

Instructions

- [Backups](#)
- [Auto-Reboot](#)
- [Nextcloud-App-Passwords](#)
- [Diceware](#)
- [Signal](#)
- [System-Updates](#)
- [Graphene-OS](#)
- [Keepassxc](#)
- [Nextcloud-Webdav](#)
- [Nextcloud](#)
- [Vera-Crypt-Encryption: Vera-Crypt-Encryption](#)
- [Vera-Crypt-Installation: Vera-Crypt-Installation](#)
- [Cryptomator](#)
- [Monero-Wallet](#)

Backups

“ [!toc] Table of Contents

In the article on [backups in the countermeasures](#) section, we described why backups are so important. Here we want to show how backups can be made.

Backup of what?

Of course, everyone has to think for themselves about what needs to be backed up. Here are a few common examples:

- Passwords
- Contact details (phone numbers, email addresses, etc.)
- Official documents
- Texts you have written yourself (or others have written)
- Logs (if necessary)
- Chats (if necessary)
- Images (photos, etc.)

How to back up

There are, of course, many ways to make backups. From simple copying and operating system functions to powerful programs such as borg/rsync, Kopia, or others.

“ [!tip] Important {static}

Only back up to [encrypted data carriers](#)!

Copy manually

The simplest way to back up is, of course, to simply insert a USB stick into the computer and copy your important files (user folder) to it, or to copy all folders from the file manager on your mobile phone to it. However, this can be very inefficient, as new data that needs to be backed up is constantly being created. Then you have to evaluate each time which files and folders need to be copied again.

“ [!success] Advantages {static}

- No technical knowledge or extra tools needed

“ [!fail] Disadvantages {static}

- Evaluate what needs to be backed up each time
- Not automated (you have to remember to do it yourself)
- All data must be copied over each time (takes a long time)

Native backup functions

MacOS

MacOS makes it very easy for users to make **regular** backups. The in-house tool is called `Time Machine`. Apple's own [instructions](#) are very easy to understand.

All you need is a storage medium that is large enough. In this case, large enough means at least twice the size of the data to be backed up.

“ [!success] Advantages {static}

- Configure once, then just connect the storage medium each time
- Fast: Files that were already in the previous backup and are still unchanged are skipped.
- Depending on your settings, `Time Machine` can keep multiple backups, so you can restore different versions of you files (*yesterday, last month, and last year, for example*). Again, the point above applies here: nothing is stored twice.
- Automatically deletes old backups that are replaced in the new run

[!fail] Disadvantages {static}

- You have to remember to connect the storage medium regularly

Auto-Reboot

“ [!toc] Table of Contents

Because all encrypted devices store their encryption keys in their RAM after you first entered the device password during the start up, bad actors could try to read your encryption keys out of the RAM, even when your device is just screen locked.

“ [!technical] What is RAM?

In very short, the RAM is a very fast memory device, that has one important feature for us: it loses all data, when the power is turned off!

Because of this, we want to automatically turn off our devices to clear our encryption keys from the RAM.

Automatic reboot can be configured on all PC platforms and some Android devices. Instructions for the native functions of the various platforms are provided below. No additional programs need to be installed.

Mobile devices

Android

An automatic restart can also be set on common Android devices. [GrapheneOS](#) even offers the option to restart the device whenever it has been unlocked for X hours.

A restart at a fixed time can be set as follows:

- `Settings`
- `Utilities`
- `Scheduled power on and off`

Here you can now specify when the device should always shut down and when it should restart.

iOS

Unfortunately, iOS does not currently offer a function for scheduled restarts. In November 2024 iOS introduced an auto reboot after 3 days of inactivity. This means that your iPhone will reboot automatically, if it won't get unlocked for 3 days in a row.

While this is still good to have, 3 days should be considered as plenty of time for law enforcement to bring this device to a professional forensics facility.

Anyways, if you want to see this reboot happen in action, you can watch [jiska's video](#) and especially read their [great write-up](#) on how this works technically.

PC

Linux

On Linux, you can use `crontab` for automatic jobs such as auto reboot. For example, to set the PC to restart every morning at 4 a.m.:

- Open Terminal (*Command Line*)
- Enter this command in the terminal: `sudo crontab -e`

An editor will now open (*or you will need to select one, TIP: select `nano`*)

- Paste the following line at the bottom: `0 4 * * * /sbin/shutdown -r`
 - To do this, copy the line above
 - Go back to the command line in the editor
 - Right-click > Paste
 - First press `Control` + `S` for “safe”
 - then press `Control` + `X` for “exit”
 - Done

“ [!technical] Explanation of the *cron* command

```
0 4 * * * /sbin/shutdown -r
```

From left to right:

- zero minutes
- fourth hour

- *th day of the month
- *th month
- *th day of the week
- Execute the terminal command `/sbin/shutdown -r`

The asterisks mean “all possible values.” This means that the complete line reads:

Execute the command `/sbin/shutdown -r` **every month** on **every day** at **hour 4** at **minute 0**.

The `-r` at the end of `/sbin/shutdown -r` stands for `reboot`. If you simply omit this `-r`, the PC will not restart automatically, but will simply remain off.

Additional settings when using suspend mode

Especially on laptops suspend mode is used often when people close the lid. This leads to the situation where the above cronjob is not sufficient, because it does not work while in suspend. This leads to the system being vulnerable to attacks. Therefore we need to introduce another automated action to ensure the device will shut down securely. This is done by waking up the system from suspend 5 minutes before it shall be shut down by using the Linux module (`systemd`)

- Open Terminal (`Command Line`)
- Enter this command in the terminal: `sudo nano /etc/systemd/system/set-wakealarm.service`
- Past the following content into the file:

```
[Unit]
Description=Daily wake up from suspend

[Service]
Type=oneshot
ExecStart=/bin/bash -c "/usr/sbin/rtcwake -a -m no -t $(date -d 'tomorrow 03:55' +%s)"
[Install]
WantedBy=multi-user.target
```

“ [!technical] Explanation of the `systemd` job

`[Unit]` just contains the description

`[Service]` contains the job which shall be executed in which mode.

`Type=oneshot` means it will be executed once

`ExecStart` is the command which shall be executed.

`/bin/bash -c` just tells systemd to run a new bash console and execute the command in `"..."`

`/usr/sbin/rtcwake` will execute the program `rtcwake` which will set a wake up alarm in the devices hardware timer

`-a` uses automatic clock detection

`-m no` tells the program to not do any direct action, only set the RTC wakeup time.

`-t $(date -d 'tomorrow 03:55' +%s)` is a complicated way of setting the wakeup time to 3:55

- After that, the following two commands will advise systemd to directly make use of the new wakeup command

```
sudo systemctl daemon-reload
sudo systemctl enable set-wakealarm.service
```

- To test if everything is setup correctly this command can be used: `sudo systemctl start set-wakealarm.service`
- In case the command finishes without any output, it's set up correctly.
- After that, you can check if the wakeup time was set correctly in the devices hardware timer: `cat /proc/driver/rtc` There you should see the following values:

```
[...]
alarm_time : 02:55:01 (Attention, this is UTC, which might have an offset to your local
timezone)
alarm_date : <date of the next day>
alarm_IRQ  : yes
[...]
```

- It is highly recommended to test if this works the next couple of nights. So put your device in suspend in the evening and check if it is shut down the next morning. With `journalctl --list-boots` you can check when your PC was running, which includes times in suspend mode.

