
GrapheneOS
pour les anarchistes

Table des matières

GrapheneOS pour les anarchistes

Guide d’installation et de bonnes pratiques, traduit à partir de *GrapheneOS for Anarchists* de anarsec.guide et modifié par nos maigres connaissances d’utilisateurices.

Cette brochure cite beaucoup de sources disponibles en ligne. On t’invite à les consulter via Tor.

Bien que les anarchistes devraient réduire la présence de téléphones dans leurs vies[1], si tu choisi d'utiliser un téléphone fais en sorte de rendre ta géolocalisation, l'interception de tes messages ou le hack de ton appareil le plus difficile possible pour tes adversaires. Donc utilise GrapheneOS.

C'est quoi GrapheneOS ?

GrapheneOS est une version du ***système d'exploitation*** d'Android spécialisé sur la sécurité. Les smartphones Android standards ont Google intégré avec eux (par exemple, les Services Google Play ont un accès irrévocable à tes fichiers, logs, position GPS, etc.). GrapheneOS supprime toute les applications et services Google par défaut, utilise une sécurité basée sur les composants informatique pour rendre beaucoup plus difficile[2] de contourner le chiffrement du disque, et est significativement renforcé contre le hacking. Il y a d'autre systèmes d'exploitation Android alternatifs, mais ils sont inférieurs en terme de sécurité[3]. Pour une liste détaillée de l'amélioration de la vie privée et de la sécurité par rapport à un Android standard, tu peux consulter la documentation de GrapheneOS[4].

Système d'exploitation
Le logiciel système qui fait fonctionner ton appareil en faisant le lien entre les composants et les logiciels. Certains exemples communs sont Windows, macOS, Linux, Android et iOS. Linux et certaines versions d'Android sont les seuls options libres de cette liste.

Cette sécurité est reconnu jusqu'à dans les rapports de ses adversaires. Cellebrite — l'entreprise spécialisée dans l'extraction de donnée de téléphone ayant passé un contrat de 7 millions d'euros avec la police française — a pu attester de leur incapacité à extraire la moindre information des téléphones sous GrapheneOS[5].

En raison de la nature même du fonctionnement de cette technologie[6], même sans SIM ton téléphone cherche en permanence à

1 anarsec.guide/fr/posts/nophones
stuut.info/Brochure-Le-fond-de-la-terre-est-rouge-8320
2 grapheneos.org/faq#encryption
3 eylenburg.github.io/android_comparison.htm
4 grapheneos.org/features
5 androidauthority.com/cellebrite-leak-google-pixel-grapheneos-security-3611794
6 citizenlab.ca/2023/10/finding-you-teleco-vulnerabilities-for-location-disclosure

se connecter aux cellules des antennes relais ce qui donne à ton opérateur un historique de ta géolocalisation. C'est pour cette raison que l'on te recommande de laisser en permanence ton appareil chez toi et de l'utiliser comme un téléphone fixe, connecté à internet en Wi-Fi en mode avion, plutôt que d'avoir une carte SIM qui se connecte aux antennes relais. Même si tu achète une carte SIM de manière anonyme. elle sera liée à ton identité par la suite, l'opérateur peut rétroactivement consulter toute tes données de géolocalisation. De plus, ce n'est pas suffisant de laisser ton téléphone à la maison seulement quand tu pars en manif ou en action, car ça va apparaître comme une anomalie[7] et servir d'indication sur ces activités pendant ce laps de temps.

Installation

Les téléphones Pixel de Google[8] sont pour le moment les seuls smartphones qui respectent les prérequis de sécurité des composants matériels (hardware) demandé par GrapheneOS — voir à ce sujet la liste des téléphones supportés[9] et recommandés[10]. « Hardware memory tagging support » est une fonctionnalité de sécurité très puissante introduite avec le Pixel 8, qui rend très difficile d'utiliser à distance des failles dans les applications installés par les utilisateurices, tel que Signal qui à « une très grande surface d'attaque à distance »[11].

À partir du Pixel 8, les téléphones Pixel vont recevoir au minimum 7 ans de mises à jour de sécurité à partir de leur date de sortie. Les téléphones en fin de vie (regroupé sous le terme GrapheneOS « extended support ») ne reçoivent pas l'entièreté des mises à jour de sécurité et ne sont donc pas recommandés. Tu peut voir la durée pendant laquelle GrapheneOS va mettre à jour chaque téléphone sur leur site[12].

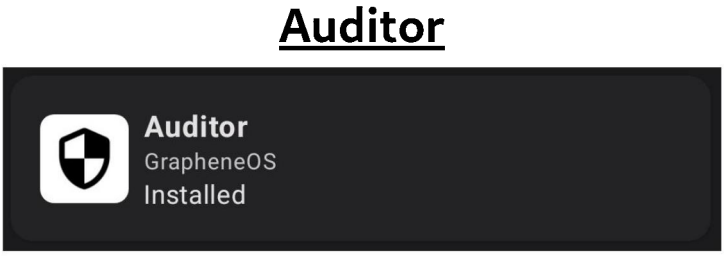
Certains opérateurs vendent des téléphones avec un forfait sur lesquels ils ajoutent une surcouche logiciel ainsi qu'un « SIM lock » qui peuvent

7 anarsec.guide/posts/nophones/#metadata-patterns
8 privacyguides.org/fr/mobile-phones/#google-pixel
9 grapheneos.org/faq#device-support
10 grapheneos.org/faq#recommended-devices
11 grapheneos.social/@GrapheneOS/111479318824446241
12 grapheneos.org/faq#device-lifetime

empêcher l'installation de GrapheneOS, on te conseille donc d'éviter ces versions de Pixel. La version la moins chère est d'acheter le modèle « a » juste après la sortie du nouveau modèle — par exemple, prendre le Google Pixel 8a après la sortie du Pixel 9.

