGP may be useful for encrypting individual files and folders, preparing files for transmission, or adding an additional layer of security to sensitive
data. With PGP, you can encrypt, decrypt, sign and verify files and folders: see PGP Tools

BitLocker is popular among Microsoft Windows and enterprise users, and provides fast, efficient and (if correctly configured) reasonably secure full drive encryption. However it is not open source, has poor compatibility with other operating systems, and has some very dodgy defaults, which could lead to your system being compromised. Similarly, Apple's FileVault on MacOS is easy and secure, but again, the source code is proprietary.

DiskCryptor is a Windows-only, open source, file and volume encryption solution, that makes a good alternative to BitLocker.

If you need to create a compressed archive, then PeaZip is a great little cross-platform open source file archiver utility. It allows you to create, open, and extract RAR TAR ZIP archives. It also has a password-protection feature, which encrypts compressed files using AES-256, which is also compatible with most other archive utilities

Word of Warning

Where possible, choose a cross-platform and well established encryption method, so that you are never faced with not being able to access your files using your current system.

Although well-established encryption methods are usually very secure, if the password is not strong, then an adversary may be able to gain access to your files, with a powerful enough GPU. If your system is compromised, then the password may also be able to be skimmed with a keylogger or other similar malware, so take care to follow good basic security practices

Browsers

Provider	Description
LibreWolf	LibreWolf is an independent fork of Firefox that aims to provide better default settings to improve on privacy, security and user freedom. Mozilla telemetry is disabled, ties with Google (Safe Browsing) are severed, the content blocker uBlock Origin is included and privacy defaults are guided by research like the Arkenfox project.
Brave Browser	Brave Browser, currently one of the most popular private browsers - it provides speed, security, and privacy by blocking trackers with a clean, yet fully-featured UI. It also pays you in BAT tokens for using it. Brave also has Tor built-in, when you open up a private tab/ window.
Firefox	Significantly more private, and offers some nifty privacy features than Chrome, Internet Explorer and Safari. After installing, there are a couple of small tweaks you will need to make, in order to secure Firefox. For a though config, see @arkenfox's user.js. You can also follow one of these guides by: Restore Privacy or 12Bytes

Provider	Description
Tor Browser	Tor provides an extra layer of anonymity, by encrypting each of your requests, then routing it through several nodes, making it near-impossible for you to be tracked by your ISP/ provider. It does make every-day browsing a little slower, and some sites may not work correctly. As with everything there are trade-offs
Bromite	Hardened and privacy-respecting fork of Chromium for Android. Comes with built-in adblock and additional settings for hardening.

Notable Mentions

Mobile Browsers: Mull Hardened fork of FF-Fenix (Android), Firefox Focus (Android/ iOS), DuckDuckGo Browser (Android/ iOS), Orbot + Tor (Android), Onion Browser (iOS)

Additional Desktop: Nyxt, WaterFox, Epic Privacy Browser, PaleMoon, Iridium, Sea Monkey, Ungoogled-Chromium, Basilisk Browser and IceCat

12Bytes also maintains a list privacy & security extensions

Word of Warning

New vulnerabilities are being discovered and patched all the time - use a browser that is being actively maintained, in order to receive these security-critical updates.

Even privacy-respecting browsers, often do not have the best privacy options enabled by default. After installing, check the privacy & security settings, and update the configuration to something that you are comfortable with. 12Bytes maintains a comprehensive guide on Firefox Configuration for Privacy and Performance

See also Browser & Search Security Checklist and recommended Browser Extensions for privacy & security.

Search Engines

Google frequently modifies and manipulates search, and is in pursuit of eliminating competition and promoting their own services above others. They also track, collect, use and sell detailed user search and meta data.

Provider	Description
DuckDuckGo	DuckDuckGo is a very user-friendly, fast and secure search engine. It's totally private, with no trackers, cookies or ads. It's also highly customisable, with dark-mode, many languages and features. They even have a .onion URL, for use with Tor and a no Javascript version
Qwant	French service that aggregates Bings results, with its own results. Qwant doesn't plant any cookies, nor have any trackers or third-party advertising. It returns non-biased search results, with no promotions. Qwant has a unique, but nice UI.

Provider	Description
Startpage	Dutch search engine that searches on google and shows the results (slightly rearranged). It has several configurations that improve privacy during use (it is not open source)

Notable Mentions

MetaGear, YaCy, Brave Search.

Searx and SearXNG are two self-hostable search engines that use the results of multiple other engines (such as Google and Bing) at the same time. They're open source and self-hostable, although using a public instance has the benefit of not singling out your queries to the engines used.

12Bytes also maintains a list of privacy-respecting search engines

See also Browser & Search Security Checklist

Encrypted Messaging

Without using a secure app for instant messaging, all your conversations, meta data and more are unprotected. Signal is one of the best options - it's easy, yet also highly secure and privacy-centric.

Provider	Description
Signal	Probably one of the most popular, secure private messaging apps that combines strong encryption (see Signal Protocol) with a simple UI and plenty of features. It's widely used across the world, and easy-to-use, functioning similar to WhatsApp - with instant messaging, read-receipts, support for media attachments and allows for high-quality voice and video calls. It's cross-platform, open-source and totally free. Signal is recommended by Edward Snowden, and is a perfect solution for most users
Session	Session is a fork of Signal, however unlike Signal it does not require a mobile number (or any other personal data) to register, instead each user is identified by a public key. It is also decentralized, with servers being run by the community though Loki Net, messages are encrypted and routed through several of these nodes. All communications are E2E encrypted, and there is no meta data.

<table>
<tr><th>Provider</th><th>Description</th></tr>
<tr><td>XMPP</td><td>XMPP, also known as Jabber, is an open standard for decentralized messaging that has been widely used for decades. It has actually been the basis upon which WhatsApp, Facebook's Chat and Google's Talk were built, but these companies (eventually) chose to remove the interoperability with other servers. Prominent XMPP clients support OMEMO end-to-end encryption, which is based on the Double Ratchet Algorithm that is used in Signal. For more hands-on information and to register an account you can visit JoinJabber. Below you can find a list of OMEMO-enabled clients for all the major platforms.

<table>
<tr><th>Program</th><th>Linux</th><th>MacOS</th><th>Windows</th><th>Android</th><th>iOS</th></tr>
<tr><td>Gajim (OMEMO plugin)</td><td>✓</td><td>~</td><td>✓</td><td></td><td></td></tr>
<tr><td>Dino ✆</td><td>✓</td><td></td><td>✓</td><td></td><td></td></tr>
<tr><td>Conversations / Blabber ✆</td><td></td><td></td><td></td><td>✓</td><td></td></tr>
<tr><td>Monal IM</td><td></td><td>✓</td><td></td><td></td><td>✓</td></tr>
<tr><td>Beagle IM / Siskin IM ✆</td><td></td><td>✓</td><td></td><td></td><td>✓</td></tr>
</table></td></tr>
<tr><td>Matrix</td><td>Matrix is a decentralized open network for secure communications, with E2E encryption with Olm and Megolm. Along with the Element client, it supports VOIP + video calling and IM + group chats. Since Matrix has an open specification and Simple pragmatic RESTful HTTP/JSON API it makes it easy to integrates with existing 3rd party IDs to authenticate and discover users, as well as to build apps on top of it.</td></tr>
</table>

Other Notable Mentions

Other private, encrypted and open source messaging apps include: Surespot, Chat Secure (iOS only) and Status. Note that Tor Messengers been removed from the list, since development has halted.

KeyBase allows encrypted real-time chat, group chats, and public and private file sharing. It also has some nice features around cryptographically proving social identities, and makes PGP signing, encrypting and decrypting messages easy. However, since it was acquired by Zoom in 2020, it has no longer been receiving regular updates.

OpenPGP can be used over existing chat networks (such as email or message boards). It provides cryptographic privacy and authentication, PGP is used to encrypt messages.

Note/ Issues with PGP PGP is not easy to use for beginners, and could lead to human error/ mistakes being made, which would be overall much worse than if an alternate, simpler system was used. Do not use 32-bit key IDs - they are too short to be secure. There have also been vulnerabilities found in the OpenPGP and S/MIME, defined in EFAIL, so although it still considered secure for general purpose use, for general chat, it may be better to use an encrypted messaging or email app instead.

Word of Warning

Many messaging apps claim to be secure, but if they are not open source, then this cannot be verified - and they **should not be trusted**. This applies to Telegram, Threema, Cypher, Wickr, Silent Phone and Viber, to name a few - these apps should not be used to communicate any sensitive data. Wire has also been removed, due to a recent acquisition

P2P Messaging

With Peer-to-Peer networks, there are no central server, so there is nothing that can be raided, shut-down or forced to turn over data. There are P2P networks available that are open source, E2E encrypted, routed through Tor services, totally anonymous and operate without the collection of metadata.

Provider	Description
Session + **LokiNet** client	Loki is an open source set of tools that allow users to transact and communicate anonymously and privately, through a decentralised, encrypted, onion-based network. Session is a desktop and mobile app that uses these private routing protocols to secure messages, media and metadata.
Briar	Tor-based Android app for P2P encrypted messaging and forums. Where content is stored securely on your device (not in the cloud). It also allows you to connect directly with nearby contacts, without internet access (using Bluetooth or WiFi).
Ricochet Refresh	Desktop instant messenger, that uses the Tor network to rendezvous with your contacts without revealing your identity, location/ IP or meta data. There are no servers to monitor, censor, or hack so Ricochet is secure, automatic and easy to use.
Jami	P2P encrypted chat network with cross-platform GNU client apps. Jami supports audio and video calls, screen sharing, conference hosting and instant messaging.
Tox + **qTox** client	Open source, encrypted, distributed chat network, with clients for desktop and mobile - see supported clients. Clearly documented code and multiple language bindings make it easy for developers to integrate with Tox.

Other Notable Mentions

Cwtch, BitMessage, RetroShare, Tor Messenger *(deprecated)*, TorChat2 *(deprecated)*, Ricochet *(deprecated)*

Encrypted Email

Email is not secure - your messages can be easily intercepted and read. Corporations scan the content of your mail, to build up a profile of you, either to show you targeted ads or to sell onto third-parties. Through the Prism Program, the government also has full access to your emails (if not end-to-end encrypted) - this applies to Gmail, Outlook Mail, Yahoo Mail, GMX, ZoHo, iCloud, AOL and more.

The below email providers are private, end-to-end encrypted (E2EE) and reasonably secure. This should be used in conjunction with good email practices

Provider	Description

Provider	Description
ProtonMail	An open-source, end-to-end encrypted anonymous email service. ProtonMail has a modern easy-to-use and customizable UI, as well as fast, secure native mobile apps. ProtonMail has all the features that you'd expect from a modern email service and is based on simplicity without sacrificing security. It has a free plan or a premium option for using custom domains (starting at $5/month). ProtonMail requires no personally identifiable information for signup, they have a .onion server, for access via Tor, and they accept anonymous payment: BTC and cash (as well as the normal credit card and PayPal).
Tutanota	Free and open source email service based in Germany. It has a basic intuitive UI, secure native mobile apps, anonymous signup, and a .onion site. Tutonota has a full-featured free plan or a premium subscription for businesses allowing for custom domains ($12/ month). Tutanota does not use OpenPGP like most encrypted mail providers, instead they use a standardized, hybrid method consisting of a symmetrical and an asymmetrical algorithm (with 128 bit AES, and 2048 bit RSA). This causes compatibility issues when communicating with contacts using PGP. But it does allow them to encrypt much more of the header data (body, attachments, subject lines, and sender names etc) which PGP mail providers cannot do
Mailfence	Mailfence supports OpenPGP so that you can manually exchange encryption keys independently from the Mailfence servers, putting you in full control. Mailfence has a simple UI, similar to that of Outlook, and it comes with bundled with calendar, address book, and files. All mail settings are highly customizable, yet still clear and easy to use. Sign up is not anonymous, since your name, and prior email address is required. There is a fully-featured free plan, or you can pay for premium, and use a custom domain ($2.50/ month, or $7.50/ month for 5 domains), where Bitcoin, LiteCoin or credit card is accepted
MailBox.org	A Berlin-based, eco-friendly secure mail provider. There is no free plan, the standard service costs €12/year. You can use your own domain, with the option of a catch-all alias. They provide good account security and email encryption, with OpenPGP, as well as encrypted storage. There is no dedicated app, but it works well with any standard mail client with SSL. There's also currently no anonymous payment option
Skiff	End-to-end encrypted, open-source, and privacy-first email that also integrates Web3 features such as crypto wallets and decentralized storage. Skiff has a simple and intuitive UI, supports mobile apps on iOS and Android, and requires no personally identifiable information to sign up or create an account. Skiff offers a Pro plan with additional storage space, aliases, custom domains, and more for $8 per month that can be paid using a credit card or with a crypto wallet.

See OpenTechFund - Secure Email for more details.

See also Comparison or Private Email Providers and Email Security Checklist

Other Notable Mentions

HushMail, Soverin, StartMail, Posteo, Lavabit. For activists and journalists, see Disroot, Autistici, CriptText and RiseUp

Word of Warning

- When using an end-to-end encryption technology like OpenPGP, some metadata in the email header will not be encrypted.
- OpenPGP also does not support Forward secrecy, which means if either your or the recipient's private key is ever stolen, all previous messages encrypted with it will be exposed. You should take great care to keep your private keys safe.

Self-Hosted Email

If you do not want to trust an email provider with your messages, you can host your own mail server. Without experience, this can be notoriously hard to correctly configure, especially when it comes to security. You may also find that cost, performance and features make it a less attractive option. If you do decide to go down this route, Mail-in-a-box, is an easy to deploy, open source mail server. It aims to promote decentralization, innovation, and privacy on the web, as well as have automated, auditable, and idempotent system configuration. Other ready-to-go self-hosted mail options include Mailu and Mail Cow, both of which are docker containers.

Email Clients

Email clients are the programs used to interact with the mail server. For hosted email, then the web and mobile clients provided by your email service are usually adequate, and may be the most secure option. For self-hosted email, you will need to install and configure mail clients for web, desktop or mobile. A benefit of using an IMAP client, is that you will always have an offline backup of all email messages (which can then be encrypted and archived), and many applications let you aggregate multiple mailboxes for convenience. Desktop mail clients are not vulnerable to the common browser attacks, that their web app counterparts are.

Provider	Description
Mozilla Thunderbird (Desktop)	Free and open source email application developed and backed by Mozilla -it's secure, private easy and customizable. ~~The Enigmail add-on allows for easy encryption/ decryption of PGP messages~~ (as of V 78.2.1 encryption is built in), and the TorBirdy extension routes all traffic through the Tor network. Forks, such as Betterbird may add additional features
eM Client (Desktop)	Productivity-based email client, for Windows and MacOS. eM Client has a clean user interface, snappy performance and good compatibility. There is a paid version, with some handy features, including snoozing incoming emails, watching for replies for a specific thread, message translation, send later, and built-in Calendar, Tasks, Contacts and Notes. Note, eM Client is proprietary, and not open source
SnappyMail (Web)	Simple, modern, fast web-based mail client. This is an IMAP-only fork of RainLoop that mitigates a severe RainLoop vulnerability and adds several new features.

Provider	Description
RoundCube (Web)	Browser-based multilingual IMAP client with an application-like user interface. It provides full functionality you expect from an email client, including MIME support, address book, folder manipulation, message searching and spell checking
FairEmail (Android)	Open source, fully-featured and easy mail client for Android. Supports unlimited accounts and email addresses with the option for a unified inbox. Clean user interface, with a dark mode option, it is also very lightweight and consumes minimal data usage
K-9 Mail (Android)	K-9 is open source, very well supported and trusted - k9 has been around for nearly as long as Android itself! It supports multiple accounts, search, IMAP push email, multi-folder sync, flagging, filing, signatures, BCC-self, PGP/MIME & more. Install OpenKeychain along side it, in order to encrypt/ decrypt emails using OpenPGP
p≡p (Android/ iOS)	The Pretty Easy Privacy (p≡p) client is a fully decentralized and end-to-end encrypted mail client, for "automatic privacy". It has some nice features, however it is not open source

Word of Warning

One disadvantage of mail clients, is that many of them do not support 2FA, so it is important to keep your device secured and encrypted

Anonymous Mail Forwarding

Revealing your real email address online can put you at risk. Email aliasing allows messages to be sent to [anything]@my-domain.com and still land in your primary inbox. This protects your real email address from being revealed. Aliases are generated automatically, the first time they are used. This approach lets you identify which provider leaked your email address, and block an alias with 1-click.

Provider	Description
Anonaddy	An open source anonymous email forwarding service, allowing you to create unlimited email aliases. Has a free plan.
33Mail	A long-standing aliasing service. As well as receiving, 33Mail also lets you reply to forwarded addresses anonymously. Free plan, as well as Premium plan ($1/ month) if you'd like to use a custom domain
SimpleLogin	Fully open source (view on GitHub) allias service with many additional features. Can be self-hosted, or the managed version has a free plan, as well as hosted premium option ($2.99/ month) for using custom domains
Firefox Private Relay	Developed and managed by Mozilla, Relay is a Firefox addon, that lets you make an email alias with 1 click, and have all messages forwarded onto your personal email. Relay is totally free to use, and very accessible to less experienced users, but also open source, and able to me self-hosted for advanced usage

Provider	Description
ForwardEmail	Simple open source catch-all email forwarding service. Easy to self-host (see on GitHub), or the hosted version has a free plan as well as a ($3/month) premium plan
ProtonMail (Professional plan or higher)	If you already have ProtonMail's Professional (€8/month) or Visionary (€30/month) package, then an implementation of this feature is available via the Catch-All Email feature.

