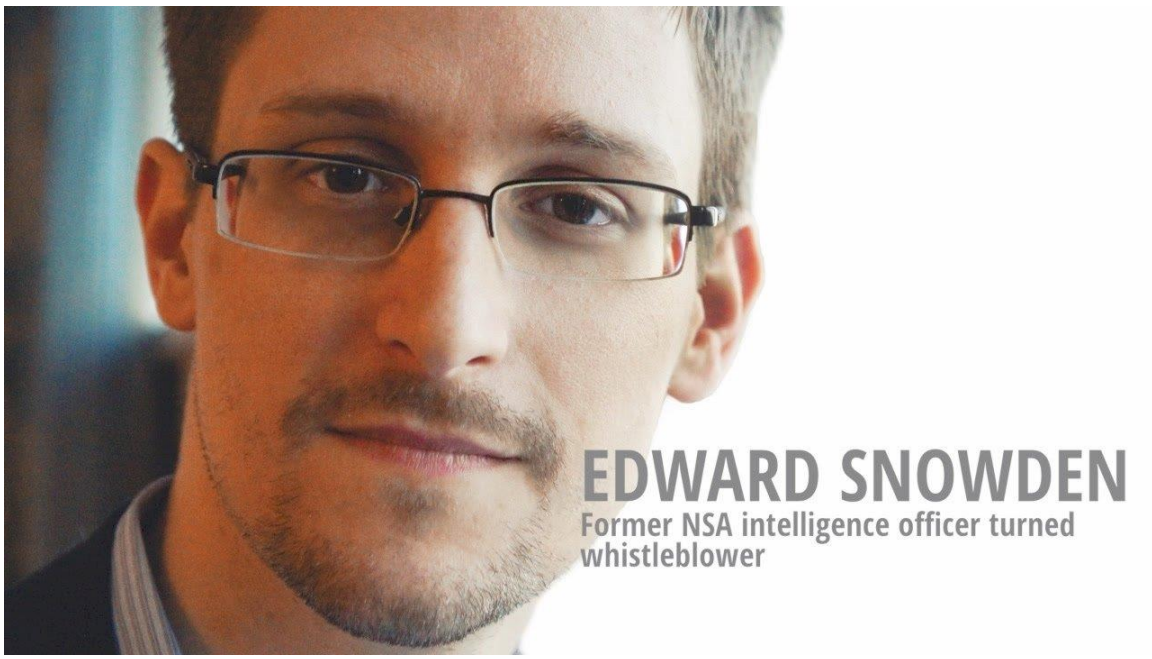
Privacy? I have nothing to hide.



“Ultimately, saying that you don't care about privacy because you have nothing to hide is no different from saying you don't care about freedom of speech because you have nothing to say. Or that you don't care about freedom of the press because you don't like to read. Or that you don't care about freedom of religion because you don't believe in God. Or that you don't care about the freedom to peacably assemble because you're a lazy, antisocial agoraphobe.”

- Edward Snowden in Permanent Record

Remember, you’re never alone when you’re on the internet. Every website you visit, every post you like on social media and anything you buy online is kept as a record by those services, sometimes indefinetly.

But why should you worry about that? Don’t those services track you to provide a betterand smoother experience for you? To some extent, yes. However, this opportunity to keep highly valuable information about you is well exploited by other entities, brands and cybercriminals.

In an ideal world, no one would have to hide, nor have to worry about protecting their internet privacy from anyone else. Unfortunately, our world is far from ideal, and this means we need to keep personal infroamtion safe from being used in the wrong way. An analogy of corporate survaillance from EFF’s most recent whitepaper is “Corporations have built a hall of one-way mirrors: from the inside, you can see only apps, web pages, ads, and yourself reflected by social media. But in the shadows behind the glass, trackers quietly take notes on nearly everything you do.”

Trackers are hiding in nearly in every corner of today’s Internet. So help you identify where your weaknesses are, you should think in terms of a threat model. You should ask yourself: Who am I protecting my data from? What will I sacrifice if I use their service? In this way, you can formulate a plan that suits your needs.