GrapheneOS peut être installé en utilisant un navigateur internet compatible[13] (attention, Firefox et ses dérivés ne le sont pas) ou en ligne de commande. Si tu n'es pas à l'aise avec l'installation en ligne de commande, l'installation par le navigateur internet fonctionne très bien. Comme l'indique les consignes d'installation : « *Même si l'ordinateur que vous utilisez pour flasher GrapheneOS a été compromis et que l'attaquant a remplacé GrapheneOS avec son propre OS malveillant, cela peut être détecté avec Auditor* », la méthode est expliqué plus loin. Les deux méthodes listent les systèmes d'exploitations à partir desquels tu peut installer GrapheneOS.

Au premier démarrage Graphene va te demander si tu veut te connecter au Wi-Fi. Ne le fais pas, il faut tout d'abord faire une « hardware-based attestation » via *Auditor*. N'utilise jamais l'authentification à partir des empreintes digitales. Utilise une phrase de passe conséquente à la place.



L'attestation basée sur les composants informatiques est la dernière étape de l'installation. L'application Auditor incluse dans GrapheneOS utilise des fonctionnalités de sécurité des composants informatiques pour vérifier l'intégrité du micrologiciel de l'appareil et du système d'exploitation. C'est très important parce que cela vous alertera si les composants de l'appareil ont été modifié de manière malveillante, par exemple par la police après qu'elle ait saisi votre téléphone. Auditor ne

13 grapheneos.org/install/web#prerequisites

vérifie pas forcément les applications que vous avez l'installé. Auditor doit être configuré immédiatement après que GrapheneOS ait été installé, avant même de le connecter à internet. Si tu lis ce guide après avoir installé GrapheneOS, ça vaut toujours le coup de le faire dès maintenant.

Comment cela fonctionne ? Votre nouvel appareil est l'*auditee*, et l'*auditor* peut être soit une autre version d'Auditor sur le téléphone d'un ami ou le service d'attestation à distance[14] — nous recommandons d'utiliser les deux. L'*auditor* et l'*auditee* forment un duo afin de créer une clé privée, si le système d'exploitation de l'*auditee* est modifié après la création de ce duo, l'*auditor* sera alerté durant le prochain test. Audite ton téléphone le plus régulièrement possible (tout les 2 mois au maximum) et à chaque fois qu'il a été manipulé hors de ta vue.

Immédiatement après avoir installé Graphene et avant de se connecter à Internet, fait une « local vérification »[15]. Cela nécessite la présence d'un ami que vous voyez de manière semi-régulière et qui dispose de Auditor (sur n'importe quel appareil Android). Lors de la première utilisation les informations vont s'afficher sur un fond marron, lors des vérifications suivantes, si rien n'a été modifié, les informations s'afficheront sur un fond vert foncé. Il n'est pas possible de faire cette vérification a distance même après avoir associé les deux téléphones, vous devez effectuer ces vérifications en personne.

Nous te recommandons de n'utiliser ce smartphone qu'avec le Wi-Fi (sans carte SIM). Active le mode avion. Cela permettra « de totalement désactiver l'émission et la réception de signaux radios, ce qui empêchera ton téléphone d'être joignable depuis le réseau cellulaire et empêchera ton opérateur (et n'importe qui se faisant passer pour lui) de suivre ton appareil avec les signaux radio ». Laisse tout le temps le téléphone en mode avion — sinon le téléphone va interagir avec le réseau cellulaire même si il n'y a pas de carte SIM dedans.

Tu es maintenant prêt à te connecter au Wi-Fi. Une fois que tu as une connexion Internet, nous te recommandons de mettre en place immédiatement une vérification à distance[16] avec un courriel que tu vérifies régulièrement. Tu peut toujours te connecter plus tard pour

14 attestation.app
15 attestation.app/tutorial#local-verification
16 attestation.app/tutorial#scheduled-remote-verification

regarder l'historique des attestations. Le délai de base avant alerte est de 48 heures, si tu sais que ton téléphone va être éteint pendant une grande période tu peut mettre à jour la configuration à un maximum de 2 semaines. Si ton téléphone va être éteint pour plus de deux semaines (par exemple, si tu le laisses à la maison quand tu pars en voyage), contente toi d'ignorer les mails.

Si Auditor détecte une modification, tu dois immédiatement considérer le téléphone comme non fiable. Une analyse forensique[17] (une analyse poussée de l'intégrité d'un appareil) pourrait permettre de révéler comment le téléphone a été compromis, ce qui pourrait permettre d'éviter que cela se reproduise. Tu peut contacter des services comme *Access Now's Digital Security Helpline*[18], même si nous te recommandons de ne pas leur envoyer d'informations personnelles.

17 notrace.how/threat-library/fr/mitigations/computer-and-mobile-forensics.html
18 accessnow.org/help

Profils Utilisateurs

Les profils d'utilisateur est une fonctionnalité qui te permet de compartimenter ton téléphone. Chaque profil à ses propres données de profils, son propre groupe d'applications et ses propres données d'applications. Les applications ne peuvent pas voir celles installées sur les autres profiles et peuvent uniquement communiquer avec les application présente sur le même profil. Autrement dit, les utilisateurs sont isolés les un des autres — si l'un est compromis les autres ne le sont pas forcément.

Le profil « Propriétaire » est le seul profil accessible au démarrage du téléphone. A partir de celui-ci tu peux créer des profils supplémentaire. Chaque profil est ***chiffré*** avec sa propre clé de chiffrement et ne peux pas accéder aux données des autres profils, même le « Propriétaire » ne peux pas avoir accès aux autres profils sans avoir les mots de passe correspondants.