Alternatively you could host your own catch-all email service. Mailu can be configured to accept wildcards, or for Microsoft Exchange see exchange-catchall

Notable Mentions

mailhero.io is a smaller service, it does not have built-in encryption, so you will need to use PGP, but it is free.

Email Security Tools

Provider	Description
Enigmail	Mail client add-on, enabling the use of OpenPGP to easily encrypt, decrypt, verify and sign emails. Free and open source, Enigmail is compatible with Interlink Mail & News and Postbox. Their website contains thorough documentation and quick-start guides, once set up it is extremely convenient to use.
Email Privacy Tester	Quick tool, that enables you to test whether your mail client "reads" your emails before you've opened them, and also checks what analytics, read-receipts or other tracking data your mail client allows to be sent back to the sender. The system is open source (on GitLab), developed by Mike Cardwell and trusted, but if you do not want to use your real email, creating a second account with the same provider, should yield identical results
DKIM Verifier	Verifies DKIM signatures and shows the result in the e-mail header, in order to help spot spoofed emails (which do not come from the domain that they claim to)

Notable Mentions

If you are using ProtonMail, then the ProtonMail Bridge enables you to sync your emails to your own desktop mail client. It works well with Thunderbird, Microsoft Outlook and others

VOIP Clients

Provider	Description
Mumble	Open source, low-latency, high quality voice chat software. You can host your own server, or use a hosted instance, there are client applications for Windows, MacOS and Linux as well as third-party apps for Android and iOS.

Provider	Description
Linphone	Open source audio, video and IM groups with E2E encryption and built-in media server. SIP-based evolving to RCS. Native apps for Android, iOS, Windows, GNU/Linux and MacOS

Notable Mentions

SpoofCard lets you make anonymous phone calls + voicemail, but not open source and limited information on security (avoid sending any secure info).
MicroSip is an open source portable SIP softphone for Windows based on PJSIP stack

Virtual Phone Numbers

Provider	Description
Silent.link	Anonymous eSIM for sending / receiving SMS, incoming calls and 4G / 5G internet + world-wide roaming. No data is required at sign-up. Affordable pricing, with payments and top-ups accepted in BTC. Requires an eSim-compatible device
Crypton.sh	Physical SIM card in the cloud, for sending + receiving SMS messages. Messages are encrypted using your chosen private key. Includes a web interface, as well as an API for interacting with it from any device. Pricing is around €7.00/month, and payment is accepted in BTC, XMR or credit card
Jmp.chat	Phone number for incoming + outgoing calls and messages, provided by Soprani. Works with Jabber, Matrix, Snikket, XMPP or any SIP client. Pricing starts at $2.99 / month. Only available in the US and Canada, as (as of 2022) the service is still in Beta
MoneroSMS	Anonymous SMS service able to activate accounts. Accessible over web, CLI, or email. Pricing starts at $3.60 / month. The service is in beta as of 2022.

Team Collaboration Platforms

Now more than ever we are relying on software to help with team collaboration. Unfortunately many popular options, such as Slack, Microsoft Teams, Google for Work and Discord all come with some serious privacy implications.

Typical features of team collaboration software includes: instant messaging, closed and open group messaging, voice and video conference calling, file sharing/ file drop, and some level or scheduling functionality.

Provider	Description
Rocket.Chat	Easy-to-deploy, self-hosted team collaboration platform with stable, feature-rich cross-platform client apps. The UI is fast, good looking and intuitive, so very little technical experience is needed for users of the platform. Rocket.Chat's feature set is similar to Slack's, making it a good replacement for any team looking to have greater control over their data

Provider	Description
RetroShare	Secure group communications, with the option to be used over Tor or I2P. Fast intuitive group and 1-to-1 chats with text and rich media using decentralized chat rooms, with a mail feature for delivering messages to offline contacts. A channels feature makes it possible for members of different teams to stay up-to-date with each other, and to share files. Also includes built-in forums, link aggregations, file sharing and voice and video calling. RetroShare is a bit more complex to use than some alternatives, and the UI is quite *retro*, so may not be appropriate for a non-technical team
Element	Privacy-focused messenger using the Matrix protocol. The Element client allows for group chat rooms, media sharing voice and video group calls.
Internet Relay Chat	An IRC-based solution is another option, being decentralized there is no point of failure, and it's easy to self-host. However it's important to keep security in mind while configuring your IRC instance and ensure that channels are properly encrypted - IRC tends to be better for open communications. There's a variety of clients to choose from - popular options include: The Longe (Web-based), HexChat (Linux), Pidgin (Linux), WeeChat (Linux, terminal-based), IceChat (Windows), XChat Aqua (MacOS), Palaver (iOS) and Revolution (Android)
Mattermost	Mattermost has an open source edition, which can be self-hosted. It makes a good Slack alternative, with native desktop, mobile and web apps and a wide variety of integrations
Dialog	A corporate secure collaborative messenger. A clean UI and all the basic features, including groups, file sharing, audio/ video calls, searching and chat bots

Notable Mentions

Some chat platforms allow for cross-platform group chats, voice and video conferencing, but without the additional collaboration features. For example, Tox, Session, Ricochet, Mumble and Jami.

For Conferences, OSEM is an open source all-in-one conference management tool, providing Registration, Schedules, Live and Recorded Sessions, Paper Submissions, Marketing Pages and Administration.

Browser Extensions

The following browser add-ons give you better control over what content is able to be loaded and executed while your browsing.

Provider	Description
Privacy Badger	Blocks invisible trackers, in order to stop advertisers and other third-parties from secretly tracking where you go and what pages you look at. **Download**: Chrome \ Firefox

Provider	Description
HTTPS Everywhere	Forces sites to load in HTTPS, in order to encrypt your communications with websites, making your browsing more secure (Similar to Smart HTTPS). Note this functionality is now included by default in most modern browsers. **Download**: Chrome \ Firefox
uBlock Origin	Block ads, trackers and malware sites. **Download**: Chrome \ Firefox
ScriptSafe	Allows you to block the execution of certain scripts. **Download**: Chrome \ Firefox
Firefox Multi-Account Containers	Firefox Multi-Account Containers lets you keep parts of your online life separated into color-coded tabs that preserve your privacy. Cookies are separated by container, allowing you to use the web with multiple identities or accounts simultaneously. **Download**: Firefox
Temporary Containers	This Extension, combined with Firefox Multi-Account Containers, let's you isolate cookies and other private data for each web site. **Download**: Firefox
WebRTC-Leak-Prevent	Provides user control over WebRTC privacy settings in Chromium, in order to prevent WebRTC leaks. **Download**: Chrome. For Firefox users, you can do this through browser settings. Test for WebRTC leaks, with browserleaks.com/webrtc
Canvas Fingerprint Blocker	Block fingerprint without removing access to HTML5 Canvas element. Canvas fingerprinting is commonly used for tracking, this extension helps to mitigate this through disallowing the browser to generate a true unique key **Download:** Chrome \ Firefox \ Edge \ Source
ClearURLs	This extension will automatically remove tracking elements from the GET parameters of URLs to help protect some privacy **Download**: Chrome \ Firefox / Source
CSS Exfil Protection	Sanitizes and blocks any CSS rules which may be designed to steal data, in order to guard against Exfil attacks **Download**: Chrome \ Firefox \ Source
First Party Isolation	Enables the First Party isolation preference (Clicking the Fishbowl icon temporarily disables it) **Download**: Firefox
Privacy-Oriented Origin Policy	Prevent Firefox from sending Origin headers when they are least likely to be necessary, to protect your privacy **Download**: Firefox \ Source
LocalCDN	Emulates remote frameworks (e.g. jQuery, Bootstrap, Angular) and delivers them as local resource. Prevents unnecessary 3rd party requests to tracking CDNs **Download**: Firefox
Decentraleyes	Similar to LocalCDN, Serves up local versions of common scripts instead of calling to 3rd-party CDN. Improves privacy and load times. Works out-of-the-box and plays nicely with regular content blockers. **Download**: Chrome \ Firefox \ Opera \ Pale Moon \ Source

Provider	Description
Privacy Essentials	Simple extension by DuckDuckGo, which grades the security of each site. **Download**: Chrome \ Firefox
Self-Destructing Cookies	Prevents websites from tracking you by storing unique cookies (note Fingerprinting is often also used for tracking). It removes all related cookies whenever you end a session. **Download**: Chrome \ Firefox \ Opera \ Source
Privacy Redirect	A simple web extension that redirects Twitter, YouTube, Instagram & Google Maps requests to privacy friendly alternatives **Download**: Firefox / Chrome
Site Bleacher	Remove automatically cookies, local storages, IndexedDBs and service workers **Download**: Firefox \ Chrome \ Source
User Agent Switcher	Spoofs browser's User-Agent string, making it appear that you are on a different device, browser and version to what you are actually using. This alone does very little for privacy, but combined with other tools, can allow you to keep your fingerprint changing, and feed fake info to sites tracking you. Some websites show different content, depending on your user agent. **Download**: Chrome \ Fireforx \ Edge \ Opera \ Source
PrivacySpy	The companian extension for PrivacySpy.org - an open project that rates, annotates, and archives privacy policies. The extension shows a score for the privacy policy of the current website. **Download**: Chrome \ Fireforx
HTTPZ	Simplified HTTPS upgrades for Firefox (lightweight alternative to HTTPS-Everywhere) **Download**: Firefox
Skip Redirect	Some web pages use intermediary pages before redirecting to a final page. This add-on tries to extract the final url from the intermediary url and goes there straight away if successful **Download**: Firefox \ Source
Web Archives	View archived and cached versions of web pages on 10+ search engines, such as the Wayback Machine, Archive.is, Google etc Useful for checking legitimacy of websites, and viewing change logs **Download**: Firefox \ Chrome \ Edge \ Source
Flagfox	Displays a country flag depicting the location of the current website's server, which can be useful to know at a glance. Click icon for more tools such as site safety checks, whois, validation etc **Download**: Firefox
Lightbeam	Visualize in detail the servers you are contacting when you are surfing on the Internet. Created by Gary Kovacs (former CEO of Mozilla), presented in his TED Talk. **Download**: Firefox \ Source

Provider	Description
Track Me Not	Helps protect web searchers from surveillance and data-profiling, through creating meaningless noise and obfuscation, outlined in their whitepaper. Controversial whether or not this is a good approach **Download**: Chrome \ Firefox \ Source
AmIUnique Timeline	Enables you to better understand the evolution of browser fingerprints (which is what websites use to uniquely identify and track you). **Download**: Chrome \ Firefox
Netcraft Extension	Notifies you when visiting a known or potential phishing site, and detects suspicious JavaScript (including skimmers and miners). Also provides a simple rating for a given sites legitimacy and security. Great for less technical users. Netcraft also has a handy online tool: Site Report for checking what any given website is running. **Download**: Chrome \ Firefox \ Opera \ Edge

Notable Mention

Extension source viewer is a handy extension for viewing the source code of another browser extension, which is a useful tool for verifying the code does what it says

Word of Warning

- *Having many extensions installed raises entropy, causing your fingerprint to be more unique, hence making tracking easier.*
- *Much of the functionality of the above addons can be applied without installing anything, by configuring browser settings yourself. For Firefox this is done in the user.js*
- *Be careful when installing unfamiliar browser add-ons, since some can compromise your security and privacy. At the time of writing, the above list were all open source, verified and 'safe' extensions.*
- *In most situations, only a few of the above extensions will be needed in combination.*
- *See the arkenfox wiki for more information on the obsolescence and purposelessness of many popular extensions, and why you may only need a very limited set.*

See also Browser & Search Security Checklist

Mobile Apps

Provider	Description
Orbot	System-wide Tor proxy, which encrypts your connection through multiple nodes. You can also use it alongside Tor Browser to access .onion sites.
NetGuard	A firewall app for Android, which does not require root. NetGuard provides simple and advanced ways to block access to the internet, where applications and addresses can individually be allowed or denied access to your Wi-Fi and/or mobile connection.
Island	A sandbox environment, allowing you to clone selected apps and run them in an isolated box, preventing it from accessing your personal data, or device information
[Insular]	An actively-maintained fork of the dead Island project with additional enhancements

Provider	Description
Exodus	Shows which trackers, each of your installed apps is using, so that you can better understand how your data is being collected. Uses data from the Exodus database of scanned APKs.
Bouncer	Gives you the ability to grant permissions temporarily, so that you could for example use the camera to take a profile picture, but when you close the given app, those permissions will be revoked
XPrivacyLua	Simple to use privacy manager for Android, that enables you to feed apps fake data when they request intimate permissions. Solves the problem caused by apps malfunctioning when you revoke permissions, and protects your real data by only sharing fake information. Enables you to hide call log, calendar, SMS messages, location, installed apps, photos, clipboard, network data plus more. And prevents access to camera, microphone, telemetry, GPS and other sensors
SuperFreezZ	Makes it possible to entirely freeze all background activities on a per-app basis. Intended purpose is to speed up your phone, and prolong battery life, but this app is also a great utility to stop certain apps from collecting data and tracking your actions while running in the background
Haven	Allows you to protect yourself, your personal space and your possessions - without compromising on security. Leveraging device sensors to monitor nearby space, Haven was developed by The Guardian Project, in partnership with Edward Snowden
XUMI Security	Checks for, and resolves known security vulnerabilities. Useful to ensure that certain apps, or device settings are not putting your security or privacy at risk
Daedalus	No root required Android DNS modifier and hosts/DNSMasq resolver, works by creating a VPN tunnel to modify the DNS settings. Useful if you want to change your resolver to a more secure/ private provider, or use DNS over HTTPS
Secure Task	Triggers actions, when certain security conditions are met, such as multiple failed login attempts or monitor settings changed. It does require Tasker, and needs to be set up with ADB, device does not need to be rooted
Cryptomator	Encrypts files and folders client-side, before uploading them to cloud storage (such as Google Drive, One Drive or Dropbox), meaning none of your personal documents leave your device in plain text
1.1.1.1	Lets you use CloudFlares fast and secure 1.1.1.1 DNS, with DNS over HTTPS, and also has the option to enable CloudFlares WARP+ VPN
Fing App	A network scanner to help you monitor and secure your WiFi network. The app is totally free, but to use the advanced controls, you will need a Fing Box
FlutterHole	Easy monitoring and controll over your Pi Hole instance. Pi Hole is great for security, privacy and speed

Provider	Description
DPI Tunnel	An application for Android that uses various techniques to bypass DPI (Deep Packet Inspection) systems, which are used to block some sites (not available on Play store)
Blokada	This application blocks ads and trackers, doesn't require root and works for all the apps on your Android phone. Check out how it works here.
SnoopSnitch	Collects and analyzes mobile radio data to make you aware of your mobile network security and to warn you about threats like fake base stations (IMSI catchers), user tracking and over-the-air updates
TrackerControl	Monitor and control hidden data collection in mobile apps about user behavior/ tracking
Greentooth	Auto-disable Bluetooth, then it is not being used. Saves battery, and prevent some security risks
PrivateLock	Auto lock your phone based on movement force/ acceleration
CamWings	Prevent background processes gaining unauthorized access to your devices camera. Better still, use a webcam sticker
ScreenWings	Prevent background processes taking unauthorized screenshots, which could expose sensitive data
AFWall+	Android Firewall+ (AFWall+) is an advanced iptables editor (GUI) for rooted Android devices, which provides very fine-grained control over which Android apps are allowed to access the network
Catch the Man-in-the-Middle	Simple tool, that compares SHA-1 fingerprints of the the SSL certificates seen from your device, and the certificate seen from an external network. If they do not match, this may indicate a man-in-the-middle modifying requests
RethinkDNS + Firewall	An open-source ad-blocker and firewall app for Android 6+ (does not require root)
F-Droid	F-Droid is an installable catalogue of FOSS applications for Android. The client enabled you to browse, install, and keep track of updates on your device

Word of Warning

Too many installed apps will increase your attack surface - only install applications that you need

Other Notable Mentions

For more open source security & privacy apps, check out these publishers: The Guardian Project, The Tor Project, Oasis Feng, Marcel Bokhorst, SECUSO Research Group and Simple Mobile Tools- all of which are trusted developers or organisations, who've done amazing work.

For offensive and defensive security, see The Kali Nethunter Catalogue of apps

For *advanced* users, the following tools can be used to closely monitor your devise and networks, in order to detect any unusual activity. PortDroid for network analysis, Packet Capture to monitor network traffic, SysLog for viewing system logs, Dexplorer to read .dex or .apk files for your installed apps, and Check and Test to check status and details of devices hardware.

