Recommendations

- Password-Manager
- Messenger
- Clear-Metadata
- Graphene-Os
- Dangerzone
- Online-Sim
- File-Encryption

Password-Manager

> [!toc] Table of Contents

> [!info] Info {static}
>
> A password manager is an essential tool for ensuring that you take the necessary precautions to keep your passwords secure. Here you can find out what makes a good password and how you should handle them:
>
> Countermeasure: Strong Passwords

KeePassXC and Bitwarden are both open source and have applications for all common operating systems/browsers.

KeePassXC works offline, Bitwarden online. However, KeePassXC can also be synchronized across multiple devices using external services.

Practical password managers for PCs:

- KeePassXC: Linux, Windows, MacOS
- Bitwarden: Linux, Windows, MacOS
  - Keep in mind, that for using Bitwarden, you will need a provider that runs a Bitwarden service and that you trust. Don't use untrusted providers.

The password managers integrated into browsers and operating systems are not necessarily recommended, as they are often proprietary and designed primarily for convenience. This regularly leads to security vulnerabilities. Browsers in particular are always a target for attackers and offer many attack vectors.

KeePass for mobile devices

Recommendation from the official KeePassXC documentation:

- Android: keepassDX, Keepass2Android

- iOS: Strongbox, KeePassium

KeePassXC

KeePassXC is one of the best-known and most widely used password managers. It is open source, regularly checked for vulnerabilities by experts, and offers a variety of very practical features. These enable us to bridge the gap between security and convenience.

Browser integration

There are plugins for KeePassXC for all common browsers *(except Safari)* to conveniently use the auto-fill function. This automatically suggests the correct login details on every website for which passwords have been saved.

This prevents you from accidentally entering your password when you click on a phishing link, because the plugin recognizes that you have landed on the wrong URL.

Key file

It is recommended to secure a password database with both: a password and a second factor. The easiest way to do this is with a key file. (See below for an example scenario.)

Key file as second factor

It is possible to encrypt the database with a separate key file in addition to the password. This means that you always need both the password and the key file to access the passwords.

Instructions for doing this can be found here.

Key file as master key

You can also encrypt your password database with just a key file, without a password. Then you must always select the key file when opening the database in KeePassXC.

Key file as master key with 2nd factor password

A common use case for this is to store the key file on an encrypted USB stick, which you always carry with you, e.g. on your key ring. This also ensures 2-factor authentication. The following is required:

1. factor: the password for the stick
2. factor: the stick (with the key file)

to access the passwords. It is essential to ensure that there is a backup USB stick in case the actual stick is lost!

Generate new passwords

One of the core features of a password manager is that it can generate strong passwords or passphrases according to your own specifications. This ensures that you don't reuse the same password out of convenience.

Synchronize and back up passwords in the cloud

Isn't that dangerous?

The password database is always encrypted, at all times. It is never decrypted in the cloud, so the cloud operators cannot read it. However, the police could potentially steal a copy of your database, as described in the following example scenario.

Example scenario

Let's assume that your password database is “only” protected with a (strong) password. If the police have access to your cloud (or obtain your database in some other way), they will only have the encrypted file and will not be able to do anything with it.

However, if they find out your password in the future (e.g., by secretly watching you type it in), they can retrieve the encrypted database and decrypt it.

If the database were also encrypted with a key file, it would not be enough to know the password; the key file would also be needed. If you were to destroy this key file, there would be no way to decrypt the stolen database.

How To

For example, you could store your database in the cloud and access it from all your devices.

The key file is stored **only locally** on your devices.

If you suspect that the authorities have obtained a copy of your password database

1. make a copy of your database
2. create a new password
3. and a new key file
4. and then delete the **old key file** from all your devices.

This will render the compromised database useless forever.

> [!warning] Warning {static}
>
> Before you delete your old key file, make sure:
>
> 1. that the new database works with the new key file
> 2. that you don't forget the new password!

In both cases, all your passwords would be irretrievably lost.

KeePassXC as a 2-factor app

KeePassXC can also be used as a 2FA app with TOTP. This even works on the apps for mobile phones.

Instructions

Here you will find instructions with further references.

Note

We consistently refer to KeePassXC here.

Older versions such as KeePassX and KeePass should no longer be used.

