Awesome Privacy

 awesome-privacy.xyz

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

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 privacy and 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
>
> **Mirror**: This repo is mirrored to codeberg.org/alicia/awesome-privacy
>
> **Repo Admin**: Website Docs | API Docs | Contributing | Acknowledgment | License

> ▶ **Contents**

Essentials

Password Managers

- 
  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.
  …
  - ▶ Stats
- 
  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 - 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.

…

- ▶ Stats

- 
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.

…

- ▶ Stats

- 
ProtonPass - From the creators of ProtonMail, ProtonPass is a new addition to their suite of services. They have a full collection of user-friendly native mobile and desktop apps. ProtonPass is one of the few "trustworthy" providers that also offers a free plan.

…

- ▶ Stats

▶ ✳ **Notable Mentions**

▶ **ℹ Further Info**

⬆ [Back to Top]

2-Factor Authentication

- 
2FAS - Free, secure and open source authenticator app for both iOS and Android. Supports creating encrypted backups and syncing between devices without the need for an account.

…

- ▶ Stats

- 
Aegis - Free, secure and open source authenticator app for Android. Has a backup/restore feature and a customisable UI with dark mode

…

- ▶ Stats

- 
Authenticator Pro - 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

…

- ▶ Stats

- 
Tofu - An easy-to-use, open-source two-factor authentication app designed specifically for iOS

…

- ▶ Stats

- 
  Authenticator - Simple, native, open source 2-FA Client for iOS, which never connects to the internet - built by @mattrubin.me

  …
  - ▶ Stats
- 
  Raivo OTP - A native, lightweight and secure one-time-password (OTP) client built for iOS; Raivo OTP! - built by @tijme

  …
  - ▶ Stats
- 
  WinAuth - 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)

  …
  - ▶ Stats
- 
  Authenticator GNOME - Rust-based OTP authenticator. Has native With GNOME Shell integration. Also available through flathub.

  …
- 
  Authenticator CC - 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).

  …
  - ▶ Stats

▶ ✳ **Notable Mentions**

▶ **ℹ Further Info**

⬆ [Back to Top]

File Encryption

-
  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.

  …
  - ▶ Stats
- 

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.

…

- ▶ Stats

-  **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

  …

  - ▶ Stats

▶ ⚠ **Word of Warning**

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

Browsers

-  **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.

  …

  - ▶ Stats

-  **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.

  …

  - ▶ Stats

-  **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

  …

- ▶ Stats

- **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
  …
  - ▶ Stats

- **Bromite** - Hardened and privacy-respecting fork of Chromium for Android. Comes with built-in adblock and additional settings for hardening.
  …
  - ▶ Stats

▶ ⚠ **Word of Warning**

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

Search Engines

- **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
  …
  - ▶ Stats

- **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.
  …
  - ▶ Stats

- **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)
  …
  - ▶ Stats

- **Mojeek** - British search engine providing independent and unbiased search results using its own crawler. Has a zero tracking policy (it is not open source)
  …

- ▶ Stats

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

Communication

Encrypted Messaging

- **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.
  …
  - ▶ Stats
- **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.
  …
  - ▶ Stats
- **XMPP** - 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.
  …
  - ▶ Stats
- **Matrix** - 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.

…

- ▶ Stats

▶ ⚠ **Word of Warning**

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

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.

- **Oxen** - Oxen (previously 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.

  …

  - ▶ Stats
- **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).

  …

  - ▶ Stats
- **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.

  …

  - ▶ Stats
- **Jami** - P2P encrypted chat network with cross-platform GNU client apps. Jami supports audio and video calls, screen sharing, conference hosting and instant messaging.

  …

  - ▶ Stats
-

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.

…

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

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.

For a more details comparison of email providers, see email-comparison.as93.net

- **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).

  …

  - ▶ Stats

- **Tuta** - 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. Tuta has a full-featured free plan or a premium subscription for businesses allowing for custom domains ($12/ month). Tuta 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.

  …

  - ▶ Stats

- **Forward Email** - An open source, privacy-focused, encrypted email service supporting SMTP, IMAP, and API access

  …

- ▶ Stats

- 
  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.
  …
  - ▶ Stats

- 
  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.
  …
  - ▶ Stats

▶ ⚠ **Word of Warning**

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

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.

- 
  Mozilla Thunderbird - Free and open source email application developed and backed by Mozilla -it's secure,
  private easy and customizable. 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.
  …
  - ▶ Stats

- **eM Client** - 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.
  …
  - ▶ Stats
- **SnappyMail** - 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.
  …
  - ▶ Stats
- **RoundCube** - 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.
  …
  - ▶ Stats
- **FairEmail** - 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.
  …
  - ▶ Stats
- **K-9 Mail** - K-9 (or Thunderbird for Android) 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.
  …
  - ▶ Stats

▶ ⚠ **Word of Warning**

⬆ [Back to Top]

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.

- 
  Addy - An open source anonymous email forwarding service, allowing you to create unlimited email aliases. Has a free plan.
  …
  - ▶ Stats
- 
  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. Note that 33Mail usese Google Analytics.
  …
  - ▶ Stats
- 
  SimpleLogin - Fully open source (view on GitHub) alias 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.
  …
  - ▶ Stats
- 
  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.
  …
  - ▶ Stats
- 
  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.
  …
  - ▶ Stats
- 
  ProtonMail - 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.
  …
  - ▶ Stats

⬆ [Back to Top]

Email Security Tools

- **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.
  …
  - ▶ Stats
- **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).
  …
  - ▶ Stats

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

VOIP Clients

- **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.
  …
  - ▶ Stats
- **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.
  …
  - ▶ Stats

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

Virtual Phone Numbers

- **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.
  …
  - ▶ Stats
- **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. See alternate instances at soprani.ca
  …
- **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.
  …

⬆ [Back to Top]

Team Collaboration

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.

- **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.
  …
  - ▶ Stats
-

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.

…

- ▶ Stats

- **Element** - Privacy-focused messenger using the Matrix protocol. The Element client allows for group chat rooms, media sharing voice and video group calls.

  …

  - ▶ Stats

- **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.

  …

  - ▶ Stats

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

Security Tools

Browser Extensions

The following browser add-ons give you better control over what content is able to be loaded and executed while your browsing.
Before installing anything, you should read the Word of Warning section below.