See also Mobile Security Checklist

Online Tools

A selection of free online tools and utilities, to check, test and protect

Provider	Description
';--have i been pwned?	Checks if your credentials (Email address or Password) have been compromised in a data breach. See also Firefox Monitor
εxodus	Checks how many, and which trackers any Android app has. Useful to understand how data is being collected before you install a certain APK, it also shows which permissions the app asks for
Am I Unique?	Show how identifiable you are on the Internet by generating a fingerprint based on device information. This is how many websites track you (even without cookies enabled), so the aim is to not be unique
Panopticlick	Check if your browser safe against tracking. Analyzes how well your browser and add-ons protect you against online tracking techniques, and if your system is uniquely configured—and thus identifiable
Phish.ly	Analyzes emails, checking the URLs and creating a SHA256 and MD5 hash of attachments, with a link to VirusTotal. To use the service, just forward a potentially malicious or suspicious email to scan@phish.ly, and an automated reply will include the results. They claim that all email data is purged after analysis, but it would be wise to not include any sensitive information, and to use a forwarding address
Browser Leak Test	Shows which of personal identity data is being leaked through your browser, so you can better protect yourself against fingerprinting
IP Leak Test	Shows your IP address, and other associated details (location, ISP, WebRTC check, DNS, and lots more)
EXIF Remove	Displays, and removes Meta and EXIF data from an uploaded photo or document
Redirect Detective	Check where a suspicious URL redirects to (without having to click it). Lets you avoid being tracked by not being redirected via adware/tracking sites, or see if a shortened link actually resolves a legitimate site, or see if link is an affiliate ad
Blocked.org	Checks if a given website is blocked by filters applied by your mobile and broadband Internet Service Providers (ISP)

Provider	Description
Virus Total	Analyses a potentially-suspicious web resources (by URL, IP, domain or file hash) to detect types of malware (*note: files are scanned publicly*)
Hardenize	Scan websites and shows a security overview, relating to factors such as HTTPS, domain info, email data, www protocols and so on
Is Legit?	Checks if a website or business is a scam, before buying something from it
Deseat Me	Tool to help you clean up your online presence - Instantly get a list of all your accounts, delete the ones you are not using
Should I Remove It?	Ever been uninstalling programs from your Windows PC and been unsure of what something is? Should I Remove It is a database of Windows software, detailing whether it is essential, harmless or dangerous
10 Minute Mail	Generates temporary disposable email address, to avoid giving your real details
MXToolBox Mail Headers	Tool for analyzing email headers, useful for checking the authenticity of messages, as well as knowing what info you are revealing in your outbound messages
Am I FloCed?	Google testing out a new tracking feature called Federated Learning of Cohorts (aka "FLoC"). It currently effects 0.5% of Chrome users, this tool developed by the EFF will detect if you are affected, and provide additional info on how to stay protected
Site Report	A tool from Netcraft, for analysing what any given website is running, where it's located and information about its host, registrar, IP and SSL certificates.

Word of Warning

Browsers are inherently insecure, be careful when uploading, or entering personal details.

Virtual Private Networks

VPNs are good for getting round censorship, increasing protection on public WiFi, obscuring your IP address, and reducing what data your ISP can log. But for the best anonymity, you should use Tor. VPNs do not mean you are magically protected, or anonymous (see below).

Provider	Description
Mullvad	Mullvad is one of the best for privacy, they have a totally anonymous sign up process, you don't need to provide any details at all, you can choose to pay anonymously too (with Monero, BTC or cash)

Provider	Description
Azire	Azire is a Swedish VPN provider, who owns their own hardware with physically removed storage and a no logging policy. Pricing starts at €3.25/mo, with crypto (including XMR) supported. Note that they've not yet been audited, and client applications are not open source, for more info, see #140.
IVPN	Independently Security Audited VPN with anonymous signup, no logs, no cloud or customer data stored, open-source apps and website. Strong ethics: no trackers, no false promises, no surveillance ads. Accepts various payment methods including crypotcurrencies.
ProtonVPN	From the creators of ProtonMail, ProtonVPN has a solid reputation. They have a full suite of user-friendly native mobile and desktop apps. ProtonVPN is one of the few "trustworthy" providers that also offer a free plan
OVPN	A court-proven VPN service with support for Wireguard and OpenVPN support, and optional ad-blocking. Running on dedicated hardware, with no hard drives

Word of Warning

- *A VPN does not make you anonymous - it merely changes your public IP address to that of your VPN provider, instead of your ISP. Your browsing session can still be linked back to your real identity either through your system details (such as user agent, screen resolution even typing patterns), cookies/ session storage, or by the identifiable data that you enter. Read more about fingerprinting*
- *Logging - If you choose to use a VPN because you do not agree with your ISP logging your full browsing history, then it is important to keep in mind that your VPN provider can see (and mess with) all your traffic. Many VPNs claim not to keep logs, but you cannot be certain of this (VPN leaks). See this article for more*
- *IP Leaks - If configured incorrectly, your IP may be exposed through a DNS leak. This usually happens when your system is unknowingly accessing default DNS servers rather than the anonymous DNS servers assigned by an anonymity network or VPN. Read more: What is a DNS leak, DNS Leak Test, How to Fix a DNS Leak*
- *Stealth - It will be visible to your adversary that you are using a VPN (usually from the IP address), but other system and browser data, can still reveal information about you and your device (such as your local time-zone, indicating which region you are operating from)*
- *Many reviews are sponsored, and hence biased. Do your own research, or go with one of the above options*
- *Using Tor (or another Mix Network) may be a better option for anonimity*

Considerations

While choosing a VPN, consider the following: Logging policy (logs are bad), Jurisdiction (avoid 5-eyes), Number of servers, availability and average load. Payment method (anonymous methods such as BTC, Monero or cash are better), Leak protection (1st-party DNS servers = good, and check if IPv6 is supported), protocols (OpenVPN and WireGuard = good). Finally, usability of their apps, user reviews and download speeds.

Self-Hosted VPN

If you don't trust a VPN provider not to keep logs, then you could self-host your own VPN. This gives you you total control, but at the cost of anonymity (since your cloud provider, will require your billing info). See Streisand, to learn more, and get started with running a VPN.
Digital Ocean provides flexible, secure and easy Linux VMs, (from $0.007/hour or $5/month), this guide explains how to set up VPN on: CentOS 7 or Ubuntu 18.4+. See more about configuring OpenVPN or IKEv2. Alternatively, here is a 1-click install scriptfor on Digital Ocean, by Carl Friess.

Recently distributed self-hosted solutions for running your own VPNs have become more popular, with services like Outline letting you spin up your own instance and share it with friends and family. Since it's distributed, it is very resistant to blocking, and gives you world-wide access to the free and open internet. And since you have full control over the server, you can be confident that there is no logging or monitoring happening. However it comes at the cost of anonymity, especially if it's only you using your instance.

Self-Hosted Network Security

Fun little projects that you can run on a Raspberry Pi, or other low-powered computer. In order to help detect and prevent threats, monitor network and filter content

Provider	Description
Pi-Hole	Network-level advertisement and Internet tracker blocking application which acts as a DNS sinkhole. Pi-Hole can significantly speed up your internet, remove ads and block malware. It comes with a nice web interface and a mobile app with monitoring features, it's open source, easy to install and very widely used
Technitium	Another DNS server for blocking privacy-invasive content at it's source. Technitium doesn't require much of a setup, and basically works straight out of the box, it supports a wide range of systems (and can even run as a portable app on Windows). It allows you to do some additional tasks, such as add local DNS addresses and zones with specific DNS records. Compared to Pi-Hole, Technitium is very lightweight, but lacks the deep insights that Pi-Hole provides, and has a significantly smaller community behind it
IPFire	A hardened, versatile, state-of-the-art open source firewall based on Linux. Its ease of use, high performance and extensibility make it usable for everyone
PiVPN	A simple way to set up a home VPN on a any Debian server. Supports OpenVPN and WireGuard with elliptic curve encryption keys up to 512 bit. Supports multiple DNS providers and custom DNS providers - works nicely along-side PiHole
E2guardian	Powerful open source web content filter
SquidGuard	A URL redirector software, which can be used for content control of websites users can access. It is written as a plug-in for Squid and uses blacklists to define sites for which access is redirected
PF Sense	Widely used, open source firewall/router
Zeek	Detect if you have a malware-infected computer on your network, and powerful network analysis framework and monitor
Firezone	Open-source self-hosted VPN and firewall built on WireGuard®.

Don't want to build? See also: Pre-configured security boxes

Mix Networks

Mix networks are routing protocols, that create hard-to-trace communications, by encrypting and routing traffic through a series of nodes. They help keep you anonymous online, and unlike VPNs -there are no logs

Provider	Description
Tor	Tor provides robust anonymity, allowing you to defend against surveillance, circumvent censorship and reduce tracking. It blocks trackers, resists fingerprinting and implements multi-layered encryption by default, meaning you can browse freely. Tor also allows access to OnionLand: hidden services
I2P	I2P offers great generic transports, it is well geared towards accessing hidden services, and has a couple of technical benefits over Tor: P2P friendly with unidirectional short-lived tunnels, it is packet-switched (instead of circuit-switched) with TCP and UDP, and continuously profiles peers, in order to select the best performing ones. I2P is less mature, but fully-distributed and self-organising, its smaller size means that it hasn't yet been blocked or DOSed much
Freenet	Freenet is easy to setup, provides excellent friend To Friend Sharing vs I2P, and is great for publishing content anonymously. It's quite large in size, and very slow so not the best choice for casual browsing

Tor, I2P and Freenet are all anonymity networks - but they work very differently and each is good for specific purposes. So a good and viable solution would be to use all of them, for different tasks.
You can read more about how I2P compares to Tor, here

Notable Mentions

See also: GNUnet, IPFS, ZeroNet, Panoramix, and Nym

Word of Warning

To provide low-latency browsing, Tor does not mix packets or generate cover traffic. If an adversary is powerful enough, theoretically they could either observe the entire network, or just the victims entry and exit nodes. It's worth mentioning, that even though your ISP can not see what you are doing, they will be able determine that you are using a mix net, to hide this - a VPN could be used as well. If you are doing anything which could put you at risk, then good OpSec is essential, as the authorities have traced criminals through the Tor network before, and made arrests. Don't let Tor provide you a false sense of security - be aware of information leaks through DNS, other programs or human error. Tor-supported browsers may might lag behind their upstream forks, and include exploitable unpatched issues. See #19

Note: The Tor network is run by the community. If you benefit from using it and would like to help sustain uncensored internet access for all, consider running a Tor relay

Proxies

A proxy acts as a gateway between you and the internet, it can be used to act as a firewall or web filter, improves privacy and can also be used to provide shared network connections and cache data to speed up common requests. Never use a free proxy.

Provider	Description
ShadowSocks	Secure socks5 proxy, designed to protect your Internet traffic. Open source, superfast, cross-platform and easy to deploy, see GitHub repo
Privoxy	Non-caching web proxy with advanced filtering capabilities for enhancing privacy, modifying web page data and HTTP headers, controlling access, and removing ads and other obnoxious Internet junk

Notable Mentions

V2ray-core is a platform for building proxies to bypass network restrictions and protect your privacy. See more

Word of Warning

Malicious Proxies are all too common. Always use open source software, host it yourself or pay for a reputable cloud service. Never use a free proxy; it can monitor your connection, steal cookies and contain malware. VPNs are a better option, better still - use the Tor network.

DNS

Without using a secure, privacy-centric DNS all your web requests can be seen in the clear. You should configure your DNS queries to be managed by a service that respects privacy and supports DNS-over-TLS, DNS-over-HTTPS or DNSCrypt.

Provider	Description
CloudFlare	One of the most performant options, Cloudflare's DNS supports DoH and DoT, and has a Tor implementation, providing world-class protection. They have native cross-platform apps, for easy set-up.
AdGuard	Open-source DNS provider, specialising in the blocking of ads, trackers and malicious domains. They have been independently audited and do not keep logs
NextDNS	An ad-blocking, privacy-protecting, censorship-bypassing DNS. Also comes with analytics, and the ability to shield kids from adult content

See also this Full List of Public DoH Servers, you can then check the performance of your chosen server with DNSPerf. Awesome Self-Hosted also has a good list. To read more about choosing secure DNS servers, see this article, and this article.

Notable Mentions

- Quad9 is a well-funded, performant DNS with a strong focus on privacy and security and easy set-up, however questions have been raised about the motivation of some of the financial backers.
- BlahDNS (Japan, Finland or Germany) is an excellent security-focused DNS

- OpenNIC, NixNet DNS and UncensoredDNS are open source and democratic, privacy-focused DNS
- Unbound is a validating, recursive, caching DNS resolver, designed to be fast and lean. Incorporates modern features and based on open standards
- Clean Browsing, is a good option for protecting kids, they offer comprehensive DNS-based Content Filtering
- Mullvad Mullvads public DNS with QNAME minimization and basic ad blocking. It has been audited by the security experts at Assured. You can use this privacy-enhancing service even if you don't use Mullvad.

Word of Warning

Using an encrypted DNS resolver will not make you anonymous, it just makes it harder for third-partied to discover your domain history. If you are using a VPN, take a DNS leak test, to ensure that some requests are not being exposed.

DNS Protocols

DNS-over-TLS was proposed in RTC-7858 by the IETF, then 2 years later, the DNS-over-HTTPS specification was outlined in RFC8484 in October '18. DNSCrypt, is a protocol that authenticates communications between a DNS client and a DNS resolver. It prevents DNS spoofing, through using cryptographic signatures to verify that responses originate from the chosen DNS resolver, and haven't been tampered with. DNSCrypt is a well battle-tested protocol, that has been in use since 2013, and is still widely used.

DNS Clients

Provider	Description
DNScrypt-proxy 2 (Desktop - BSD, Linux, Solaris, Windows, MacOS & Android)	A flexible DNS proxy, with support for modern encrypted DNS protocols including DNSCrypt V2, DNS-over-HTTPS and Anonymized DNSCrypt. Also allows for advanced monitoring, filtering, caching and client IP protection through Tor, SOCKS proxies or Anonymized DNS relays.
Unbound (Desktop - BSD, Linux, Windows & MacOS)	Validating, recursive, caching DNS resolve with support for DNS-over-TLS. Designed to be fast, lean, and secure Unbound incorporates modern features based on open standards. It's fully open source, and recently audited. *(For an in-depth tutorial, see this article by DNSWatch.)*
Nebulo (Android)	Non-root, small-sized DNS changer utilizing DNS-over-HTTPS and DNS-over-TLS. *(Note, since this uses Android's VPN API, it is not possible to run a VPN while using Nebulo)*

Provider	Description
RethinkDNS + Firewall (Android)	Free and open source DNS changer with support for DNS-over-HTTPS, DNS-over-Tor, and DNSCrypt v3 with *Anonymized Relays*. *(Note, since this uses Android's VPN API, it is not possible to run a VPN while using RethinkDNS + Firewall)*
DNS Cloak (iOS)	Simple all that allows for the use for dnscrypt-proxy 2 on an iPhone.
Stubby (Desktop - Linux, Mac, OpenWrt & Windows)	Acts as a local DNS Privacy stub resolver (using DNS-over-TLS). Stubby encrypts DNS queries sent from a client machine (desktop or laptop) to a DNS Privacy resolver increasing end user privacy. Stubby can be used in combination with Unbound - Unbound provides a local cache and Stubby manages the upstream TLS connections (since Unbound cannot yet re-use TCP/TLS connections), see example configuration

Firewalls

A firewall is a program which monitors the incoming and outgoing traffic on your network, and blocks requests based on rules set during its configuration. Properly configured, a firewall can help protect against attempts to remotely access your computer, as well as control which applications can access which IPs.

Provider	Description
NetGuard (Android)	Provides simple and advanced ways to block access to the internet. Applications and addresses can individually be allowed or denied access to Wi-Fi and/or mobile connection
NoRoot Firewall (Android)	Notifies you when an app is trying to access the Internet, so all you need to do is just Allow or Deny. Allows you to create filter rules based on IP address, host name or domain name, and you can allow or deny only specific connections of an app
AFWall+ (Android - Rooted)	Android Firewall+ (AFWall+) is an advanced iptables editor (GUI) for rooted Android devices, which provides very fine-grained control over which Android apps are allowed to access the network
RethinkDNS + Firewall (Android)	An open-source ad-blocker and firewall app for Android 6+ (does not require root)
Lockdown (iOS)	Firewall app for iPhone, allowing you to block any connection to any domain
SimpleWall (Windows)	Tool to control Windows Filtering Platform (WFP), in order to configure detailed network activity on your PC
LuLu (Mac OS)	Free, open source macOS firewall. It aims to block unknown outgoing connections, unless explicitly approved by the user
Little Snitch (Mac OS)	A very polished application firewall, allowing you to easily manage internet connections on a per-app basis

Provider	Description
OpenSnitch (Linux)	Makes internet connections from all apps visible, allowing you to block or manage traffic on a per-app basis. GNU/Linux port of the Little Snitch application firewall
Gufw (Linux)	Open source GUI firewall for Linux, allowing you to block internet access for certain applications. Supports both simple and advanced mode, GUI and CLI options, very easy to use, lightweight/ low-overhead, under active maintenance and backed by a strong community. Installable through most package managers, or compile from source
Uncomplicated Firewall (Linux)	The ufw (Uncomplicated Firewall) is a GUI application and CLI, that allows you to configure a firewall using `iptables` much more easily
IPFire (hardware)	IPFire is a hardened, versatile, state-of-the-art Open Source firewall based on Linux. Easy to install on a raspberry Pi, since it is lightweight and heavily customizable
Shorewall (hardware)	An open source firewall tool for Linux that builds upon the Netfilter system built into the Linux kernel, making it easier to manage more complex configuration schemes with iptables
OpenSense (hardware)	Enterprise firewall and router for protecting networks, built on the FreeBSD system

Word of Warning

There are different types of firewalls, that are used in different circumstances. This does not omit the need to configure your operating systems defences. Follow these instructions to enable your firewall in Windows, Mac OS, Ubuntu and other Linux distros.
Even when properly configured, having a firewall enabled does not guarantee bad network traffic can not get through and especially during boot if you don't have root privileges.