MacOS

- Click on the `Apple Logo` in the menu bar.
- `System Preferences`
- `Energy Saver`
- `Schedule`

MacOS Energy Saver

The top checkbox can be used to specify when the PC should be restarted when it is turned off. We are not interested in this. We want to automatically turn off the PC to clear the RAM.

- So we select the bottom checkbox
- `Every day`
- Choosing the reboot time is up to you, but we would recommend a time at night (e.g., 2 a.m.), as this is when we usually do not use the computer. Additionally, house searches are often conducted in the morning, so rebooting our computer beforehand makes sense.

Windows

We can use the `Task Scheduler` to shut down the computer, restart it, or perform any action once or at regular intervals.

If you prefer to follow a video tutorial, there is also [YouTube video](#) on this topic.

- Enter `taskschd.msc` in the Start search and open Task Scheduler.
- In the right-hand bar, click on `Create basic task`
 - Give the task a name, e.g. `Auto Reboot`
 - `Execute whether the user is logged on or not`
- Go to the next tab and select `Triggers`
 - `Daily`
 - Set the restart time (e.g. *2 a.m.*).
 - Start date and start time: Select the current time *i.e. valid from now*
- `OK` and go to the next tab `Action`. Here, select `Start a program`
 - Now enter `shutdown` in the `Program/script` field
 - Now enter `/r /f` in the `Add arguments` field
 - The `\r` stands for `reboot`. If you only enter `/f` there, the PC will not restart automatically, but will simply remain off.
- `Next` and go to the next tab `Conditions`
- Make sure that under the “Power” section:
 - the top two checkboxes are unchecked, i.e. off
 - and the last one, “Wake the computer to run this program,” is checked.
- Click `Next` to check everything and then click “Finish.”
- Finally, you will probably have to enter your password.

Nextcloud-App-Passwords

“ [!toc] Table of Contents

Nextcloud allows you to create app passwords. This allows you to assign a different password to each device or app that you connect to your account. The advantage of this is that you can easily revoke access to your account for individual devices or apps from your account settings.

- Log in to the cloud and click on the avatar in the top right corner

Nextcloud avatar

- Select `Settings` > `Security`

Nextcloud security settings

Here you can create a new app password:

1. First, give the new password a name so that you know what it is used for later. Give each app password a unique name so you don't accidentally revoke access to the wrong application. Here, we will call it “Sync Client.”
2. Click `Create new app password`

name new app password

The password is now displayed for the first and last time! So make sure you copied the password to the application you want to connect with Nextcloud you before close the password window. In case you closed the password window too early, simply delete the lost password and create a new one instead.

The button `Show QR code for mobile apps` allows Nextcloud apps for mobile devices to log in once. In case you want to connect Nextcloud to a mobile application, this is more convenient then typing the password manually.

one-time view app password

Here we can see the different “sessions” that can access our account.

different sessions

Delete old sessions

Here you will notice that every time we log in to the browser and do not log out later using the `Logout button`, this “session” remains valid. This is a bit annoying, as we quickly lose track of whether these are our own “sessions” or whether, for example, an attacker has logged in in the meantime.

delete old sessions

Here, for example, you can see that we did not log out properly 10 hours ago, but simply closed the browser window. The session is theoretically still valid, but no longer useful to us. So we delete the old session.

Diceware

“ [!toc] Table of Contents

Diceware is a method for generating passphrases/passwords using dice and a word list. These contain genuine randomness and, if sufficiently long, can be considered secure.

This tutorial briefly describes how you can create a secure password in just a few steps. Detailed instructions on Dice-Generated Passphrase can also be found on the [EFF Website](#).

“ [!tip] Tip {static}

We recommend that you read the page on [passwords](#) first. There, we also explain how long your passphrase should be and why they should be generated randomly. In any case, it is not sufficient to think up ‘random’ words yourself or select them from a list. We also recommend that you use a [password manager](#) so that you only have to remember a few really secure passwords.

Concept

The idea is that you select different words for your password from a list of approximately 7,000 words. This gives you a password that is easy to remember and still contains real randomness. All you need is a dice.

Step 1

Select a word list in a language you are comfortable with. If your language is not in the list, you can find a word list by searching for “Diceware Wordlist” + “language.” Choose a list that is designed for at least five dice, i.e., contains at least 7776 words.

- [dys2p/wordlists-en EN](#)
- [EFF's Long Wordlist EN](#)

- [Website with other languages](#)

For this example, we will use the EFF Long Wordlist. However, you can also use any other list designed for five dice.

Step 2

Now roll the dice five times and write down the results in the order you rolled them. For example: 14314

Now look up the word that matches this number in the word list.

In the [EFF's Long Wordlist](#) the word corresponding to 14314 is bucktooth.

Step 3

Repeat step 2 at least six times.

You should now have six words. For example:

battery tacker horses blow counter note

Congratulations! You just created a secure and truly random passphrase!

Step 4

If there is no immediate danger of repression, write the password on a piece of paper and enter it once or twice a day. After one to two weeks, most people can remember their new password well. Then destroy the piece of paper!

There are different techniques for better remembering random passphrases. For some people, making up a story to go with the words can help to remember them better.

“ [!technical] Technical

The recommendation to use six words comes from the official [EFF Guide to Diceware](#)

Signal

“ [!toc] Table of Contents

Credit: The article is a translation of the [LG Wiki](#) Signal section.

“ [!tip] Tip {static}

In addition to the following practical guides, we have a general [article](#), in which we discuss the advantages and disadvantages of Signal and other messengers.

Register an anonymous account

Since Signal requires a phone number for creating an account, you should evaluate whether it is necessary for you to use an anonymous phone number not linked to your name. If you can't find a local shop selling anonymous SIM cards, you can also have a look at our article about [online SIMs](#).

Set up registration PIN

It is very important that you set up a PIN in Signal. This protects against unauthorized re-registration. Your network provider is required by law to forward SMS messages to the police. Without a PIN, the police can re-register your account and thus read your Signal messages – However, you would notice it if someone tries to re-register your device. Only one mobile phone can be registered with Signal, so you would be logged out of your Signal account.

Enabling a registration lock triggers a [7-day inactivity timer](#) if your number is registered on another device. After 7 days of inactivity on your phone, a new PIN can be created, but the old PIN and information associated with it would no longer be available. This means that if you have no access to your signal, an attacker could re-register the account after 7 days - but would not be able to see your old messages.

To set up a PIN:

- iOS: tap your avatar » Settings » Account
- Android: Settings » Account » Registration Lock

Self-destructing messages

In individual chats/groups:

- Click on the name at the top of the chat
- Disappearing messages

You can also set a default period of time for the feature to be automatically activated for new chats:

- Settings
- Privacy
- Disappearing messages
- Default timer for new chats: set a time interval, e.g. 1 week

Restrict push notifications

[Here we explain](#), why we recommend this.

iOS

- Click on your profile picture and open Settings
- Notifications
- Notification Content
- Select No Name or Content

Android

- Click on your profile picture and open Settings
- Notifications
- Show and Select No name or message

Create usernames

Username makes it possible to share your contact without revealing your phone number. For more information, see Signal's [blog](#).