Chiffré
Le chiffrement est le processus consistant à modifier un message de tel manière qu'il ne puisse être re-modifié pour être lisible que par des personnes choisies.

Bien que les profils soient chiffrés indépendamment les uns des autres, certaines données sont tout de même partagés entre eux. Cette perméabilité permet de n'avoir a mettre a jour ses applications que sur un seul profil, c'est pour cette raison que nous recommandons d'utiliser le Propriétaire comme seul profil d'installation (voir partie *Déléguer les applications*). Dans les autres informations partagées il y a tout ce qui correspond au système : connexion internet (Wi-Fi et réseau mobile), bluetooth, localisation, accès camera & micro, partage de connexion, volumes, contact (si le profil est autorisé à y avoir accès). De plus, même si l'autorisation a passer des appels/SMS n'est pas accordée, tout les profils peuvent peuvent recevoir un appel « classique ».

Utiliser au quotidien un profil qui n'est pas le « Propriétaire » apporte 2 avantages : il permet d'avoir une phrase de passe avant 1er déverrouillage (là où le téléphone est le plus sécurisé) robuste sans alourdir l'utilisation quotidienne et il réduit drastiquement le risque d'obtention de ton code via du « **shoulder surfing** »[19].

Shoulder surfing Technique utilisée par la police pour obtenir des mots de passe en espionnant les personnes entrain de l'écrire « par dessus l'épaule » généralement à l'aide de caméra.

Création de profils utilisateur

On va maintenant créer un 2e profil utilisateur pour les applications qui n'ont pas besoin des services Google Play (et qui correspondra donc à ton profil « Principal ») :

- **Paramètres → Système → Utilisateurs**, clique sur **Ajouter un utilisateur**. Choisit un nom, idéalement qui n'indique pas son usage (« Profil », nom d'objet, nom de personnage...), et une icône si tu le souhaite. Une fois créé le nom et l'icône de ce profil ne pourront être changé que directement depuis celui-ci. Sélectionne **Passer à [NomduProfil]**.
- Choisit un mot de passe différent du mot de passe du profil Propriétaire.
  - C'est le profil que tu va régulièrement déverrouiller durant la journée. Avoir ce profil te permet donc de n'avoir à rentrer le mot de passe Propriétaire qu'au démarrage du téléphone, ce qui te permet d'en avoir un très complexe. Pour le mot de passe du profil Principal, tu peux choisir entre un faible mot de passe + un temps de verrouillage court, ou une forte phrase de passe + un temps de verrouillage plus long. La première option repose sur la confiance sur le taux de limitation de tentative de déverrouillage permise par la sécurité du système[20]. La deuxième option ne repose par sur la confiance dans cette limitation de déverrouillage, puisqu'elle pourrait être contournée par une faille de sécurité, mais présente l'inconvénient que les données du profil sont vulnérables si l'appareil est laissé sans surveillance alors qu'il est déverrouillé. Tu peux aussi avoir une forte phrase de

19 attaque.noblogs.org/post/2025/08/28/italie-des-choses-bonnes-a-savoir
20 grapheneos.org/faq#encryption

passe + un temps de verrouillage court si tu ne déverrouille pas ton téléphone régulièrement. Garde en tête que si la police saisi ton téléphone (par exemple lors d'une perquisition), il doit idéalement être éteint, et au minimum être verrouillé (ce qui démarre le compte a rebours de la fonctionnalité de redémarrage mentionnée plus tard).

- Dans le profil Principal, tu peux paramétrer le temps de verrouillage dans **Paramètres → Sécurité et confidentialité → Déverrouillage de l'appareil → Roue de paramètre → Verrouiller après la mise en veille**, et le temps de mise en veille dans **Paramètres → Affichage → Délai de mise en veille de l'écran.**

Par la suite, tu pourra créer un 3e profil pour les applications qui ont besoin des services Google Play. Quand tu appuie sur **Fermer la session**, la données de ce profil sont de nouveau totalement chiffrées et inaccessibles sans la phrase de passe. Un raccourcis pour basculer d'un profil à un autre est situé en bas des Options Rapides (accessible en glissant 2 fois le haut de l'écran).

Tu peut aussi utiliser la fonctionnalité **Espace privé** pour créer à l'intérieur d'un profil une sorte de profil sécurisé à l'intérieur d'un autre profil qui contiendra tes services Google Play. Cet espace privé dispose de nombreuses fonctionnalités qui le rendent similaire à un autre profil (possibilité de l'activer ou non, phrase de passe spécifique, possibilité d'utiliser un VPN...). C'est aussi plus facile de partager des fichiers entre un profil et son **Espace privé** qu'entre deux profils.

Pour répéter, les profils utilisateurs et leurs utilités sont :

1) Propriétaire : Où les applications sont installées

2) Principal : Où les applications sont utilisées

3) Google (optionnel) : Où les applications qui ont besoin des services Google Play sont installées

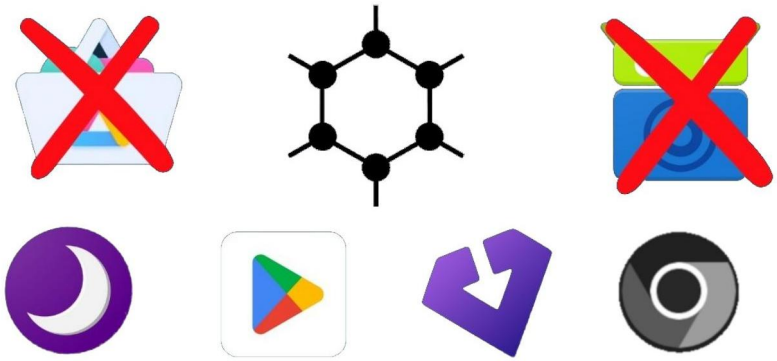
Tu peux évidement créer d'autres profils par la suite, selon tes besoins (exemple : une session pour les apps crackées, pour ne pas compromettre les autres profils en cas d'appli vérolée).