Ad Blockers

There are a few different ways to block ads - browser-based ad-blockers, router-based / device blockers or VPN ad-blockers. Typically they work by taking a maintained list of hosts, and filtering each domain/ IP through it. Some also have other methods to detect certain content based on pattern matching

Provider	Description
Pi-Hole (Server/ VM/ Pi)	Incredibly powerful, network-wide ad-blocker. Works out-of-the-box, light-weight with an intuitive web interface, but still allows for a lot of advanced configuration for power users. As well as blocking ads and trackers, Pi-Hole speeds up your network speeds quite significantly. The dashboard has detailed statistics, and makes it easy to pause/ resume Pi-Hole if needed.
Diversion (Router)	A shell script application to manage ad-blocking, Dnsmasq logging, Entware and pixelserv-tls installations and more on supported routers running Asuswrt-Merlin firmware, including its forks

Provider	Description
DN66 (Android)	DNS-based host and ad blocker for Android. Easy to configure, but the default config uses several widely-respected host files. aimed at stopping ads, malware, and other weird stuff
BlockParty (iOS/ MacOS)	Native Apple (Swift) apps, for system-wide ad-blocking. Can be customized with custom host lists, primarily aimed for just ad-blocking
hBlock (Unix)	A POSIX-compliant shell script, designed for Unix-like systems, that gets a list of domains that serve ads, tracking scripts and malware from multiple sources and creates a hosts file (alternative formats are also supported) that prevents your system from connecting to them. Aimed at improving security and privacy through blocking advert, tracking and malware associated domains
Blokada (Android/ iOS)	Open source mobile ad-blocker that acts like a firewall. Since it's device-wide, once connected all apps will have ads/ trackers blocked, and the blacklist can be edited. The app is free, but there is a premium option, which has a built-in VPN
RethinkDNS + Firewall (Android)	Free and open source ad-blocker and a firewall for Android 6+ (no root required)
Ad Block Radio (Sound)	Python script that uses machine learning to block adverts in live audio streams, such as Radio, Podcasts, Audio Books, and music platforms such as Spotify. See live demo
uBlock Origin (Browser)	Light-weight, fast browser extension for Firefox and Chromium (Chrome, Edge, Brave Opera etc), that blocks tracking, ads and known malware. uBlock is easy-to-use out-of-the-box, but also has a highly customisable advanced mode, with a point-and-click firewall which can be configured on a per-site basis
uMatrix (Browser)	**uMatrix is no longer being actively maintained**. Another light-weight browser extension, for Chromium and Firefox browsers. uMatrix acts more like a firewall, giving you the option for super fine-grained control over every aspect of resource blocking. It is possible to use both uBlock (for simple/ cosmetic ad blocking) and uMatrix (for detailed JavaScript blocking) at the same time

Notable Mentions

AdGuardHome is a cross-platform DNS Ad Blocker, similar to Pi Hole, but with some additional features, like parental controls, per-device configuration and the option to force safe search. This may be a good solution for families with young children.

Some VPNs have ad-tracking blocking features, such as TrackStop with PerfectPrivacy.
Private Internet Access, CyberGhost, PureVPN, and NordVPN also have ad-block features.

Host Block Lists

Provider	Description
SomeoneWhoCares/ Hosts	An up-to-date host list, maintained by Dan Pollock - to make the internet not suck (as much)
Hosts by StevenBlack	Open source, community-maintained consolidated and extending hosts files from several well-curated sources. You can optionally pick extensions to block p0rn, Social Media, gambling, fake news and other categories
No Google	Totally block all direct and indirect content from Google, Amazon, Facebook, Apple and Microsoft (or just some)
EasyList	Comprehensive list of domains for blocking tracking, social scripts, bad cookies and annoying stuff
iBlockList	Variety of lists (free and paid-for) for blocking content based on certain topics, inducing: spam, abuse, political, illegal, hijacked, bad peers and more
Energized	A variety of well-maintained lists, available in all common formats, with millions of hosts included

Router Firmware

Installing a custom firmware on your Wi-Fi router gives you greater control over security, privacy and performance

Provider	Description
OpenWRT	Plenty of scope for customization and a ton of supported addons. Stateful firewall, NAT, and dynamically-configured port forwarding protocols (UPnP, NAT-PMP + upnpd, etc), Load balancing, IP tunneling, IPv4 & IPv6 support
DD-WRT	Easy and powerful user interface. Great access control, bandwidth monitoring and quality of service. IPTables is built-in for firewall, and there's great VPN support as well as additional plug-and-play and wake-on-lan features

Notable Mentions

Tomato, Gargoyle, LibreCMC and DebWRT

Word of Warning

Flashing custom firmware may void your warranty. If power is interrupted mid-way through a firmware install/ upgrade it is possible for your device to become bricked. So long as you follow a guide, and use a well supported system, on a supported router, than it should be safe

Network Analysis

Whether you live in a country behind a firewall, or accessing the internet through a proxy - these tools will help you better understand the extent of blocking, deep packet inspection and what data is being analysed

Provider	Description
OONI	Open Observatory of Network Interference - A free tool and global observation network, for detecting censorship, surveillance and traffic manipulation on the internet. Developed by The Tor Project, and available for Android, iOS and Linux
Mongol	A Python script, to pinpoint the IP address of machines working for the The Great Firewall of China. See also gfwlist which is the Chinese ban list, and gfw_whitelist. For a list of Russian government IP addresses, see antizapret
Goodbye DPI	Passive Deep Packet Inspection blocker and Active DPI circumvention utility, for Windows
DPITunnel	An Android app to bypass deep packet inspection
Proxy Checker	You can quickly check if a given IP is using a proxy, this can also be done through the command line

Intrusion Detection

An IDS is an application that monitors a network or computer system for malicious activity or policy violations, and notifies you of any unusual or unexpected events. If you are running a server, then it's essential to know about an incident as soon as possible, in order to minimize damage.

Provider	Description
Zeek	Zeek (formally Bro) Passively monitors network traffic and looks for suspicious activity
OSSEC	OSSEC is an Open Source host-based intrusion detection system, that performs log analysis, integrity checking, monitoring, rootkit detection, real-time alerting and active response
Kismet	An 802.11 layer2 wireless network detector, sniffer, and intrusion detection system
Snare	SNARE (System iNtrusion Analysis and Reporting Environment) is a series of log collection agents that facilitate centralized analysis of audit log data. Logs from the OS are collected and audited. Full remote access, through a web interface easy to use manually, or by an automated process
picosnitch	picosnitch helps protect your security and privacy by "snitching" on anything that connects to the internet, letting you know when, how much data was transferred, and to where. It uses BPF to monitor network traffic per application, and per parent to cover those that just call others. It also hashes every executable, and will complain if some mischievous program is giving it trouble.

Cloud Hosting

Whether you are hosting a website and want to keep your users data safe, or if you are hosting your own file backup, cloud productivity suite or VP - then choosing a provider that respects your privacy and allows you to sign up anonymously, and will keep your files and data safe is be important.

Provider	Description
Njalla	Njalla is a privacy and security-focused domain registrar and VPN hosting provider. They own and manage all their own servers, which are based in Sweden. They accept crypto, for anonymous payments, and allow you to sign up with OTR XMPP if you do not want to provide an email address. Both VPS and domain name pricing is reasonable, with packages starting at $15/ month
Vindo	Provides anonymous shared hosting, semi-managed virtual private servers and domain registration
Private Layer	Offers enterprise-grade, high-speed offshore dedicated servers, they own their own data centres, have a solid privacy policy and accept anonymous payment
Servers Guru	Servers Guru provides affordable and anonymous VPS and cloud servers with dedicated cpu resources. They accept crypto-currencies (Bitcoin, Monero, Ethereum etc..) and don't require any personal informations. They resell from reliable main actors in the industry and provide multiple hosting locations across europe. Their VPS offers starts at 4.99€/ month

Notable Mentions

See also: 1984 based in Iceland. Shinjiru, which offers off-shore dedicated servers. Orange Website specialises in protecting online privacy and free speech, hosted in Iceland. RackBone (previously DataCell) provides secure and ethical hosting, based in Switzerland. And Bahnhof offers high-security and ethical hosting, with their data centres locates in Sweden. Finally Simafri has a range of packages, that support Tor out of the box

Word of Warning

The country that your data is hosted in, will be subject to local laws and regulations. It is therefore important to avoid a jurisdiction that is part of the 5 eyes (Australia, Canada, New Zealand, US and UK) and other international cooperatives who have legal right to view your data.

Domain Registrars

Provider	Description
Njal.la	Privacy-aware domain service with anonymous sign-up and accepts crypto currency
Orange Website	Anonymous domain registration, with low online censorship since they are based outside the 14-eyes jurisdiction (in Iceland)

DNS Hosting

Provider	Description
deSEC	Free DNS hosting provider designed with security in mind, and running on purely open source software. deSEC is backed and funded by SSE.

Pre-Configured Mail-Servers

Provider	Description
Mail-in-a-box	Easy-to-deploy fully-featured and pre-configured SMTP mail server. It includes everything from webmail, to spam filtering and backups
Docker Mailserver	A full-stack but simple mailserver (smtp, imap, antispam, antivirus, ssl...) using Docker. Very complete, with everything you will need, customizable and very easy to deploy with docker

Word of Warning

Self-hosting your own mail server is not recommended for everyone, it can be time consuming to setup and maintain and securing it correctly is critical

---

Digital Notes

Provider	Description
Cryptee	Private & encrypted rich-text documents. Cryptee has encryption and anonymity at its core, it also has a beautiful and minimalistic UI. You can use Cryptee from the browser, or download native Windows, Mac OS, Linux, Android and iOS apps. Comes with many additional features, such as support for photo albums and file storage. The disadvantage is that only the frontend is open source. Pricing is free for starter plan, $3/ month for 10GB, additional plans go up-to 2TB
Standard Notes	S.Notes is a free, open-source, and completely encrypted private notes app. It has a simple UI, yet packs in a lot of features, thanks to the Extensions Store, allowing for: To-Do lists, Spreadsheets, Rich Text, Markdown, Math Editor, Code Editor and many more. You can choose between a number of themes (yay, dark mode!), and it features built-in secure file store, tags/ folders, fast search and more. There is a web app as well as native Windows, Mac OS, Linux, Android and iOS apps. Standard Notes is actively developed, and fully open-source, so you can host it yourself, or use their hosted version: free without using plug-ins or $3/ month for access to all features
Turtle	A secure, collaborative notebook. Self-host it yourself (see repo), or use their hosted plan (free edition or $3/ month for premium)
Joplin	Cross-platform desktop and mobile note-taking and todo app. Easy organisation into notebooks and sections, revision history and a simple UI. Allows for easy import and export of notes to or from other services. Supports synchronisation with cloud services, implemented with E2EE - however it is only the backed up data that is encrypted
Notable	Markdown-based note editor for desktop, with a simple, yet feature-rich UI. All notes are saved individually as .md files, making them easy to manage. No mobile app, or built-in cloud-sync or encryption

Provider	Description
Logseq	Privacy-first, open-source knowledge base that works on top of local plain-text Markdown and Org-mode files
AFFiNE	Privacy first, open-source alternative to Notion, monday.com and Miro.

Notable Mentions

If you are already tied into Evernote, One Note etc, then SafeRoom is a utility that encrypts your entire notebook, before it is uploaded to the cloud.

Org Mode is a mode for GNU Emacs dedicated to working with the Org markup format. Org can be thought of as a more featureful Markdown alternative, with support for keeping notes, maintaining todo lists, planning projects, managing spreadsheets, and authoring documents -all in plaintext.

For a simple plain text note taking app, with strong encryption, see Protected Text, which works well with the Safe Notes Android app. Laverna is a cross-platform secure notes app, where all entries are formatted with markdown.

Cloud Productivity Suites

Provider	Description
CryptPad	A zero knowledge cloud productivity suite. Provides Rich Text, Presentations, Spreadsheets, Kanban, Paint a code editor and file drive. All notes and user content, are encrypted by default, and can only be accessed with specific URL. The main disadvantage, is a lack of Android, iOS and desktop apps - CryptPad is entirely web-based. You can use their web service, or you can host your own instance (see CryptPad GitHub repo). Price for hosted: free for 50mb or $5/ month for premium
NextCloud	A complete self-hosted productivity platform, with a strong community and growing app store. NextCloud is similar to (but arguably more complete than) Google Drive, Office 365 and Dropbox, originally it was a fork from OwnCloud, but since have diverged. Clear UI and stable native apps across all platforms, and also supports file sync. Supports encrypted files, but you need to configure this yourself. Fully open source, so you can self-host it yourself (or use a hosted solution, starting from $5/ month)
Disroot	A platform providing online services based on principles of freedom, privacy, federation and decentralization. It is an implementation of NextCloud, with strong encryption configured - it is widely used by journalists, activists and whistle-blowers. It is free to use, but there have been reported reliability issues of the cloud services
Sandstorm	An open source platform for self-hosting web apps. Once you've set it up, you can install items from the Sandstorm App Market with -click, similar to NextCloud in terms of flexibility
Vikunja	Vikunja is an open-source to-do application. It is suitable for a wide variety of projects, supporting List, Gantt, Table and Kanban views to visualize all tasks in different contexts. For collaboration, it has sharing support via private teams or public links. It can be self-hosted or used as a managed service for a small fee.

Provider	Description
Skiff Pages	Skiff Pages is an end-to-end encrypted, privacy-first collaborative document, note-taking, and wiki product. Skiff Pages has a modern, easy-to-use UI and supports rich text documents with embedded content. Skiff also supports end-to-end encrypted file upload and sharing (Skiff Drive), as well as workspaces for multiple users to collaborate. Skiff Pages is available on web, iOS, and Android.

Backup and Sync

Provider	Description
SeaFile	An open source cloud storage and sync solution. Files are grouped into Libraries, which can be individually encrypted, shared of synced. Docker image available for easy deployment, and native clients for Windows, Mac, Linux, Android and iOS
Syncthing	Continuous file synchronization between 2 or more clients. It is simple, yet powerful, and fully-encrypted and private. Syncthing can be deployed with Docker, and there are native clients for Windows, Mac, Linux, BSD and Android
NextCloud	Feature-rich productivity platform, that can be used to backup and selectively sync encrypted files and folders between 1 or more clients. See setting up sync. A key benefit the wide range of plug-ins in the NextCloud App Store, maintained by the community. NextCloud was a hard fork off OwnCloud.

Notable Mentions

Alternatively, consider a headless utility such as Duplicacy or Duplicity. Both of offer an encrypted and efficient sync between 2 or more locations, using the rsync algorithm.

SpiderOak, Tresorit and Resilio are good enterprise solutions, all with solid encryption baked-in

FileRun and Pydio are self-hosted file explorers, with cross-platform sync capabilities.

Word of Warning

You should always ensure that any data stored in the cloud is encrypted. If you are hosting your own server, then take the necessary precautions to secure the server. For hosted solutions - use a strong password, keep your credentials safe and enable 2FA.

Encrypted Cloud Storage

Backing up important files is essential, and keeping an off-site copy is recommended. But many free providers do not respect your privacy, and are not secure enough for sensitive documents. Avoid free mainstream providers, such as Google Drive, cloud, Microsoft Overdrive, Dropbox.

It is recommended to encrypt files on your client machine, before syncing to the cloud. Cryptomator is a cross-platform, open source encryption app, designed for just this.

Provider	Description
Tresorit	End-to-end encrypted zero knowledge file storage, syncing and sharing provider, based in Switzerland. The app is cross-platform, user-friendly client and with all expected features. £6.49/month for 500 GB
IceDrive	Very affordable encrypted storage provider, with cross-platform apps. Starts as £1.50/month for 150 GB or £3.33/month for 1 TB
Sync.com	Secure file sync, sharing, collaboration and backup for individuals, small businesses and sole practitioners. Starts at $8/month for 2 TB
pCloud	Secure and simple to use cloud storage, with cross-platform client apps. £3.99/month for 500 GB
Peergos	A peer-to-peer end-to-end encrypted global filesystem with fine grained access control. Provides a secure and private space online where you can store, share and view your photos, videos, music and documents. Also includes a calendar, news feed, task lists, chat and email client. Fully open source and self-hostable (or use hosted solution, £5/month for 50 GB)
Internxt	Store your files in total privacy. Internxt Drive is a zero-knowledge cloud storage service based on best-in-class privacy and security. Made in Spain. Open-source mobile and desktop apps. 10GB FREE and Paid plans starting from €0.99/month for 20GB.
FileN	Zero knowledge end-to-end encrypted affordable cloud storage made in Germany. Open-source mobile and desktop apps. 10GB FREE with paid plans starting at €0.92/month for 100GB.