Messenger

> [!toc] Table of Contents

While emails are still regularly used for digital communication, messengers have become more popular in recent years.

One advantage of (good) messengers over emails is that encryption and secure communication are part of their initial design, while email is unencrypted and rather insecure by default.

Some criteria for what constitutes a good messenger can be found at PrivacyGuides. For activists, depending on the threat model, it is particularly important to have secure and anonymous communication.

Two messengers that are widely used in activist circles and can be recommended are Signal, Matrix and Delta Chat.

> [!example] TL;DR {static}
>
> **Signal** sets the highest standards for it's encryption and data protection and is probably the easiest to use. The disadvantage: it requires a phone number for registration.
>
> **Matrix** also uses modern encryption, but can be less intuitive to use. It is decentralized, meaning you can choose a server you like for registration and don't need a phone number.
>
> **Delta Chat** relies on old email protocols uses PGP for encryption. PGP is still considered secure. However, if your private key is stolen by an attacker, the whole communication history can be leaked. The advantage of Delta Chat is it's decentralized and that you just need a working email account to get started.

Signal

Signal was developed by the anarchist Moxie Marlinspike and is one of the best-known alternatives to the monopolist messenger WhatsApp.

Advantages of Signal

- **Easy to use**: Signal is simple to install and everything “just works.” There isn't much you can do wrong that would compromise security.
- **Widespread use**: As of January 2025, the platform had approximately 70 million monthly active users. While this is still far behind WhatsApp's 2 billion users, it is nevertheless widespread, in contrast to some other Messengers in this list.
- **Secure encryption**: Signal has its own communication protocol that is open source and regularly audited. Some other messengers, such as WhatsApp, have also adopted the protocol, meaning that it is used daily by billions of users. Communication in Signal is therefore securely end-to-end encrypted.
- **Data minimization**: Signal stores as little as possible about its users and can therefore only disclose very little information when forced by authorities to hand over user data. The only data that Signal *was able to* disclose in past court cases was the date the account was created and the date the account was last used. When legally forced to provide information to government or law enforcement agencies, Signal discloses the transcripts of that communication here.
- **Option for automatic deletion**: Chats can be set to automatically delete messages after a certain period of time. This means that they are secure even if the police gains access to the device (but only after this period).

Disadvantages of Signal

- **Anonymity**: Signal was not designed to be anonymous, but to provide secure encryption. As of today (2026), a phone number is required to register. In many countries, phone numbers must (legally) be registered to a real person. The phone number used to be visible to everyone you communicate with, but Signal now enables users to hide their phone number from other users. When using a phone number that is not linked to your identity for registration, Signal can therefore be considered as anonymous as the other messengers in this list.
- **Based in the US**: The Signal Foundation is based in the US and can therefore be forced to to hand over data to intelligence agencies. However, Signal has very little data that can be handed over.
- **Centrality**: Signal only runs on its own infrastructure (which is located at Amazon, Microsoft, Google, and Cloudflare) and cannot be self-hosted. This means that users must trust Signal to some extent to do its job well. On the other hand, a compromised signal

server does not mean that all your chats are also compromised, as long as your security numbers stay verified. But, it does mean that there is a central point of failure: If signal gets shut down one day, you may need another channel of communication to your contacts.
- **Censorship**: Since Signal is centralized, it is possible for governments to try to block connections to Signal servers. While Signal introduced proxies that can bypass censorship, it makes the bar-of-entry higher. Statistics from other projects such as the Tor project show that usage of a technology significantly declines when it is censored, even if there are ways to circumvent it. The plans of the EU to possibly introduce "Chat Control" and Signal's response that they may will exit the European market if the proposed regulation is passed highlight this issue. If the law passes, EU users may need to rely on proxies to connect to Signal or fallback on alternative messengers

> [!tip] See our recommendations about how to purchase phone numbers online anonymously. (The crypto currency Monero is required)

Signal groups

Signal groups are popular and frequently used for communication in larger groups *(up to ~150 contacts)*. In general, Signal chats offer automatic deletion of messages after a set period of time, which should also be set for groups that have a higher risk potential.

Unfortunately, there is no function yet that automatically deletes entire groups after a set period of time. Therefore, especially when devices are confiscated, it is important to consider which contacts are connected in which groups *(or which group names!)* and could also be compromised.

