Installer et paramétrer GrapheneOS

Info

`Prérequis`

- *lien vers les documents en commençant par @*

  `Intérêts de la mesure et menaces qu'elle permet de tempérer`

  `Difficulté`

  intermédiaire *(outil peu user friendly qui peut repousser certain·e·s, inconvénients d'utilisation/perte de praticité notable mais globalement facile en suivant les instructions*

  `Temps requis` 1h

  `Matériel requis`

- Téléphone de marque `Pixel 6` ou plus récent, compatible avec https://grapheneos.org/faq#supported-devices
- câble USB-C qui permet l'échange de données
- ordinateur avec le navigateur Google Chrome

  `Inconvénients`

  Rares problèmes de compatibilité avec certaines applications

  `Ce qu'on va faire dans ce tutoriel`

- installer et paramétrer https://grapheneos.org , un système d'exploitation alternatif à Android qui renforce fortement la sécurité d'un téléphone

Vocabulaire

Concept : blabla

Introduction et parti pris

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). Voir le détail ici → https://grapheneos.org/faq#device-lifetime

Déverouillage de l'OEM

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

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

Installation de GrapheneOS

Elle est simple, tant que l'on suit scrupuleusement les étapes indiquées. Il faut se rendre sur https://grapheneos.org/install/web et suivre le déroulé du tutoriel.

En voilà les grandes lignes :

1. Déverrouillage de l'`OEM` (la protection du système d'exploitation installé) : allez dans `Paramètres > À propos` et cliquer 7 fois sur "`Numéro de build`" pour déverrouiller le mode développeur. Puis aller dans `Paramètres > Options pour les développeurs`, et cliquer sur "`Déverrouillage OEM`".
2. Démarrer le bootloader du téléphone : redémarrer le téléphone en maintenant le bouton "volume bas" jusqu'à arriver sur l'interface bootloader.
3. Connecter le téléphone à son ordinateur par un câble USB (attention si l'ordinateur ne trouve pas le tel, certain câble ne font que recharger), puis cliquer sur le bouton "`Unlock bootloader`" sur cette page web : https://grapheneos.org/install/web#unlocking-the-bootloader . Confirmer cette commande en appuyant sur les boutons volumes du téléphone pour changer la sélection, puis le bouton de démarrage pour confirmer.

4. Cliquer sur le bouton "Download release" pour télécharger la dernière version de GrapheneOS
5. Cliquer sur le bouton "Flash release" pour l'installer ; ne pas toucher 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. Verrouiller en cliquant sur le bouton "`Lock bootloader`" puis en confirmant la commande avec les boutons de volumes sur le téléphone.
7. Sélectionner "`Start`" sur le téléphone et confirmer 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 fonctionnement du téléphone qui pourraient apporter des failles exploitable 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 :
    a. Ouvrir "`App store`", télécharger le "`Google Play Store`" puis l'ouvrir
    b. Créer un compte Google 'bidon'. La création de ce compte ne nécessite pas de numéro de téléphone ou d'adresse-mail. N'utilise pas de VPN à cette étape-là ! N'utilise jamais ce compte gmail par la suite.
    c. Comme première appli, vous pouvez par exemple télécharger et connecter un VPN <3 *(pour les sessions peu utilisées, Proton VPN en gratuit fonctionne très bien)*
    d. `Paramètres > Sécurité et confidentialité > ``Déverrouillage de l'appareil` :
    e. Si ce n'était pas le cas à l'installation, mettre **un mot de passe d'au moins 16 chiffres aléatoires** (ou 5 mots aléatoires, plus facile à retenir mais plus lourd au quotidien)
    f. activer 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 ou un dérivé de "1312" (éviter les mdp si courants que tes données pourraient être effacées accidentellement par ton entourage ou lors d'une fausse manip)
    g. `Paramètres > Sécurité et confidentialité > ``Exploit protection` :
    h. Auto reboot : le mettre à 8h ou moins
    i. USB-C port : `charging-only when locked`

j. Mettre `Turn off Bluetooth automatically` sur 30 minutes

k. Désactiver les paramètres `WebView JIT, Dynamic code loading via memory` et `Dynamic code loading via storage` *(cela provoquera une notification pour les applis utilisant ces fonctionnements peu sécurisés, que vous pourrez ignorer si l'appli fonctionne ou ré-activer spécifiquement si elle plante systématiquement)*

> **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. *Plus d'infos*

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**.