Notable Mentions

An alternative option, is to use a cloud computing provider, and implement the syncing functionality yourself, and encrypt data locally before uploading it - this may work out cheaper in some situations. You could also run a local server that you physically own at a secondary location, that would mitigate the need to trust a third party cloud provider. Note that some knowledge in securing networks is required.

See Also:

- File Encryption Software
- File Sync Software
- Cloud Hosting Providers

File Drop

Provider	Description
FilePizza	Peer-to-peer based file transfer from the browser, using Web Torrent. It's quick and easy to use, and doesn't require any software to be installed. Can also be self-hosted: repo

Provider	Description
FileSend	Simple, encrypted file sharing, with a 500mb limit and 5-day retention. Files are secured with client-side AES-256 encryption and no IP address or device info is logged. Files are permanently deleted after download or after specified duration. Developed by StandardNotes, and has built-in integration with the SN app.
OnionShare	An open source tool that lets you securely and anonymously share a file of any size, via Tor servers. OnionShare does require installing (compatible with Windows, Mac OS and Linux), but the benefit is that your files are transferred directly to the recipient, without needing to be hosted on an interim server. The host needs to remain connected for the duration of the transfer, but once it is complete, the process will be terminated. Source code: repo

Notable Suggestions

Instant.io, is another peer-to-peer based solution, using Web Torrent. For specifically transferring images, Up1 is a good self-hosted option, with client-side encryption. Finally PsiTransfer is a feature-rich, self-hosted file drop, using streams.

Browser Sync

It is not advised to sign into your browser, since it allows for more of your browsing data to be exposed, and can tie anonymous identities to your real account. If you require your bookmarks to be synced across devices or browsers then these tools can help, without you having to rely on an untrustworthy third-party.

Provider	Description
Floccus	Simple and efficient bookmark syncing using either NextCloud Bookmarks, a WebDAV server (local or remote) or just a local folder through LoFloccus. Browser extensions available for extensions for Chrome, Firefox and Edge
XBrowserSync	Secure, anonymous and free browser and bookmark syncing. Easy to setup, and no sign up is required, you can either use a community-run sync server, or host your own with their docker image. Extensions are available for Chrome, Firefox and on Android
Unmark	A web application which acts as a todo app for bookmarks. You can either self-host it, or use their managed service which has a free and paid-for tier
Reminiscence	A self-hosted bookmark and archive manager. Reminiscence is more geared towards archiving useful web pages either for offline viewing or to preserve a copy. It is a web application, that can be installed with Docker on either a local or remote server, although it has a comprehensive and well-documented REST API, there is currently no browser extension
Geekmarks	An API-driven, quick-to-use bookmark manager with powerful organisation features. Geekmarks is thoroughly documented, but a little more technical than other options, extension is currently only available for Chromium-based browsers

Provider	Description
Shiori	Simple bookmark manager written in Go, intended to be a clone of Pocket, it has both a simple and clean web interface as well as a CLI. Shiori has easy import/ export, is portable and has webpage archiving features

Notable Mentions

Ymarks is a C-based self-hosted bookmark synchronization server and Chrome extension.
syncmarx uses your cloud storage to sync bookmarks (Chrome and Firefox).
NextCloud Bookmarks has several community browser extensions, inducing FreedomMarks (Firefox) and OwnCloud Bookmarks (Chrome).
Finally, Turtl Notes has excellent link saving functionality built-in

RainDrop is a fully-featured all-in-1 bookmarking and web-snip suite. It has a beautiful UI, good data controls and some very handy integrations and features. Available on desktop, mobile, web and through a browser extension. The catch is that it is not open source, there is a free and premium plan, but no option for self-hosting.

Word of Warning

Strip out unneeded GET parameters if they reveal any device or referrer information, so as to not inadvertently allow a website to link your devices. ClearURLs may help with this.

Video Conference Calls

With the many, many security issues with Zoom, and other mainstream options, it becomes clear that a better, more private and secure alternative is required. As with other categories, the "best video calling app" will be different for each of us, depending on the ratio of performance + features to security + privacy required in your situation.

Provider	Description
Jami	A free and open source, distributed video, calling and screenshare platform with a focus on security. Jami is completely completely peer-to-peer, and has full end-to-end encryption with perfect forward secrecy for all communications, complying with the X.509 standard. Supported nativity on Windows, macOS, iOS, GNU/Linux, Android and Android TV. Video quality is quite good, but very dependent on network speeds, some of the apps are lacking in features
Jitsi	Encrypted, free and open source video calling app, which does not require creating an account/ providing any personal details. Availible as a web app, and native app for Windows, MacOS, Linux, Android and iOS. You can use the public Jitsi instance, self-host your own, or use a community hosted instance

Notable Mentions

Apache OpenMeetings provides self-hosted video-conferencing, chat rooms, file server and tools for meetings. together.brave.com is Brave's Jitsi Fork.

For remote learning, BigBlueButton is self-hosted conference call software, aimed specifically at schools and Universities. It allows for the host/ teacher to have full control over the session, and provides high-quality video streaming, multi-user whiteboards, breakout rooms, and instant chat.
For 1-to-1 mobile video calls, see Encrypted Messaging, and for P2P single and group calls, see P2P Messaging.

PGP Managers

Tools for signing, verifying, encrypting and decrypting text and files using GnuPG standard

Provider	Description
SeaHorse (Linux/ GNOME)	Application for managing encryption keys and passwords, integrated with the GNOME Keyring
Kleopatra (Linux/ KDE)	Certificate manager and a universal crypto GUI. It supports managing X.509 and OpenPGP certificates in the GpgSM keybox and retrieving certificates from LDAP server
GPG4Win (Windows)	Kleopatra ported to Windows
GPG Suite (MacOS)	Successor of MacGPG. Note: no longer free
OpenKeychain (Android)	Android app for managing keys, and encrypting messages. Works both stand-alone, and as integrated into other apps, including k9-Mail
PGP Everywhere (iOS)	iOS app for encrypting/ decrypting text. Has native keyboard integration, which makes it quick to use. Note: Not open source
FlowCrypt (Browser)	Browser extension for using PGP within Gmail, for Chrome and Firefox. Mobile version supported on Android and iOS
EnigMail (Thunderbird)	OpenPGP extension for Thunderbird and PostBox, integrates natively within mail app
p≡p	Easy-to-use decentralied PGP encryption for Android, iOS, Thunderbird, Enigmail, and Outlook. Popular solution for enterprises
Mailvelope (Email)	Mailvelope is an addon for email applications, that makes using PGP very easy for beginners. You can use the hosted version for free, or opt to host your own instance. It has good compatibility with all common mail applications, both on desktop and mobile
PGP4USB (Portable)	A portable desktop app, that can be run directly off a USB, useful for when you need to use without installing

Metadata Removal Tools

Exif/ Metadata is "data about data", this additional information attached to files can lead us to share significantly more information than we intended to.
For example, if you upload an image of a sunset to the internet, but don't remove the metadata, it may reveal the location (GPS lat + long) of where it was taken, the device is was taken on, precise camera data, details about modifications and the picture source + author. Social networks that remove metadata from your photos, often collect and store it, for their own use. This could obviously pose a security risk, and that is why it is recommended to strip out this data from a file before sharing.

Provider	Description
ExifCleaner	Cross-platform, open source, performant EXIF meta data removal tool. This GUI tool makes cleaning media files really easy, and has great batch process support. Created by @szTheory, and uses ExifTool
ExifTool (CLI)	Platform-independent open source Perl library & CLI app, for reading, writing and editing meta data. Built by Phill Harvey. Very good performance, and supports all common metadata formats (including EXIF, GPS, IPTC, XMP, JFIF, GeoTIFF, ICC Profile, Photoshop IRB, FlashPix, AFCP and ID3). An official GUI application is available for Windows, implemented by Bogdan Hrastnik.
ImageOptim (MacOS)	Native MacOS app, with drag 'n drop image optimization and meta data removal

Notable Mentions

It's possible (but slower) to do this without a third-party tool. For Windows, right click on a file, and go to: `Properties --> Details --> Remove Properties --> Remove from this File --> Select All --> OK`.

Alternatively, with ImageMagic installed, just run `convert -strip path/to/image.png` to remove all metadata. If you have GIMP installed, then just go to `File --> Export As --> Export --> Advanced Options --> Uncheck the "Save EXIF data" option`.

Often you need to perform meta data removal programmatically, as part of a script or automation process. GoLang: go-exif by @dsoprea | JS: exifr by @MikeKovarik | Python: Piexif by @hMatoba | Ruby: Exif by @tonytonyjan | PHP: Pel by @mgeisler.

Data Erasers

Simply deleting data, does not remove it from the disk, and recovering deleted files is a simple task. Therefore, to protect your privacy, you should erase/ overwrite data from the disk, before you destroy, sell or give away a hard drive.

Provider	Description
Eraser (Windows)	Allows you to completely remove sensitive data from your hard drive by overwriting it several times with carefully selected patterns
Hard Disk Scrubber (Windows)	Easy to use, but with some advanced features, including custom wipe patterns. Data Sanitation Methods: AFSSI-5020, DoD 5220.22-M, and Random Data

Provider	Description
SDelete (Windows)	Microsoft Secure Delete is a CLI utility, uses DoD 5220.22-M
OW Shredder (Windows)	File, folder and drive portable eraser for Windows. Bundled with other tools to scan, analyze, and wipe, and other traces that were left behind. Includes context menu item, recycle bin integration
DBAN (bootable)	Darik's Boot and Nuke ("DBAN") is a self-contained boot disk that securely wipes the hard disks of most computers. DBAN will automatically and completely delete the contents of any hard disk that it can detect, which makes it an appropriate utility for bulk or emergency data destruction. DBAN is the free edition of Blanco, which is an enterprise tool designed for legal compliance.
nwipe (Cross-platform)	C-based secure light-weight disk eraser, operated through the easy-to-use CLI or a GUI interface
shred (Unix)	A CLI utility that can be used to securely delete files and devices, to make them extremely difficult to recover. See also, wipe for erasing files from magnetic media
Secure Remove (Unix)	CLI utility for securely removing files, directories and whole disks, works on Linux, BSD and MacOS
Mr. Phone (Android/ iOS)	Proprietary, closed-source suite of forensic data tools for mobile. The data eraser allows for both Android and iOS to be fully wiped, through connecting them to a PC.

Notable Mentions

There's no need to use a third-party tool. You can boot into a UNIX-based system, mount the disk you need to erase, and use a command to write it with arbitrary data. For best results, this process should be repeated several times. This is a good way to wipe a disk, before selling or destroying it, to protect your data.

Such as the `dd` command, is a tool to convert and copy files, but running `sudo dd if=/dev/zero of=/dev/sdX bs=1M` will quickly overwrite the whole disk with zeros. Or badblocks which is intended to search for all bad blocks, but can also be used to write zeros to a disk, by running `sudo badblocks -wsv /dev/sdd`. An effective method of erasing an SSD, it to use hdparm to issue a secure erase command, to your target storage device, for this, see step-by-step instructions via: wiki.kernel.org. Finally, `[srm](https://www.systutorials.com/docs/linux/man/1-srm/)` can be use to securely remove files or directories, just run `srm -zsv /path/to/file` for a single pass over.

Virtual Machines

A virtual machine (VM) is a sandboxed operating system, running within your current system. Useful for compartmentalisation and safely testing software, or handling potentially malicious files

Provider	Description
VirtualBox	Open source, powerful, feature-rich virtualization product, supporting x86 and AMD64/Intel64 architectures. Available for Windows, MacOS, Linux and BSD, and free for both personal and enterprise use. VirtualBox is backed by a strong community, and has been under active development since 2007.
Xen Project (Servers)	Open source virtual machine monitor intended to serve as a type-1 hyperviser for multiple operating systems using the same hardware - very useful for servers, as it allows for fully independent virtual Linux machines
UTM	Open source, feature rich, powerful type 2 hypervisor for Mac, can emulate x86-64 OSes on Apple Silicon Macs

Notable Mentions

QEMU is a virtual hardware emulation tool, meaning it is less appropriate for creating fully independant sandboxes, but performance is considerable better than that of a traditional virtual machine.

VMWare is popular in the enterprise world, it is not open source, and although there is a free version, a license is required to access all features. VMWare performs very well when running on a server, with hundreds of hosts and users. For Mac users, Parallels is a popular option which performs really well, but again is not open source. For Windows users, there's Hyper-V, which is a native Windows product, developed by Microsoft.

Social Networks

Over the past decade, social networks have revolutionized the way we communicate and bought the world closer together - but it came at the cost of our privacy. Social networks are built on the principle of sharing - but you, the user should be able to choose with whom you share what, and that is what the following sites aim to do.

Provider	Description
Aether	Self-governing communities with auditable moderation - a similar concept to Reddit, but more privacy-sensitive, democratic and transparent. Aether is open source and peer-to-peer, it runs on Windows, Mac and Linux
Discourse	A 100% open source and self-hostable discussion platform you can use as a mailing list, discussion forum or long-form chat room.
Mastodon	A shameless Twitter clone, but open-source, distributed across independent servers, and with no algorithms that mess with users timelines
Minds	A social media site, which aims to bring people together and support open conversations. Get paid for creating content

Provider	Description
Vero	(closed-source) A mobile-based social network, whose USP is that they have "No Ads. No Data Mining. No Algorithms." Since Vero is not open source, it is not possible to verify the validity of these claims

Other Notable Mentions

- diaspora*, Pleroma, Friendica and Hubzilla - distributed, decentralized social networks, built on open protocols
- Tildes, Lemmy and notabug.io - bulletin boards and news aggregators (similar to Reddit)
- Pixelfed - A free, ethical, federated photo sharing platform (FOSS alternative to Instagram)

Main-stream networks

The content on many of these smaller sites tends to be more *niche*. To continue using Twitter, there are a couple of tweaks, that will improve security. For Reddit, use a privacy-respecting client - such as Reditr. Other main-stream social networking sites do not respect your privacy, so should be avoided, but if you choose to keep using them see this guide for tips on protecting your privacy

Video Platforms

Provider	Description
PeerTube	Free and open-source federated video platform that uses peer-to-peer technology to reduce load on individual servers when viewing videos. You can self-host, or find an instance, and then watch videos from any PeerTube server
DTube	A decentralized and ad-free video platform with little to no moderation that uses cryptocurrency and blockchain technology to pay its users.
BitTube	A peer-to-peer, decentralized, censorship-free, ad-free video sharing and live streaming platform based on IPFS and blockchain technology
BitChute	A video hosting platform, that was founded in 2017 to allow uploaders to avoid content rules enforced on other platforms, such as YouTube

Word of Warning

Without moderation, some of these platforms accommodate video creators whose content may not be appropriate for all audiences

YouTube Proxies

The content on many of the smaller video sites, often just doesn't compare to YouTube. So another alternative, is to access YouTube through a proxy client, which reduces what Google can track.

- Good options are: Invidious (web), Piped (web), FreeTube (Windows, Mac OS, Linux), NewPipe (Android), YouTube++ (iOS)
- Or download videos with youtube-dl (cli) or youtube-dl-gui (gui). For just audio, there is PodSync

Video Search Engines

Petey Vid is a non-biased video search engine. Unlike normal search engines it indexes videos from a lot of sources, including Twitter, Veoh, Instagram, Twitch, MetaCafe, Minds, BitChute, Brighteon, D-Tube, PeerTube, and many others.

Blogging Platforms

Provider	Description
Write Freely	Free and open source software with a clean UI, for creating a minimalist, federated blog. For premium or enterprise hosted plans, see Write.as, or to host your own, check out the repo on GitHub
Telegraph	Created by Telegram, Telegraph is fast, anonymous and simple
Mataroa	Naked blogging platform, for minimalists. Open source and privacy-conscious.
Bear Blog	A privacy-first, no-nonsense, super-fast blogging platform. Repo on GitHub.
Movim	An open-source web frontend for XMPP that supports decentralized blogging and chatrooms.

Notable Mentions

If you use Standard Notes, then Listed.to is a public blogging platform with strong privacy features. It lets you publish posts directly through the Standard Notes app or web interface. Other minimalistic platforms include Notepin.co and Pen.io.

Want to write a simple text post and promote it yourself? Check out telegra.ph, txt.fyi and NotePin. For seriously anonymous platforms, aimed at activists, see noblogs and autistici. It is also possible to host a normal WordPress site, without it being linked to your real identity, although WP does not have the best reputation when it comes to privacy.

Of course you could also host your blog on your own server, using a standard open source blog platform, such as Ghost and configure it to disable all trackers, ads and analytics.

