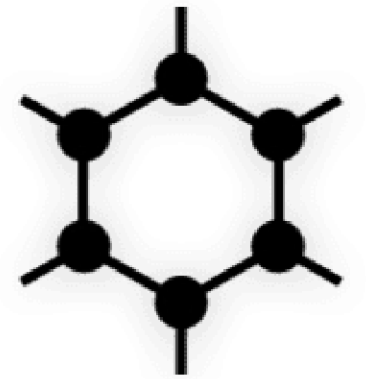


GrapheneOS

Guida all'installazione di GrapheneOS (con Web Installer)

Leggete la guida fino alla fine prima di iniziare l'installazione!

0. Perchè?

Graphene è un sistema operativo mobile open source (codice visualizzabile e modificabile) e sviluppato con l'obiettivo di salvaguardare la privacy e la sicurezza dellx utenti; qua potete trovare una lista completa di feature: https://grapheneos.org/features.

Graphene permette inoltre di avere molto più controllo sulle applicazioni installate sul proprio dispositivo, quindi evitare sia I servizi Google sia le app installate di default e impossibili da disinstallare (tipo il Facebook di turno). È tuttavia possibile anche utilizzare le app Google se si necessitasse.

Infine, secondo le ultime informazioni di cui disponiamo, non è ancora possibile aprire con Cellebrite[1] molti dispositivi con GrapheneOS installato, quindi in caso di sequestro potrebbe essere un vantaggio non indifferente. https://osservatorionessuno.org/blog/2025/03/a-deep-dive-into-cellebrite-android-support-as-of-february-2025/[2].

1. Dove?

Purtroppo al momento è possibile installare GrapheneOS solo su telefoni Google Pixel. Qua trovate una lista completa dei modelli: https://grapheneos.org/releases#devices. Alcuni modelli decisamente costosi, ma quelli meno recenti si trovano usati in buone condizioni sui 100 euro.

È stata recentemente annunciata una collaborazione tra Motorola e GrapheneOS, quindi ci aspettiamo che in futuro anche alcuni telefoni Motorola consentano di installare questo sistema operativo.

1 Cellebrite è una compagnia israeliana che ha sviluppato diversi software, tra cui uno celebre è Cellebrite UFED (Universal Forensics Extraction Device), ossia uno strumento capace di estrarre I contenuti dai telefoni. È stato usato diverse volte dalla polizia in caso di sequestro di dispositivi; è utilizzato anche al di fuori dell'Italia.

2 L'articolo è del 2025 quindi è possibile che la situazione sia cambiata o cambi in futuro.

2. Backup

Installando Graphene, tutto ciò che c'è sul dispositivo verrà irrimediabilmente cancellato. Per questo, prima di procedere è importante pensare a cosa c'è sul telefono, cosa vogliamo salvare, e come farlo.

Di norma, se vi è un account Google collegato sul telefono, si potrà realizzare un backup tramite I loro servizi. Andando nelle impostazioni del backup, si può scegliere cosa salvare e cosa no. Tuttavia, **non** sarà possibile ripristinare il backup Google direttamente su Graphene, se non utilizzando uno strumento terzo. Invece, dopo aver effettuato il backup, si potranno reimportare manualmente contatti, foto, video, documenti, esportandoli da Google Drive e importandoli sul dispositivo. Altre applicazioni dovranno essere reinstallate e riconfigurate da zero.
Se non volete caricare il backup del vostro dispositivo su Google, potete esportare/copiare manualmente su un pc/hard disk le informazioni che volete salvare (contatti, foto, documenti, ecc…).

Signal necessita di una procedura a parte. Innanzitutto bisogna controllare se si è inserito un PIN per la registrazione (che verrà richiesto ri-registrando il numero), e nel caso salvarlo. Bisogna poi andare nelle impostazioni di Signal, in backup, e operare un backup sul dispositivo; verrà generata una passphrase di 30 caratteri da salvarsi. Bisognerà poi spostare la cartella del backup dal telefono ad un altro dispositivo (es un pc). Infine quando verrà re-installato Signal su Graphene bisognerà rispostare la cartella del backup sul dispositivo, importarlo e inserire la passphrase.

Whatsapp: solitamente I backup di Whatsapp sono salvati sull'account Google e non sono crittografati. Si consiglia innanzitutto di abilitare la crittografia. È anche possibile fare un backup in locale, che come per Signal dovrà essere copiato su un altro dispositivo per poi essere reimportato.