- [Settings](#)
- Click on your mobile phone number at the top
- Set a username after the [@](#)

The username must end with a period and at least two digits, e.g.: [username.12](#). However, there can also be more digits after the period.

Disable [Find by phone number](#)

You can prevent your Signal account from being found using your phone number. This will make it harder for people who know your phone number to find out if you are using Signal, which is important if you live in a country where Signal usage may be suspicious or illegal.

- [Settings](#)
- [Privacy](#)
- [Phone number](#)
- “Who can see my number”: [Nobody](#)
- “Who can find me by my number?” [Nobody](#)

Multiple Signal accounts on one device

There are various options for using multiple Signal accounts on one device. The options depend on your operating system:

Multiple Signal accounts on PC

The easiest way is to download the tool [signal-account-switcher](#). This allows you to use four additional Signal accounts at the same time. To do this

1. Click on this link: <https://github.com/kmille/signal-account-switcher/releases/tag/v0.1.0>
2. Download the tool for your operating system. At the bottom of the page: “signal-account-switcher.exe” for Windows, “signal-account-switcher” for Linux and “signal-account-switcher-mac-[{amd,arm}](#)” for Mac (depending on your [CPU](#)).

3. Start the tool (Windows may complain at first because it is “unsafe” to run a file from the Internet) and simply click on “Start Signal Account #1.” A new signal-desktop instance will open.

If you don't want to install an extra tool for using multiple signal profiles on your PC, you can also do it yourself with a little manual configuration:

- Instructions for Windows: <https://www.youtube.com/watch?v=TejhH80jktE>
- Instructions for Mac:
 1. open the command line/terminal
 2. paste the following command inside the terminal and hit `Enter`

```
mkdir $HOME/Library/Application/Signal-Account-1  
/Applications/Signal.app/Contents/MacOS/Signal --user-data-  
dir="$HOME/Library/Application/Signal-Account-1"
```

Multiple Signal Accounts on Android

Molly

There is a Signal fork called [Molly](#), which can be installed alongside the normal Signal app and set up with a different account.

“ [!technical] What is a fork?

In software development, a fork is an application that is created by duplicating an existing codebase, in this case the Signal codebase, and subsequently modifying it independently of the original. Molly modifies the Signal codebase to add functionality such as having multiple accounts.

1. If you haven't already, install [F-Droid](#), a free and open source app store:
 - Download the F-Droid.apk file from the website.
 - Install f-droid by opening the .apk file you downloaded.
 - Allow “Installation of apps from unknown sources” when prompted.
 - Allow “Install apps from this source” if necessary.
2. Add Molly's [package source](#) to your F-Droid by following these [instructions](#) on the F-Droid website. Molly is not automatically included in F-Droid and therefore needs to be manually added.
 - Go to <https://molly.im/download/fdroid/> and select Molly (if you are reading this on your phone), or scan the QR code if you are reading this article on your PC. **Select Molly, not Molly-FOSS, unless you know what you are doing** (e.g., no Google

Play services).

- Open F-Droid and refresh once by swiping down from the top edge of your phone; this will load information about all available apps, which can take up to 2 minutes.
3. Install Molly via F-Droid
 - Search for Molly in F-Droid and install it. If necessary, allow “install from this source” for F-Droid again.

Molly is now ready and you can set up the app as you would normally set up Signal.

However, you will be asked at the beginning whether you want to use additional *password encryption*. Your choice cannot be changed later. This is useful for sensitive accounts.

Create a Signal PIN that you can remember for sure, or save it in your secure [password manager](#), but don't write it down on a piece of paper! This could be used by the police to intercept messages intended for you after a house search.

App clones

Some manufacturers offer a dual app feature to run multiple accounts on one phone. Search online to see if your device has this feature. Starting with Android 14, this option may be available by default on many devices.

You can also use this feature to clone Signal and Molly, which would enable you to use up to four different Signal accounts. You could also do without Molly and use Signal twice, but Molly is more useful because it has slightly better encryption and security mechanisms, which offer an advantage in the event of a house search.

You can easily activate the feature in the Android settings:

Samsung: `Settings > Advanced features > Dual Messenger`

Huawei: `Settings > Apps > App Twin`

LG: `Settings > General > Dual App`

A menu with all clonable apps should then appear, where you can simply select Signal (and any other apps you want to clone) and duplicate them.

Additional Android profiles

Android offers the option of creating multiple user profiles, just like Linux, MacOS, and Windows. For more information, visit the responding Android [support page](#).

System-Updates

“ [!toc] Table of Contents

One of the first answers to questions about IT security is always: **Install updates**. Since apps and systems should always be up to date, it is advisable to set **automatic updates**.

Depending on your operating system, you may need to distinguish between system updates and app updates. Where relevant, we explain the differences and provide step-by-step instructions on this page.

- [Linux](#)
- [macOS](#)
- [Windows](#)
- [iOS](#)
- [Android](#)

macOS

System updates on macOS

This updates the macOS operating system to the latest version. System updates on macOS will also update all standard apps such as Mail and Safari. However, apps installed via the App Store need to be updated separately

1. Click on the `Apple icon` in the upper left corner of the screen.
2. Select `System Preferences` from the drop-down menu.
3. Click on `Software Update`.
4. If updates are available, you can click on `Update Now` to download and install the updates.

App updates on macOS

1. Open the App Store on your Mac.
2. Click on the `Updates` tab in the sidebar.

3. Here you will see a list of available updates for the apps you have installed. Click on “Update All” to install all available updates.

Automatic updates on macOS

Go to `Software Update` as described above and enable `Automatic Updates` to ensure that your system is always up to date. There is a small arrow next to `Automatic Updates`. Underneath it, `Download new updates in the background` and `Install app updates from the App Store` should be enabled.

Windows

In Windows, it is important to distinguish between system and app updates, mainly because all programs installed after the initial installation have their own individual update mechanisms. This means that in Windows, you must regularly check for updates for each program installed. This information can usually be found somewhere in the settings of the respective program.

System updates on Windows

1. Click on the Start menu (Windows logo) and select the gear icon for Settings.
2. Click on `Update & Security` (*Windows 10*) or `Windows Update` (*Windows 11*).
3. Click on the `Check for updates` button.
4. If updates are available, click on `Install updates`.
5. Click on `Restart now` if a restart is required to complete the installation.

Automatic system updates on Windows

- Go to the update settings as described [above](#)
- Click on `Advanced options`
- Enable `Download updates automatically`

Linux

In most cases, system and app updates on Linux can be considered as the same thing. Depending on the Linux [distribution](#), the individual settings may vary slightly, but the principle is the same everywhere.

Ubuntu (including: Debian, Mint, PopOS,...)

System updates can be performed in two ways: via desktop programs similar to the App Store, or directly with a command in the terminal. In fact, modern versions of Ubuntu should be preset to perform all updates automatically. However, this should be checked. If in doubt, [take a look here](#).