News Readers and Aggregation

Provider	Description
Tiny RSS	A free and open source web-based news feed (RSS/Atom) reader and aggregator
RSSOwl	A desktop-based RSS reader, with powerful organisation features
Feedly	A more premium option. Feedly displays news from your selected sources in an easy-to-digest clean and modern interface. It works with more than just RSS feeds, since it is well integrated with many major news outlets. It does not manipulate the stories you see, and is mostly open source

Notable Mentions

For iPhone users in the US, Tonic is a great little app that provides you with a selection of personalized new stories and articles daily. It is possible to use Reddit anonymously too - you can use throwaway accounts for posting.

Word of Warning

News reader apps don't have a good reputation when it comes to protecting users privacy, and often display biased content. Many have revenue models based on making recommendations, with the aim of trying to get you to click on sponsored articles - and for that a lot of data needs to have been collected about you, your habits, interests and routines.

Proxy Sites

These are websites that enable you to access existing social media platforms, without using their primary website - with the aim of improving privacy & security and providing better user experience. The below options are open source (so can be self-hosted, if you wish), and they do not display ads or tracking (unless otherwise stated).

Provider	Description
Nitter (Twitter)	Nitter is a free and open source alternative Twitter front-end focused on privacy, it prevents Twitter from tracking your IP or browser fingerprint. It does not include any JavaScript, and all requests go through the backend, so the client never talks directly to Twitter. It's written in Nim, is super lightweight, with multiple themes and a responsive mobile version available, as well as customizable RSS feeds. Uses an unofficial API, with no rate limits or and no developer account required.
Invidious (YouTube)	Privacy-focused, open source alternative frontend for YouTube. It prevents/ reduces Google tracking, and adds additional features, including an audio-only mode, Reddit comment feed, advanced video playback settings. It's super lightweight, and does not require JavaScript to be enabled, and you can import/ export your subscriptions list, and customize your feed. See list of Invidious Public Instances.
Libreddit (Reddit)	Private front-end for Reddit written in Rust. Massively faster than Reddit by not including ads, trackers or bloat. Libreddit can be deployed and selfhosted through `cargo`, Docker and Repl.it and proxies all requests through the back-end. Libreddit currently implements most of Reddit's functionalities that don't require users to be signed in.
WebProxy	Free proxy service, with Tor mode (which is recommended to enable). Designed to be used to evade censorship and access geo-blocked content. The service is maintained by DevroLabs, who also run the OnionSite web proxy, they claim to that all traffic is 256-bit SSL-encrypted, but this cannot be verified - never enter any potentially personally identifiable information, and use it purely for consuming content.

Notable Mentions

- **NewPipe** is an open source, privacy-respecting YouTube client for Android.

- **FreeTube** an open source YouTube client for Windows, MacOS and Linux, providing a more private experience, with a native-feel desktop app. It is built upon the Invidious API.

Word of Warning

When proxies are involved - only use reputable services, and **never** enter any personal information

Cryptocurrencies

Provider	Description
Monero	One of the most private cryptocurrencies, since no meta data is available (not even the transaction amount). It uses complex on-chain cryptographic methods such as Ring signatures, RingCT, Kovri, and Stealth addresses all of which help protect the privacy of users
ZCash	Uses zero-knowledge proofs to protect privacy cryptographic technique, that allows two users to transact without ever revealing their true identity or address. The Zcash blockchain uses two types of addresses and transactions, Z transactions and addresses are private and T transactions and addresses are transparent like Bitcoin.

It is still possible to use currencies that have a public ledger 'privately', but you will need to take great care not to cause any transactions to be linked with your identity or activity. For example, avoid exchanges that require KYC, and consider using a service such as Local Bitcoins. If you use a Bitcoin ATM, then take care to not be physically tracked (CCTV, phone location, card payments etc)

Notable Mentions

Other privacy-focused cryptocurrencies include: PIVX, Bitcoin Private, Verge, and Piratechain.

Word of Warning

Not all cryptocurrencies are anonymous, and without using a privacy-focused coin, a record of your transaction will live on a publicly available distributed ledger, forever. If you send of receive multiple payments, ensure you switch up addresses or use a mixer, to make it harder for anyone trying to trace your transactions. Cryptocurrencies that allow private and public transactions may reveal meta data about your transactions and balances when funds are moving from private to public addresses which can compromise your privacy with methods similar to a knapsack problem. Store private keys somewhere safe, but offline and preferably cold.

Note: Cryptocurrency prices can go down. Storing any wealth in crypto may result in losses. If you are new to digital currencies - do your research first, don't invest more than you can afford, and be very weary of scams and cryptocurrency-related malware.

Crypto Wallets

Provider	Description

Provider	Description
Wasabi Wallet (Bitcoin)	An open source, native desktop wallet for Windows, Linux and MacOS. Wasabi implements trustless CoinJoins over the Tor network. Neither an observer nor the participants can determine which output belongs to which input. This makes it difficult for outside parties to trace where a particular coin originated from and where it was sent to, which greatly improves privacy. Since it's trustless, the CoinJoin coordinator cannot breach the privacy of the participants. Wasabi is compatible with cold storage, and hardware wallets, including OpenCard and Trezor.
Trezor (All Coins)	Open source, cross-platform, offline, crypto wallet, compatible with 1000+ coins. Your private key is generated on the device, and never leaves it, all transactions are signed by the Trezor, which ensures your wallet is safe from theft. There are native apps for Windows, Linux, MacOS, Android and iOS, but Trezor is also compatible with other wallets, such as Wasabi. You can back the Trezor up, either by writing down the seed, or by duplicating it to another device. It is simple and intuitive to use, but also incredible customisable with a large range of advanced features.
ColdCard (Bitcoin)	An easy-to-use, super secure Bitcoin hardware wallet, which can be used independently as an air-gapped wallet. ColdCard is based on partially signed Bitcoin transactions following the BIP174 standard. Built specifically for Bitcoin, and with a variety of unique security features, ColdCard is secure, trustless, private and easy-to-use. Companion products for the ColdCard include: BlockClock, SeedPlate and ColdPower
Electrum (Bitcoin)	Long-standing Python-based Bitcoin wallet with good security features. Private keys are encrypted and do not touch the internet and balance is checked with a watch-only wallet. Compatible with other wallets, so there is no tie-in, and funds can be recovered with your secret seed. It supports proof-checking to verify transactions using SPV, multi-sig and add-ons for compatibility with hardware wallets. A decentralized server indexes ledger transactions, meaning it's fast and doesn't require much disk space. The potential security issue here would not be with the wallet, but rather your PC - you must ensure your computer is secure and your wallet has a long, strong passphrase to encrypt it with.
Samourai Wallet (Bitcoin)	An open-source, Bitcoin-only privacy-focused wallet, with some innovative features. Samourai Wallet works under any network conditions, with a full offline mode, useful for cold storage. It also supports a comprehensive range of privacy features including: STONEWALL that helps guard against address clustering deanonymization attacks, PayNym which allows you to receive funds without revealing your public address for all to see, Stealth Mode which hides Samourai from your devices launcher, Remote SMS Commands to wipe or recover your wallet if device is seized or stolen, and Whirlpool which is similar to a coin mixer, and OpenDime is also supported for offline USB hardware wallets.
Sparrow Wallet (Bitcoin)	Sparrow is a Bitcoin wallet for those who value financial self sovereignty. Sparrow’s emphasis is on security, privacy and usability. Sparrow does not hide information from you - on the contrary it attempts to provide as much detail as possible about your transactions and UTXOs, but in a way that is manageable and usable.

Provider	Description
Atomic Wallet (All Coins)	Atomic is an open source desktop and mobile based wallet, where you're private keys are stored on your local device, and do not touch the internet. Atomic has great feature sets, and supports swapping, staking and lending directly from the app. However, most of Atomic's features require an active internet connection, and Atomic does not support hardware wallets yet. Therefor, it may only be a good choice as a secondary wallet, for storing small amounts of your actively used currency
CryptoSteel (All Coins)	A steel plate, with engraved letters which can be permanently screwed - CryptoSteel is a good fire-proof, shock-proof, water-proof and stainless cryptocurrency backup solution.
BitBox02 (Bitcoin or Ethereum & ERC-20 tokens)	Open source hardware wallet, supporting secure multisig with the option for making encrypted backups on a MicroSD card.
ColdCard (Bitcoin)	Secure, open source Bitcoin cold storage wallet, with the option for making encrypted backups on a MicroSD card.

Word of Warning

Avoid using any online/ hot-wallet, as you will have no control over the security of your private keys. Offline paper wallets are very secure, but ensure you store it properly - to keep it safe from theft, loss or damage.

Notable Mentions

Metamask (Ethereum and ERC20 tokens) is a bridge that allows you to visit and interact with distributed web apps in your browser. Metamask has good hardware wallet support, so you can use it to swap, stake, sign, lend and interact with dapps without you're private key ever leaving your device. However the very nature of being a browser-based app means that you need to stay vigilant with what services you give access to.

Crypto Exchanges

Provider	Description
Bisq	An open-source, peer-to-peer application that allows you to buy and sell cryptocurrencies in exchange for national currencies. Fully decentralized, and no registration required.
LocalBitcoins	Person-to-person exchange, find people local to your area, and trade directly with them, to avoid going through any central organisation. Primarily focused on Bitcoin, Ethereum, Ripple and LiteCoin, as it gets harder to find people near you selling niche alt-coins
AtomicDEX	Person-to-person cryptocurrency exchange with no KYC or registration required and uses atomic swaps to perform trustless trades. The orderbook uses a modified libp2p protocol to prevent censorship and maintain decentralization. Fiat currencies are not supported, but hundreds of alt-coins and major cryptocurrencies are supported.

Provider	Description
RoboSats	RoboSats is an easy way to privately exchange Bitcoin for national currencies It simplifies the peer-to-peer experience and makes use lightning hold invoices to minimize custody and trust requirements. The deterministically generated avatars help users stick to best privacy practices.

Notable Mentions

For traders, BaseFEX doesn't require ID and has a good privacy policy. BitMex has more advanced trading features, but ID verification is required for higher value trades involving Fiat currency. For buying and selling alt-coins, Binance has a wide range of currencies, and ID verification is not needed for small-value trades.

Virtual Credit Cards

Virtual cards generated provide an extra layer of security, improve privacy and help protect from fraud. Most providers have additional features, such as single-use cards (that cannot be charged more than once), card limits (so you can be sure you won't be charged more than you expected) and other security controls.

Provider	Description
Privacy.com	Privacy.com has a good reputation, and is the largest virtual card provider in the US. Unlike other providers, it is free for personal use (up to 12 cards per month) with no fees, apps and support is good. There is a premium is plan for $10/month, with 1% cashback 36 cards/ month
Revolut Premium	Revolut is more of a digital bank account, and identity checks are required to sign up. Virtual cards only availible on Premium/ Metal accounts, which start at $7/month.
MySudo	Much more than just virtual cards, MySudo is a platform for creating compartmentalised identities, each with their own virtual cards, virtual phone numbers, virtual email addresses, messaging, private browsing and more. There is a free plan for up to 3 identities, and premium plans start at $0.99/ month
Blur	Blur by Abine has virtual card functinality,

PayLasso, JoinToken, EntroPay are now discontinued

Other Payment Methods

Provider	Description
Cash	Actual physical cash is still the most private option, with no chance of leaving any transactional records
Gift Cards	Gift cards can be purchased for cash in many convenience stores, and redeemed online for goods or services. Try to avoid CCTV as best as possible.

Provider	Description
Pre-paid Cards	Similarly to gift cards, buying a pre-paid card for cash, can enable you to purchase goods and services in stores that only accept card payments.

Paying for goods and services is a good example of where privacy and security conflict; the most secure option would be to pay with credit card, since most providers include comprehensive fraud protection, whereas the most private option would be to pay using crypto currency or cash, since neither can be easily tied back to your identity.

Word of Warning

Note that credit card providers heavily track transaction metadata, which build up a detailed picture of each persons spending habits. This is done both to provide improved fraud alerts, but also because the data is extremely valuable and is often 'anonymized' and sold to 3rd parties. Hence your privacy is degraded if these cards are used for daily transactions

Budgeting Tools

Provider	Description
Firefly III (Self-hosted)	A free and open source personal finance manager. Firefly III has all essential features, a clean and clear UI and is easy to set up and use (see live demo). It's backed by a strong community, and is regularly updated with new features, improvements and fixes. There is also a hass.io addon, and it works nicely with Home Assistant. Note: Since it is self-hosted, you will need to ensure that your server (either local or remote) is correctly configured for security.
EasyBudget (Android)	Clean and easy-to-use app open source budgeting app. It doesn't have all the features that alternatives offer, but it does simple budget management and planning very effectively
HomeBank (Desktop)	Desktop personal financial management option. Great for generating charts, dynamic reports and visualising transactions. HomeBank makes it easy to import financial data from other software (Quick Books, Microsoft Money etc) and bank accounts (in OFX/QFX, QIF, CSV format), and has all the essential features you'd expect. Available on Linux and Windows (and a 3rd-party port for Mac OS)
GnuCash (Desktop)	Full-featured cross-platform accounting application, which works well for both personal and small business finance. First released in 1998, GnuCash is long standing and very stable, and despite a slightly dated UI, it's still a very popular option. Originally developed for Linux, GnuCash is now available for Windows, Mac and Linux and also has a well rated official Android app
Plain Text Accounting	Plain text accounting is a way of doing bookkeeping / accounting with plain text files and scriptable, command-line-friendly software, such as Ledger](https://www.ledger-cli.org), hledger, Beancount and more. Unlike other tools, you have full control over your data, and are not tied to a particular vendor

Notable Mentions

Spreadsheets remain a popular choice for managing budgets and financial planning. Collabora or OnlyOffice (on NextCloud), Libre Office and EtherCalc are popular open source spread sheet applications. Mintable allows you to auto-populate your spreadsheets from your financial data, using publicly accessible API - mitigating the requirement for a dedicated budgeting application.

Other notable open source budgeting applications include: Smart Wallet (iOS), My-Budget (Desktop), MoneyManager EX, Skrooge, kMyMoney and Budget Zen (a simple E2E encrypted budget manager)

See Also: Cryptocurrencies, Virtual Credit Cards and Other Payment Methods

See Also: Personal Finance Security Tips

Mobile Operating Systems

If you are an Android user, your device has Google built-in at its core. Google tracks you, collecting a wealth of information, and logging your every move. A custom ROM, is an open source, usually Google-free mobile OS that can be flashed to your device.

Provider	Description
GrapheneOS	GrapheneOS is an open source privacy and security focused mobile OS with Android app compatibility. Developed by Daniel Micay. GrapheneOS is a young project, and currently only supports Pixel devices, partially due to their strong hardware security.
CalyxOS	CalyxOS is an free and open source Android mobile operating system that puts privacy and security into the hands of everyday users. Plus, proactive security recommendations and automatic updates take the guesswork out of keeping your personal data personal. Also currently only supports Pixel devices and Xiaomi Mi A2 with Fairphone 4, OnePlus 8T, OnePlus 9 test builds available. Developed by the Calyx Foundation.
DivestOS	DivestOS is a vastly diverged unofficial more secure and private soft fork of LineageOS. DivestOS primary goal is prolonging the life-span of discontinued devices, enhancing user privacy, and providing a modest increase of security where/when possible. Project is developed and maintained solely by Tad (SkewedZeppelin) since 2014.
LineageOS	A free and open-source operating system for various devices, based on the Android mobile platform - Lineage is light-weight, well maintained, supports a wide range of devices, and comes bundled with Privacy Guard

Other Notable Mentions

Replicant OS is a fully-featured distro, with an emphasis on freedom, privacy and security. MmniRom, Recursion Remix, and Paranoid Android are also popular options. Alternatively, Ubuntu Touch is a Linux (Ubuntu)- based OS. It is secure by design and runs on almost any device, - but it does fall short when it comes to the app store.

To install apps on the Play Store without using the Play Store app see Aurora Store. For Google Play Service see MicroG

Word of Warning

It is not recommended to root, or flash your device with a custom ROM if you are not an advanced user. There are risks involved

- Although the above ROMs omit Google, they do open up other security issues: Without DM-verity on the system partition, the file system *could* be tampered with, and no verified boot stack, the kernel/initramfs also *could* be edited. You should understand the risks, before proceeding to flash a custom ROM to your device
- You will need to rely on updates from the community, which could be slower to be released - this may be an issue for a time-urgent, security-critical patch
- It is also possible to brick your device, through interrupted install or bad software
- Finally, rooting and flashing your device, will void your warranty

Desktop Operating Systems

Windows 10 has many features that violate your privacy. Microsoft and Apple are able to collect all your data (including, but not limited to: keystrokes, searches and mic input, calendar data, music, photos, credit card information and purchases, identity, passwords, contacts, conversations and location data). Microsoft Windows is also more susceptible to malware and viruses, than alternative systems.

