Tutoriels Téléphonie

GrapheneOS

Difficulté ★ ★ ★ ☆ ☆ Temps requis 1h

Objectif

GrapheneOS est un système d'exploitation alternatif à Android qui renforce fortement la sécurité d'un téléphone.

Étapes

keyboard_arrow_right Installation sur un téléphone adapté

keyboard_arrow_right Paramétrage adapté au modèle de menace

Prérequis

task Connexion internet "anonyme"

Matériel requis

sell Téléphone `Google Pixel 6` ou plus récent

sell câble USB-C qui permet l'échange de données

sell ordinateur ou smartphone Android avec le navigateur Google Chrome

Intérêts de la mesure

thumb_up Avoir un téléphone de confiance

Inconvénients

thumb_down Rares problèmes de compatibilité avec certaines applications

thumb_down Prix (~150€)

— Introduction et parti pris

Conseil

Ce tuto n'est pas exhaustif, ni sur tous les paramétrages intéressants, ni sur les pratiques de sécurité non-numériques à avoir autour, et se concentre sur les paramètres qui nous semblent important vis-à-vis de la sécurité ainsi que des points de vigilance à avoir. C'est ce que nous connaissons de mieux et le recommandons au plus grand nombre, toutefois attention à ne pas y faire confiance aveuglément, des erreurs techniques et humaines restent possibles.

— Choix du téléphone

Les Google Pixel sont les seuls téléphones à répondre aux exigences de sécurité du projet ☼ GrapheneOS - notamment grâce aux composants qui sécurisent la mémoire et aux protections qu'ils conservent pour les versions modifiées d'Android.

Le choix du téléphone se fait ensuite sur la durée de mise à jour dont il va bénéficier : les plus récents sont plus chers mais sont maintenus pendant encore 5 ans, là où les plus vieux encore supportés ne le sont que jusque juillet 2027, tout en étant beaucoup plus accessibles (autour de 170 € d'occasion ou neuf)[2].

Déverrouillage de l'OEM[1]

Certains téléphones avec des références US n'ont pas la possibilité de déverrouiller l'OEM[1] pour installer ☼ GrapheneOS[4].

Nous n'avons pas trouvé de solution pour les téléphones achetés en ligne autre que les renvoyer, mais pour les achats d'occasion n'hésite pas à faire la première étape du tuto devant la personne pour ne pas être bloqué·e ensuite.

Pour chaque numéro de version, la version `Pixel *a` est à privilégier, car elle se trouve pour moins cher, a des composants un peu moins performants qui font que la batterie tient plus longtemps.

- `Pixel 6a` : supporté jusqu'en juillet 2027. On en déniche à 100-130€ d'occasion en Mars 2026
- `Pixel 7a` : supporté jusqu'en mai 2028. On en déniche à 150-180€ d'occasion en Mars 2026
- `Pixel 8a` : support jusqu'en mai 2031. On en déniche à 200-250€ d'occasion en Mars 2026. Le processeur de ce modèle implémente une nouvelle sécurité matérielle qui réduit les possibilités d'exploitation de failles : le memory tagging. Si tu as le budget et que tu as un modèle de menace élevé, privilégie ce téléphone[3]

Le *support* du téléphone mentionné ici est relatif aux mises à jour de sécurité du microcode des composants internes fournies par Google. GOS fournit en général un support étendu en continuant à diffuser des mises à jour de sécurité pour les téléphones en fin de vie. Un *Pixel 6a* dont le support de Google est dépassé mais qui bénéficie toujours des mises à jour du système d'exploitation par GOS, sera a priori toujours plus sécurisé qu'un téléphone bas de gamme neuf. Mieux sécurisé face aux outils d'extraction physique des flics type *Cellebrite* (grâce à sa puce de sécurité Titan M2 dont aucun contournement n'est connu), mais également face à des malware mercenaires contre lesquels GOS met en place tout un ensemble de contre-mesures.

— Installation de GrapheneOS

Elle est simple, tant que l'on suit scrupuleusement les étapes indiquées. Rends-toi sur https://grapheneos.org/install/web et suis le déroulé du tutoriel.

