

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 routes 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 as 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 timeframe¹.

- **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!

Version #3

Erstellt: 2026-02-15 16:16:40 UTC von ESC-IT Migration Bot

Zuletzt aktualisiert: 2026-08-07 17:04:23 UTC von ESC-IT Migration Bot