Switching to Linux is a great choice in terms of security and privacy - you don't need necessarily need to use a security distro, any well-maintained stable distro is going to be considerably better than a proprietary OS

Provider	Description
Qubes OS (containerized apps)	Open-source security-oriented operating system for single-user desktop computing. It uses virtualisation, to run each application in its own compartment to avoid data being leaked. It features Split GPG, U2F Proxy, and Whonix integration. Qubes makes is easy to create disposable VMs which are spawned quickly and destroyed when closed. Qubes is recommended by Edward Snowden
Whonix (VM)	Whonix is an anonymous operating system, which can run in a VM, inside your current OS. It is the best way to use Tor, and provides very strong protection for your IP address. It comes bundled with other features too: Keystroke Anonymization, Time Attack Defences, Stream Isolation, Kernel Self Protection Settings and an Advanced Firewall. Open source, well audited, and with a strong community - Whonix is based on Debian, KickSecure and Tor
Tails (live)	Tails is a live operating system (so you boot into it from a USB, instead of installing). It preserves your privacy and anonymity through having no persistent memory/ leaving no trace on the computer. Tails has Tor built-in system-wide, and uses state-of-the-art cryptographic tools to encrypt your files, emails and instant messaging. Open source, and built on top of Debian. Tails is simple to stop, configure and use

Provider	Description
Parrot (security)	Parrot Linux, is a full Debian-based operating system, that is geared towards security, privacy and development. It is fully-featured yet light-weight, very open. There are 3 editions: General Purpose, Security and Forensic. The Secure distribution includes its own sandbox system obtained with the combination of Firejail and AppArmor with custom security profiles. While the Forensics Edition is bundled with a comprehensive suite of security/ pen-testing tools, similar to Kali and Black Arch
Discreete Linux (offline)	Aimed at journalists, activists and whistle-blowers, Discreete Linux is similar to Tails, in that it is booted live from external media, and leaves no/ minimal trace on the system. The aim of the project, was to provide all required cryptographic tools offline, to protect against Trojan-based surveillance
Alpine Linux	Alpine is a security-oriented, lightweight distro based on musl libc and busybox. It compiles all user-space binaries as position-independent executables with stack-smashing protection. Install and setup may be quite complex for some new users

Notable Mentions

Septor is a Debian-based distro with the KDE Plasma desktop environment, and Tor baked-in. Designed for surfing the web anonymously, and completing other internet-based activities (with Thunderbird, Ricochet IM, HexChat, QuiteRSS, OnionShare). Septor is light-weight, but comes bundled with all the essential privacy + security utilities (including: Gufw, Ark, Sweeper, KGpg, Kleopatra, KWallet, VeraCrypt, Metadata Anonymisation Toolkit and more).

Subgraph OS is designed to be an *adversary resistant computing platform*, it includes strong system-wide attack mitigations, and all key applications run in sandbox environments. Subgraph is still in beta (at the time of writing), but still is well tested, and has some nice anonymization features

For defensive security, see Kali and BlackArch, both are bundled with hundreds of security tools, ready for pretty much any job.

Other security-focused distros include: TENS OS, Fedora CoreOS, Kodachi and IprediaOS. (Avoid systems that are not being actively maintained)

General Purpose Linux Distros

If you do not want to use a specalist security-based distro, or you are new to Unix - then just switching to any well-maintained Linux distro, is going to be significantly more secure and private than Windows or Mac OS. Since it is open source, major distros are constantly being audited by members of the community. Linux does not give users admin rights by default - this makes is much less likely that your system could become infected with malware. And of course, there is no proprietary Microsoft or Apple software constantly monitoring everything you do.

Some good distros to consider would be: **Fedora**, **Debian**, or **Arch**- all of which have a large community behind them. **Manjaro** (based of Arch) is a good option, with a simple install process, used by new comers, and expers alike. **POP_OS** and **PureOS** are reasonably new general purpose Linux, with a strong focus on privacy, but also very user-friendly with an intuitive interfac and install process. See Simple Comparison or Detailed Comparison.

BSD

BSD systems arguably have far superior network stacks. **OpenBSD** is designed for maximum security — not just with its features, but with its implementation practices. It's a commonly used OS by banks and critical systems. **FreeBSD** is more popular, and aims for high performance and ease of use.

Windows

Two alternative options for Windows users are Windows 10 AME (ameliorated) project and the LTSC stream. **Windows 10 AME** AME project aims at delivering a stable, non-intrusive yet fully functional build of Windows 10 to anyone, who requires the Windows operating system natively. Core applications, such as the included Edge web-browser, Windows Media Player, Cortana, as well as any appx applications (appx apps will no longer work), have also been successfully eliminated. The total size of removed files is about 2 GB. Comes as a pre-built ISO or option to build from scratch with de-bloat scripts. Strong, supportive community on Telegram. **Windows 10 LTSC** LTSC provides several security benefits over a standard Win 10 Installation. LTSC or Long Term Servicing Channel is a lightweight, low-cost Windows 10 version, that is intended for specialized systems, and receives less regular feature updates. What makes it appealing, is that it doesn't come with any bloatware or non-essential applications, and needs to be configured from the ground up by the user. This gives you much better control over what is running on your system, ultimately improving security and privacy. It also includes several enterprise-grade security features, which are not available in a standard Windows 10 instance. It does require some technical knowledge to get started with, but once setup should perform just as any other Windows 10 system. Note that you should only download the LTSC ISO from the Microsoft's official page

Improve the Security and Privacy of your current OS

After installing your new operating system, or if you have chosen to stick with your current OS, there are a couple of things you can do to improve security. See: Windows 10 security guide, Mac OS security guide or Linux security guide.

Linux Defences

Provider	Description
Firejail	Firejail is a SUID sandbox program that reduces the risk of security breaches by restricting the running environment of untrusted applications using Linux namespaces and seccomp-bpf. Written in C, virtually no dependencies, runs on any modern Linux system, with no daemon running in the background, no complicated configuration, and it's super lightweight and super secure, since all actions are implemented by the kernel. It includes security profiles for over 800 common Linux applications. FireJail is recommended for running any app that may potential pose some kind of risk, such as torrenting through Transmission, browsing the web, opening downloaded attachments
Gufw (Linux)	Open source GUI firewall for Linux, allowing you to block internet access for certain applications. Supports both simple and advanced mode, GUI and CLI options, very easy to use, lightweight/ low-overhead, under active maintenance and backed by a strong community. Installable through most package managers, or compile from source Other popular firewalls are OpenSnitch and Uncomplicated Firewall, see more firewalls

Provider	Description
ClamTk	ClamTk is basically a graphical front-end for ClamAV, making it an easy to use, light-weight, on-demand virus scanner for Linux systems
chkrootkit	Locally checks for signs of a rootkit
Snort	open source intrusion prevention system capable of real-time traffic analysis and packet
BleachBit	Clears cache and deletes temporary files very effectively. This frees up disk space, improves performance, but most importantly helps to protect privacy

Notable Mentions

SecTools.org is a directory or popular Unix security tools.

Windows Defences

Provider	Description
Windows Spy Blocker	Capture and interprets network traffic based on a set of rules, and depending on the interactions certain assignments are blocked. Open source, written in Go and delivered as a single executable
HardenTools	A utility that disables a number of risky Windows features. These "features" are exposed by the OS and primary consumer applications, and very commonly abused by attackers, to execute malicious code on a victim's computer. So this tool just reduces the attack surface by disabling the low-hanging fruit
ShutUp10	A portable app that lets you disable core Windows features (such as Cortana, Edge) and control which data is passed to Microsoft. (Note: Free, but not open source)
WPD	Portable app with a GUI, that makes it really easy to safely block key telemetry features, from sending data to Microsoft and other third parties (It uses the Windows API to interact with key features of Local Group Police, Services, Tasks Scheduler, etc)
GhostPress	Anti low-level keylogger: Provides full system-wide key press protection, and target window screenshot protection
KeyScrambler	Provides protection against software keyloggers. Encrypts keypresses at driver level, and decrypts at application level, to protect against common keyloggers - read more about how it works. Developed by Qian Wang
SafeKeys V3.0	Portable virtual keyboard. Useful for protecting from keyloggers when using a public computer, as it can run of a USB with no administrative permissions
RKill	Useful utility, that attempts to terminate known malware processes, so that your normal security software can then run and clean your computer of infections
IIS Crypto	A utility for configuring encryption protocols, cyphers, hashing methods, and key exchanges for Windows components. Useful for sysadmins on Windows Server

Provider	Description
NetLimiter	Internet traffic control and monitoring tool
Sticky-Keys-Slayer	Scans for accessibility tools backdoors via RDP
SigCheck	A CLI utility that shows file version number, timestamp information, and digital signature details. It's useful to audit a Windows host's root certificate store against Microsoft's Certificate Trust List (CTL), and lets you perform VirusTotal lookups
BleachBit	Clears cache and deletes temporary files very effectively. This frees up disk space, improves performance, but most importantly helps to protect privacy
Windows Secure Baseline	Group Policy objects, compliance checks, and configuration tools that provide an automated and flexible approach for securely deploying and maintaining the latest releases of Windows 10
USBFix	Detects infected USB removable devices
GMER	Rootkit detection and removal utility
ScreenWings	Blocks malicious background applications from taking screenshots
CamWings	Blocks unauthorized webcam access
SpyDish	Open source GUI app built upon PowerShell, allowing you to perform a quick and easy privacy check, on Windows 10 systems. Highlights many serious issues, and provides assistance with fixing
SharpApp	Open source GUI app built upon PowerShell, for disabling telemetry functions in Windows 10, uninstalling preinstalled apps, installing software packages and automating Windows tasks with integrated PowerShell scripting
Debotnet	Light-weight, portable app for controlling the many privacy-related settings within Windows 10- with the aim of helping to keep private data, private
PrivaZer	Good alternative to CCleaner, for deleting unnecessary data - logs, cache, history, etc

Word of Warning

(The above software was last tested on 01/05/20). Many of the above tools are not necessary or suitable for beginners, and can cause your system to break - only use software that you need, according to your threat model. Take care to only download from an official/ legitimate source, verify the executable before proceeding, and check reviews/ forums. Create a system restore point, before making any significant changes to your OS (such as disabling core features). From a security and privacy perspective, Linux may be a better option.

See Also

- github.com/Awesome-Windows/Awesome#security
- github.com/PaulSec/awesome-windows-domain-hardening
- github.com/meitar/awesome-cybersecurity-blueteam#windows-based-defenses

Mac OS Defences

Provider	Description
LuLu	Free, open source macOS firewall. It aims to block unknown outgoing connections, unless explicitly approved by the user
Stronghold	Easily configure macOS security settings from the terminal
Fortress	Kernel-level, OS-level, and client-level security for macOS. With a Firewall, Blackhole, and Privatizing Proxy for Trackers, Attackers, Malware, Adware, and Spammers; with On-Demand and On-Access Anti-Virus Scanning

Anti-Malware

Cross-platform, open source malware detection and virus prevention tools

Provider	Description
ClamAV	An open source cross-platform antivirus engine for detecting viruses, malware & other malicious threats. It is versatile, performant and very effective
VirusTotal	Web-based malware scanner, that inspects files and URLs with over 70 antivirus scanners, URL/domain services, and other tools to extract signals and determine the legitimacy
Armadito	Open source signature-based anti-virus and malware detection for Windows and Linux. Supports both ClamAV signatures and YARA rules. Has a user-friendly interface, and includes a web-based admin panel for remote access.

Notable Mentions

For 1-off malware scans on Windows, MalwareBytes is portable and very effective, but not open source

Word of Warning

For Microsoft Windows, Windows Defender provides totally adequate virus protection in most cases. These tools are intended for single-use in detecting/ removing threats on an infected machine, and are not recommended to be left running in the background, use portable editions where available.

Many anti virus products have a history of introducing vulnerabilities themselves, and several of them seriously degrade the performance of your computer, as well as decrease your privacy. Never use a free anti-virus, and never trust the companies that offer free solutions, even if you pay for the premium package. This includes (but not limited to) Avast, AVG, McAfee and Kasperky. For AV to be effective, it needs intermate access to all areas of your PC, so it is important to go with a trusted vendor, and monitor its activity closely.

Home Automation

If you have smart devices within your home, you should consider running the automation locally, rather than using a cloud service. This will reduce the amount of exploits you could potentially be vulnerable to. It is also important to have network monitoring and firewalls enabled, to ensure suspicious activity is flagged or blocked. The following projects will make controlling and monitoring IoT devices within your home easier, safer and more private.

Provider	Description
Home Assistant	Open source home automation that puts local control and privacy first - 1500+ integrations. Runs well on a Raspberry Pi, accessible though a web interface and CLI, as well as several controller apps (such as HassKit and the official Home Assistant App)
OpenHAB	A vendor and technology agnostic open source automation software for your home, with 2000+ supported devices and addons. Works well on a Raspberry Pi, or low-powered home server, and again there are some great apps for, such as the official OpenHabb App and the HomeHabit wall dashboard
Domoticz	Another home automation system, Domoticz is more geared towards connecting and monitoring sensors within your space. Allows you to monitor your environment without anyone but you having access to the data
Node-RED	Node-RED is a programming tool for wiring together hardware devices, APIs and online services, it provides a browser-based editor that makes it easy to build flows with a wide range of supported nodes, and it is easy to deploy locally in your network

Notable Mentions

For creating dashboard from IoT devices, see ThingsBoard. Another home automation tool is FHEM, which has been around for a while and needs a bit more work to get up and running, but is still a popular option.

Word of Warning

IoT smart home devices can open you up to many security risks and exploits. It is really important that you configure them correctly, setting strong unique passwords, turn off data sharing, and if possible restrict internet access so devices can only communicate within your local network. See Smart Home Security Checklist for more tips.

Code Hosting

Provider	Description
SourceHut	Git and mercurial code hosting, task management, mailing lists, wiki hosting and Alpine-based build pipelines. Can be self-hosted, or used through the managed instance at sr.ht
Codeberg	A fully-managed instance of Forgejo
GitLab	Fully-featured git, CI and project management platform. Managed instance available, but can also be self-hosted

Provider	Description
Gitea	Lightweight self-hosted git platform, written in Go
Gogs	Lightweight self-hosted git platform, written in Go

AI Voice Assistants

Google Assistant, Alexa and Siri don't have the best reputation when it comes to protecting consumers privacy, there have been many recent breaches. For that reason it is recommended not to have these devices in your house. The following are open source AI voice assistants, that aim to provide a human voice interface while also protecting your privacy and security

Provider	Description
Mycroft	An open source privacy-respecting AI platform, that runs on many platforms (Raspberry Pi, desktop, or dedicated Mycroft device). It is in active development, with thorough documentation and a broad range of available skills, but also Mycroft makes it really easy to develop new skills
Kalliope	An open source, modular always-on voice controlled personal assistant designed for home automation. It runs well on Raspberry Pi, Debian or Ubuntu and is easy to program with simple YAML-based skills, but does not have a wide library of pre-built add-ons

Notable Mentions

If you choose to continue using Google Home/ Alexa, then check out **Project Alias**. It's a small app that runs on a Pi, and gives you more control over your smart assistants, for both customisation and privacy.

For a desktop-based assistant, see Dragonfire for Ubuntu, and Jarvis for MacOS. LinTO, Jovo and Snips are private-by-design voice assistant frameworks that can be built on by developers, or used by enterprises. Jasper, Stephanie and Hey Athena are Python-based voice assistant, but neither is under active development anymore. See also OpenAssistant.

Word of Warning

If you are building your own assistant, you may want to consider a hardware-switch for disabling the microphone. Keep tabs on issues and check the code, to ensure you are happy with how it works, from a privacy perspective.

Bonus #1 - Alternatives to Google

Moving away from Google, and using multiple alternative apps will mean there is no single source of tracking. Open source and privacy-focused software is best

- Academic: RefSeek, Microsoft Academic, More Academic Search Engines
- Analytics: Matomo, Privalytics, Plausible, Fathom, GoatCounter, ShyNet, Pirsch
- Assistant: Mycroft, Kalliope, Project-Alias (for Google Home/ Alexa)

- Authenticator: Aegis (Android), Authenticator (ios)
- Blogging: Write Freely, Telegraph, Mataroa, Bear Blog, Ghost (Self-Hosted)
- Browsers: Brave, Firefox (with some tweaks), Vivaldi
- Calendar: EteSync, ProtonCalendar, NextCloud Calendar (self-hosted), Radicale (self-hosted, also supports contact lists)
- Cloud: Njalla, Vindo, Private Layer
- DNS: Cloudflare, Quad9
- Docs: NextCloud, CryptPad, Skiff
- Finance: Wallmine, MarketWatch, Nasdaq Lookup
- Flights: SkyScanner, Kayak (Note: Beware of tracking, use Tor)
- Location Tracker: Private Kit
- Mail: ProtonMail, Tutanota, MailFence, HushMail, Skiff
- Maps: OpenStreetMaps (web), OsmAnd (Android + iOS)
- Messaging: Signal (Mobile Number Required), KeyBase, Session (beta)
- Mobile OS: LineageOS, GrapheneOS, Ubuntu Touch
- Notes: Cryptee, Joplin, Standard Notes, Joplin
- Passwords: BitWarden, 1Password, KeePassXC, LessPass
- Pay (Currencies): Monero, ZCash
- Pay (Virtual Cards): Privacy.com, Revolut (disposable virtual credit cards)
- Photos: PhotoPrism (Self-Hosted)
- Play Store: F-Droid, APK Mirror
- Search: DuckDuckGo, Searx (self-hosted), Qwant
- Sync: SeaFile, Syncthing, NextCloud, Duplicacy
- Translate: Apertium
- Weather: Geometric Weather (Android), Open Weather Map (Web)
- Workspace / Group Messaging: Riot (Through Matrix), Jami
- Video Platforms: PeerTube, BitChute (Caution: Not moderated), Invidio (YouTube Proxy)

Bonus #2 - Open Source Media Applications

Community-maintained media software can help you migrate away from providers that may not respect privacy. The following creative software packages are open source, cross-platform and free.