Updates via the desktop app

- Search for `Software Updater`

App Updater asks for installing updates App Updater is installing updates

Updates via terminal (Ubuntu)

1. Open the terminal (`Ctrl + Alt + T`, or search for “Terminal” in the app menu)
2. Paste the following command into the terminal (`right-click`, `Paste`)

```
sudo apt update && sudo apt upgrade -y && sudo snap refresh
```

“ [!technical] What does this command do?

Three commands are executed here, separated by `&&`. The difference between `apt` and `snap` will not be explained here to avoid confusion. A good comparison is provided in the the following [article](#). `sudo`: means “super-user do...” The following command is therefore executed with admin rights. This is necessary for updates, as programs are uninstalled and reinstalled. `sudo apt update`: This command basically “compares” the version numbers of your installed programs with the latest version numbers in the repository (*App Store*). This tells the PC which programs need to be updated in the next step. `sudo apt upgrade`: Based on the results of the previous `update` command, this command downloads the latest versions and installs them directly. `-y`: The `yes` flag automatically confirms the upgrade process so that it does not have to be done manually. `sudo snap refresh`: snap is a different package manager. If you installed your apps using the graphical App Store in Ubuntu, most of them were installed using `snap`

Automatic updates (Ubuntu)

In GNOME:

- Open “Software & Updates”
- Open the `Updates` tab

- Under “When security updates are available,” select the “Automatically download and install” option

Fedora

System updates can be performed in two ways: via desktop programs similar to the App Store, or directly with a command in the terminal. Modern versions of Fedora usually enable automatic updates by default. However, It is best practice to check if this is the case.

Updates via the desktop app (Fedora)

See [Ubuntu](#)

Updates via terminal (Fedora)

1. Open the terminal (`ctrl + Alt + T`, or search for "terminal" in the app menu)
2. Paste the following command into the terminal (`right-click`, `Paste`)

- `sudo dnf update`

Upgrade to new Fedora version (about once a year)

To update to a higher version of Fedora, refer to the [official documentation](#) from the Fedora Project.

Automatic updates (Fedora)

See [above](#) under Ubuntu.

Tails

Tails comes with its own [Tails Upgrader](#), which automatically checks for updates and installs them. However, this requires that the system is running long enough to complete the updates. So check again before shutting down to see if any updates are available. (Open Tails Upgrader in the app menu)

It is recommended to manually upgrade your Tails installation every few months. This is slightly more secure, and will decrease the time needed for future updates. For concrete instructions, go the [Tails documentation](#).

iOS

System updates on iOS

1. Open the Settings app
2. **General**
3. **Software Update**: This will check for available updates.
4. **Download and Install**. You may need to enter your password.
 - Accept the terms of use when prompted.
 - The update will be downloaded and installed. Your device may restart during the installation process.

App updates

1. Open the App Store
2. Go to **Updates**
 - Tap your profile picture or the **Updates** icon in the lower right corner.
3. Tap **Update All** to update all apps.

Enabling automatic updates

For system updates

1. General
2. Software Update
3. Here you will find the option Automatic Updates. Enable this option.

For app updates

1. Open the Settings app
2. Apps (*usually at the bottom*)
3. App Store
4. Enable App Updates

Android

The exact names of the menu items may vary depending on the manufacturer of your Android device, but the principle is the same across all devices.

System updates on Android

1. Open the Settings app
2. At the bottom, tap `About this phone` or `System`
3. `Software update` or `System updates`
4. `Download` or `Install`. You may need to enter your PIN or password.

Automatic system updates on Android

Automatic system updates are usually enabled by default on Android. They are only accessible via the `Developer options`, which should not be touched unless you know exactly what you are doing.

GrapheneOS

In theory, the above also applies to “normal” Android versions, but the following usually applies to GrapheneOS users:

If you don't use your “Owner” profile regularly and are mostly in a user profile, the auto-updater (which only works in the Owner profile) may not always check for updates.

For all users: switch to the owner profile regularly and follow the [manual method](#) described above.

App updates on Android

Since different app stores are used here, we will simply list them all in order. While auto-updates are usually enabled by default for all of App Stores, it is best to confirm this manually.

Google Play Store

1. Open the Google Play Store
2. Go to “My apps and games”
3. “Update all”

Automatic updates in Google Play Store

1. Open the Google Play Store
2. Under the user icon, tap `Settings`
3. “Network settings”
4. “Enable automatic app updates”

Automatic updates in Aurora Store

1. Tap the gear icon in the top right corner
2. Tap “Settings”
3. Tap “Updates”
4. Tap “Auto-update apps”
5. Select “Install automatically.”

Automatic updates in F-Droid

- Settings
- Automatic update interval
 - Here you can set how often to check for new updates. (*e.g. daily*)
- Activate Install updates automatically

Automatic updates in Accrescent

- Settings
- Activate Automatic updates

Automatic updates in Obtainium

- Settings
- Enable background updates
- For faster updates: Allow parallel downloads

Graphene-Os

“ [!toc] Table of Contents

Recommended Apps

Install Accrescent

Download the `Accrescent` App Store from the default `App Store`, that comes preinstalled with GrapheneOS From `Accrescent` install `App Verifier` and `Inter Profile Sharing`, if you plan to share files between different Android Profiles.

Install Signal

- Download the Signal APK from Signals own website: <https://signal.org/android/apk/>. After downloading the APK, verify it via the `App Verifier` You can do so by selecting the downloaded APK in your `Downloads` folder and `share` the APK with the `App Verifier`. This will display **SUCCESS** at the top. On the bottom it can say **UNKNOWN**, that's ok. If the top also says **UNKNOWN**, than something went wrong and downloaded a wrong APK!
- Go back to the `Download` folder and click on the signal APK to start the installation.
- In case the warning `For your security, your phone currently isn't allowed to install unknown apps from this sources.` pops up, this is correct. You have to give you `Files` App the permission to install Applications. Click `Settings` and toggle `Allow from this source`

“ [!warning] Warning {static}

For security reasons, eg. preventing yourself from unintentionally installing some malicious APK you downloaded from the internet, **remove this permission after successfully installing signal**, by turning it off again under: `Settings`, `Apps`, `Files`, `Install unknown apps`

Only for very high threat levels:

If you are at home, in your personal WiFi and you want to active you signal anonymously, wait with the activation of your account until you installed [Orbot](#) from [F-Droid](#). Just follow the guide below.

Install F-Droid

- As with signal, get the APK **from their official website**: <https://f-droid.org>

Your Browser `Vanadium` might show you a warning, that `This file might be harmful`. This is also a good warning, since usually one shouldn't download random APK's from the web, but instead from an app store, like F-Droid. Since we don't have an app store yet, from which we can install the apps we like, we need to do this once: `Download anyway`

- Share the downloaded APK with the `App Verifier` and confirm the **"SUCCESS"** at the top of `App Verifier`
- Go back to the `Download` folder and click on the signal APK to start the installation.
- In case the warning `For your security, your phone currently isn't allowed to install unknown apps from this sources.` pops up, this is correct. You have to give you `Files` App the permission to install Applications. Click `Settings` and toggle `Allow from this source`

“ [!warning] Warning {static}

For security reasons, eg. preventing yourself from unintentionally installing some malicious APK you downloaded from the internet, **remove this permission after successfully installing f-droid**, by turning it off again under: `Settings`, `Apps`, `Files`, `Install unknown apps`

Install Orbot and Tor Browser from F-Droid

`orbot` will direct all your phones internet traffic through [Tor](#).