We therefore recommend *(for all group chats, not just on Signal)*: Based on the principle of *plausible deniability*, give your groups names that are as inconspicuous as possible and that cannot be used against you! In case of doubt, the chat history will only show **that** the group name has been changed, but not what the group was called before.

> [!danger] Attention {static}
>
> In the event of confiscation, the affected account should also be removed from all groups immediately!

>

> [!tip] {static}
>
> You can read our instructions on how to use Signal as anonymously and securely as possible.

Matrix

Matrix is a communication protocol. There are various client apps for this protocol, the best known being Element.

Matrix has become increasingly popular in activist and hacker circles, especially in recent times.

How it works

The most important difference between Matrix and other messengers, such as Signal, is its decentralization, or *federation*. Similar to email, there are many different servers (*"home servers"*) (such as *matrix.org* or *matrix.systemli.org*). If an activist with a Matrix account at matrix.org communicates with an activist with a Matrix account at matrix.systemli.org, the (encrypted) messages must be synchronized between the two servers.

Matrix Federation Functionality

Advantages of Matrix

- **Secure encryption**: Matrix uses its own implementation of the Signal protocol. It has some disadvantages compared to the Signal protocol, but is still similarly secure.
- **Decentralization**: Matrix is federated and therefore decentralized. There are many different servers that communicate with each other, so there are many points that would have to be attacked to completely paralyze Matrix. It is therefore more resistant to censorship then Signal, both legally and technically.
- **Anonymity**: Some servers do not require any personal information to create an account. This makes it possible, in principle, to use Matrix anonymously.
- **Openness**: The source code of Matrix and Element is open source and can be audited for security.

Disadvantages of Matrix

- **Complicated to use**: Matrix can be complicated to use at times. The principle of federation is counterintuitive for non-technical people, there are many different clients to choose from (which be overwhelming), and some things do not work smoothly yet.
- **Not yet widely used**: People often need to be persuaded to set up a Matrix account.
- **Lack of data minimization**: Because Matrix is federated, all data must be synchronized across all federated servers. This also means that it is practically impossible to delete data. By default, the Matrix ID, personal information, usage data, IP addresses, device information, other servers with which communication takes place, and room IDs [1] are stored on all servers by default.

> [!info] {static}
>
> Overall, choosing the right messenger depends on the threats you face, the people you want to communicate with and personal preference. From a technical and security perspective, the above, especially Signal, are most recommended.

[1]: The source refers to an older version of Matrix. It is unclear to what extent the amount of data stored by default and the deletion behavior are transferable to current versions.

Clear-Metadata

> [!toc] Table of Contents

> [!tip] Tip {static}
>
> If you don't know exactly what metadata is, read the
>
> article about this threat.

The following is mostly taken from the entry on metadata in the Systemli Wiki.

Exifcleaner

Platform: Linux, Mac, Windows Exifcleaner is an application for removing metadata from files.

Metadata Cleaner

Platform: Linux Metadata Cleaner is a popular program for deleting all metadata from various file formats with a single click. It supports all common file formats and is very easy to use. It is based on Mat2, which is presented here. Mat2 is particularly interesting to us because of its web application, which can be a good alternative for on the go.

Mat2

Platform: Web browser (online, all systems) and file manager (offline, Linux)

Mat2 is pre-installed on the anonymous operating system Tails and can be installed on other Linux systems. Instead of being a standalone program, mat2 is installed as an extension for the file browser and used by right-clicking on the file to be cleaned up. screenshot of mat2 in file browser

Web application

You can also use mat2 without installation as a web application at https://metadata.systemli.org. The files are uploaded to the Systemli server, cleaned up there, and then you can download them again. The web application is therefore an alternative for when you are on the go.

Scrambled Exif

Platform: Android

Scrambled Exif is an open-source app for cleaning up image files. You can download the app from the Google Play Store or F-Droid. After installation, you need to open the app once and give it permission to access your storage in order to set it up. Then, every time you want to share an image, you can share it via Scrambled Exif. It will clean up the file and ask you which app you want to share the cleaned file with.

Printerdots

As described at HacksAndLeaks: Instead of uploading original documents whose printer dots could reveal your identity, it is better to type or reproduce the originals by hand, print them on an “anonymous” printer, and publish them that way.