Si tu as GrapheneOS depuis longtemps et que tu n'utilisais qu'un seul profil jusqu'à maintenant, le transfert de profil est détaillé dans la partie *Comment faire des sauvegardes*.

Limites des profils secondaires

Utiliser un profil secondaire comme profil principal offre un gain de sécurité non négligeable puisqu'il permet de mettre en place une phrase de passe complexe à l'allumage du téléphone sans rendre l'utilisation quotidienne du téléphone fastidieuse. Cette mise en place vient tout de même avec quelques limites. Tout d'abord les paramètres **Exploit protection** ne sont pas modifiables sur ces profils secondaire et dépendent donc des paramétrages du profil Propriétaire (et c'est logique car ça rentrerait en contradiction avec le gain de sécurité apporté par l'utilisation de différents profils). Plus contraignant, les paramètres Wi-Fi sont uniquement accessible sur le Propriétaire tout comme la possibilité de démarrer un partage de connexion.
En dehors des paramètres de connectivité, chaque profil redémarre à zéro et le paramétrage de ceux ci peut être long si tu as l'habitude de changer beaucoup d'options.

Comment installer des applications



L'App Store de GrapheneOS contient les applications développées par l'équipe de GrapheneOS, telle que Vanadium, Auditor, Camera et PDF Viewer. Elles sont mises à jour automatiquement.

Pour installer plus d'applications, tu peut trouver deux autres magasins d'applications directement sur l'App Store de GrapheneOS : Google Play Store et Accrescent[21]. Le Google Play Store de l'App Store de GrapheneOS a été modifié afin de n'avoir aucun accès spécial ou privilège[22]. Accrescent dispose seulement d'une petite sélection d'applications.

Évite F-Droid à cause de ses nombreux problèmes de sécurités[23]. Nous ne recommandons pas non plus Aurora Store, car elle a les mêmes problèmes de sécurité que F-Droid[24]. Cependant l'utilisation du Google Play Store s'accompagne de la création d'un identifiant publicitaire personnalisé, un formidable outils de surveillance de Google qu'il est nécessaire de désactiver (détails dans la partie suivante).

Nous allons installer toutes les applications dans le profil Propriétaire, en utilisant le Google Play Store et/ou Accrescent. Nous allons ensuite désactiver ces applications dans le profil Propriétaire et les confier au

21 accrescent.app
22 grapheneos.org/features#sandboxed-google-play
23 privacyguides.org/fr/android/obtaining-apps/
24 privsec.dev/posts/android/f-droid-security-issues/#conclusion-what-should-you-do

profil Principal. C'est parce que nous allons uniquement les utiliser dans le profil Principal (à l'exception, si jamais tu utilises ton téléphone hors de chez toi, d'un VPN qui aura besoin d'être installé sur chaque profils).

Applications du Google Play Sandboxé et d'Accrescent

> **Sandboxé**
> Le sandboxing désigne le fait de limiter un logiciel à un environnement isolé afin de restreindre les dégâts qu'il pourrait faire si il était défectueux ou malveillant.

Pour installer et configurer le Google Play sandboxé :

1. Dans le profil Propriétaire, installe le Google Play en ouvrant l'App Store de GrapheneOS et en installant les services Google Play (ça installera aussi Google Services Framework et le Google Play Store).
2. Le Google Play Store a besoin d'un compte Google pour se connecter, mais tu peux créer un profil avec des fausses informations qui ne sert qu'à ça.
3. Une fois installé et connecté, désactive l'identifiant publicitaire : **Paramètres → Applications → Sandboxed Google Play → Google Settings → Ads**, puis sélectionne *Delete advertising ID*.
4. Les mises à jours automatiques sont activées par défaut dans le Google Play Store: **Google Play Store Settings → Network Preferences → Auto-update apps**.
5. Pour que les mises à jour automatiques fonctionnent il faut que les notifications soient activées pour le Google Play Store et les Services Google Play : **Paramètres → Applications → Google Play Store / Google Play Services → Notifications**. Si tu obtiens une notification du Play Store pour qu'il se mette a jour lui même, accepte[25].

Pour Accrescent, installe la simplement à partir de l'App Store de GrapheneOS dans le profil Propriétaire.
Tu es maintenant prêt à installer des applications depuis le Google Play Store et d'Accrescent. Tu peux consulter *Encrypted Messaging for Anarchists*[26] pour avoir quelques idées.

25 discuss.grapheneos.org/d/4191-what-were-your-less-than-ideal-experiences-with-grapheneos/18
26 anarsec.guide/posts/e2ee

Applications qui ne sont ni sur le Play Store ni sur Accrescent

La plupart des applications sont disponibles sur ces deux catalogues d'application. Pour les quelques applications qui ne le sont pas, télécharger individuellement les fichiers **APK** n'est pas une bonne solution parce que tu devras te souvenir de les mettre à jour toi-même (il y a des exceptions, comme Signal[27], qui est conçu pour se mettre à jour tout seul).

APK
Fichier d'installation d'un logiciel sur Android.