First, you have to copy the guardian projects repository link from their [website](#). The link on the very top of the webpage should work.

- add the repository of the guardian project to your F-Droid by following these [instructions](#)
- go back to the main page of your F-Droid App and pull down on the screen, to refresh the page. Now the newly added repositories should be included
- search for `Orbot` from the "Guardian Project" and install it
- search for `Tor Browser` from the "Guardian Project" and install it

[!technical] For high threat level

If you are at home in your personal WiFi and you would like to register your signal account anonymously, first activate Orbot, then start the registration.

The reason for that lies in the potential metadata. The only information signal store on it's users are the timestamp of the registration of the account and the timestamp from when the account was logged in the last time.

Theoretically, if you one day will have do [plausible deny](#) to be the owner of this signal account and your network was tapped, while you created the account, one could "prove" that you connected to the signal servers just at that moment, when this account was created.

But this is, to be quit honest, a very theoretical threat scenario.

Recommended Settings

“ [!tip] Tip {static}

To see, why we recommended the following settings on GrapheneOS, go to our [GrapheneOS recommendations](#)

Device Unlock

In the settings app, go to: `Security and Privacy` > `Device unlock`. Here you find settings for:

- Screen lock: set your [strong password](#) here
- Fingerprint unlock and it's strong [2FA](#) feature
 - also see the [PIN scrambling](#) feature
- [Duress Password](#)
- [PIN scrambling](#):
 - if you don't use the fingerprint unlocking with it's 2FA Pin: `Device unlock` > `Cog-wheel icon` to the right of Screen lock > `Scramble PIN input layout`
 - if you're already using the 2FA method, than you have to go to: `Device unlock` > `fingerprint unlock` > `input your password` > `second factor PIN` > `toggle Scramble PIN input layout`

If you're interested why this is in two different locations, see:

<https://discuss.grapheneos.org/d/18661-where-is-pin-scramble-feature/11>

Exploit Protection

In the settings app, go to: `Security and Privacy` > `Exploit protection`. Here you find settings for:

- `auto reboot`
- `USB-C Port` *Tip: `Charging only`*
- `Turn off WiFi & Bluetooth automatically`

More Security & Privacy

In the settings app, go to: `Security and Privacy` > `More security & privacy`. Here you find settings for:

- Allow Sensors permission to apps by default: *Tip: turn this off*
- `Notifications on lock screen`: *Tip: turn off: show sensitive content*

Apps

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

- `Install unknown apps`

KeePassXC

“ [!toc] Table of Contents

“ [!info] Getting Started {static}

The official *English-language* KeePassXC [documentation](#) offers a very good and comprehensive “[Getting Started](#)” article. We recommend reading it to get an overview of the available features!

Below, we summarize what we consider to be the most important points from the KeePassXC documentation linked above. Throughout the article, we refer back to the individual sections of the KeePassXC documentation. If you find it difficult to follow so much text, [this video](#), (on YouTube), explains the core features of KeePassXC quite well. Once you are familiar with the basic usage of KeePassXC, there is also a [sequel](#) for advanced use cases.

Create a database

The database is basically just a file in which passwords are stored in encrypted form. It always ends with `.kdbx`

KeePassXC is the program used to decrypt and use this file.

If you don't have a database yet, you must first create a new one. Before you create your first database, you need to consider the protection methods you want to use. The simplest form of protection is to use a strong password. For additional protection, you can consider adding another protection "layers", such as a [key file](#) (key files).

To create a new database without a key file, follow the steps in this guide: [Create new database](#)

Key file

When creating the database, there is a button labeled “Add additional protection” where you set the password for the database.

Then, under the “Key file” field, click the `Add key file` button.

Here you can now either:

- Create a new key file.
 - `Generate`: Specify a name and location for saving the new key file
- Specify an existing key file to be used to encrypt this database:
 - `Browse`: Here you can select your existing key file

Decrypt database with key file and password

If you have protected your database with a password and an additional key file, you will need both to unlock it again:

- Open the database with KeePassXC
- `I have a key file`
- Select the key file in the file manager
- Enter the password
- Confirm

Add key file later

If you already have a password database, you can also add a key file later.

We strongly recommend that you back up your database beforehand. This will prevent the loss of all passwords if something goes wrong. *To do this, simply make a copy of the database with a new name. For example, if the database is called “Passwords.kbdx,” create a copy called “Passwords-keyfile.kbdx” or something similar.*

- Open the (new) database in KeePassXC
 - Now you may have both databases open at the same time: multiple db tabs
 - This is not a problem, but be careful not to get confused and edit the wrong database. Close the original database, so that nothing goes wrong.
- In the top bar, click on `Database`
- Then click on `Database security...`
- From here, follow the instructions in the section [on adding a key file](#)
- Caution: Once you have created and saved a key file, KeePassXC assumes that you now want to use **only** this key file to unlock the database. If you have already clicked `OK`,

you will have seen a warning message to this effect.

- Therefore, you must reset and confirm the password using `Change password`.
- `OK`

Password entries

Follow the official documentation to [create a password entry](#).

You can also [edit existing entries later](#) (double-click on the entry).

Create strong password according to entropy

Click the dice icon in the tool bar. This opens the password generator. Here we have two options:

1. Create a password, out of selected character types

Screenshot of KeePass password generator character view

2. Create a password, out of a selected word list

Screenshot of KeePass password generator word list view

In both screenshots you can see the amount of entropy bits for the generated password. We recommend creating password with an entropy of 120 bits.

“ [!tip] You can download word lists for various languages

For example [from here](#). You can also combine words from different languages, although you would have to do this manually, since KeePassXC only lets you select one word list at a time.

Browser integration

KeePassXC can be integrated into your browser. The integration makes it possible to automatically fill Browser Log-Ins for passwords that are saved in your Database. This saves a lot of time, as you don't need to manually copy-and-paste your passwords into the browser.

There are [official instructions](#) for installing the browser plugin (except for Safari).

TOTP

[Official KeePassXC instructions](#) with helpful screenshots.

TOTP is a form of [two-factor authentication](#) used by many web services, such as email or cloud access. To set up 2FA for a service, you need two things:

1. The appropriate setting in the web service, e.g. in the email settings.
2. The configuration of the corresponding KeePassXC entry for this web service.

The settings for web services all look slightly different, of course, but in most cases you will find the following in the account settings:

- A section with `Security` or `Privacy`.
- Here you should find the `2FA` or `TOTP` settings.
- “Enable TOTP” or similar

Now a QR code and, in the best case, a random string should appear (see [KeePassXC instructions](#)). The QR code is useful if you set up TOTP on your mobile phone, as you can easily read the `Secret` with the mobile phone apps using the camera. On a PC, we need the character string for this.