En voilà les grandes lignes :

1. **Déverrouillage de l'**OEM[1] (la protection du système d'exploitation installé) : va dans `Paramètres > À propos` et clique 7 fois sur `Numéro de build` pour déverrouiller le mode développeur. Puis va dans `Paramètres > Options pour les développeurs`, et clique sur `Déverrouillage OEM`
2. **Démarre le bootloader du téléphone** : redémarre le téléphone en maintenant le bouton "volume bas" jusqu'à arriver sur l'interface bootloader
3. **Connecte le téléphone à ton ordinateur ou à un autre Pixel GrapheneOS** par un câble USB (attention si le tel n'est pas détecté, certains câbles ne font que recharger), puis clique sur le bouton `Unlock bootloader` sur cette page web : grapheneos.org/install/web. Confirme cette commande en appuyant sur les boutons volumes du téléphone pour changer la sélection, puis le bouton de démarrage pour confirmer
4. Clique sur le bouton `Download release` pour télécharger la dernière version de GrapheneOS

5. Clique sur le bouton `Flash release` pour l'installer ; ne touche pas au téléphone tant que l'installation n'est pas finie et que le téléphone n'est pas revenu sur l'interface du bootloader
6. Verrouille en cliquant sur le bouton `Lock bootloader` puis confirme la commande avec les boutons de volume sur le téléphone
7. Sélectionne `Start` sur le téléphone et confirme avec le bouton de démarrage pour lancer GrapheneOS. Il affichera ensuite un magnifique `Your device is loading a different operating system` ; c'est super ! Ça veut dire que ça a marché et qu'il faut maintenant te faire à cet écran un peu flippant, il sera affiché à chaque démarrage :)

— Paramétrage de GrapheneOS

Une fois GrapheneOS installé, ces paramètres à définir depuis la session *propriétaire* permettent de limiter les fonctionnements du téléphone qui pourraient apporter des failles exploitables par un logiciel espion :

- Côté installation d'applications, pour éviter les applis non à jour et la multiplication des droits d'installation, nous recommandons d'**utiliser uniquement le** `Google Play Store` sur la session *propriétaire* avec un compte créé exprès pour cette session qui ne servira à rien d'autre :
  - Ouvre `App store`, télécharge le `Google Play Store` puis ouvre-le
  - Crée un compte Google 'bidon'. La création de ce compte ne nécessite pas de numéro de téléphone ou d'adresse e-mail. N'utilise pas de VPN à cette étape-là ! N'utilise jamais ce compte Gmail par la suite.
  - Comme première appli, tu peux par exemple télécharger et connecter un VPN ♥ *(pour les sessions peu utilisées, Proton VPN en gratuit fonctionne très bien)* : Connexion internet "anonyme"
- `Paramètres > Sécurité et confidentialité > Déverrouillage de l'appareil` :
  - Si ce n'était pas le cas à l'installation, mets **un mot de passe d'au moins 18 chiffres aléatoires** (ou 5 mots aléatoires, plus facile à retenir mais plus lourd au quotidien)
  - Active le PIN `Duress password`, qui effacera toutes les données s'il est renseigné ; mettre un nombre facile à retrouver, par exemple sa date de naissance. Cependant, évite de mettre ton ancien code ou un code si courant que toi ou une autre personne pourraient taper par erreur, que tes données pourraient être effacées accidentellement par ton entourage
- `Paramètres > Sécurité et confidentialité > Exploit protection` :
  - Auto reboot : le mettre à 8h ou moins
  - USB-C port : `charging-only when locked`
  - Mets `Turn off Bluetooth automatically` sur 30 minutes

- Désactive les paramètres `WebView JIT, Dynamic code loading via memory` et `Dynamic code loading via storage`

Cela provoquera une notification pour les applications qui sont perturbées par ces limitations. Tu peux ignorer si l'application fonctionne ou désactiver la protection, la mesure de protection spécifique qui la fait planter. * `Paramètres > Réseau et Internet > Internet connectivity checks` * Choisis `Standard (Google) server` * Le téléphone envoie de simples ping à un serveur sans passer par le VPN pour vérifier qu'il est connecté à Internet. Cette option permet de cacher à l'opérateur téléphonique que tu utilises GOS.