Obtainium[28] est une appli de gestion d'applications qui te permet de faire automatiquement les mises à jour automatiquement depuis le site des développeurs ou depuis des plateformes tel que GitHub. Obtainium s'installe depuis leur page des sorties GitHub[29] à partir du fichier `app-arm64-v8a-release.apk` de la version la plus à jour (arm64-v8a correspond à l'architecture du processeur).

Si tu as besoin d'applications qui ne sont pas disponibles sur le Play Store ou Accrescent, installe Obtainium dans le profil propriétaire (et ne le désactive pas) après avoir vérifié son authenticité avec AppVerifier (disponible sur Accrescent). AppVerifier s'intègre très bien avec Obtainium. Avant qu'Obtainium installe une APK, tu peut vérifier son authenticité automatiquement si elle fait parti des applications sélectionnées par les développeurs d'AppVerifier, ou manuellement à partir de l'empreinte publié par les développeurs de l'application que tu souhaite installer si elle est disponible.

Si tu souhaite utiliser Obtainium comme source principale d'application il faut savoir que Github restreint le nombre de demande qui lui sont faite, ce qui provoque un message d'erreur si tu as plus que 10 applications. Ce message est facilement contournable mais nécessite un compte GitHub[30] (quitte a en créer un exprès) :

27 signal.org/android/apk
28 privacyguides.org/fr/android/obtaining-apps/#obtainium
29 github.com/ImranR98/Obtainium/releases
30 wiki.obtainium.imranr.dev/sources/#github

1. Connecte toi à GitHub[31].
2. Va dans **Settings → Developer settings → Personal access tokens → Fine-grained tokens**[32].
3. Sélectionne **Generate new token**.
4. Donne un nom et une date d'expiration à ton jeton, tu peux choisir « No expiration ».
5. Descend en bas de la page et sélectionne **Generate token**.
6. Copie le jeton et enregistre le quelque part, le moment de sa création est le seul moment auquel tu y a accès. Colle ton jeton dans le paramètre *Jeton d'accès personnel GitHub* d'Obtainium.

Applications qui ont besoin des Services Google Play

> **Open-Source**
> Signifie que le code du logiciel est accessible pour tout le monde afin de l'examiner.

Si tu souhaite utiliser des applications qui nécessitent les services Google Play, créé un profil pour ces applications. C'est aussi une bonne manière d'isoler toute appli que tu utilise qui n'est pas ***open-source*** ou qui n'a pas une bonne réputation. Tu doit installer et configurer le Sandboxed Google Play dans ce profil « Google ». Il existe une liste des applications bancaires compatibles disponibles sur le forum GrapheneOS ainsi qu'une liste mise-à-jour[33].

Beaucoup d'applis de banque ont besoin du Sandboxed Google Play. Cependant, les banques peuvent être accédées par un ordinateur pour ne pas avoir besoin de ce profil « Google ».

Applications qui sont basées sur un site web

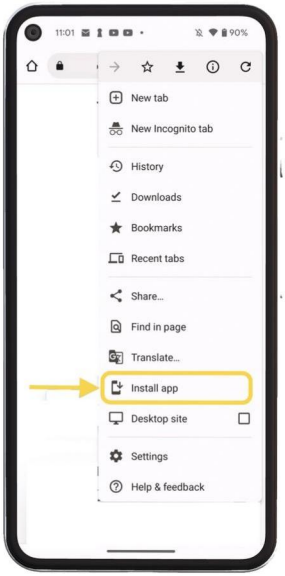
Beaucoup d'applications existantes permettent principalement d'accéder à des sites disponibles depuis n'importe quel navigateur (réseaux sociaux, transport...). Bien que ces applications peuvent apporter quelques fonctionnalités, elle viennent généralement avec leur lots de traqueurs.

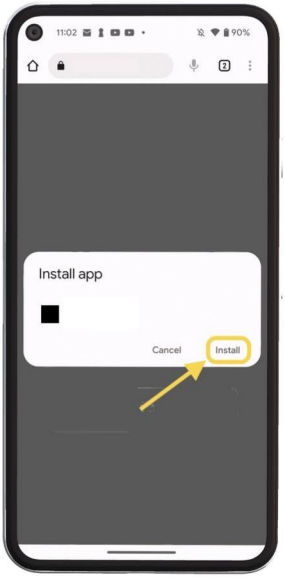
31 github.com/login
32 github.com/settings/tokens?type=beta
33 privsec.dev/posts/android/banking-applications-compatibility-with-grapheneos/#international-banking-apps

Puisque la version web de ces applications est généralement largement suffisante. Il est possible d'installer une copie de ces sites depuis vanadium en tant qu'application web progressive (***PWA***).

PWA
Page de navigateur apparaissant comme une application native à l'utilisateurice.

Pour ça il suffit de se rendre sur le site internet cible, d'ouvrir les paramètres de vanadium et de sélectionner « ajouter à l'écran d'accueil ».





Ce raccourcis ouvrira désormais le site web dans vanadium en tant qu'application indépendante et en plein écran. Seul vrai inconvénient : il n'est pas possible d'ajouter cette application au menu défilant de base d'Android.

Déléguer les application

Comme expliqué plus haut, installer les applications dans des profils secondaires depuis le profil Propriétaire permet une mise a jour simultanée entre les profils. Si une même application est installée manuellement sur 2 profils différents, elle se seront pas considéré

comme identique et devront être mise à jour indépendamment dans ces profils.

Pour déléguer une application :

- Dans le profil Propriétaire, désactive toute les applications qui n'ont pas besoin d'être active pour faire une une mise a jour (à l'exception de ton VPN): **Paramètres → Applications → [Exemple] → Désactiver**
- Pour installer n'importe quelle application dans un autre profil : **Paramètres → Système → Utilisateurs → [NomduProfil] → Installer les applis disponibles**, puis sélectionne l'application.