Anonymize scanned documents

Okular

Platform: Linux, Windows, (MacOS officially only with unstable version, but works quite well according to experience)

Okular is a PDF viewer that can also be used to black out documents.

Obfuscate

Platform: Linux

With Obfuscate, image files can be reliably pixelated/blacked out.

Libre Office

Documents can also be blacked out with Libre Office. However, most people find the above methods much more intuitive and simpler. An older but very good English-language guide can be found here.

Graphene-Os

> [!toc] Table of Contents

GrapheneOS is a mobile operating system based on Android. It is often recommended as an alternative to pre-installed (OEM) operating systems, as it can be used entirely without Google services. In addition to this feature, which protects user privacy, GrapheneOS, in combination with supported devices, offers state-of-the-art security features, which is why we strongly recommend its use here.

Recommended Apps

GrapheneOS comes as a very blank operating systems, with just the very necessary tools installed. Because app installations are crucial to security, we would like to give a recommendation on how to install apps from which sources/app stores.

We consider the following apps as part of most activists standard installations. The following list, as far as necessary, contains links to our instructions on how to install those apps securely, on a fresh GrapheneOS installation. We:

- Accrescent App Store: `Accrescent is a trusted app store that can be installed by the default GrapheneOS app store
- Signal messenger
- F-Droid: F-Droid provides apps, that Accrescent does not
- Orbot: Orbot routs all your phones network traffic through the Tor network
- Tor Browser
- CoMaps: is an offline map. Simply install it from F-Droid

> [!technical] What about Organic Maps?
>
> CoMaps is a community fork of the well known

> Organic Maps, which unfortunately upset their own community, by making private profit from community contributions

Recommended settings

Confidential profile

For many, data-hungry apps such as WhatsApp and the like are still a must-have in their digital repertoire. As a result, separate work profiles are often set up to use these apps. The “private space” feature can be a welcome alternative here:

> [!quote] Quote {static}
>
> Android 15 introduces the ability to install apps in a completely isolated area, separate from the rest of the system. [...] Unlike the previous work profile, which required a separate user login, Private Space is integrated directly into the system, making it much easier to use and more accessible.

The GrapheneOS team has written this feature announcement, which gives further details on how the private space feature can be used.

It is important to note that the confidential profile has its own network settings. This means that if you use TOR or VPNs, you have to set this up again in the confidential profile, as the settings from the normal owner profile do not apply here. This can also be seen a privacy feature, since exit IPs can be separate.

Data protection & security

Exploit protection

In the settings under `Security and Privacy` > `Exploit protection`:

- **auto reboot**: This option defines when your phone auto-reboot, measured by the time since last unlock. The auto reboot time should be as low as possible, but still comfortable for users. After rebooting, no signal messages/calls will be received without first unlocking the device, for example. However, a lower reboot time can possibly protect your data from physical extraction in cases where it was confiscated. It puts a limit on how long

attackers have to try to exploit the device while the user is still logged in, since it's going to reboot automatically if it's not successfully unlocked in the defined timeframe[1].

- **USB - C Port**: This option controls the behavior of the USB-c Port. It should optimally be set at least to “Charging only”. The “Charging only when locked” option is one level stricter and thus potentially more secure, but it means that the phone cannot be charged when it is used at the same time.
- **Turn off WiFi & Bluetooth automatically**: Turning of WiFi and Bluetooth when not needed is good not only for your battery life, but also for security and privacy. A convenient time period should be selected for both.

> [!technical] WiFi privacy risks
>
> When your WiFi is activated, your phone constantly checks for any known previous WiFi connections nearby. It thereby reveals information on your saved WiFi networks, which can be a significant privacy risk. Combined with other resources, it may be used by advanced adversaries to identify you or to track your location. As an example, the WIGLE map can be potentially used by anyone to track certain devices [2].

More Security and Privacy

In the settings under `Security and Privacy` > `More security and privacy`:

- **Notifications on lock screen**: `Show sensitive content` should be turned off. In case you phone gets stolen, the thief can see all incoming messages, including the names of the persons who sent them. This is a major security and privacy risk. At least prevent the notifications from showing sensitive content.
- **Allow Sensors permissions by default**: This should be turned off. This way, you will be asked about the sensor permissions you want to give an app, every time you install one. By this, you will have more consciousness about what different apps are capable of.