> **Appels WiFi**
>
> Le VPN du téléphone ne s'applique pas au paramètre `Appel WiFi`, donc laisse-le désactivé au risque d'exposer ton IP à ton opérateur téléphonique

— Les stratégies d'utilisation

Afin de limiter le risque d'infection et cloisonner les différents usages du téléphone, GrapheneOS facilite l'utilisation de **multiples sessions utilisateurs cloisonnées**.

> **Information**
>
> Le VPN est pris dans le cloisonnement, il en faut donc un par session et/ou par espace (avec possibilité d'utiliser les versions gratuites de confiance pour les sessions peu utilisées)

Configuration 1 - le téléphone militant sans SIM :

Un téléphone sans carte SIM utilisé seulement en WiFi pour ses activités militantes.

> **Principe :** La session principale a des permissions plus étendues, ne l'utiliser QUE pour installer les applications. Chaque usage (militant ouvert, confidentiel++, com' et réseaux sociaux, ...) est ensuite cloisonné sur sa propre session secondaire, qui peut facilement être supprimée ou recréée.

C'est la meilleure manière sur un appareil de limiter les possibilités qu'un logiciel espion puisse s'installer et ensuite corrompre d'autres usages que celui par lequel il s'est diffusé, mais ce n'est pas une étanchéité magique et ne permet pas la même confiance que l'usage d'appareils distincts ou l'absence de communication numérique.

- **Ajouter un profil et le configurer**

- Va dans `Paramètres > Système > Utilisateurs > Ajouter un utilisateur` (choisis un nom quelconque)
- Change le paramètre : `App installs and updates > Enable for first party sources only`
- Reviens en arrière et dans `Installer les applis disponibles`, choisis l'appli de VPN que tu utiliseras sur le profil
- Passe au nouveau profil pour lui mettre un super mot de passe (ce peut être le même que la session propriétaire, sauf si tu vas le déverrouiller souvent dans la journée et qu'il y a un risque qu'un attaquant ou une caméra te voit le taper, auquel cas il vaut mieux choisir un mot de passe distinct de la session propriétaire pour ne pas risquer qu'elle soit infectable) et **active le VPN**
- `Paramètres > Notifications > Notifications sur l'écran de verrouillage > Désactiver` : Empêche les notifications sur l'écran de verrouillage pour éviter que n'importe quelle personne qui ait le téléphone dans les mains puisse lire du contenu via les notifications

- **Installer des applis**
  - Reviens sur la session *propriétaire*, utilise le PlayStore pour installer les applis voulues, puis désactive-les : dans la liste des applis, reste appuyé sur l'icône des nouvelles installées `> ⓘ Infos sur l'appli > Ø Désactiver`
  - Dans `Paramètres > Système > Utilisateurs > "Utilisateur X" > Installer les applis disponibles >` choisis les applis utiles pour l'usage de la session, comme par exemple :
    - Signal
    - CoMaps *(GPS)*
    - Jitsi Meet *(visios)*
    - FairEmail
    - ProtonVPN
    - SimpleX → Installation de SimpleX
    - OpenDocument Reader
  - Certaines applis peuvent nécessiter les `Google Play services` pour fonctionner correctement, à tester si jamais tu rencontres des problèmes *(type Signal qui ne passe pas commande d'un SMS de confirmation pour la création d'un nouveau compte)*
- Partager des infos entre sessions, deux méthodes :
  - Moyennement sécu mais rapide et simple à utiliser :
    a. avoir un compte `Telegram` partagé sur chaque session
    b. se faire passer les infos dans les messages persos enregistrés