- **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
…
    - ▶ Stats
- 
uBlock Origin - Block ads, trackers and malware sites. **Download**:
Chrome -
Firefox
…
    - ▶ Stats
- 
ScriptSafe - Allows you to block the execution of certain scripts. **Download**:
Chrome -
Ppera
…
    - ▶ Stats
- 
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
…
    - ▶ Stats
- 
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
…
    - ▶ Stats
- 
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
…
    - ▶ Stats
- 
ClearURLs - This extension will automatically remove tracking elements from the GET parameters of URLs to
help protect some privacy **Download**: Chrome -

Firefox / Source

…

- ▶ Stats

- 
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

…

- ▶ Stats

-
First Party Isolation - Enables the First Party isolation preference (Clicking the Fishbowl icon temporarily disables it)
Download: Firefox

…

- ▶ Stats

- 
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

…

- ▶ Stats

- 
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

…

- 
Privacy Essentials - Simple extension by DuckDuckGo, which grades the security of each site.
Download:
Chrome
Firefox

…

- ▶ Stats

- **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
  …
  - ▶ Stats
- **Privacy Redirect** - A simple web extension that redirects Twitter, YouTube, Instagram & Google Maps requests to privacy friendly alternatives
  Download: Firefox - Chrome
  …
  - ▶ Stats
- **Site Bleacher** - Remove automatically cookies, local storages, IndexedDBs and service workers
  Download:
  Firefox -
  Chrome -
  Source
  …
  - ▶ Stats
- **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 -
  Firefox -
  Edge -
  Opera -
  Source
  …
  - ▶ Stats
- **PrivacySpy** - The companion 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 -
  Firefox
  …

- ▶ Stats

- **HTTPZ** - Simplified HTTPS upgrades for Firefox (lightweight alternative to HTTPS-Everywhere)
Download:
Firefox
…
  - ▶ Stats

- **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
…
  - ▶ Stats

- **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
…
  - ▶ Stats

- **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
…
  - ▶ Stats

- **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
…
  - ▶ Stats

- **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**: Firefox - Source
…
  - ▶ Stats

-

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

…

- ▶ Stats

- 
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 site's 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

…

- 
HTTPS Everywhere - **NOTE** On modern browsers, this is no longer needed
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

…

- ▶ Stats

▶ ⚠ **Word of Warning**

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

Mobile Apps

- 
Orbot - System-wide Tor proxy, which encrypts your connection through multiple nodes.
You can also use it alongside Tor Browser to access .onion sites.

…

- ▶ Stats

- 
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.

…

- ▶ Stats

- 
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.

…

- ▶ Stats

- 

Insular - An actively-maintained fork of the Island project with additional enhancements

…

- ▶ Stats

- 

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.

…

- ▶ Stats

- 

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.

…

- ▶ Stats

- 

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. See on F-Droid

…

- 

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.

…

- ▶ Stats

- 

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.

…

- ▶ Stats

- 

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.

…

- ▶ Stats

- 
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.

…

- 
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).

…

- ▶ Stats

- 
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.

…

- ▶ Stats

- 
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.
Get from F-Droid

…

- ▶ Stats

- 
TrackerControl - Monitor and control hidden data collection in mobile apps about user behavior/ tracking.
Get from F-Droid

…

- ▶ Stats

- 
Greentooth - Auto-disable Bluetooth, then it is not being used. Saves battery, and prevent some security risks.
Get from F-Droid

…

- 
PrivateLock - Auto lock your phone based on movement force/ acceleration.
Get from F-Droid
See also PluckLock

…

- ▶ Stats

- 
  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.
  Get from F-Droid
  …
  - ▶ Stats
- 
  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).
  …
  - ▶ Stats
- 
  F-Droid - F-Droid is an installable catalogue of FOSS applications for Android. The client enables you to browse, install, and keep track of updates on your device.
  …
  - ▶ Stats

▶ ⚠ **Word of Warning**

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

Online Tools

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

- 
  Have i been pwned - Checks if your credentials (Email address or Password) have been compromised in a data breach.
  See also Firefox Monitor.
  …
  - ▶ Stats

- **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.
  …
  - ▶ Stats
- **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.
  …
  - ▶ Stats
- **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.
  …
  - ▶ Stats
- **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.
  …
  - ▶ Stats
- **IP Leak Test** - Shows your IP address, and other associated details (location, ISP, WebRTC check, DNS, and lots more).
  …
  - ▶ Stats
- **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).

  …

- **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*).

  …

  - ▶ Stats

- **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.

  …

- **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.

  …

  - ▶ Stats

- **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**

⬆ [Back to Top]

Networking

Virtual Private Networks

- **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).

  …

  - ▶ Stats

- **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.

  …

  - ▶ Stats

- **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 cryptocurrencies.

  …

  - ▶ Stats

- **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.

  …

  - ▶ Stats

- **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.

  …

  - ▶ Stats

▶ ⚠ **Word of Warning**

▶ ✳ **Notable Mentions**

▶ ℹ **Further Info**

⬆ [Back to Top]

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

- 
  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.

  …
  - ▶ Stats
- 
  Technitium - Another DNS server for blocking privacy-invasive content at its 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.

  …
  - ▶ Stats
- 
  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.

  …
  - ▶ Stats
- 
  PiVPN - A simple way to set up a home VPN on 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.

  …
  - ▶ Stats
- 
  E2guardian - Powerful open source web content filter.

  …
  - ▶ Stats
- 
  PF Sense - Widely used, open source firewall/router.

  …
  - ▶ Stats
- 
  Zeek - Detect if you have a malware-infected computer on your network, and powerful network analysis framework and monitor.

  …
  - ▶ Stats

- **Firezone** - Open-source self-hosted VPN and firewall built on WireGuard®.
  …
  - ▶ Stats

⬆ [Back to Top]

Mix Networks

- **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.
  …
  - ▶ Stats
- **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.
  …
  - ▶ Stats

▶ ⚠ **Word of Warning**

▶ ✳ **Notable Mentions**

▶ **i Further Info**

⬆ [Back to Top]

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.

ShadowSocks - Secure socks5 proxy, designed to protect your Internet traffic. Open source, superfast, cross-platform and easy to deploy, see GitHub repo.