VoIP

Un smartphone qui utilise uniquement le Wi-Fi n'a pas besoin d'un abonnement. Comme expliqué dans *Tue le flic dans ta poche*[34], l'administration a souvent besoin d'un numéro de téléphone qui peut être appelé depuis un téléphone normal (sans chiffrement). Pour cela tu peux utiliser la VoIP.

La VoIP (pour Voice over Internet Protocol — Voix sur IP) est une technologie qui fait passer tes appels via Internet (comme le fait Signal) au lieu d'utiliser la transmission standard par antenne-relais. Contrairement à Signal, la VoIP te permet de recevoir des appels de n'importe qui, et pas seulement des utilisateurices ayant la même application.

L'avantage d'utiliser la VoIP pour les appels via un forfait de données est que tu peux créer différents numéros pour différentes activités (un pour les factures, un pour créer un compte Signal, etc.) et que tu n'as jamais besoin de désactiver le mode Avion.

L'avantage d'utiliser un forfait de données à la place est que tu peux l'utiliser loin du Wi-Fi, au prix de la géolocalisation.

34 anarsec.guide/fr/posts/nophones/#bureaucratie

Forcer tout le trafic internet à passer par un VPN

C'est une bonne chose d'obliger GrapheneOS à faire passer toute les connections au réseau internet au travers d'un VPN — ça permet de de faire reposer ta confiance dans ton VPN au lieu de ton opérateur en qui on ne peut pas avoir confiance. Comme le *Security Lab d'Amnesty International*[35] le dit:

> *« L'utilisation d'un fournisseur VPN réputé peut vous offrir une meilleure confidentialité face à la surveillance de votre FAI ou du gouvernement et empêcher les attaques par injection réseau provenant de ces entités. Un VPN rendra également les attaques par corrélation de trafic, en particulier celles qui ciblent les applications de messagerie, plus difficiles à réaliser et moins efficaces. »*

Il y a 2 façon de faire tourner un VPN : depuis ton téléphone ou depuis ton périphérique réseau (soit un routeur ou un pare-feu matériel). Quand tu utilise ton téléphone depuis chez toi, on recommande cette dernière option.

Ça n'est pas nécessaire de « doubler » un VPN — si ça tourne sur ton périphérique réseau, tu n'as pas besoin de la faire tourner sur ton téléphone, et vice-versa. Ça veut dire qu'un téléphone qui fait tourner un VPN devrait être désactivé avant de se connecté à un Wi-Fi avec un « VPN Kill Switch ».

Si jamais tu utilises ton smartphone en dehors de chez toi, on te recommande de configurer GrapheneOS pour qu'il force tout le trafic internet à passer par un VPN — installe l'application du VPN pour chaque profil utilisateur. Toute les connections standard de GrapheneOS passeront par le VPN (à l'exception des connectivity check[36], qui peut être désactivé à partir de Propriétaire en allant dans *Paramètres → Réseau et Internet → Internet connectivity check* et sélectionne *Off*). Il

35 securitylab.amnesty.org/latest/2023/10/technical-deep-dive-into-intellexa-alliance-surveillance-products

36 grapheneos.org/faq#default-connections

faut noter que les options **VPN Permanent** et **Bloquer les connexions sans VPN** sont activées par défaut sur GrapheneOS. Garde en tête qu'il faut désactiver ton appli VPN avant de te connecter à ton Wi-Fi « VPN Kill Switch ».

Si tu peux te permettre de payer pour un VPN, on te recommande Mullvad[37] et IVPN[38]. Sinon tu peux utiliser RiseupVPN[39], bien qu'il ait beaucoup moins d'utilisateurice au milieu desquels se fondre et qu'il ne répond pas à plusieurs critères important de sécurité pour un fournisseur de VPN[40], tel que la publication des audits de sécurité de son code et de son infrastructure. Un abonnement VPN devrait être acheté anonymement — des bons d'achat sont disponibles pour Mullvad et IVPN pour avoir un abonnement anonyme sans utiliser Monero (une cryptomonnaie anonyme).

Tor

Côté navigateur, tu auras sûrement envie d'utiliser Tor depuis un téléphone[41]. Néanmoins, si tu as besoins de l'anonymat de Tor plutôt que la confidentialité de Riseup VPN, tu devrais plutôt utiliser Qubes OS ou Tails[42] sur un ordinateur. La documentation de Graphene[43] recommande d'éviter d'utiliser les navigateurs internets utilisant Gecko (comme Tor Browser), car ces navigateurs ne « disposent pas d'un sandboxing interne ».

Côté VPN, Orbot est une application qui permet de faire passer le trafic de n'importe quelle application à travers le réseau Tor, mais utiliser Vanadium à travers Orbot n'assure pas la même certitude sur l'anonymisation qu'en utilisant Tor Browser[44].

37 privacyguides.org/fr/vpn/#mullvad
38 privacyguides.org/fr/vpn/#ivpn
39 riseup.net/fr/vpn
40 privacyguides.org/fr/vpn/#criteres
41 torproject.org/download/#android
42 anarsec.guide/posts/qubes/#when-to-use-tails-vs-qubes-os
43 grapheneos.org/usage#web-browsing
44 support.torproject.org/tor-browser/security/using-tor-with-other-browsers

Si l'option *Bloquer les connexions sans VPN* est activée avec Orbot, Tor Browser ne sera pas capable d'accéder à internet car Orbot est configuré pour l'ignorer par défaut. Si tu souhaite utiliser Tor Browser pour garantir ton anonymat, configure Orbot pour qu'il ne fonctionne que pour certaines applications, ou utilise un profil dédié pour utiliser Tor Browser.