If only the QR code appears here without the character string, we have to read the “Secret” from the QR code.

“ [!info]

Read Secret from QR code This works with all common mobile phone cameras that can read QR codes. It is very likely that more than just the `Secret` will appear here, but rather a URL that is actually intended for mobile apps, e.g.:
`otpauth://totp/example.org:username?secret=PABRSLZNHFLAIENT&issuer=Example` The `secret` is hidden here between `secret=` and the next special character, in this case `&issuer...`.

Our `secret` is therefore: `PABRSLZNHFLAIENT`.

- Copy secret

Now we go to the KeePassXC database:

- Right-click on the corresponding password entry
- TOTP
- Set up TOTP
- Paste Secret
- OK

Now you should see a small clock next to the password entry. *This symbolizes the temporary nature of the TOTP codes.* totp clock symbol

Finally, we need to synchronize the TOTP setup. To do this, the current TOTP token must be re-entered in the web service settings. The TOTP token can be copied in two ways:

- Control + T, or
- Right-click > TOTP > Copy TOTP

Go back to the web service settings:

- Paste the TOTP token
- Confirm

You should now see a message indicating that the setup was successful.

Backup

KeePassXC offers an automatic backup feature. This ensures that you always have an up-to-date version of your password database in a different “location” than the one you mainly use.

Under Settings (gear icon) > General > File Management, you will find the option Create backup of database before saving. There you can specify a path where the replacement file should be saved.

It may be a good idea to specify cloud storage if you are not already [synchronizing the database via cloud storage](#).

“ [!warning] Warning {static}

Although the database is always encrypted, even in the cloud, there are scenarios that need to be considered. Read the [example scenario](#) of a potential

Synchronization/backup in Nextcloud

You can also synchronize your KeePassXC database via a cloud across devices. See [our Nextcloud instructions](#) on how to set this up.

The principle works the same with iCloud, OneDrive, Dropbox, etc.

Nextcloud-Webdav

“ [!toc] Table of Contents

Nextcloud Sync Client

The Nextcloud Sync Client is Nextcloud's own software for synchronizing content in the cloud with your own devices (PC, mobile phone, tablet). Installation and setup is very easy in most cases.

Content synchronization means that Nextcloud creates a folder on the device where all files from the cloud are stored. If a file in this folder is changed, it is changed directly in the cloud and thus also on all other devices linked to it. An example for the practical use of synchronization is described in the module [Using KeePassXC as a group](#)

Installation

- Download and install the sync client: <https://nextcloud.com/install/#desktop-files>

Setup

1. `Login`
2. Enter the URL of your cloud instance (*where you have an account*)
3. A browser window with the cloud login should then open

sync client login process

There are two options here:

- Log in with your normal login details
- For more security: `Alternative log in using app password`. Quickly follow our instructions on [how to set up an app password](#) and come back here!

“ [!warning]

If you have 2FA enabled in your general settings, you won't be able to log in with your main (normal) password here, since the client app does not support 2FA.

In this case you have to [create an app password](#). We recommend using this anyway.

login with app password

Once we have logged in, a configuration window appears where we can specify which folders from our cloud should be synchronized with our computer. We can either select specific folders (`Choose what to sync`) or simply select all. Under `Choose different folder` , we can also specify where the synchronized Nextcloud folder should be located on our computer.

sync options

Depending on how much data we have in the cloud, the synchronization process may take a while. Once the synchronization is finished, we should have all our personal cloud files directly accessible on the computer in the specified `Nextcloud` folder.

Encrypt your files in Nextcloud

Per default, files in NextCloud are not end-to-end encrypted. While they could be stored on an encrypted server, end-to-end encryption has to be setup additionally. If you want to understand what end-to-end encryption means, have a look [at the following article](#). Although it is on E2EE in email, the described example works here too, just without a second server involved.

“ [!tip] The easiest way to encrypt you files in Nextcloud (or any other cloud), is by using Cryptomator! Go ahead and checkout [our short guide](#), or the [official user manual](#)!

You may later want to adjust which files you want to sync. So if you wonder, why you big folders are not present on you computer, you have to enable syncing them n the settings:

In the sync client, click on you profile name on the top left >> `Settings` >> Select

Nextcloud

“ [!toc] Table of Contents

Nextcloud is often used as a privacy-preserving alternative to Google Drive, iCloud or other commercial Cloud providers. Nextcloud is open-source software that can be installed (hosted) by anyone on their own server. Solidarity-based technology collectives sometimes operate their own “instances.” “Instances” are the individual Nextcloud installations, e.g., those of different groups/associations/companies, etc. Depending on the settings of the respective instance, the individual Nextcloud is completely “self-sufficient,” meaning it has nothing to do with other instances.

“ [!tip]

Nextcloud can be an attractive tool for political groups to organize their work with shared passwords, calendars, documentation, pads, etc.

We have two articles on how to use nextcloud with [encrypted folders as a group](#) and how to use [KeePassXC as a group](#).

Account management

If you want to use the cloud as a group, the problem arises as to which user owns the shared data (documents, calendars, deck boards, etc.). In most cases, we recommend the use of teams for groups.

Teams

- Each member of your group gets a **personal account**.
- In addition, you create a **group account** as an admin, which is managed by several people.
- Use the group account in the **Collectives app** (*if available*) to create a collective for the group.
 - Add all personal accounts under `Manage members`.

- If necessary, grant admin rights to individual accounts.
 - Next to “Teams,” click on the “+” and add a description.

“ [!note] Technical detail: Why not in Contacts?

You could also create the team under `Contacts`, but then the team would **belong** to you, which we want to avoid, as described below. If the Collectives app is not available, create a team under `Contacts`, but keep in mind the problems with this (see warning below)

Now you have created a collective "team" (*with the group account*). From now on, you can share pretty much everything you do in Nextcloud with this team: files, calendars, Kanban boards (Deck app), polls, etc.

However, there is one thing to keep in mind: `Ownership`. All files (*including calendars, Kanban boards, etc*) always belong to the account that created them! Even if these **resources** (*technical term*) are then shared with the entire team, they still **belong** to the creator account.

“ [!warning]

If the creator account of a resource is suddenly deleted, all files belonging to that account will also be deleted!

“ [!tip]

It is therefore highly advisable to create all shared resources with the **group account** and share them with the team from there.

ownership & sharing concept

The graphic above shows that the group account uploads a password database to its files and then shares this file with the team. They can then access this file.

This makes it easy to add or remove people from your team/collective later on. You don't have to share all resources again for each new person. You can also easily pass on the administration of the admin account, and it's no problem if the original admins become inactive.

Conversely, individual accounts can be removed from the team with a single click, so that they no longer have access to group resources.

Transfer ownership

If you ever lose access to the group account, you can transfer ownership of a file created from your personal account to the group account. Nextcloud provides its [own instructions for this](#).

- However, the transfer must always be confirmed by the group account (*to which ownership is being transferred*) before it takes effect.
- Experience has shown that it can take a few minutes for the group account to receive the confirmation notification. You may therefore have to wait a little while.