…

- ▶ Stats

- **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.

  …

▶ ⚠ **Word of Warning**

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

DNS Providers

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.

- **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.

  …

  - ▶ Stats

- **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.

  …

  - ▶ Stats

- **NextDNS** - An ad-blocking, privacy-protecting, censorship-bypassing DNS. Also comes with analytics, and the ability to shield kids from adult content.

  …

  - ▶ Stats

▶ ⚠ **Word of Warning**

▶ ✳ **Notable Mentions**

▶ ℹ **Further Info**

⬆ [Back to Top]

DNS Clients

- **DNScrypt-proxy 2** - 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.
  …
  - ▶ Stats
- **Unbound** - 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.)
  …
  - ▶ Stats
- **Nebulo** - 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.)
  …
  - ▶ Stats
- **RethinkDNS & Firewall** - 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.)
  …
  - ▶ Stats
- **DNS Cloak** - Simple all that allows for the use for dnscrypt-proxy 2 on an iPhone.
  …
  - ▶ Stats
- **Stubby** - 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.
  …
  - ▶ Stats

⬆ [Back to Top]

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.

- 
  NetGuard - 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.
  …
  - ▶ Stats
- 
  NoRoot Firewall - 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 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.
  …
  - ▶ Stats
- 
  RethinkDNS & Firewall - An open-source ad-blocker and firewall app for Android 6+ (does not require root).
  …
  - ▶ Stats
- 
  Lockdown - Firewall app for iPhone, allowing you to block any connection to any domain.
  …
- 
  SimpleWall - Tool to control Windows Filtering Platform (WFP), in order to configure detailed network activity on your PC.
  (Windows)
  …
  - ▶ Stats
- 
  LuLu - Free, open source macOS firewall. It aims to block unknown outgoing connections, unless explicitly approved by the user.
  …
  - ▶ Stats

- 
  Little Snitch - A very polished application firewall, allowing you to easily manage internet connections on a per-app basis.
  (Mac OS)
  …
  - ▶ Stats
- 
  OpenSnitch - 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.
  …
  - ▶ Stats
- 
  Gufw - 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.
  …
  - ▶ Stats
- 
  Uncomplicated Firewall - The ufw (Uncomplicated Firewall) is a GUI application and CLI, that allows you to configure a firewall
  using `iptables` much more easily.
  …
- 
  IPFire - 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.
  …
  - ▶ Stats
- 
  Shorewall - 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.
  …
- 
  OPNSense - Enterprise firewall and router for protecting networks, built on the FreeBSD system.
  …

▶ ⚠ **Word of Warning**

⬆ [Back to Top]

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

- **Pi-Hole** - 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.
  …
  - ▶ Stats
- **Diversion** - 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.
  …
- **DN66** - 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.
  …
  - ▶ Stats
- **BlockParty** - Native Apple (Swift) apps, for system-wide ad-blocking. Can be customized with custom host lists,
  primarily aimed for just ad-blocking.
  …
  - ▶ Stats
- **hBlock** - 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.
  …
  - ▶ Stats
- **Blokada** - 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.

…

- ▶ Stats

- 
RethinkDNS & Firewall - Free and open source ad-blocker and a firewall for Android 6+ (no root required).

…

- ▶ Stats

- 
Ad Block Radio - 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.

…

- ▶ Stats

- 
uBlock Origin - 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.

…

- ▶ Stats

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

Host Block Lists

- 
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.

…

- ▶ Stats

- 
No Google - Totally block all direct and indirect content from Google, Amazon, Facebook, Apple and Microsoft (or just some).

…

- ▶ Stats

- **EasyList** - Comprehensive list of domains for blocking tracking, social scripts, bad cookies and annoying stuff.
  …
  - ▶ Stats
- **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.
  …
  - ▶ Stats

⬆ [Back to Top]

Router Firmware

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

- **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.
  …
  - ▶ Stats
- **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.
  …
  - ▶ Stats

▶ ⚠ **Word of Warning**

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

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

- **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.
  …
  - ▶ Stats
- **Goodbye DPI** - Passive Deep Packet Inspection blocker and Active DPI circumvention utility, for Windows.
  …
  - ▶ Stats
- **DPITunnel** - An Android app to bypass deep packet inspection.
  …
  - ▶ Stats
- **Proxy Checker** - You can quickly check if a given IP is using a proxy, this can also be done through the command line.
  …

⬆ [Back to Top]

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.

- **Zeek** - Zeek (formally Bro) Passively monitors network traffic and looks for suspicious activity.
  …
  - ▶ Stats
- **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.
  …
  - ▶ Stats
-

Kismet - An 802.11 layer2 wireless network detector, sniffer, and intrusion detection system.
…
- ▶ Stats

- **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.
…
  - ▶ Stats

⬆ [Back to Top]

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.

- **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.
…
  - ▶ Stats

- **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
reputable providers.

…

- ▶ Stats

▶ ⚠ **Word of Warning**

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

Domain Registrars

- 
Njal.la - Privacy-aware domain service with anonymous sign-up and accepts cryptocurrency.

…

- ▶ Stats

- 
Orange Website - Anonymous domain registration, with low online censorship since they are based outside the
14-eyes jurisdiction (in Iceland).

…

⬆ [Back to Top]

DNS Hosting

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

…

- ▶ Stats

⬆ [Back to Top]

Mail Servers

- 
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.

…

- ▶ Stats

- 
  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.
  …
  - ▶ Stats
- 
  mailcow - A mail server with everything you need (SMTP, IMAP, webmail, NextCloud support..) using Docker.
  …
  - ▶ Stats

▶ ⚠ **Word of Warning**

⬆ [Back to Top]

Productivity

Digital Notes

- 
  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.
  Standard Notes is actively developed, and fully open-source.
  …
  - ▶ Stats
- 
  Turtle - A secure, collaborative notebook. Self-host it yourself, or use their hosted plan (free edition or $3/ month for premium).
  …
  - ▶ Stats
- 
  Notable - An offline 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, built-in cloud-sync, encryption or web UI. But due to the structure of the files,
  it is easy to use your own cloud sync provider, and additional features are provided through extensions.
  …
  - ▶ Stats
- 
  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.