Duress Password

- Duress password: A duress password ensures that when it is entered, the phone is completely reset to factory settings. This is very useful if you are ever coerced or forced to unlock your phone. This also works if an attacker tries to guess your password using brute force. Of course, having regular backups of your phone or at least of your critical data is needed to ensure the reset does not lead to data loss.

It is best to choose a Duress Password that:

- you can remember immediately also in stressful situations. this is important so you can quickly type the duress password when needed

- that the police or your adversary would likely guess, so your data would be wiped if an unlock is attempted
- one that you would never choose as your real password, so that people who know you would not accidentally wipe your data if they try to unlock your phone

WiFi

For all WiFis that you do not have full control over:

- In the settings for the respective connection (gear icon next to the WiFi name): activate non-persistent MAC address randomization for this connection. This is a privacy feature which makes it harder to track or identify you via WiFi.

2FA for fingerprint

It has recently become possible to use a second factor for unlocking your phone via fingerprint. This represents a huge step forward in the conflict between usability and security!

What was the problem before?

Normally, biometric unlocking methods should be used with extreme caution for the simple reason that they can be forced by others. In case of doubt, the police can force your finger onto your phone and unlock it This means that, until now, the use of biometric unlocking has always been accompanied by the risk of being taken by surprise and forced to unlock your phone before it can be turned off.

What is the solution?

The 2FA option offers the possibility of setting up a minimum 4-digit (6 digits are recommended) PIN number, which must be entered each time after the fingerprint to unlock the phone.

You still have to type something, but a 6-digit PIN on the large number pad is much easier and faster to type than a 7-word passphrase on the small keyboard. In addition, the PIN can be changed much more easily when necessary, as you don't have to worry about learning a new long password.

Your password should still follow the recommended passphrase guidelines, but using this feature means that the cell phone can be encrypted with a very strong password without having to type it several times a day, since the long password is only required when the phone is first unlocked.

Can the PIN be brute-forced?

Only to a very limited extent:

- The entire fingerprint method is only available for 48 hours after the last entry of the primary (long) password.

- A maximum of 4 * 5 failed attempts are allowed. There is a 30-second timeout between every 5th failed attempt. This means that there are a maximum of 20 failed attempts. [1].
- As long as your PIN is truly random and thus hard to guess (not your birthday, for example), it can be considered secure.

PIN scrambling

PIN scrambling is pretty nerdy, but it does have its use cases:

Depending on whether you already have enabled the 2. factor pin for fingerprints, the locations are different from each other. See here in our instructions.

Instead of the digits always being displayed in numerical order on the screen, the digits are displayed in random positions on the screen when the PIN is entered. This means that if an attacker has been watching you entering your PIN from a short distance and has only been able to see the direction of your thumb on the screen, for example, they will not be able to reconstruct your PIN. The same applies to CCTV / surveillance cameras.

PIN scrambling is also available for the fingerprint 2FA.

Apps

In the settings under `Apps` > `Special app access`:

- `Install unknown apps`: Here are all apps listed that could potentially be able to install other programs on your phone. Check this list, so that only the app stores you use, are allowed to install other apps, such as: `Accrescent`, `App Store`, `F-Droid`, `Aurora Store` and so on ...

> [!tip] Tip {static}
>
> Also allow Signal to install apps! Although this seems counter intuitive, this enables signal to update it self!

Dangerzone

> [!toc] Table of Contents

Dangerzone is a very useful tool to securely open potentially dangerous files.

It supports more than 20 file types, including PDFs, all major office-suite formats, and the most common image types, which it can convert to safe PDFs.

> [!tip] Tip {static} If you are in doubt whether you can safely open a file - just open it with Dangerzone!

Instructions on how to install Dangerzone can be found on their website. They support all major operating systems.

How does it work?

Dangerzone destroys malware by rendering your document into pixels in a secure sandbox and reconstructing it locally as a PDF. Documents are sanitized in a sandbox with no network access, so if a malicious document can compromise the sandbox, it can't "phone home". The sandbox is based on container technology.

> [!info] Info {static}
>
> Dangerzone is a free and open source project, maintained by Freedom of the Press Foundation (FPF), a nonprofit organization that protects and defends press freedom.