Credit: This article was partly influenced and copied from

<https://wiki.systemli.org/howto/nextcloud/gruppen>

Vera-Crypt-Encryption: Vera-Crypt-Encryption

“ [!toc] Table of Contents

The software [VeraCrypt](#) is required for all methods mentioned here. This means that this program must be installed on your PC in order to encrypt and decrypt (reopen) encrypted storage, such as folders or USB sticks.

Encrypt entire hard drives/USB sticks or folders with VeraCrypt

There are two main ways to encrypt an entire USB stick or hard drive:

1. Create and encrypt a folder that is as large as the entire storage medium.
2. Encrypt the file system of the hard drive itself.

Because a lot can go wrong with option 2, we generally recommend option 1. This should not have any disadvantages. This also means that with option 1, the process for encrypting individual folders or the entire USB stick/hard drive is identical.

However, if the device to be encrypted is formatted with FAT32 and is larger than 4 GB, this will not work, which is unfortunately often the case.

“ [!technical] Details about FAT32

New USB sticks are often delivered with FAT32 formatting. This is a problem since files larger than 4 GB cannot be stored on FAT32 and similar formats.

Since the USB stick is probably larger than 4 GB, option 1 would also require a file (in this case - the encrypted folder file) larger than 4 GB to be created on it, which will fail in this case.

If your storage medium has this type of formatting, it must either be reformatted for option 1, which requires other software, or option 2 must be selected.

“ [!technical] Reformat your drive

By formatting your drive, you will lose access to your data. However, authorities might still be able to recover it. The following are instructions for reformatting your device to exFAT:

- On Linux: <https://linuxconfig.org/how-to-format-usb-with-exfat-on-linux>
- On MacOS: <https://support.apple.com/en-gw/guide/disk-utility/dskutl1010/mac>
- On Windows: <https://learn.microsoft.com/en-us/answers/questions/4281222/how-to-format-usb-drive-to-exfat-on-windows-10-home>

From now on, we will describe both options in parallel. If there are differences between the two options, they will be marked with the headings “Option 1” or “Option 2.” The rest applies to both options.

Open VeraCrypt

- Click on `Create Volume`

Screenshot of newly opened VeraCrypt

Option 1: Create file for encrypted container

The encrypted “folder” is actually just a file, called a *container* in VeraCrypt. We can only use it later as a normal folder when it is opened and decrypted via VeraCrypt.

“ [!info] Note {static}

- A VeraCrypt container is just a file for the PC
- For us, the container will look like a normal folder when decrypted

- Here, we select a “Encrypted file container”: `Next>`

VeraCrypt view: Encrypt File Container

- Then select `Standard VeraCrypt Volume` and `Next>`

Under the Location menu, we now select the location where VeraCrypt should store the container for us. This should, as said, be our USB stick/hard drive.

- First click `Select File`
- This will open the file manager. Navigate to the USB stick/hard drive that you want to encrypt.
- Now we create the container, which will later become our encrypted folder. Enter a name for the file in the field provided. The name is technically irrelevant, but it will be the name of the file that you will see later when you simply insert the stick and open it.

VeraCrypt Location Menu

- Confirm with `Save`

Option 2: Encrypt the entire file system

select partition drive

- `Standard VeraCrypt Volume` > `Next>`

device location view

Now we have to select the storage medium.

⚠ [!warning] Attention {static}

The list now shows all available storage media connected to the computer, including other hard drives, USB sticks, SD cards, etc.

All files on the device selected here will be irretrievably deleted, so make sure you select the correct device!

device selection list on Linux

It is usually helpful to look at the storage size to identify the correct stick. If you want to encrypt a hard disk that may be the same size as other connected storage media, you must look at the path/mount points, which can include the name of the device. In the above screenshots you can see **two devices** with 3 and 1 partitions: `nvme0n1*` and `sda*`. The listings directly below them are their separate partitions.

For example here, the upper `nvme0n1` device is a 1.8TB (~2TB) large SSD, while the lower `sda` one is a 29,3GB (~32GB) USB drive.

If you are still not sure which device or partitions is the correct one, remove the device you want to encrypt and check the list again. The ones that still show up, are not the right ones!

- Once you are sure which device should be encrypted, confirm the warning that all files on the selected device will be destroyed.

Encryption Options

The default settings should suffice. Explaining the technical details would go beyond the scope of this guide. If interested, you can read more about the different encryption [algorithms here](#).

- Click [Next>](#)

VeraCrypt encryption options

Option 1: Volume Size

Here we specify how large the container (folder) should be later. You can choose any size depending on the amount of free storage space available.

“ [!info] {notitle}

Just keep in mind that if you want to put a file that's 100 MB in the folder later, you should choose a bit more space here, like 110 MB. That's because the encryption itself takes up some space.

VeraCrypt view: select Volume Size

Option 1: Folder as large as the entire stick

As you can see in the image above, there is an extra checkbox to use all available space for creating the container (folder).

“ [!info] Example

So if there is already 1 GB of data on a 4 GB stick, the new container will be 3 GB with this option and the existing data will remain intact.

This is why we chose the first option at the very beginning, because with the second option, all data will be deleted if, for example, the wrong hard drive is

selected.

A warning appears stating that files larger than 4 GB cannot be stored on FAT32. You can simply click here, if you made sure, that your drive is not formatted as FAT32.

Set password

Here you can set the password that will be used to encrypt the container. You should choose a [strong password](#), otherwise it can be easily guessed.

It is best to generate and save a password using a [password manager](#) such as KeePass:

Screenshot KeePass with USB Stick Password

VeraCrypt view: set password

File system settings

Now we are asked whether we want to store files larger than 4GB in our folder.

Large Files yes or no

If you are sure that you do not want to do this, click , otherwise click . Next, a file system must be specified.

File System selection

- Select if you want to use the storage on Windows computers.
- Select if you only want to use the storage on Linux and MacOS.
- Select if you only want to use the storage on Windows and Linux. Although NTFS is not made for Linux itself, Linux can handle it fairly OK.

The respective platforms may be able to handle all formats, but these recommendations should work without any problems.

Quick Format

The checkbox next to is usually only available for option 2. It means that the storage will **not** be overwritten with random bits during encryption. The advantage of this is that, especially for large data carriers, the encryption process is extremely shortened and only takes a few seconds.

However, this also brings uncertainties with regard to security, which is why we only select this option if:

- No sensitive data has **ever** been stored on this storage medium. (*Never really means never, see [Data hygiene](#)*), or
- The storage medium is already encrypted, its password is not known to any adversary, and it is only being encrypted “again” (*for whatever reason*).

quick format warning

“ [!tip] {static}

The safest option is to use Quick Format only for brand new storage media!

Next, specify whether you want to use the storage medium on operating systems other than your current one (if in doubt, always select this option, just in case).

Cross platform support checkbox

Random generator

The “Random generator” window will now open. Without going into further detail, it should be noted here that good encryption depends on randomly generated data being “mixed in” with the encryption.

Since computers are not perfect at this, VeraCrypt asks you to make random movements with your mouse in the window. This slowly fills the blue bar under “Randomness Collected From Mouse Movements.”

Randomness Collector

The bar should be at least half full. The more the better!