Habitudes et Réglages recommandés

Éteint ton téléphone pendant la nuit et lorsque tu pars de chez toi. Le chiffrement complet du disque est plus robuste lorsque l'appareil est éteint. En plus de ça, si le système d'exploitation est compromis par un malware un redémarrage peut le supprimer de ton système, c'est donc une bonne pratique d'éteindre ton téléphone tout les jours.

Dans le profil Propriétaire

- **Paramètres → Sécurité et confidentialité → Exploit protection → Auto reboot :** 18 heures ou moins (au hasard, un contrôle d'identité dure 4h)

  Le redémarrage automatique, si aucun profil n'a été déverrouillé pendant plusieurs heures, va mettre ton téléphone complètement au repos. Il redémarrera automatiquement pendant que tu dors si tu oublie de l'éteindre. Si la police réussi à mettre la main sur ton téléphone allumé alors qu'il n'y a que le verrouillage d'écran, ce paramètre permettra de revenir à un chiffrement plus puissant une fois que le délai se sera écoulé. Et si jamais tu as des impératifs de réveil ton alarme va bel et bien se déclenchée (une sonnerie personnalisée sera remplacée par une par défaut).
- **Paramètres → Sécurité et confidentialité → Exploit protection → USB-C port** : *Charging-only* ou *Off*
- **Paramètres → Système → Utilisateurs → [NomduProfil] → App installs and updates**: Disabled

  Une fois que tu as toute les applications dont tu as besoin, désactive l'installation d'appli sur ce profil — les applis déléguées dans un profil secondaire depuis le profil Propriétaire (à partir de l'option *Installer les applis disponibles*, comme décrit plus haut) continueront d'être mise à jour. Si tu souhaite en installer de nouvelles, réactive cette option le temps de les installer.

- **Paramètres → Système → Utilisateurs :** activer *Send notifications to current user*

  C'est assez pratique de pouvoir recevoir les notifications depuis n'importe quel profil.
- **Paramètres → Sécurité et confidentialité → Déverrouillage de l'appareil → Duress password** : Met en place un mot de passe *duress*[45] qui peut être utilisé pour détruire les données du téléphone.

Dans tout les profils

- Dans le menu de raccourcis, laisse les indicateurs pour le Bluetooth, la localisation, l'accès à l'appareil photo et le microphone désactivé quand tu n'en as pas besoin pour un usage spécifique. Les applications ne peuvent pas utiliser des fonctionnalités désactivées (même si elle en ont l'autorisation) jusqu'à ce qu'elles soient réactivées. Aussi tu peux ajouter un **Paramètres → Sécurité et confidentialité → Exploit protection → Turn off Bluetooth automatically :** 2 minutes

- Dans l'application SMS/MMS (celle par défaut), désactive **Paramètres → Paramètres avancés → Récupération automatique**

- Si, pour déverrouiller un profil, tu utilise un code a chiffre tu peux rendre leur position aléatoire pour réduire les risques de déduction lié à la salissure de l'écran ou par du shoulder surfing. **Paramètres → Sécurité et confidentialité → Déverrouillage de l'appareil Déverrouillage de l'écran → Scramble PIN input layout**

- Beaucoup d'applications permettent de « partager » un fichier pour l'envoie de media. Par exemple, si tu envois une image sur Signal, ne donne pas accès à Signal aux « photos et vidéos » car elle aura accès à toute tes images. A la place, dans l'application « Fichiers », fait un appuie-long sur l'image et partage-la avec Signal (et idéalement avec l'application *Scramble Exif* avant Signal pour en enlever les métadonnées).

- Quand une application demande la permission du stockage, sélectionne ***Storage Scopes***. Ça va faire croire à l'application qu'elle a la permission à ton espace de stockage comme demandé,

45 grapheneos.org/features#duress

alors que ce n'est pas le cas. C'est également valable avec le *Contact Scopes*.

Comment faire des sauvegardes

N'utilise pas des sauvegardes en ligne. Tu ne peut pas faire confiance aux options proposés par les entreprises et c'est la manière la plus simple pour la police d'accéder à tes données. Si tu dois faire une sauvegarde de ton téléphone, fais le sur un ordinateur chiffré.

GrapheneOS permet actuellement d'utiliser Seedvault[46] comme solution de sauvegarde, disponible en allant dans **Paramètres → Système → Sauvegarde**, mais ce n'est pas toujours fiable (SMS manquant ou en désordre, paramètres d'appli pas sauvegardés...). Comme décrit dans leur propre documentation[47], la connexion à un ordinateur nécessite de faire confiance à un ordinateur moins sécurisé que ton smartphone sous GrapheneOS, donc c'est mieux d'éviter de l'utiliser. À la place, tu peut manuellement sauvegarde les fichiers en les copiant sur une clé USB-C en utilisant l'application de fichiers, ou de te les envoyer en utilisant une messagerie chiffrée[48].

Le Seedvault est aussi un bon moyen pour copier un profil vers un autre sur un même téléphone, ce qui peut servir pour transférer un profil de longue date qui était utilisé par défaut sur le Propriétaire vers un nouveau profil Principal ou pour importer les paramètres d'un profil vers un nouveau.