…

- ▶ Stats

- **Logseq** - Privacy-first, open-source knowledge base that works on top of local plain-text Markdown and Org-mode files.
  Supports lots of different note modes, including task management,
  PDF annotation, flashcards, whiteboards strong markdown support and more.
  Includes themes and extensions, backed by a strong community

  …

  - ▶ Stats

- **Obsidian** - A powerful knowledge base that works on top of local plain-text Markdown files. It has a strong
  community, and a lot of plugins and themes. Generally privacy-respecting, but no
  encryption out of the box, and some of the code is obfuscated or not fully open source

  …

  - ▶ Stats

- **AFFiNE** - Privacy first, open-source alternative to Notion, monday.com and Miro.
  It is a knowledge management tool that allows you to create, organize and share your knowledge.

  …

  - ▶ Stats

- **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 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.

  …

  - ▶ Stats

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

Calendar

⚠ This section is still a work in progress ⚠

Check back soon, or help us complete it by submitting a pull request

⬆ [Back to Top]

Backup and Sync

- **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.
  …
  - ▶ Stats
- **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.
  …
  - ▶ Stats
- **NextCloud** - Feature-rich productivity platform, that can be used to backup and
  selectively sync encrypted files and folders between 1 or more clients.
  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.
  …
  - ▶ Stats

▶ ⚠ **Word of Warning**

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

Cloud Productivity Suites

- **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. Price for hosted: free
  for 50mb or $5/ month for premium.
  …
  - ▶ Stats
- **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. 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.

…

- ▶ Stats

- 
  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.

  …

  - ▶ Stats

- 
  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.

  …

  - ▶ Stats

- 
  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.

  …

  - ▶ Stats

- 
  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.

  …

  - ▶ Stats

⬆ [Back to Top]

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.

- **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.
  …
  - ▶ Stats
- **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.
  …
  - ▶ Stats
- **Sync.com** - Secure file sync, sharing, collaboration and backup for individuals, small businesses and sole practitioners.
  Starts at $8/month for 2 TB.
  …
  - ▶ Stats
- **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.
  …
  - ▶ Stats
- **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.
  …
  - ▶ Stats

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

File Drop

- 
  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.
  …
  - ▶ Stats
- 
  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, 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.
  …
  - ▶ Stats

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

Browser Sync

- 
  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 Chrome, Firefox, and Edge.
  …
  - ▶ Stats
- 
  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.
…
    - ▶ Stats

- 
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.
…
    - ▶ Stats

- 
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.
…
    - ▶ Stats

- 
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.
…
    - ▶ Stats

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

Secure 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.

- 
Jami - A free and open source, distributed video, calling and screenshare platform with a focus on security. Jami is
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 natively 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.

…

- ▶ Stats

- **Jitsi** - Encrypted, free and open source video calling app, which does not require creating an account/ providing any personal
details. Available 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.

  …

  - ▶ Stats

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

Utilities

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

- **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** - 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.
There's also an iOS version (so you can run Windows on your iPhone!)

  …

  - ▶ Stats

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

PGP Managers

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

- 
  SeaHorse - Application for managing encryption keys and passwords, integrated with the GNOME Keyring.
  …
- 
  Kleopatra - Certificate manager and a universal crypto GUI. It supports managing X.509 and OpenPGP certificates in the GpgSM
  keybox and retrieving certificates from LDAP servers.
  …
- 
  GPG4Win - Kleopatra ported to Windows.
  …
  - ▶ Stats
- 
  GPG Suite - Successor of MacGPG. Plays nice with MacOS apps, including Finder, Appple Mail, Keychain and Spotlight.
  Makes encrypting files, emails, and messages / data very easy.
  As well as GUI for generating keys, verifying signatures, etc.
  …
- 
  OpenKeychain - Android app for managing keys, and encrypting messages.
  Works both stand-alone, and as integrated into other apps, including k9-Mail.
  Everything can be done through a simple yet powerful GUI.
  Open source, security audited, transparent permissions, and activley maintained.
  …
  - ▶ Stats
- 
  PGP Everywhere - iOS app for encrypting/ decrypting text.
  Has native keyboard integration, keychain support and app integrations which makes it quick to use in any app.
  …
- 
  FlowCrypt - Browser extension for using PGP within Gmail, for Chrome and Firefox.
  Mobile version supported on Android and iOS.
  …
  - ▶ Stats
- 
  EnigMail - OpenPGP extension for Thunderbird and PostBox, integrates natively within mail app.
  …
- 
  Mailvelope - 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.

Works with Gmail, Yahoo, Outlook, GMX, Posteo, Web.de, FreeNet.de, Mailbox.org and many others.

…

- ▶ Stats

⬆ [Back to Top]

Metadata Removal

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.

- 
  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.

  …

  - ▶ Stats
- 
  ExifTool - 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. An official GUI application is available
  for Windows, implemented by Bogdan Hrastnik.

  …

  - ▶ Stats
- 
  ImageOptim - Native MacOS app, with drag 'n drop image optimization and meta data removal.

  …

  - ▶ Stats

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

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.

- 
  Eraser - Allows you to completely remove sensitive data from your hard drive by overwriting it several times with carefully
  selected patterns.
  …
  - ▶ Stats
- 
  Hard Disk Scrubber - Easy to use, but with some advanced features, including custom wipe patterns. Data Sanitation Methods: AFSSI-5020,
  DoD 5220.22-M, and Random Data.
  …
- 
  SDelete - Microsoft Secure Delete is a CLI utility, uses DoD 5220.22-M.
  …
- 
  OW Shredder - 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 - 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 - C-based secure light-weight disk eraser, operated through the easy-to-use CLI or a GUI interface.
  …
  - ▶ Stats
- 
  shred - A CLI utility that can be used to securely delete files and devices, to make them extremely difficult to recover.
  …
-
  Secure Remove - CLI utility for securely removing files, directories and whole disks, works on Linux, BSD and MacOS.
  …

- **Mr. Phone** - 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**

⬆ [Back to Top]

Operating Systems

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.

