

PRIVACY GUIDE

GrapheneOS

The principles, in plain language

What it is, how it protects your phone and why it differs from stock Android.

01

What GrapheneOS is

GrapheneOS is an operating system for phones focused on security and privacy. It is developed by a non-profit, open-source project funded by donations. It starts from Android, but hardens it and removes what leaks the most data.

MORE SECURE

Added defenses so that a flaw in one app cannot take control of the phone.

MORE PRIVATE

No Google services by default, and permissions you can trim.

OPEN SOURCE

Anyone can review how it is built and check what it promises.

02

Four ideas first

With these four ideas, everything else makes sense.

1. **The operating system.** It is the program that controls the phone: it hands out memory, manages the screen and decides what each app may do. If it has a flaw, no app can fully protect you.
2. **Android.** It is the system used by almost every phone that is not an iPhone. Its foundation is open source, but each manufacturer, and above all Google, adds its own services to it.
3. **Permissions.** Each app asks for access to things like the camera, the location or the contacts. You decide what to give it and what not to.
4. **The sandbox.** It is a sandbox in the literal sense: each app lives in its own space and cannot see the others' or touch the system.

03

The problem: a phone trusts too much

On an ordinary phone, many apps and services with access to your data live side by side, and all that software has flaws. An attack usually exploits an error in an app or in a file you receive to break out of its box and take control.

> **The central idea.** GrapheneOS does not promise that the phone is invulnerable. It tries to make attacking it much harder and to make apps know far less about you.

04

The three principles of GrapheneOS

INSIDE

Isolate

Each app, each profile and each piece of the system in its own box.

OUTSIDE

Reduce

Switch off by default what is not needed and could be an entry point.

YOU

Control

Finer permissions to decide what each app sees.

Isolate: boxes within boxes

GrapheneOS strengthens Android's isolation. It also lets you create several profiles on one phone, each with its own apps, its own data and its own encryption keys. You can have a personal profile, another for work and another for an identity you do not want to mix. It is like having several phones inside one.

Reduce: fewer open doors

Every feature that is switched on is a possible route for attack, so the system turns off what you do not need. The USB port, while the phone is locked, only charges the battery. Radios such as Bluetooth, NFC and UWB come disabled from the factory. And defenses are added in memory, which is where programming errors tend to be exploited: the processor tags blocks of memory and blocks any access carrying the wrong tag.

Control: real permissions

Android already lets you say no to the camera or the location. GrapheneOS goes further. You can take away an app's internet access, stop it from reading the sensors, give it access only to certain files or show it an address book with only some contacts. If a calculator asks for internet, you can refuse and it will keep working.

> The three principles reinforce each other: isolating limits the damage, reducing gives the attacker fewer chances and controlling hands the decision about your data back to you.

05

From the power button to the screen

1. When you switch the phone on, a security chip checks that the system is what it should be. If it has been tampered with, it warns you.
2. The system starts and decrypts the data with a key that depends on your PIN or password. Without it, the contents are unreadable.
3. Each app runs in its own box, with only the permissions you have given it.
4. If the phone has been locked for a while, it restarts by itself: after the restart, the data is encrypted again until you enter the password.
5. Updates arrive often, download without bothering you and, if they fail, the system goes back to the previous version.
6. If someone forces you to unlock the phone, a duress PIN can wipe the device instead of opening it.

06

The apps you already use

GrapheneOS does not include Google's services, but that does not leave you without apps. If you need something that depends on Google, you can install Google Play like any other app.

IN A BOX

Sandboxed Google Play

Google Play works with no special privileges, inside a profile's isolation.

BROWSER

Vanadium

A hardened Chromium-based browser that is the system's web engine.

VERIFICATION

Auditor

Checks from another phone that the system has not been tampered with.

Why it matters

Normally, Google's services have very broad permissions over the system. Here, Google Play is just an app and has no more power than any other. Some banking or payment apps demand checks that only certified phones meet: it is worth trying them first.

07

How to get started

1. **Check that your phone is supported.** Official support is for Pixel models, from the 6 to the 10a. The Pixel 8 and later receive seven years of updates.
2. **Back up whatever you want to keep.** The installation wipes the phone completely.
3. **Install from the browser.** The official website guides you: you connect the phone by cable to a computer with Chrome or Chromium and follow the steps.
4. **Set a long PIN** or a password, enable automatic reboot and leave the USB port in its default mode.

REFERENCE

Quick glossary

TERM	MEANING
Operating system	The program that controls the phone and its apps
Android	The most widespread mobile system, with an open foundation
Sandbox	Isolated box in which each app lives
Permission	Authorization to access a feature or your data
Bootloader	First program to start and load the system
Verified boot	Check that the system has not been altered
MTE	Memory tags to block erroneous accesses
Profile	Separate space with its own apps, data and keys
Duress PIN	Special PIN that wipes the phone when entered

> **Next step.** The complete guide, "GrapheneOS in depth", explains each piece in more detail: verified boot, memory defenses, permissions, profiles, installation and the comparison with stock Android and iOS.

Sources: GrapheneOS website (features, FAQ and installation) and Android Authority.