- Propre, mais plus longue à paramétrer la première fois :

c. Dans la session propriétaire, ouvre l'`App store` et installe `Accrescent`, puis dans `Accrescent` installe `Inter Profile Sharing`, et désactive-le pour cette session pour l'installer seulement dans les sessions utilisées

d. Passe dans chaque session pour ouvrir `Inter Profil Sharing`, lui donner les accès nécessaires puis va sur l'icône ⚙ `Paramètres` en haut à droite pour y `Activer le chiffrement` (en utilisant par exemple ton **code à 18 chiffres**)

e. Le partage fonctionne ensuite en ouvrant l'appli dans la session source pour partager un texte copier ou un fichier, puis en se rendant dans la session qui en a besoin pour récupérer le texte ou fichier depuis la notification (si aucune notification s'affiche, ouvre `Inter Profil Sharing` pour la re-déclencher)

✓ **Les astuces du quotidien**

- Il n'y aura aucune notification d'application d'une session qui n'a pas été déverrouillée une première fois

⚠ **Inconvénients résiduels…**

- Musique : coupure de la connexion Bluetooth et de la musique au changement de session
- Si SIM : seule la session principale peut gérer le partage de connexion

Configuration 2 - le téléphone du quotidien / collectif :

Un téléphone pour celles et ceux qui ont besoin d'avoir une carte SIM en permanence (activité pro, SIM perso…).

> **Principe :** il n'y a que la session propriétaire qui est utilisée, et les applications capitalistes ou pouvant t'être reliées sont utilisées dans l'espace privé

- **Paramétrer l'espace privé**
  - L'activer dans `Paramètres > Sécurité et confidentialité > Espace privé` *(tu peux y mettre le même déverrouillage que le téléphone)*
  - Change le paramètre `Verrouiller l'espace privé automatiquement` à `Uniquement après le redémarrage de l'appareil` (ça signifie qu'il ne faut pas oublier de déverrouiller l'espace privé dans la liste des applications à chaque redémarrage)
  - Choisis les applications du profil principal à y installer par `Installer les applis disponibles` → l'espace privé doit avoir son propre VPN ! C'est bien de commencer par ça :)

- **Utiliser l'empreinte**
  - Ce n'est pas le plus recommandé, mais suivant les usages du téléphone, il est préférable d'utiliser le déverrouillage par empreinte plutôt qu'avoir un mauvais mot de passe. Tu peux configurer un auto-reboot assez court (par exemple **1h**), ce qui maximise les chances que ton téléphone soit dans un état BFU avant d'être dans les mains des flics (un contrôle qui tourne mal, ou une perquisiotion à 6h)
- **Allonger le temps de verrouillage**
  - Dans `Paramètres > Sécurité et confidentialité > Déverrouillage de l'appareil`, augmenter `Verrouiller après la mise en veille` à 30 sec et désactiver `Verrouiller instantanément avec le bouton Marche/Arrêt` *(le téléphone reste verrouillé instantanément en tentant de l'éteindre puis en cliquant sur Verrouiller)*
- **Le partage de connexion et appel wifi**
  - Il n'est possible que depuis la session propriétaire — d'où l'intérêt de cette configuration si tu utilises une carte SIM - toutefois attention : comme sur les autres téléphones, celui-ci comme les appels WiFi, ne passe pas par le VPN de la session ! Chaque appareil doit avoir son propre VPN, et il ne faut pas activer l'option `Appel Wifi` *(c'est une option qui permet avec certains opérateurs d'échanger en clair quand un WiFi est connecté et que le réseau GSM passe mal, voir* `Paramètres > Réseau et Internet > Carte SIM > Opérateur > Appels Wi-Fi` *–et si le paramètre n'y est pas c'est que ton forfait ne le permet pas)*
- **Désactive la 2G**
  - `Paramètres > Réseau et Internet > Sécurité du réseau mobile > Protection réseaux 2G`

Les astuces du quotidien

- Personnaliser les raccourcis de paramètres du panneau de notification pour y ✈! **enlever le mode avion**. Il est plus compliqué d'y accéder en devant aller dans les paramètres, mais ça aurait évité de fausses manip' à quelques camarades ♥
- Attention aux réveils qui peuvent provoquer le rallumage du téléphone quand il est éteint → le mettre en mode avion avant de l'éteindre pour ce type d'erreur, c'est super !