- **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.
  …
  - ▶ Stats
- **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.
  …
  - ▶ Stats
- **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.
  …
  - ▶ Stats
-

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.
…

- ▶ Stats

▶ ⚠ **Word of Warning**

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

Desktop Operating Systems

Windows and MacOS have 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

- **Qubes OS** - 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.
…
  - ▶ Stats
- **Whonix** - 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** - 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.
…

- **Parrot** - 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.
  …
  - ▶ Stats
- **Discreete Linux** - 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**

▶ **ℹ Further Info**

⬆ [Back to Top]

Linux Defenses

- **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.
…
    - ▶ Stats

- **Gufw** - 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.
…
- **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.
…
    - ▶ Stats

- **chkrootkit** - Locally checks for signs of a rootkit.
…
- **Snort** - Open source intrusion prevention system capable of real-time traffic analysis and packet logging.
…
- **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**

⬆ [Back to Top]

Windows Defences

- **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.
…
    - ▶ Stats

- **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.

…

- ▶ Stats

-  **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.

  …

-  **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.

  …

-  **NetLimiter** - Internet traffic control and monitoring tool.

  …

  - ▶ Stats

-  **Sticky-Keys-Slayer** - Scans for accessibility tools backdoors via RDP.

  …

    - ▶ Stats
-  **SigCheck** - A CLI utility that shows file version number, timestamp information, and digital signature details.

  …
-  **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.

  …
    - ▶ Stats
-  **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.

  …
    - ▶ Stats
-  **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.

  …
    - ▶ Stats
-  **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.

  …
    - ▶ Stats
- 

PrivaZer - Good alternative to CCleaner, for deleting unnecessary data - logs, cache, history, etc.

…

▶ ⚠ **Word of Warning**

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

Mac OS Defences

- 
  LuLu - Free, open source macOS firewall. It aims to block unknown outgoing connections, unless explicitly approved by the user.

  …
  - ▶ Stats
- 
  Stronghold - Easily configure macOS security settings from the terminal.

  …
  - ▶ Stats
- 
  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.

  …
  - ▶ Stats

⬆ [Back to Top]

Anti-Malware

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

- 
  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.

  …
  - ▶ Stats

▶ ⚠ **Word of Warning**

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

Development

Code Hosting

- **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.

  …
  - ▶ Stats
- **Codeberg** - A fully-managed instance of Forgejo.

  …
  - ▶ Stats
- **GitLab** - Fully-featured git, CI and project management platform. Managed instance available, but can also be self-hosted.

  …
  - ▶ Stats
- **Gitea** - Lightweight self-hosted git platform, written in Go.

  …
- **Gogs** - Lightweight self-hosted git platform, written in Go.

  …

⬆ [Back to Top]

IDEs

⚠ This section is still a work in progress ⚠

Check back soon, or help us complete it by submitting a pull request

⬆ [Back to Top]

Terminal Emulators

⚠ This section is still a work in progress ⚠

Check back soon, or help us complete it by submitting a pull request

⬆ [Back to Top]

Smart Home & IoT

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

- **Mycroft** - An open source privacy-respecting AI platform, compatible with a wide range of devices including Raspberry Pi, desktop computers, or dedicated Mycroft hardware.
  Actively developed, with extensive documentation and a broad skill set. Facilitates easy development of new skills.
  …
  - ▶ Stats
- **Kalliope** - A modular, always-on, voice-controlled personal assistant geared towards home automation.
  Optimized for Raspberry Pi, Debian, or Ubuntu. Skills are easily programmable in YAML, though the library of pre-built add-ons is not as extensive.
  …
  - ▶ Stats

▶ ⚠ **Word of Warning**

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

Smart Home

- **Gladys Assistant** - An open source privacy-respecting Home Assistant, compatible with a wide range of devices including Raspberry Pi, desktop computers, or NAS systems.
  Actively developed, with good french community and various integrations (Zigbee, Philips, Camera, Tuya, MQTT, Telegram, ...).
  …
  - ▶ Stats

⬆ [Back to Top]

Finance

Cryptocurrencies

- **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.

  …

  - ▶ Stats

- **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.

  …

  - ▶ Stats

▶ ⚠ **Word of Warning**

▶ ✳ **Notable Mentions**

▶ **i Further Info**

⬆ [Back to Top]

Crypto Wallets

- **Wasabi Wallet** - 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.

  …

  - ▶ Stats

- **Trezor** - 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 incredibly customizable with a large range of advanced features.

  …

  - ▶ Stats

- **ColdCard** - 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.

…

- ▶ Stats

- **Electrum** - 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.

  …

  - ▶ Stats

- **Samourai Wallet** - 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 the device is seized or stolen, and Whirlpool which is similar to a coin mixer, and OpenDime is also supported for offline USB hardware wallets.

  …

  - ▶ Stats

- **Sparrow Wallet** - 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.

  …

  - ▶ Stats

- **Atomic Wallet** - Atomic is an open-source desktop and mobile-based wallet, where your private keys are stored on your local device, and do not touch the internet. Atomic has a great feature set, 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. Therefore, it may only be a good choice as a secondary wallet, for storing small amounts of your actively used currency.

  …

  - ▶ Stats

- **CryptoSteel** - 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 - Open source hardware wallet, supporting secure multisig with the option for making encrypted backups on a MicroSD card.
  …
  - ▶ Stats

▶ ⚠ **Word of Warning**

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

Crypto Exchanges

- 
  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 organization.
  Primarily focused on Bitcoin, Ethereum, Ripple, and LiteCoin,
  as it gets harder to find people near you selling niche alt-coins.
  …
  - ▶ Stats
- 
  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.
  …
  - ▶ Stats
- 
  RoboSats - RoboSats is an easy way to privately exchange Bitcoin for national currencies.
  It simplifies the peer-to-peer experience and makes use of lightning hold invoices to minimize custody and trust requirements.
  The deterministically generated avatars help users stick to best privacy practices.
  …
  - ▶ Stats

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

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.

In most countries KYC is required. The bank will of course be able to see all your transactions. Be sure to read their privacy policy and terms of service beforehand. Not all services are available in all countries.

- **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 plan for $10/month, with 1% cashback and 36 cards/month.

  …
  - ▶ Stats
- **Revolut Premium** - Revolut is more of a digital bank account, and identity checks are required to sign up. Virtual cards are only available on Premium/ Metal accounts, which start at $7/month.

  …
  - ▶ Stats
- **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.

  …
  - ▶ Stats

⬆ [Back to Top]

Other Payment Methods

- **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.

  …
- **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.