3. Web Installer

Usare il Web Installer è il metodo più facile per installare Graphene, poichè si opera facilmente dalla pagina web. Ecco il link alla pagina: https://grapheneos.org/install/web.

Prerequisiti:

- un pc, o un altro telefono con uno di questi browser: Chromium, Vanadium, Google Chrome, Microsoft Edge o Brave (con Brave Shields disabilitato)
- un cavo USB dati; preferibilmente, se il pc ha una porta USB-C, di quello fornito con il telefono.

Passaggi:

a. Nelle impostazioni del telefono, cercate il **build number** e cliccateci sopra diverse volte. Vedrete che andando avanti vi comparirà un pop-up in basso che vi avviserà del fatto che state per abilitare le **opzioni sviluppatore**. Infine vi verrà chiesto di inserire la password del dispositivo per autorizzare questa operazione.
b. Una volta in modalità sviluppatori, abilitate **OEM unlocking**[3].
c. **Spegnete il telefono** (nei modelli Pixel, bisogna premere il tasto di spegnimento e quello del volume insieme).
d. Riaccendete il telefono ed entrate nell'**interfaccia bootloader**[4]. Questo si può fare premendo il tasto di accensione e nel mentre il tasto per abbassare il volume.
e. A questo punto potete connettere il dispositivo al pc con il cavo. Se avete USB guard attivato sul pc, ricordatevi di autorizzare il telefono.
f. Ora **sbloccate il bootloader**: navigate nella pagina di installazione fino alla sezione "Unlocking the bootloader"; premete il pulsante subito sotto. Vi si aprirà un pop-up che chiede conferma di quale sia il dispositivo su cui fare questa operazione; se non vedete il telefono, provate a scollegare e ricollegare al cavo usb, oppure a spegnere il telefono e rientrare nel bootloader. Se il problema persiste, provate a cambiare cavo o porta USB.
g. La richiesta deve essere **autorizzata** sul telefono: usate

3 Sta per "Original Equipment Manufacturer". Sbloccare OEM dà la possibilità di sbloccare il bootloader e modificare il sistema operativo che è in funzione sul telefono; a volte viene attivato anche per accedere ad altre impostazioni di sviluppo. In generale, a meno che non serva per qualcosa di specifico, è meglio tenere OEM bloccato.

I tasti del volume per selezionare l'opzione corretta e successivamente premete il tasto di accensione per confermare.
h. **Scaricare l'immagine** del sistema operativo Graphene: nella sezione "Obtaining factory images" potrete premere il pulsante, e come prima aprirà un pop-up che chiede conferma di quale sia il dispositivo corretto. Una volta selezionato, procederà a scaricare automaticamente la versione corretta di Graphene, e quando avrà terminato ve lo segnalerà subito sotto al pulsante.
I. **Flashare l'immagine**[5]: nella sezione "Flashing factory images" troverete il pulsante corrispondente; premetelo e attendete che abbia finito di fare tutte le operazioni. Potrebbe durare qualche minuto, durante I quali non bisogna interagire con il dispositivo.
j. Una volta che l'immagine del sistema operativo è stata flashata, dovete **ribloccare il bootloader**, un'operazione molto simile a quella di sblocco: nella sezione "Locking the bootloader" troverete il tasto corrispondente. L'operazione dovrà essere confermata sul dispositivo, usando I tasti del volume per muoversi tra le opzioni e quello di acensione per confermare.
k. Scollegate il dispositivo e accendetelo. Inizierà la sequenza di configurazione; tra I vari passaggi è molto importante ricordarsi di **disabilitare OEM unlocking** (quello che abbiamo abilitato per rendere possibile l'installazione).

Magagne:

- se avete Arch come sistema operativo sul pc, dovete installare il pacchetto android-udev; se avete Debian o Ubuntu, il pacchetto android-sdk-platform-tools-common.
- Chromium su Ubuntu non funziona.
- non usate la modalità Incognito o simili per l'installazione, perchè solitamente viene allocata poca memoria.
- per altre magagne, chiedete allx amichx informatichx, lx quali probabilmente chiederanno con voi ad internet. Molti

4 Il bootloader è un programma che fa partire l'immagine del sistema operativo. Per questo motivo, per installarne uno nuovo è necessario che sia sbloccato.
5 Flashare un sistema operativo significa installarlo nella memoria del dispositivo, cosa che permette di cancellare quello vecchio e utilizzare quello nuovo.

problemi sono già stati segnalati a Graphene e sono inclusi nel sito.