- Graphics: GIMP, Scribus, SwatchBooker, InkScape, Krita
- Audio: Audacity, Mixxx, MusicBrainz, Qtractor, SpotiFlyer
- Video: Shortcut, OpenShot, kdenlive
- Video Transcoders: HandBreak
- Media Players: VLC Player
- Media Servers: Kodi, Plex, Subsonic, Emby, Gerbera, OpenELEC, OpenFlixr 2, OCMC
- 3D Rendering: Blender, Wings3D
- Game Engines: GoDot, SpringEngine, Panda3D, Cocos

- Rendering Engines: LuxCoreRender, AppleSeed

Bonus #3 - Self-Hosted Services

- Analytics: Matomo, Privalytics, Plausible, Fathom, GoatCounter, ShyNet
- Blogging: Hexo, Noddity, Plume, Ghost, Write.as
- Bookmarks: Shiori, Geek Marks, Ymarks, xBrowserSync, reminiscence, unmark
- Chat Networks: Gotify, GNU:net, Centrifugo, Mumble, Tox, Matrix + Riot, Retroshare
- CMS: Strapi (headless), ApostropheCMS, Plone, Publify, Pico
- Conference: Jami, Jitsu, BigBlueButton (Academic Institutions), OpenMeetings
- Document Management: Paperless
- E-Commerce: Qor, Magento, Grandnode
- Email Clients: Rainloop, RoundCube
- Email Setup: Mailu, MailCow, Mail-in-a-Box
- File Drop: PsiTransfer, Up1, FilePizza
- File Explorer: FileRun, Pydio
- Groupware: SoGo, SuiteCRM
- News Letters: LewsNetter, PHP List, Dada Mail
- Office Suites: CryptPad, LibreOffice, onlyoffice, NextCloud
- Paste Bins: Snibox, PrivateBin, 0bin, Stikked
- Photo Managers: PhotoPrism
- Search Engine: Searx
- Social Networks: Mastodon, Pixelfed, diaspora
- Ticketing: Zammad, osTicket, Helpy
- URL Shortners: Shlink, Polr, Istu, Linkr
- WiKi/ Knowledge Sharing: Gollum, Outline, Wiki JS, Gitit, TidyWiki5, Cowyo
- XMPP: Server: ejabberd, MongooseIM, OpenFire, Prosody. Clients: Converse, JSXC, Movim, XMPP Web

Bonus #4 - Self-Hosted Sysadmin

- Ad-Block (network-wide): PiHole
- Content Filter: E2Guardian, Squid Guard
- Cron Jobs: HealthChecks
- Dashboards: Homer, Heimdall, SWMP, Uchiwa (for Sensu), Linux Dash
- DNS: CoreDNS, KnotDNS, Bind 9, PowerDNS
- Domain Control: DomainMod, OctoDNS, DNSControl
- Firewall: IPFire, PFSense, OpenSense, ShoreWall
- Log Management: GoAccess
- Monitoring: Alerta, Cabot, Cadvisor, CheckMK, Linux Dash. NetData, PS Dash
- Proxy: ShaddowSocks, Privoxy

- Server Status: Statup, BotoX / ServerStatus, Mojeda / ServerStatus, Statusfy, Cachet
- SSH Tools: RTop (sts stats), Fiche (cli pastepin)
- Storage DB: OpenTSBD, KairosDB, InfluxData
- VPN: OpenVPN, Pritunl
- Web Servers: NGINX, Caddy, Light TPD

Bonus #5 - Self-Hosted Development Tools

- API Management: Kong, Krakend, tyk, Hasura
- Browser-based IDE: Code Server (VS Code), Che (Eclipse), ICEcoder, ml-workspace (for Data science and ML), r-studio (for R programming)
- Code Reviews: Phabricator. See also: Git Servers, most of which have CR features
- Containers: Docker, LXC, OpenVZ
- Continuous Integration: Drone, Concourse, BuildBot, Strider, Jenkins
- Deployment Automation: Capustrano, Fabric, Mina, Munki, Rocketeer, Sup
- Doc Generators: FlatDoc, Docsify, Sphinx, ReadTheDocs, Docusarus, mkdocs
- Git Server: GitBucket, GitTea, GitLab, Gogs
- Localization: Weblate, Translate/ Pootle, Accent
- Serverless: OpenFaas, IronFunctions, LocalStack, fx
- Static Site Gen: See StaticGen.com
- UI Testing: Selenoid, Zalenium, Selenium
- More Tools:
  - Request Bin - Inspect HTTP requests and Debug webhooks
  - Regexr - Web tool for for creating, testing, and learning about Regular Expressions
  - JS Bin - Collaborative JavaScript Debugging App, create, test, run and send web code snippets
  - Koding - A development platform to orchestrates your project-specific dev environment
  - Judge0 - A web compiler accessed through either an API of web-IDE, for executing trusted or untrusted code
  - SourceGraph - Self-hosted universal code search and navigation engine

Bonus #6 - Security Testing Tools

This list is intended to aid you in auditing the security of your own systems, and help detect and eliminate vulnerabilities. It is intended for advanced users and sysadmins. For penetration testing, see enaqx/awesome-pentest GitHub list instead

- Amass - In-depth Attack Surface Mapping and Asset Discovery, to help you identify issues and secure your network
- CloudFail - Ensure there are no misconfigured DNS and old database records, accessible by bypassing CloudFlare network
- CrackMapExec - A CLI tool for pen testing all areas of your local and remote networks, to ensure their integrity

- DNSdumpster - A domain research tool that can discover hosts related to a domain. It can be used to test and ensure there are no visible hosts that a hacker could exploit
- DNSTracer - Scan your domain, to show which records are publicly visible and need to be obfuscated
- dnstwist - Domain name permutation engine for detecting typo squatting, phishing and corporate espionage, to protect those on your network
- GRR - incident response framework focused on remote live forensics
- Impacket - A collection of Python classes for working with network protocols, focused on providing low-level programmatic access to the packets and for the protocol implementation themselves
- Kali Linux - A Debian-based distro for security testing, bundled with 1000's of powerful packages and scripts. Saves a lot of time configuring sys-admin tools and drivers
- Lynis - A security tool that performs an extensive health scan of your systems to support system hardening and compliance testing
- Masscan - TCP port scanner, that checks packets asynchronously, configure it to check only your IP ranges and it completes in milliseconds
- Metasploit - Popular and powerful penetration testing framework, for exploitation and vulnerability validation - bundled with a full suite of tools, it makes it easy to divide your penetration testing workflow into manageable sections. Very useful for testing your entire network E2E
- Moloch - Full packet capture, indexing, and database system. The elastic search backend makes searching through pcaps fast, and the frontend displays captured data clearly with good support for protocol decoding
- Nikto2 - Well-established web server testing tool, useful for firing at your web server to find known vulnerable scripts, configuration mistakes and related security problems
- Nmap - Powerful utility for network discovery and security auditing. Useful for your network inventory, managing service upgrade schedules, and monitoring host or service uptime
- OpenAudit - An application to tell you exactly what is on your network, how it is configured and when it changes
- OpenVAS - Fully-featured security vulnerability management system, with web-based dashboards. Useful for fast and easy scans of your network
- OSQuery - SQL powered operating system instrumentation, monitoring, and analytics. Very performant cross-platform tool, useful for monitoring a host for changes and providing endpoint visibility
- OSSEC HIDS - A host based intrusion detection system that is easy to setup and configure, which performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response
- Otseca - Search and dump your system configuration + generate HTML reports
- RouterSploit: An exploitation framework for checking the security of local embedded devices, to ensure they are safe
- Security Onion - Linux distro for intrusion detection, enterprise security monitoring, and log management. It includes a suite of security testing tools. Useful for collecting, storing and managing a variety of system data, for use on your networks
- Snort - Intrusion detection system aimed at real time traffic analysis and packet logging tool
- SPARTA - GUI tool that makes pen testing your network infrastructure easier
- Wireshark - Popular, powerful feature-rich network protocol analyser. Lets you analyse everything that is going on in your network in great detail

- Zeek - Powerful intrusion detection system and network security monitoring, that (rather than focusing on signatures) decodes protocols and looks for anomalies within the traffic

Bonus #7 - Raspberry Pi/ IoT Security Software

- OnionPi - Create an Anonymizing Tor Proxy using a Raspberry Pi
- CIRCLean - A Pi-based USB Sanitizer, plug an untrusted USB in, and get clean files out
- Pi Hole - A network-wide ad-block, that improves network performance as well as privacy
- Project Alias - Gives you full-control, and better privacy of your Google Home or Alexa
- Raspiblitz - Build your own Bitcoin & Lightning Node on a Pi, see also Trezor wallet
- PiVPN - Simple low-cost yet secure VPN, for the Raspberry Pi (or set up manually, as outlined in this guide)
- DeauthDetector - Detect deauthentication frames using an ESP8266, useful to be aware of ongoing wireless attacks
- IPFire - Hardened open source firewall to prevent common attacks on your network. Capable of running on a Pi
- SquidGuard - Fast and free URL redirector, which can work well as a home caching server
- E2guardian - Comprehensive content filtering, with powerful configuration options

USB-based projects include:

- DBAN - Bootable hard drive erasers for destroying data
- Syncthing - Create automated backups to an external medium
- KeePass Portable - Portable password manager. For hardware-encrypted password manager, see HardPass 2.0
- VeraCrypt - Full drive encryption for USB devices

See more hardware-based security solutions

More Awesome Software Lists

This list was focused on privacy-respecting software. Below are other awesome lists, maintained by the community of open source software, categorised by operating system.

- Windows: awesome-windows-apps by 'many'
- MacOS: awesome-macOS-apps by @iCHAIT
- Linux: awesome-linux-software by @luong-komorebi
- iOS: open-source-ios-apps by @dkhamsing
- Android: open-source-android-apps by @pcqpcq
- Server: awesome-selfhosted by 'many'
- **More GitHub Awesome Lists →**

News & Updates

A custom Reddit feed covering news and updates for privacy-respecting apps, software & services can be found here

Final Notes

Conclusion

Many corporations put profit before people, collecting data and exploiting privacy. They claim to be secure but without being open source it can't be verified, until there's been a breach and it's too late. Switching to privacy-respecting open source software will drastically help improving your security, privacy and anonymity online.

However, that's not all you need to do. It is also important to : use strong and unique passwords, 2-factor authentication,
adopt good networking practices and be mindful of data that are collected when browsing the web. You can see the full
personal security checklist for more tips to stay safe.

Important Considerations

Compartmentalise, Update and Be Ready

No piece of software is truly secure or private. Further to this, software can only as secure as the system it is running on. Vulnerabilities are being discovered and patched all the time, so you much keep your system up-to-date. Breaches occur regularly, so compartmentalise your data to minimise damage. It's not just about choosing secure software, you must also follow good security practices.

Attack Surface

It is a good idea to keep your trusted software base small, to reduce potential attack surface. At the same time trusting a single application for too many tasks or too much personal data could be a weakness in your system. So you will need to judge the situation according to your threat model, and carefully plan which software and applications you trust with each segment of your data.

Convenience Vs Security

There is often a trade-off between convenience and security. Construct a threat model, and choose a balance that is right for you. In a similar way in some situations there is privacy and security conflict (e.g. Find My Phone is great for security, but terrible for privacy, and anonymous payments may be good for privacy but less secure than insured fiat currency). Again it is about assessing your situation, understanding the risks and making an informed decision.

Hosted Vs Self-Hosted Considerations

When using a hosted or managed application that is open-source software - there is often no easy way to tell if the version running is the same as that of the published source code (even published signatures can be faked). There is always the possibility that additional backdoors may have been knowingly or unknowingly implemented in the running instance. One way round this is to self-host software yourself. When self-hosting

you will then know for sure which code is running, however you will also be responsible for the managing security of the server, and so may not be recommended for beginners.

Open Source Software Considerations

Open source software has long had a reputation of being more secure than its closed source counterparts. Since bugs are raised transparently, fixed quickly, the code can be checked by experts in the community and there is usually little or no data collection or analytics.
That being said, there is no piece of software that it totally bug free, and hence never truly secure or private. Being open source, is in no way a guarantee that something is safe. There is no shortage of poorly-written, obsolete or sometimes harmful open source projects on the internet. Some open source apps, or a dependency bundled within it are just plain malicious (such as, that time Colourama was found in the PyPI Repository)

Proprietary Software Considerations

When using a hosted or proprietary solution - always check the privacy policy, research the reputation of the organisation, and be weary about which data you trust them with. It may be best to choose open source software for security-critical situations, where possible.

Maintenance

When selecting a new application, ensure it is still being regularly maintained, as this will allow for recently discovered security issues to be addressed. Software in an alpha or beta phase, may be buggy and lacking in features, but more importantly - it could have critical vulnerabilities open to exploit. Similarly, applications that are no longer being actively maintained may pose a security risk, due to lack of patching. When using a forked application, or software that is based on an upstream code base, be aware that it may receive security-critical patches and updates at a slightly later date than the original application.

This List: Disclaimer

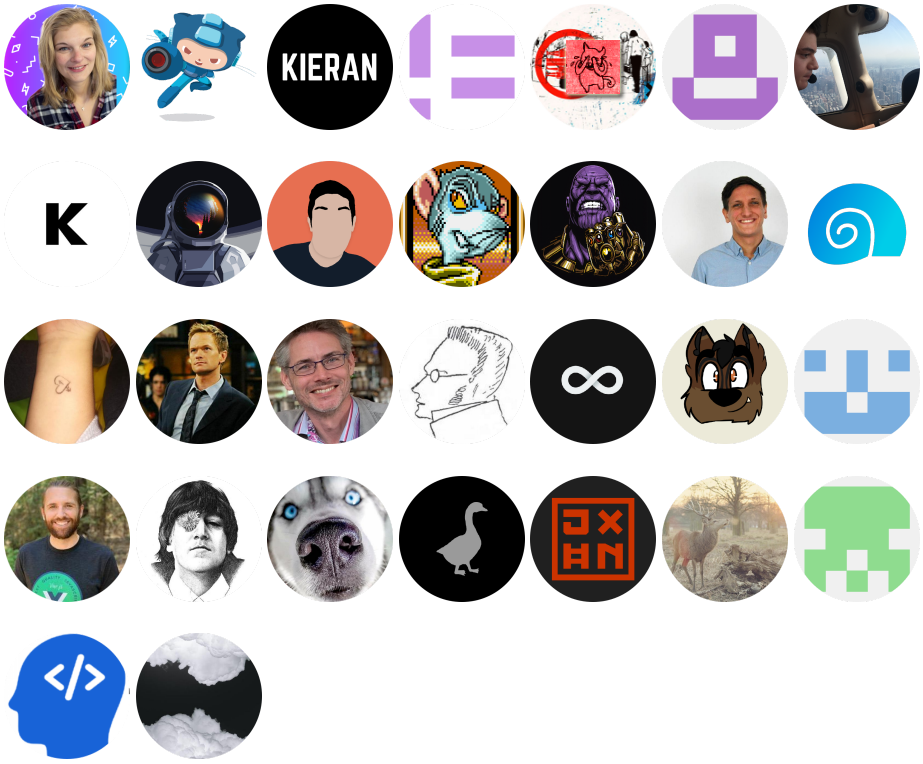
This list contains packages that range from entry-level to advanced, a lot of the software here will not be appropriate for all audiences. It is in no way a definitive list of secure applications, and aims only to be a guide, a collection of software and services that myself and other contributors have used, and would recommend. There will always be new vulnerabilities discovered or introduced, bugs and security-critical glitches, malicious actors and poorly configured systems. It is up to you to do your research, draw up a threat model, and decide where and how your data are managed.

If you find something on this list that should no longer be deemed secure or private/ or should have a warning note attached, please raise an issue. In the same way if you know of something that is missing, or would like to make an edit, then pull requests are welcome, and are much appreciated!

Contributors

This is a community-maintained project, which wouldn't have been possible without help from all these wonderful people.

Top Contributors:



Contributing

Thanks for visiting! If you have suggestions, then you open an issue, or submit a PR, see: `CONTRIBUTING.md`. *Contributions are welcome, and always much appreciated ☺*

License

Licensed under Creative Commons, CC BY 4.0, © Alicia Sykes 2022

Thank you

Thank you for checking out this project - I hope you found it somewhat useful 😊

This list was initially compiled by Alicia Sykes / :octocat: @Lissy93, with a lot of help from the community.

Follow me on GitHub for updates and other projects.

If you found this project helpful, consider dropping us a star, and sharing with your network.