Pour y parvenir il suffit de suivre les étapes suivantes :

1. Fait une sauvegarde en allant dans **Paramètres → Système → Sauvegarde**, ce qui va créer un dossier *.SeedVaultAndroidBackup* dans ton stockage interne. Note les 12 mots qui ont été générés.
2. Ouvre l'application *Fichiers*, ouvre le menu en haut à gauche (3 traits) et sélectionne ***Pixel***
3. Ouvre le menu de droite (3 points) et sélectionne ***Afficher les fichiers masqués***

46 grapheneos.org/features#encrypted-backups
47 grapheneos.org/faq#file-transfer
48 anarsec.guide/posts/e2ee

4. Tu va voir apparaître le **dossier *.SeedVaultAndroidBackup***, fait un **appuie long** pour le sélectionner → **menu de droite → Compresser**. Une archive *.SeedVaultAndroidBackup.zip* devrait apparaître.
5. Ouvre l'application *Inter Profile Sharing* (disponible sur le store Accrescent), sélectionne « Partager des fichiers » puis sélectionne l'archive que tu viens de créer.
6. Assure toi que le profil vers lequel tu veux faire le transfert a *Inter Profile Sharing* d'installé puis passe à ce nouveau profil.
7. Lance *Inter Profile Sharing*, une notification devrait s'afficher avec le nom de l'archive que tu viens de partager. Télécharge là.
8. Ouvre l'application ***Fichiers**, va dans* **Téléchargement → .SeedVaultAndroidBackup.zip → .SeedVaultAndroidBackup → Sélectionne tout les dossiers avec un appuie long → Menu de droite → Extraire sur.. → Menu de gauche → Pixel → .SeedVaultAndroidBackup** (si il n'est pas visible, affiche les fichiers masqués) **→ Extraire.**
9. **Paramètres → Système → Sauvegarde**, puis importe a partir du téléphone à l'aide des 12 mots noté à la 1ere étape.

Gestion des mots de passe

Pour ton gestionnaire de mot de passe, KeePassDX est une bonne option. Cependant, la plupart des identifiants nécessaire pour les applications peuvent être stockées sur un ordinateur avec KeePassXC parce qu'ils n'ont pas besoin d'être entrés régulièrement. La mise en place décrite dans ce guide requiert deux mots de passe :

1. Celui du profil Propriétaire (mot de passe de démarrage)
2. Celui du profil Principal
3. (Optionnel) Des applications comme Cwtch et Molly ont leur propre mot de passe.

Pour des conseil sur la qualité de tes mots de passe, consulte l'article *Tails Best Practices*[49].

49 anarsec.guide/posts/tails-best/#passwords

Téléphones sous Linux

Pourquoi recommander un Pixel plutôt qu'un téléphone Linux ? Les téléphones Linux (comme le PinePhone Pro[50]) sont beaucoup plus faciles à pirater que GrapheneOS[51] parce qu'ils manquent de fonctionnalités de sécurités moderne comme le « ***full system MAC policies*** », la vérification du *boot*, un sandboxing solide des applications, et des parades contre les failles modernes. Le fonctionnement matérielle manque aussi de mesures de sécurité modernes comme le chiffrement basé sur des composants matériels (à travers un système d'élément sécurisé et de système d'exécution de confiance) et à une intégration questionnable de composants tels que le modem.

Full system MAC policies
La technologie qui permet de contrôler précisément les accès des applications.

50 fr.wikipedia.org/wiki/PinePhone_Pro
51 madaidans-insecurities.github.io/linux-phones.html

Pour conclure

Avec la mise en place décrite dans ce guide, si un flic commence par ton nom, il ne pourra pas simplement le chercher dans la base de données d'un opérateur pour obtenir ton numéro de téléphone. Si tu utilise ton téléphone uniquement avec le Wi-Fi et que tu le laisse toujours chez toi, il ne pourra pas être utilisé pour déterminer ton profil et ton historique de déplacement. Si tu utilise un numéro de téléphone VoIP auquel tu accèdes à travers un VPN, même si ce numéro est connu, cela ne peut pas être utilisé pour te localiser. Toute les communications avec des camarades utilisent un chiffrement de bout-en-bout ce qui ne facilite pas la cartographie de tes fréquentations et du milieu militant. Même si tu es suffisamment malchanceux pour être ciblé par une enquête, le système d'exploitation renforcé rend difficile la compromission par un logiciel espion, et une telle compromission devrait être détectable en utilisant Auditor.

En stockant ton téléphone rendant évident toute manipulation lorsqu'il n'est pas utilisé, tu sera capable de savoir si un accès physique a été fait. Pour plus d'infos consulte le guide *Make Your Electronics Tamper-Evident*[52].

Le forum[53] de GrapheneOS est généralement très utile pour toute les questions restantes que tu peux avoir, bien que les réponses soient souvent très techniques et en anglais elles ont le mérite d'être précises et rapide.

Pour des informations sur les « burners », consulte le projet No Trace[54].

52 anarsec.guide/posts/tamper
53 discuss.grapheneos.org
54 notrace.how/threat-library/fr/mitigations/anonymous-phones.html

Brochure mise a jour le 01/12/2025
Contact : granarpheneOS@riseup.net
Empreinte Clé PGP, disponible sur keys.openpgp.org :
B1A6 C614 A18B 601E 04F7 599A 97BC 2616 4FB2 02A0

Après la parution de plusieurs articles du Parisien relayant des menace de la part de la police française et l'augmentation notable d'installations de l'OS en france suite à ces publications, GrapheneOS a annoncé prioriser la traduction de ses applications et des fonctionnalités spécifique de l'OS vers le français. Les noms de paramètres en anglais dans cette brochure peuvent donc être amenés à changer.

Bien que les anarchistes devraient réduire la présence des téléphones dans leurs vies, si tu choisi d'utiliser un téléphone fais en sorte de rendre ta géolocalisation, l'interception de tes messages ou le hack de ton appareil le plus difficile possible pour tes adversaires.
Donc utilise GrapheneOS.

Cette brochure est une traduction assortie de quelques modifications de la brochure GrapheneOS for Anarchists du site anarsec.guide.