Retour sur les points d'attention

- Le VPN est pris dans le cloisonnement, il en faut donc un par espace (avec possibilité d'utiliser les versions gratuites de confiance pour les sessions peu utilisées)
- Certains téléphones avec des références US n'ont pas la possibilité de déverrouiller l'OEM pour installer GrapheneOS[4]. Nous n'avons pas trouvé de solution pour les téléphones achetés en ligne autre que de les renvoyer. Cependant, pour les achats d'occasion, n'hésitez pas à faire la première étape du tuto devant la personne pour ne pas être bloquée ensuite.

— Vrac d'astuces autres

- Possibilité de combiner les configs 1 et 2, en cloisonnant les applis les moins fiables (Whatsapp & co…) d'une session secondaire dans l'espace privé.
- Priorise l'utilisation d'applications pouvant fonctionner hors ligne pour limiter la dépendance aux connexions en déplacement (type CoMaps avec la carte du pays pour le GPS, Thunderbird ou FairEmail plutôt que l'interface web pour les mails, …)

Installation d'applications bancaires

La *Play Integrity* API sous le viseur

Le Play Integrity pose également des problèmes géopolitiques ; ça revient à donner à Google un pouvoir de veto sur l'installation des applications les plus critiques : banque, identité, services publics. Un consortium européen lance un projet libre d'attestation de sécurité baptisé *UnifiedAttestation *permettant de valider des appareils avec des ROM alternatives (/e/OS ou GOS) ou reconditionnés s'il est supporté par les banques. Cela va de pair avec un projet d'application d'identité unique à l'échelle de l'UE, le UEDI Wallet, qui doit rentrer en application dans les États membres en 2026 et être obligatoirement accepté par les banques en 2027.

- GOS produit une documentation sur la compatibilité des applications bancaires → sur leur forum (en)
- Privsec.dev maintient à jour une liste communautaire des compatibilités des applications bancaires avec GOS, et des désactivations éventuelles de protections de GOS à appliquer pour qu'elles fonctionnent. Tu peux consulter **ici** la section concernant la France

Les applications bancaires font appel à la PIA pour définir si un téléphone est rooté ou qu'une ROM alternative (comme GrapheneOS) est installée, et éventuellement bloquer la connexion si c'est le cas. C'est un sujet de discussion récurrent et volubile sur le forum de GrapheneOS.

Cependant un contournement est permis par GOS ; il est possible de **bloquer** simplement la vérification de l'intégrité, et cela fonctionne sur certaines applications.

Pour cela, `faire un appui long sur l'icône de l'application > infos sur l'appli > Play Integrity API > Blocked`

Souvent, ces applications vont aussi nécessiter d'activer `Exploit protection compatibility mode` dans le même menu.

Ressources externes

- (en) GrapheneOS sur anarsec.guides
- la brochure "GrapheneOS pour les anarchistes" qui traduit principalement le guide ci-dessus en français
- le blog https://wonderfall.space/ (ne semble plus être encore entretenu) avec de nombreux articles détaillés sur GOS et des prises de positions non consensuelles sur la sécurité
- https://1312blogs.org/arg/installation-et-configuration-de-grapheneos

2025-12-082026-08-09

---

1. Le déverrouillage de l'OEM désigne le déblocage de la possibilité d'accéder au système de fichiers et d'y installer un autre OS depuis le mode recovery. C'est comparable au fait de démarrer sur une clé bootable pour installer une distribution Linux. Mais, pour les ordinateurs, il n'y a pas réellement de sécurité qui empêche de démarrer sur un autre système d'exploitation. ↩ ↩ ↩
2. https://grapheneos.org/faq#device-lifetime ↩
3. https://discuss.grapheneos.org/d/8439-mte-support-status-for-grapheneos ↩
4. https://discuss.grapheneos.org/d/11788-oem-unlocking-carrier-locked ↩ ↩
5. https://discuss.grapheneos.org/d/3158-wifi-calling-bypasses-vpn/6 ↩