4. Next steps

App store

Di default esiste quello di Graphene che si chiama App Store. Da lì è possibile scaricare Accrescent, un app store incentrato sulla sicurezza; all'interno c'è una selezione di poche (molto poche) applicazioni disponibili. Altre opzioni sono:
- F-Droid: scaricabile da https://f-droid.org/, è uno store di applicazioni open source. Questo non significa necessariamente che tutte le applicazioni siano benevole, quindi fate attenzione!
- Aurora Store: scaricabile da F-Droid (vedi sopra - https://f-droid.org/en/packages/com.aurora.store/), è un client open source per Google Play (che significa che potete trovare tutte le app del Play Store). Si può utilizzare sia con un account Google sia con una sessione anonima.
Se siete paranoichx andate a leggervi questo: https://privsec.dev/posts/android/f-droid-security-issues/#conclusion-what-should-you-do
- Obtainium: non è un vero e proprio app store, ma consente di scaricare l'applicazione direttamente dai repository[6] ufficiali (tipicamente dalla pagina github). Nonostante sembri complesso è un'ottima opzione.

Google

Su Graphene è possibile installare i Google Play Services[7] in maniera sandboxata[8], ed online si trovano principalmente due approcci:

1. Su un altro profilo[9]: su android in generale è possibile configurare diversi profili utente completamente separati da quello principale che permette una compartimentazione completa.

6 Sostanzialmente un luogo virtuale in cui sono conservate tutte le componenti per un software.
7 Pacchetto proprietario di Google che include servizi di background e librerie per altre applicazioni (come Play Store, autenticazione, contatti, localizzazione, ecc...)
8 Esistono vari approcci per installare o sostituire questi servizi. Graphene sceglie di installarla come un App classica quindi potendo gestire ogni permesso e configurazione.
9 https://source.android.com/docs/devices/admin/multi-user

2. Sul private space[10]: è simile ad avere un altro profilo, tuttavia non garantisce lo stesso livello di compartimentalizzazione (ad esempio uno spyware può passare con facilità da uno spazio all'altro, ma le app che sono nel private space non possono avere dati su quelle al di fuori e viceversa).
In generale avere I servizi Google potrebbe tornare utile per alcune applicazioni come quella della banca o dello spid.

Alcune configurazioni possibili

- disabilitare 2G: Impostazioni → Rete e internet → SIM (dovete selezionare la SIM che state usando) → Protezione rete 2G
- PIN/password/biometria:
    a. PIN: almeno 10 cifre. Si può attivare lo Scramble Pin (mette I pulsanti dei numeri in posizioni diverse)
    b. Password: anche qui, almeno 10 caratteri.
    c. Biometria: valutate se metterla in base al vostro modello di rischio[11]. Su Graphene è anche possibile usare l'impronta e un PIN insieme.
    d. Duress password: si può impostare una password (diversa da quella di sblocco) che se inserita attiva un reset alle impostazioni di fabbrica.
- Autoreboot: per motivi di sicurezza[12] può essere utile fare sì che, se il dispositivo non viene sbloccato per un numero di ore, si riavvi da solo automaticamente.
- USB-C port: charging-only when locked (quando il dispositivo è bloccato, è possibile solo caricare il telefono e non trasferire dati).

Cercate altre guide

Queste sopra sono solo alcuni consigli, ma è bene che ogni persona spulci le impostazioni e configuri il proprio dispositivo a seconda del modello di rischio suo e della comunità che lx circonda.

10 https://discuss.grapheneos.org/d/16670-private-space-on-android-15-grapheneos
11 Ad esempio, se vi dovesse servire accedere al dispositivo molto in fretta per far partire wasted (un'app che effettua un reset alle impostazioni di fabbrica) la biometria potrebbe essere un'opzione utile. Ricordate però anche che è molto facile costringervi allo sblocco.
12 Riprendendo il link di sopra di Osservatorio Nessuno riguardo a Cellebrite, si può fare una differenza sulla facilità di accedere al dispositivo BFU (Before Fisrt Unlock, quindi dopo un riavvio/un'accensione) e AFU (After First Unlock, quindi dopo che il dispositivo è già stato sbloccato una volta)

Inoltre online sono disponibili molte altre guide che forniscono liste di strumenti, applicazioni e attenzioni per mantenere privacy e sicurezza di telefoni (e non solo!).