  …

▶ ⚠ **Word of Warning**

▶ **ℹ Further Info**

⬆ [Back to Top]

Secure Budgeting

- **Firefly III** - A free and open source personal finance manager. Firefly III features a clean and clear UI, is easy to set up and use, and is backed by a strong community. Regular updates bring new features, improvements, and fixes. There's also a hass.io addon, and compatibility with Home Assistant. Ensure your server is securely configured.
  …
  - ▶ Stats
- **GnuCash** - A full-featured cross-platform accounting application suitable for personal and small business finance. Stable and reliable, GnuCash offers a comprehensive suite of financial management tools. Available for Windows, Mac, Linux, and Android.
  …
  - ▶ Stats
- **Plain Text Accounting** - Utilizes plain text files and scriptable, command-line-friendly software for bookkeeping/accounting, offering full control over data. Popular tools include Ledger, hledger, and Beancount among others, providing a flexible and vendor-independent approach to accounting.
  …
  - ▶ Stats

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

Social

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.

- 
  Aether - Offers self-governing communities with auditable moderation, akin to Reddit but prioritizing privacy, democracy, and transparency. Aether is peer-to-peer and open source, available for Windows, Mac, and Linux.
  …
  - ▶ Stats
- 
  Discourse - A fully open-source, self-hostable discussion platform usable as a mailing list, discussion forum, or long-form chat room.
  …
  - ▶ Stats
- 
  Mastodon - An open-source, distributed social media platform functioning similarly to Twitter, without algorithmic timeline manipulations. It operates across independent servers.
  …
  - ▶ Stats
-
  Minds - A social media platform designed to foster open conversations and community engagement. Rewards content creation.
  …
  - ▶ Stats

▶ ✳ **Notable Mentions**

▶ **i Further Info**

⬆ [Back to Top]

Video Platforms

- 
  PeerTube - A federated video platform leveraging peer-to-peer technology to decrease server load during video streaming. Supports self-hosting or joining existing instances, enabling video viewing from any PeerTube server.
  …
  - ▶ Stats
- 
  DTube - A decentralized, ad-free video platform emphasizing minimal moderation. It rewards users with cryptocurrency, leveraging blockchain technology.
  …
  - ▶ Stats
- 
  BitChute - Established in 2017, BitChute is a video hosting service that offers a platform for uploaders to evade the content restrictions found on other sites like YouTube.
  …
  - ▶ Stats

▶ ⚠ **Word of Warning**

▶ **ℹ Further Info**

⬆ [Back to Top]

Blogging Platforms

- **Write Freely** - A minimalist, federated blogging platform offering a clean UI. It's free, open source, and caters to writers seeking simplicity and federation capabilities. For hosted options, visit Write.as.
  …
  - ▶ Stats
- **Telegraph** - A quick, anonymous blogging platform by Telegram. It's designed for simplicity and speed, allowing for straightforward content publishing without registration.
  …
- **Mataroa** - A minimalist blogging platform focused on privacy and simplicity. It's open source and eschews complex features for a straightforward writing and publishing experience.
  …
  - ▶ Stats
- **Bear Blog** - A no-nonsense, super-fast blogging platform prioritizing privacy. It strips back unnecessary features to focus on straightforward blogging. The platform is open source.
  …
  - ▶ Stats
- **Movim** - A web frontend for XMPP, offering decentralized blogging and chatrooms. Movim is open source,
  integrating social and communication tools in a unified platform.
  …
  - ▶ Stats

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

News Readers

- **Tiny RSS** - A web-based news feed reader and aggregator, supporting RSS/Atom feeds. It's free, open source,
  and offers a customizable and self-hostable platform for managing your news feeds.
  …

- **RSSOwl** - A powerful, desktop-based RSS reader offering extensive organization features. It facilitates managing and curating news feeds from various sources.
  …
- **Feedly** - Offers a premium news aggregation experience, presenting news from chosen sources in a clean,
  modern interface. Beyond RSS, it integrates with various news outlets, ensuring a tailored
  news feed without manipulated content. Parts of the service are open source.
  …
  - ▶ Stats

⬆ [Back to Top]

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).

- **Nitter** - A privacy-centric alternative to Twitter's front-end, focusing on preventing user tracking.
  It's free, open source, lightweight, supports multiple themes, and offers customizable RSS feeds.
  All client requests are proxied, enhancing privacy. No JavaScript required.
  …
- **Invidious** - An open source, privacy-focused YouTube frontend. It minimizes Google tracking, supports audio-only mode,
  integrates Reddit comments, and offers advanced playback options. Lightweight and can function without JavaScript. Supports import/export of subscriptions and feed customization.
  …
  - ▶ Stats
- **Libreddit** - A private, fast Reddit frontend written in Rust. Excludes ads, trackers, and bloat, making it much faster
  than the official site. Can be self-hosted via Docker or other methods. Implements most Reddit features for anonymous browsing.
  …
- **WebProxy** - A free proxy service offering a Tor mode for evading censorship and accessing geo-restricted content.
  Claims to encrypt traffic, but caution is advised for personal information. Managed by DevroLabs.
  …

▶ ⚠ **Word of Warning**

▶ ✳ **Notable Mentions**

⬆ [Back to Top]

Media

Gaming

⚠ This section is still a work in progress ⚠

Check back soon, or help us complete it by submitting a pull request

⬆ [Back to Top]

Media Servers

⚠ This section is still a work in progress ⚠

Check back soon, or help us complete it by submitting a pull request

⬆ [Back to Top]

Music Players

⚠ This section is still a work in progress ⚠

Check back soon, or help us complete it by submitting a pull request

⬆ [Back to Top]

Video Players

⚠ This section is still a work in progress ⚠

Check back soon, or help us complete it by submitting a pull request

⬆ [Back to Top]

Photo Viewers

⚠ This section is still a work in progress ⚠

Check back soon, or help us complete it by submitting a pull request

⬆ [Back to Top]

E-Book Readers

⚠ **This section is still a work in progress** ⚠

Check back soon, or help us complete it by submitting a pull request

⬆ [Back to Top]

Podcast Players

⚠ **This section is still a work in progress** ⚠

Check back soon, or help us complete it by submitting a pull request

⬆ [Back to Top]