- Click `Next>` once the bar is full enough

Encryption process

VeraCrypt now begins to encrypt the file in the specified size and with the selected settings. To do this, it first writes random "ones" and "zeros" to the entire container (unless `Quick Format` is selected). Depending on its size and speed, this can take from a few minutes to several hours.

encryption process with time prediction running

Change password later

You can also change the password of a VeraCrypt container later.

- Mount container

mount file

- Click `Change Volume Password`

change Volume Password

- Enter the old password at the top and the new password twice at the bottom. _(Tip: Generate and save passwords with a password manager)

set new password

move mouse for randomness collector

successfully changed

Vera-Crypt-Installation: Vera-Crypt-Installation

“ [!toc] Table of Contents

Downloading the installer file

To install VeraCrypt, you must first download the appropriate installer file. Installer files for various operating systems are available [on the VeraCrypt website](#).

Verifying the installer file

Before installing VeraCrypt, it is important to verify the authenticity and integrity of the downloaded installer file. Integrity means that the file has not been damaged or tampered with during the download. Authenticity means that we downloaded the file from the intended source and not from someone posing as VeraCrypt. The verification is done using two verification techniques: *checksums* and *PGP/GPG signatures*.

“ [!technical] How does the verification work?

The developers calculate a hash value from the file they make available for download. This quickly shows whether a file has been tampered with during download or is incomplete. The developers sign the hash value of the download file with their private PGP key. The result of this is called a signature. We can now verify the signature by trying to decrypt it with the appropriate public PGP key. A program usually helps us with this. The correct signature indicates that it was the developers themselves who provided the download file and the hash value.

Installing PGP

For the next steps, we need to install a program that can handle PGP signatures. This is already pre-installed on Linux. For Windows, it must be [downloaded here](#) and installed. For MacOS, [homebrew can be downloaded](#) and installed.

Downloading, verifying, and importing the developers' public key

First, we need the developers' public PGP key. This allows us to verify that the signature of the download file is correct. The public key can be [downloaded here](#) and saved under Downloads. Now you need to check that you have downloaded the correct key by comparing the public key fingerprint (a unique identifier for a key). To do this, open a CMD window in Windows or a terminal in Linux/macOS and enter the following:

```
cd Downloads
gpg VeraCrypt_PGP_public_key.asc
```

The fingerprint (36-digit number) that is displayed must match the one on the [Veracrypt website](#). If it does, the key is correct and can be imported. To do this, go back to the CMD window in Windows or the terminal in Linux and enter the following:

```
gpg --import VeraCrypt_PGP_public_key.asc
```

Make sure that you are in the folder or directory in which the public key is stored, e.g. *Downloads*.

Download the signature from VeraCrypt

Now we need to download the signature matching the installer file [from the VeraCrypt website](#) and to save it in Downloads. It is important to download the signature that is directly behind the installer file you downloaded earlier.

Checking the signature of the installer file

Now we use the signature and the public key to check whether the installer file is complete and was actually downloaded from the VeraCrypt developers. To do this, open a CMD in Windows or a terminal in Linux/macOS and enter the following (**replace the placeholders in [] with your actual file names**):

```
gpg -verify [full name of the signature file] [full name of the installer file]
```

For example: `gpg --verify veracrypt-1.26.20-Ubuntu-24.04-amd64.deb.sig veracrypt-1.26.20-Ubuntu-24.04-amd64.deb`

The output should now read `"Signature OK from 'VeraCrypt Team (2018 - Supersedes Key ID=0x54DDD393) <veracrypt@idrix.fr>' [unknown]"`. The installer file is now trusted and can be installed. You can ignore the warning that the key does not have a trusted signature.

VeraCrypt Installation Process

Double-click on the installer file to install VeraCrypt.

Updating VeraCrypt

In some cases, VeraCrypt may prompt you to update automatically, which is the preferred update process since it is quick and simple.

If VeraCrypt does not ask to automatically update, a manual update works in the same way as the above. You need to download the installation file, verify it, and then install it again, replacing your outdated version. This should be done every time a new version is available.

Cryptomator

“ [!toc] Table of Contents

In this article we will describe how to set up Cryptomator. We highly recommend Cryptomator if you want to synchronize encrypted files to/from the cloud, as it is much faster than using VeraCrypt containers.

Installation

First install Cryptomator. If you use anything other than Linux, simply follow the [instructions](#) for your operating system. If you are using Linux you may want to use the Cryptomator [flatpak package](#). Depending on your distribution, you could also use your package manager repository, such as `apt` on Ubuntu/Debian or download the AppImage.

Setup

“ [!tip] **Cryptomator has [pretty good documentation](#)!** Go ahead and check it out for more detailed instructions on lots of other functionalities.

Follow these steps to create your first vault:

- Click the `+` symbol in the lower-left corner and select `Create New Vault` if you don't have one already.

fresh cryptomator install

- Choose a name for the new vault and click `Next`
- Choose the location where your vault should be stored. This will be the place where you will access all your files later. Click `Next`
- Don't change the "expert settings", just click `Next`

- Enter your new password. It is important to choose a [strong password](#) to have solid encryption.

⚠ [!warning] Recovery Key

A recovery key can decrypt your data, without knowing your password. This raises the question where to store the recovery key. As you hopefully know, passwords should be stored in a [good password manager](#). As long as your password is stored in a password manager and you have backups of your cryptomator vault and password database, you won't need a recovery key.

We often experienced that people simply stored the recovery key file on their desktop, although they secured all their passwords in a password manager. Doing this defeats the purpose of the password manager, so if you don't have a good strategy for securing your recovery key - just don't save it and [make regular backups](#).

- Finish creating your new vault.

Usage

After opening Cryptomator, press `Unlock` and enter your password. It also asks you whether to remember your password. If you use one of the built-in password managers of your operating system you can check that. Otherwise, leave it blank.

Now you see the general interface. With `Reveal Drive` you can directly open your decrypted vault, just as you can find it with your file manager.

screenshot: cryptomator interface

With `Lock` you will "close" the vault again, so that you will have to enter your password again.

Use Cryptomator in the Cloud

The huge benefit of Cryptomator is, that it can sync your encrypted vault to a cloud very efficiently.



[!tip] To do this, simply move your vault into your sync cloud directory. See our example on [setting up the sync client for Nextcloud](#).

Monero-Wallet

“ [!toc] Table of Contents

There are two main applications for using the Monero cryptocurrency on desktop operating systems:

- The official, open-source [Monero GUI wallet](#)
- The open-source [Feather](#) wallet.

From our experience, Feather is the most easy to setup and interact with.

Install Feather

Feather can be installed on all desktop operating systems. See their [documentation](#) for specific instructions. Especially for Linux, we would recommend [installing feather through flatpak](#) and not as a standalone executable or AppImage, as this is more secure.

Use Feather

With feather, you can easily send and receive Monero. Although we would like to add some tips in the future, for now refer to the official feather documentation. Have a look at:

- [Creating a new wallet.](#)
- [First Start](#)

For sending and receiving Monero, you will always have to use an "address" which you can think of as an anonymous and (if you wish) temporary IBAN.