> **Info**
>
> 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)

Config 1 - le téléphone militant : optimal pour la sécurité

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'autre usage 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
  - Aller dans `Paramètres > Système > Utilisateurs > Ajouter un utilisateur` (choisir un nom quelconque)
  - Changer le paramètre : `App installs and updates > Enable for first party sources only`

    - Revenir en arrière et dans `Installer les applis disponibles`, choisir l'appli de VPN que vous utiliserez sur le profil.
    - Passer au nouveau profil pour lui mettre un super mot de passe (ce peut être le même que la session propriétaire, mais si c'est une session que vous déverrouillerez 40 fois par jour, c'est parfois bien qu'elle n'ait pas le même mdp que les sessions plus sensibles) et activer 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 perssone qui ait le téléphone dans les mains puisse lire du contenu via les notifications.
- Installer des applis
    - Retour sur la session *propriétaire*, passer par le Playstore pour installer les applis voulues, puis les désactiver : dans la liste des applis, rester appuyer sur l'icône des nouvelles installées `> ⓘ Infos sur l'appli > Ø Désactiver`
    - Dans `Paramètres > Système > Utilisateurs > "``*Utilisateur X*``" > Installer les applis disponibles >` choisir les applis utiles pour l'usage de la session
    - Certaines applis peuvent nécessiter les "`Google Play services`" pour fonctionner correctement, à tester si jamais vous rencontrer 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` partager sur chaque session
        b. se faire passer les infos dans les messages perso enregistrés
            - Propre, mais plus longue à paramétrer la première fois :
        c. Dans la session propriétaire, ouvrir l'`App store` et installer `Accrescent`, puis dans `Accrescent` installer `Inter Profile Sharing`, et le désactiver pour cette session pour l'installer seulement dans les sessions utilisées
        d. Passer dans chacune des sessions pour ouvrir `Inter Profil Sharing`, lui donner les accès nécessaires puis aller sur l'icone `⚙ Paramètres` en haut à droite pour y `Activer le chiffrement` (en utilisant par exemple votre code à 16 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, ouvrez `Inter Profil Sharing` pour la redéclencher)
- 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

Config 2 - le téléphone du quotidien / collectif : assouplie

Un téléphone pour celles et (activité pro, SIM perso…)

Principe : il n'y a que la session propriétaire qui est utilisée, et les applis qui ne sont pas open source et pouvant être reliées à vous sont utilisées dans l'espace privé

- Paramétrer **l'espace privé**
    - L'activé dans `Paramètres > Sécurité et confidentialité > Espace privé` *(vous pouvez y mettre le même déverrouillage que le téléphone)*
    - Changer 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
    - Choisir 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'un mauvais mot de passe. Vous pouvez configurer un auto-reboot assez court (par exemple 1h) ensuite éteindre le téléphone pour chaque moment où vous craignez d'être prise avec *(contrôle de flic, avant de se coucher pour les risques de perquisition à 6:00…)*
- 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 verrouillage 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 config si vous utilisez une SIM - toute fois attention : comme sur les autres téléphones, celui-ci comme les appels WiFi ne passent pas par le VPN de la session ! Il est nécessaire d'avoir un VPN sur chaque appareil et de ne pas activer l'option `Appel Wifi` *(c'est*

une option qui permet avec certain opérateur d'échanger en clair quand une wifi est connectée 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)*

- Désactiver la 2G
  - Paramètres > Connectivité …
- Astuces au quotidien
  - Personnaliser les raccourcis de paramètres du paneau de notification pour y enlever le mode avion. C'est plus relou de devoir passer par la liste des paramètres, mais ça aurait évité de fausses manip' à quelques camarades ♥
  - Pareil, 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 !

???+ warning Retour sur les points d'attention

Text Only

```
1       * 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)
2       * Certains téléphones avec des références US n'ont pas la possibilité de déverrouiller l'OEM pour installer GrapheneOS. Nous n'avons pas trouvé de solution pour les téléphones achetés en ligne autre que les renvoyer, mais 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 config 1 et 2, en cloisonnant les applis les moins fiables (Whatsapp & co…) d'une session secondaire dans l'espace privé.
- Prioriser l'utilisation d'application pouvant fonctionner hors ligne pour limiter la dépendance aux connexions en déplacement (type CoMaps avec la carte du pays pour le GPS, Thunderbird plutôt que l'interface web pour les mails…)