If you want to mitigate the chances of your information being collected, but don't want to go through the trouble of reading the rest of the guide, here are some easy steps that you can take to protect your privacy:

- Avoid using your real name when you register for a service unless it's school or government related
- Use passwords that don't contain personal information such as your name or birth date
- Use Firefox as your default browser for all your devices
- Use DuckDuckGo as your default search engine

Level 1 – For normies

Watch this video as a quick introduction: How to protect your online privacy in 2020 | Tutorial

Comments on this video:

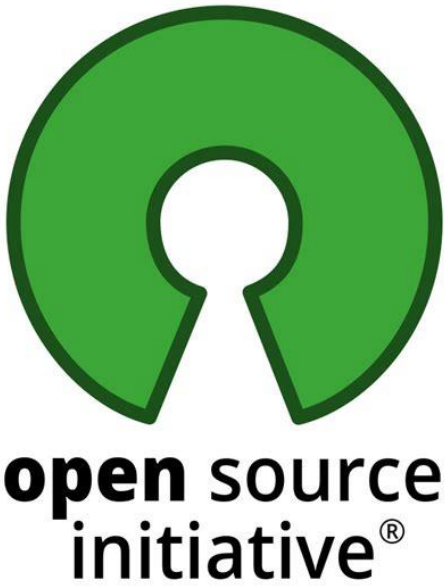
- I don't recommend WPAs as they are much slower to load than normal apps and it's frustrating to use.
- For my setup I compartiilise as much of my online activities as possible. I use separate privacy-hardened Firefox profiles for each of the following: studies (i.e. school), watching videos and accessing social media. I recommend adding these add-ons to Firefox: uBlock Origin, HTTPS Everywhere, Decentraleyes and Privacy Badger.
- For browsing the internet, use the Tor without changing any setting or adding additional add-ons.

Explore this guide: Surveillance Self-Defense | New to Security?

Level 2 – Privacy conscious

From here on out, all suggested videos will be be in Invidio links. Invidio is an alternative front-end for YouTube that doesn't track you.

Explore PrivacyTools - Encryption Against Global Mass Surveillance



FOSS (DeGoogle in the process)

FOSS, an acronym for Free and Open Source Software, are alternatives to proprietary software that respect your privacy. You can watch a quick intro to the conecpt of FOSS here. My recommendation is to use FOSS as much as possible. If you're feeling spicy, you can try out Linux in a Virtual Machine or even dual boot with you Windows device.

Here is a list of FOSS alternatives and recommendations for your Android and Windows device.

Explore this guide on this site – Surveillance Self-Defense | Tool Guides

Comments on this guide:

- Further guidance on the Tor browser here: How to use Tor Browser
- Don't try to access .onion sites with the Tor browser unless you have something specific in mind.
- To sync the KeePassXC file or any other file across devices use the FOSS and P2P syncthing software Syncthing (F-Droid).
- I recommend AndOTP for 2-factor authentication on Android
- Use VeraCrypt to encrypt all your files and partitions/storage devices

Email

ProtonMail

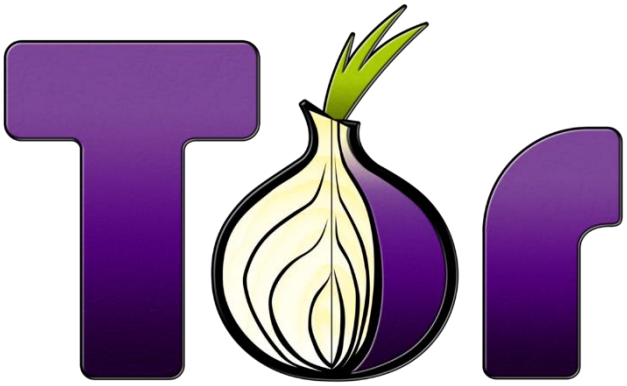
For email provider use ProtonMail as operates outside of the US and is one of the most secure in the world. Make sure to use 2FA for all your emails.

Connect with like-minded people

Browse the r/Privacy forum on Reddit

Join the Fosstodon instance on Mastodon Fosstodon. To learn more about Mastodon, read How Does Mastodon Work?

Browser



If you followed level 1 you should have uBlock Origin installed on Firefox. To get the most out of it, learn how to use it on median mode: uBlock Origin tutorial. Disable JavaScript if you have the patience to deal with a lot of broken websites.

For all profiles except the one I use to for my studies, I change the setting so that no history is remembered. Ideally you would want to erase all cookies and data, but this may be disrupting your studies; that is why I recommend the add-on Cookie AutoDelete for your study profile. You can whitelist the websites you don't want to log in over and over. Also tweak your other profiles for maximum privacy following the guide at the bottom of this page: PrivacyTools – Web Browsers