In case you are not satisfied with the above explanation:

> [!technical] Dangerzone "under-the-hood"

> This information is from the project's "about" page. Dangerzone uses Linux containers, which are isolated application environments that share the Linux kernel with their > host. On Windows and macOS, it uses Podman under the hood, which spins containers in a dedicated virtual machine. Since > Dangerzone 0.10.0, all this complexity is hidden from the user. First, the sandbox:
>
> 1. Reads the original document from standard input
> 2. Uses LibreOffice or PyMuPDF to convert original document to a PDF
> 3. Uses PyMuPDF to split PDF into individual pages, and to convert those into RGB pixel data
> 4. Writes the number of pages and the RGB pixel data to its standard output Then that sandbox quits. The host reads the RGB pixel data from the container's standard output and:
> 5. If OCR is enabled, uses PyMuPDF to convert RGB pixel data into a compressed, searchable PDF
> 6. Otherwise uses PyMuPDF to convert RGB pixel data into a compressed, flat PDF
> 7. Stores the safe PDF in the specified directory with the -safe.pdf suffix, and archives the original one

Online-Sim

Some services, such as Signal, require a phone number to setup a new account. In most countries it became really difficult to purchase new SIM cards anonymously. Therefore services that offer online SIMs are a good alternative to that, e.g https://smspool.net or https://smsplaza.io.

> [!warning]
>
> We do not know any of the operators of those sites and we don't know what their political or moral stances are.
>
> Just by paying with anonymous methods, such as Monero, you can be sure to stay anonymous when purchasing a SIM, or SMS.

In most cases, those web services offer a wide range of countries, from which you can select your number. You can either purchase a one-time SMS for just a few cents, or you can permanently rent a number for a few Euros/Dollars per month. While using one-time SIMs may appear attractive, keep in mind that numbers may be re-distributed. It may happen that the one-time number you used will be assigned to another customer, who could then technically "push you out" of the service when re-registering at the same service again.

While this is technically possible and there have been reported cases of people losing their accounts because of this, it seems this rarely happens.

Generally, the method for registering an online SIM is the same everywhere:

1. Create an account for an online SMS service.
2. Add Monero to your account.
3. Decide if you want to have a one-time SMS or if you prefer to rent a SIM for a period of time.
4. Choose a country of origin.
5. Purchase/rent the SIM. This will display your new phone number.
6. Use the phone number to register a new account.
7. The registration PIN may occur at the web interface of the online sms service.

> [!note]

> It is common that purchased numbers don't work for registering new accounts at the first time. Usually the success rate is somewhere between 30-60%. So, if even after a few minutes no registration PIN arrived at you online SMS account, just buy another new SIM/SMS until it works.

File-Encryption

> [!toc] Table of Contents

There are several ways to encrypt files or entire folders. However, in most cases, the same underlying methods are used.

Here, we'll introduce two tools that allow you to securely and reliably encrypt files locally on your device. If you need some help deciding:

- Cryptomator is the go-to solution when you use Nextcloud and want to synchronize your encrypted files with your group.
- VeraCrypt is the go-to solution for encrypting storage devices (e.g USB drives) and creating encrypted folders.

VeraCrypt

- VeraCrypt can either create an encrypted container *(a container is essentially just a file)* that can then be opened like a folder. Encrypted containers offer a second layer of protection but should not be considered a replacement to fully encrypting the disk.
- VeraCrypt can be used to encrypt entire storage devices (USB drives, internal and external hard drives, etc.).
- With VeraCrypt you can also fully encrypt your Windows systems, making it an open-source alternative to *BitLocker*, Windows' less secure native disk encryption software.

> [!tip]
>
> In our guide to VeraCrypt, you'll find step-by-step instructions for installation and the most important features.

Cryptomator

- Cryptomator was primarily developed for end-to-end encryption of files in the cloud.
- Unlike VeraCrypt, Cryptomator doesn’t simply create a single “file” as a volume. Instead, it divides this volume into many small parts. This enables much more efficient synchronization because the entire volume doesn’t always have to be uploaded or downloaded when editing or adding files.
- Cryptomator also has a mobile app, which makes E2E-encrypted file synchronization via the cloud very easy to use. At the same time, it can also be used to easily encrypt files locally on your device.

> [!tip]
>
> See our instructions on Cryptomator and syncing files with Nextcloud.