Torrent Downloaders

⚠ **This section is still a work in progress** ⚠

Check back soon, or help us complete it by submitting a pull request

⬆ [Back to Top]

File Converters

⚠ **This section is still a work in progress** ⚠

Check back soon, or help us complete it by submitting a pull request

⬆ [Back to Top]

Creativity

Image Editors

- 
  Gimp - A free, open source, cross-platform image editor. GIMP is a powerful tool for photo retouching, image composition, and image authoring. It is highly customizable, and supports a wide range of file formats.
  …
  - ▶ Stats
- 
  InkScape - A free, open source, professional vector graphics editor. It is a powerful tool for creating illustrations, icons, logos, diagrams, maps, and web graphics.
  …
  - ▶ Stats
- 

Paint.NET - A more advanced take on Microsoft Paint. Suitable for basic image editing, with support for basic layers, unlimited undo/redo, and extendable via plugins

…

- ▶ Stats

- 
PixlrX - A free web-based image editor, with a modern UI.
Also offers premium/paid features, such as AI-powered generation, touchup and editing

…

- ▶ Stats

- 
RawTherapee - A powerful raw photo processing system and editor, for non-destructive editing of raw digital photos

…

- ▶ Stats

- 
PhotoPea - A free online image editor, for both raster and vector graphics, with a very wide range of supported formats

…

- ▶ Stats

- 
Krita - Digital painting application.
Free and open source (backed by KDE), with cross-platform support,
Krita is popular among both professional and amateur artists
due to it's comprehensive feature set, and intuitive UI

…

- ▶ Stats

- 
DarkTable - A photography workflow application (similar to Adbobe Lightroom)
Includes a non-destructive raw developer for raw images and managing digital negatives.

…

- ▶ Stats

⬆ [Back to Top]

Video Editors

- 
Shotcut - A free, open source, cross-platform video editor, using FFmpeg
Shotcut supports a wide range of formats, and has a comprehensive feature set, including 4K & 8k resolution, webcam + audio capture, batch opperations and much more

…

- ▶ Stats

- 

OpenShot - A free, simple, cross-platform video editor.
Great for trimming/slicing, video effects, adding titles, scene animations
and more
…

- ▶ Stats

- 
Kdenlive - KDE Non-Linear Video Editor, is an editor based on the MLT Framework, KDE and Qt, written using C++ and using FFmpeg
…
  - ▶ Stats
- 
FlowBlade - A multitrack non-linear video editor with a simple interface
…
  - ▶ Stats
- 
Cinelerra GG Infinity - Simple video editor, for applying transitions, effects and text as well as splicing video clips
…
  - ▶ Stats
- 
VitCutter - A simple Python-based cross-platform tool for cutting and splicing videos
…
  - ▶ Stats
- 
Natron - Free & open desktop node-graph based video compositing software.
Similar in functionalities to Adobe After Effects.
Features flexible rotoscoping, 2D & planner tracking, keying tools,
curve & dope-shift editor, GPU & network rendering, and is
easily extendable via community plugins, or by writing Python scripts
…
  - ▶ Stats

⬆ [Back to Top]

Audio Editors & Recorders

- 
Audacity - An easy-to-use, multi-track audio editor and recorder for desktops,
great free alternative to Adobe Audition.
Features recording from real and virtual devices,
import/export to a wide range of formats, high-quality processing
advanced multi-track editing, noise reduction, pitch correction,
audio restoration and much more.
It's easily extendable via community plugins, and

also supports cusotm macros and many scripting options

…

- ▶ Stats

⬆ [Back to Top]

Casting & Streaming

- 
  OBS Studio - Powerful desktop software for live streaming and screen recording.
  Free and open source software for video recording and live streaming.
  Features real-time video/audio capturing, scene composition, encoding,
  recording, and broadcasting. It supports a wide range of formats,
  and is easily extendable via community plugins

  …

  - ▶ Stats

⬆ [Back to Top]

Screenshot Tools

⚠ This section is still a work in progress ⚠

Check back soon, or help us complete it by submitting a pull request

⬆ [Back to Top]

3D Graphics

- 
  Blender - Free desktop 3D creation suite, with a wide range of tools for
  modeling, sculpting, texturing, rigging, animation, rendering, compositing,
  motion tracking, and video editing. It's easily extendable via community plugins

  …

  - ▶ Stats

- 
  Wings3D - A simple and easy-to-use subdivision 3D modeler
  with AutoUV facility for unfolding a models surface for painting/texturing.
  Unlike Blender, it has no built-in animation capabilites, and it's feature set
  is more limited, but it's a good choice for beginners.

  …

  - ▶ Stats

⬆ [Back to Top]

Animation

⚠ This section is still a work in progress ⚠

Check back soon, or help us complete it by submitting a pull request

⬆ [Back to Top]

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!

Further Reading

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 →**

Security List

- Personal Security Checklist - A curated list of security and privacy advice, tools, and resources.