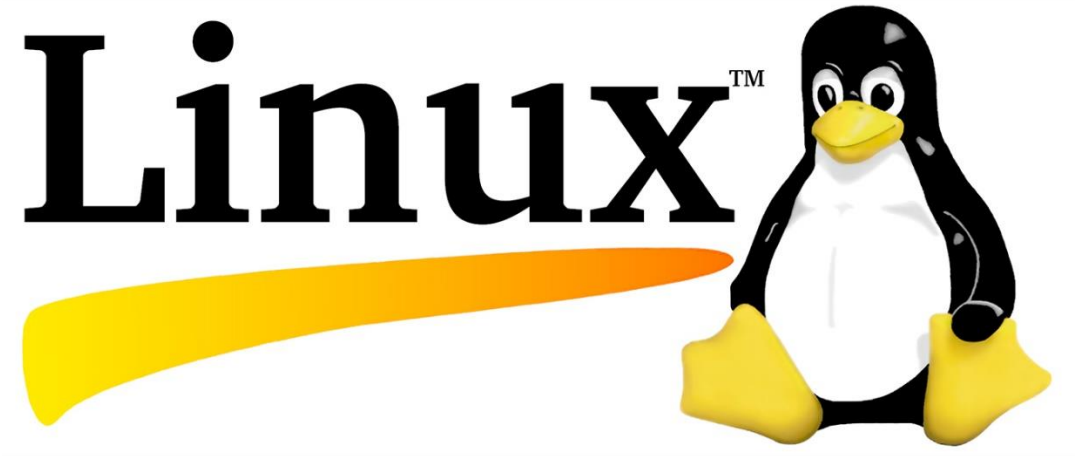
Avoid mixing your compartments as it will make it easy to link your different online identities together. Make sure to use a different email (ideally ProtonMail) for each compartment.

Network

Secure your network with this video: How to secure your network | Tutorial | Wi-Fi security guide

Level 3 –

OS



Switch to Linux completely. You can find very comprehensive installation guides for a range of Linux distros on this website (it also has information on FOSS in general): It's FOSS. I recommend Linux Mint and Ubuntu for those just entering the world of Linux.

As a bonus for installing Linux, you now can learn a few command lines and play around with the terminal. You can take free Linux courses here: edX – Linux Courses , Udemy – Linux Courses. Here is the one I took: Linux Mastery: Master the Linux Command Line in 11.5 Hours.

Flash a custom ROM for android if your device manufacturer allows you to unlock the bootloader. I recommend LineageOS as it is popular and doesn't come with Google Services preinstalled. Note: make a backup of everything on your phone as a fresh OS install will wipe everything from your phone. Here is a starting point.

Pihole (+ Unbound + OpenVPN)

If you have a Raspberry Pi at hand or a old computer left unused

Pihole is an network-wide ad blocker that can can be easily installed in any Raspberry Pi or a old computer running Linux. Combined with Unbound, this solution will prevent ISPs from logging the websites you visit. To take this to the next level, you can also combine this solution with OpenVPN, and voilà, you can now access your ad-blocking features from anywhere in the world!

Official Pihole site: Pi-hole®: A black hole for Internet advertisements

Official documentation (includes guides for Unbound and OpenVPN): Overview - Pi-hole documentation

Digital signatures

Verfy signature of software you download. This is a crucial step in installing software downloaded from your browser as it checks whether the software you downloaded has been tampered with.

Guide for Windows

Guide for Linux

If all this information seems to overwhelm you, don't worry! The important thing here is to know what you're dealing with and to take action. Take it slow and protect your privacy one step at a time and try to strike the right balance between usability and privacy.

Conclusion

When you have all your information stored in one place, every service handled by one company, one security breach is enough to leak your personal information to the internet or even lock you out of your account. That is why you cannot only depend on one company to handle everything for you.

Privacy is not an individual thing. If you are secure online but your parents aren't, they will expose you regardless of how well you yourself are protected. Therefore, I advise you to share some of these practises with others and spread the word of internet privacy.

Resources

Youtube channels

TheHatedOne – Learn to protect your online privacy and guard your digital freedoms against corporate and government surveillance

Techlore – Has guides and weekly news that covers topics on privacy and security

Tools

Privacytools.io – Provides services, tools and knowledge to protect your privacy against global mass surveillance and one of the best privacy tool guides on the internet

PRISM break – We all have a right to privacy, which you can exercise today by encrypting your communications and ending your reliance on proprietary services. FOSS for life!

Guides

Surveillance Self-Defense by EFF – Guide to defending yourself from surveillance by using secure technology and developing careful practices. A very good starting place for newcomers

The ultimate privacy guide – Excellent privacy guide written by the creators of the bestVPN.com website. Covers a range of topics in detail but may be too overwhelming for newcomers

Information/news

Electronic Frontier Foundation – Founded in 1990, it is a leading non-profit organization defending civil liberties in the digital world. It contains excellent whitepapers for those interested in the technology used in surveillance

Freedom of the Press Foundation – Supporting and defending journalism dedicated to transparency and accountability since 2012

Check your fingerprint

AmIUnique

Panopticlick

Book recommendations

Permanent Record by Edward Snowden

The Art of Invisibility by Kevin Mitnick