Things to be aware of

The most important thing to learn is a basic security **mindset**: an awareness of the fact that things can (and how they might) **fail** or be abused.

There is **no such thing** as **100% secure**, there are **no guarantees**, and there is always a **weakest link.**

Security is a process, not a purchase.

Security is **not about tools**; it's about **understanding** the **threats** you face and how you can **counter** them. You need to figure out **what** you need to (and can) **protect** and **from whom**; and how this **changes** depending on where and what you're doing and how and with whom you're doing it.

You need a **basic understanding** of the way the **Internet** works, what **metadata** is and what the **tools** you use do.

Make sure you know the **limitations** of the tools you use: you need to know what they *do* but also what they **do *not* protect** you against and how they can (be made to) fail.

When you use the "**cloud**", you're giving control over your data to someone else.

Be aware of the **trust** you place in the people that made the software (and hardware) you use and that run the services you use; ask yourself whether that trust is deserved.

See also

https://ssd.eff.org
https://securityinabox.org
https://toolbox.bof.nl (dutch)

"Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on."

There is no cloud just other people's computers

Free Software

Who controls your computer?

Free Software is software that anyone can **use**, **study**, **share** and **improve** freely. Most Free Software is gratis, but Free Software is not about price: it's about **liberty**.

When you don't control a program, the program controls you. Whoever controls the software therefore controls you.

Non-free software often leaks your data or hides other malicious features; no one is allowed to study how it works and what it actually does on your computer or phone.

Using exclusively Free Software on your computer or device puts you in full control and allows you to safeguard your privacy. Even though you may not have the skills to exercise each of the four freedoms yourself, you will benefit from the knowledge and expertise of vibrant communities.

Learn more

Technology should empower us, instead of opressing us.

Organisations like the Free Software Foundation (FSF) and Free Software Foundation Europe (FSFE) are dedicated to promoting Free Software and working to build a free digital society.

https://fsf.org
https://fsfe.org

Digital rights

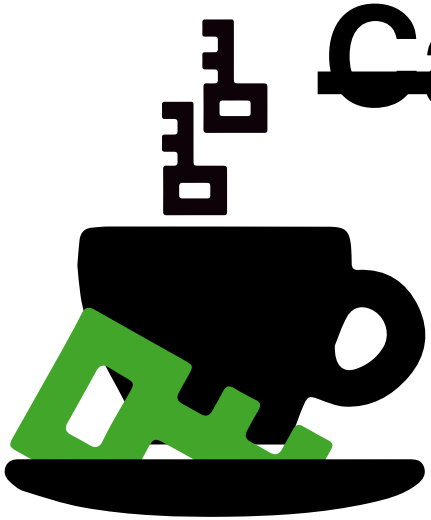
Digital rights organisations like the Electronic Frontier Foundation (US), EDRi (Europe) and Bits of Freedom (Netherlands) are dedicated to promote, protect and uphold civil rights like privacy and communications freedom.

https://eff.org
https://edri.org
https://bof.nl

https://github.com/obfusk/cryptoparty-privacycafe-menu

learn digital self-defense

~~Privacy Café~~



CRYPTO PARTY

https://privacycafe.nl
https://cryptoparty.in

Starters

Firefox: a Free web browser without spyware (though you may want to disable the ads in the new tab page)
https://mozilla.org/firefox

Privacy Badger: block tracking (cookies)
https://eff.org/privacybadger

HTTPS Everywhere: automatically use HTTPS more often
https://eff.org/https-everywhere

Startpage & DuckDuckGo: search the web with (more) privacy
https://startpage.com
https://duckduckgo.com

Security basics

Install **updates** (automatically); **verify** origin and trustworthyness of software.

Use a **firewall** and **virus scanner** (if applicable); make sure you don't have e.g. file sharing enabled when connected to public (or someone else's) Wi-Fi.

Automatically **lock** the screen with password or PIN.

Use strong **passwords** (e.g. sentences of at least 4 random words); use separate passwords for separate (categories of) accounts; use a password manager if you don't want to remember them all. Be careful with **security questions**: make sure the answers are actually secret.

Protect you **primary email address**: it often provides access to many other accounts.

Ensure **physical security** of computers and devices.

Make **backups** (encrypted if necessary). But be careful with (automatic) cloud backups: you may lose **control over your data** unintentionally.

Use **encrypted connections** for web (HTTPS) and email (SSL/TLS/STARTTLS).

Main courses

Tor: surf the Internet anonymously
https://torproject.org

GnuPG: encrypt your emails
https://emailselfdefense.fsf.org
https://gnupg.org

OTR (& Pidgin): encrypt your chats
https://pidgin.im
+ https://otr.cypherpunks.ca

Encrypt your hard disk: make sure your data is protected when your device is lost or stolen.

Tails: the live operating system that aims to preserve your privacy and anonymity (using **Tor**, **GnuPG**, **OTR**, etc.)
https://tails.boum.org

Android

Free Your Android: regain control of your Android device
https://freeyourandroid.org

F-Droid: App Store with Free Software
https://f-droid.org

The Guardian Project & Open Whisper Systems: secure mobile apps (including **Tor**, **encypted email** and **encrypted messaging**)
https://guardianproject.info/apps
https://whispersystems.org

Encrypt your device: make sure your data is protected when it's lost or stolen.

Check the privacy settings: like location data and backups.

Desserts

Use a Free operating system like **Debian** (or other **GNU**/**Linux** distibution).
https://debian.org

PRISM Break: Privacy-aware recommendations to proprietary software (& services)
https://prism-break.org

Terms of Service; Didn't Read (**ToS;DR**): analyzed and graded terms of service and privacy policies
https://tosdr.org

xkcd: A webcomic of romance, sarcasm, math, and language.
https://xkcd.com

iOS

Encrypt your device: make sure your data is protected when it's lost or stolen.

Check the privacy settings: like location data and backups.

ChatSecure: OTR-encrypted text messaging
https://chatsecure.org

Feel free to visit a **hackerspace** or **Linux user group near you**; the people there are more than happy to talk to you about important topics like privacy. You can also find help online by subscribing to **mailing lists** or visiting **Internet forums** dedicated to specific projects or more generic topics.

NB: Even using the software recommended here, your privacy may be compromised; e.g. by non-free operating systems like Windows, OS X, iOS, and stock Android.