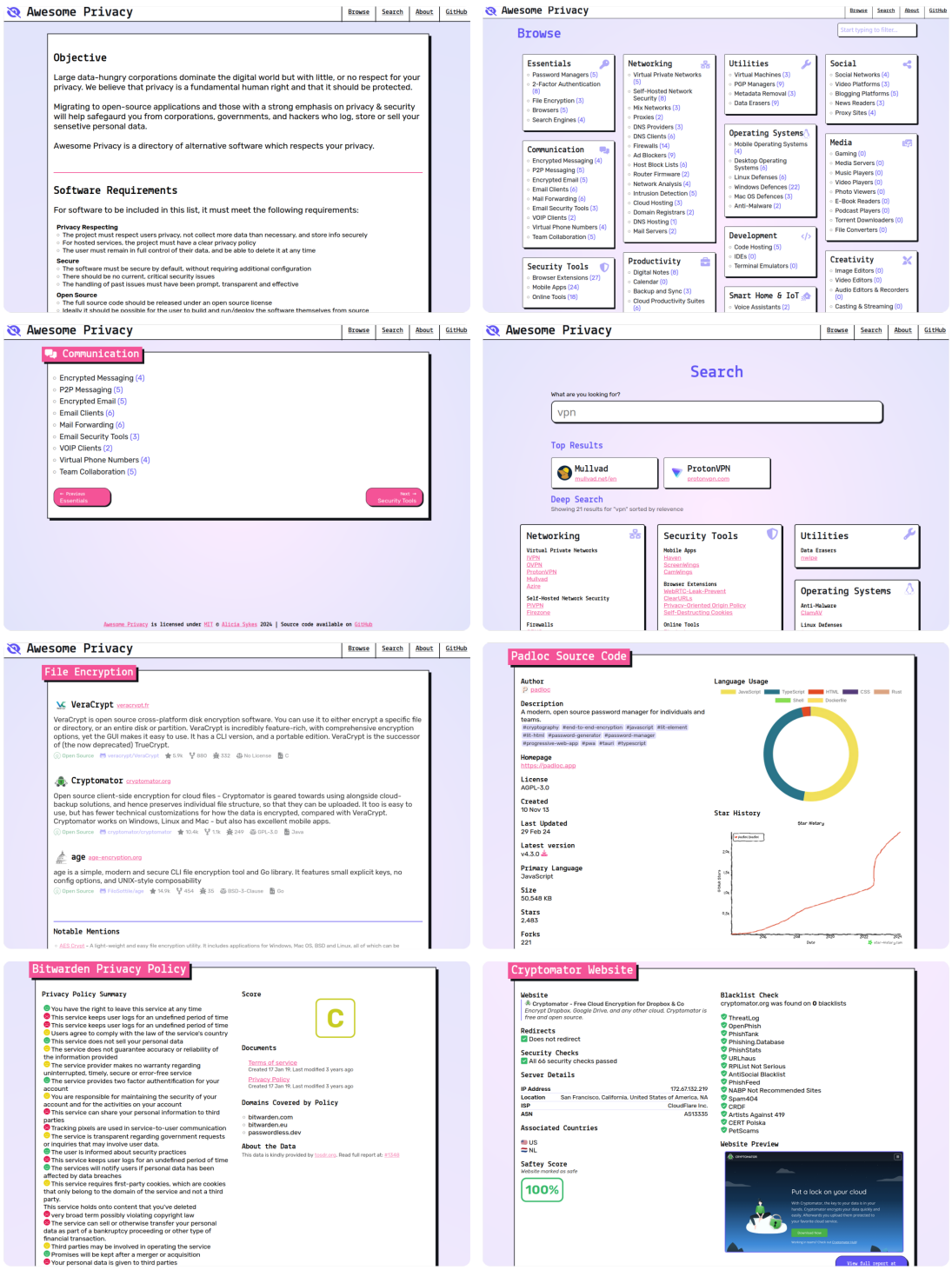
News & Updates

A custom Reddit feed covering news and updates for all the apps covered here can be found here

---

The Website

The easist way to browse Awesome Privacy, is via our website, at **awesome-privacy.xyz**



About Website

The source for the website is in the `web/` directory.

This is a statically generated site, built with Astro, Svelte, TypeScript an SCSS.

At build-time, it reads the data from `awesome-privacy.yml` and generates the pages.

Running the Website Locally

You'll need Node.js (20.11.1 or later) and Git installed.

Then run the following commands to fetch the code, install dependencies and start the dev server.

```
git clone git@github.com:Lissy93/awesome-privacy.git
cd awesome-privacy/web
cp .env.sample .env
yarn install
yarn dev
# Then open 127.0.0.1:4321 in your browser
```

Deploying the Website

Follow the steps above, then run `yarn build` to generate the static files.

You can then upload the `./dist` directory to any web server, static host or CDN.

Alternatively, you can fork the repo and import it into either Vercel or Netlify.

Contributing

We welcome suggestions, additions, edits and removals to the list.

It's thanks to contributors like you that this project is possible

All data is stored in `awesome-privacy.yml`.
If you're adding, editing or removing a listing - **this is the only file you need to edit**.

Please familiarise yourself with the Contributing Guidelines before submiting your pull request, as we have some guidelines that **must be followed** to ensure your PR can be accepted.

If you're new to open source, you can find some resources to get you started at git-in.to,
but feel free to reach out if you need any help 😊

The API

We also have a free, no-auth, CORS-enabled RESR API, which you can use to access
Awesome Privacy's data programmatically, or to build your own apps on top of it.

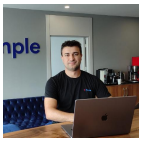
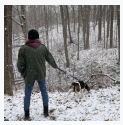
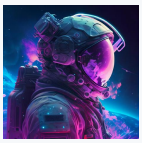
To get started, try our Swagger Explorer,
which outlines all endpoints, usage and examples.

You can either use our public instance, at: `https://api.awesome-privacy.xyz`
or self-host your own, with the source of the `api/` directory.

Acknowledgements

Sponsors

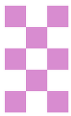
Huge thanks to the following sponsors, for their ongoing support ❤

 Vincent Koc	 Peng1can	 B.G.Adrian	 Torgny Bjers	 Eddy Lazzarin	 Anand Chowdhary
 Shrippen	 Zach Biles	 Ulises Gascón	 Digital Archeology	 InDieTasten	 Brian McGonagill
 Vlad	 HeliXZz	 Göksel Yeşiller	undefined Undefined	 Bastii717	 Frankdez93
 Brent	 Nixy	 Nrvo	 Mezza93		

Contributors

This project exists thanks to all the people who've helped build and maintain it ❤

 Alicia Sykes	 Alicia Bot	 Kieran	 Lilith	 Guillaume	 A-childs-encyclopedia
 Andrew Milich	 Kerbless	 GhoulBoi69	 Titanism	 Slade991	 Sam A.
					

Coccocoa's Helper	Alex Ogden	Ujjawal Saini	Upstream8022	Ward	Wesley-Ryan
 Zachary Taylor	 Zhymabek Roman	 Sanmonji	 Cole	 Jxhn	 Kolaente
 Magical-heyrovsky	 Pavan	 Paul Nodet	 RASTIQ	 Rollsicecream	 Tim Schlotfeldt

License

> ***Lissy93/Awesome-Privacy/web*** *is licensed under MIT*
>
> ***awesome-privacy.yml*** *is licensed under CC0-1.0 license*
>
> *Copyright © Alicia Sykes <aliciasykes.com> 2024.*
>
> For information, see TLDR Legal > MIT

▶ Expand License

Thanks for visiting :)