Sécurité du téléphone: 1 - Comment chiffrer son téléphone ?

Contenu transféré depuis la base: Sécurité du téléphone: 1 - Saisie par la police

Le téléphone est un point critique de sécurité, car il contient de nombreuses informations et il est toujours saisi lors de perquisitions ou d'arrestations. Il est donc important de vous demander si votre téléphone est vraiment nécessaire avant d'aller sur une action.

D'une manière générale, plutôt que chacun·e ait des documents sensibles sur son téléphone, il vaut mieux désigner quelques personnes garantes de ces documents, qui sécurisent bien leurs téléphones et qui sont conscientes qu'elles pourraient le perdre au cours de l'action.

> **Modèle de menace :** lors d'une arrestation ou d'une perquisition, un téléphone qui contient des informations sur des actions futures ou passées et/ou sur l'identité de rebelles est saisi par la police.

Note : *en dessous de ce post vous trouverez un message d'Avocatvert donnant quelques indications précises dans le cas d'une demande de déchiffrement du téléphone par les forces de police.*

Chiffrer le contenu d'un téléphone

i Dans cette première étape, nous allons voir comment chiffrer les données de son téléphone. Le chiffrement (ou cryptage) est une technique qui vise à rendre impossible la compréhension d'un fichier par quelqu'un qui ne possède pas la clef de chiffrement (mot de passe). Les téléphones qui ne peuvent ni prendre de photos ni se connecter à internet ne peuvent pas être chiffrés. Ils stockent les contacts et des fichiers textes, rien de plus. □□ Attention : rien sur ces téléphones ne

peut être considéré comme sécurisé.

> ⚠ Si vous pensez qu'il y ai le moindre risque que votre téléphone ne tombe dans les mains de la police, assurez-vous de l'éteindre. C'est seulement lorsqu'un téléphone est chiffré **et** éteint qu'il est le plus sécurisé.

La plupart des téléphones fonctionnent avec deux systèmes d'exploitation (OS) : Apple (iOS) et Android. Ce sont les deux cas qui sont traités ici.

Téléphones Apple

Les téléphones Apple les plus récents intègrent déjà un chiffrement. Mais ça n'empêche pas d'accéder à vos données. Le chiffrement doit être protégé par un mot de passe, auquel "l'attaquant·e" n'a pas accès, c'est seulement dans ce cas que les données sont sécurisées.

*Pour connaitre quelle version fonctionne sur votre téléphone : Identification de la version du logiciel de votre iPhone, iPad ou iPod - Assistance Apple (FR)

Pour les appareils qui tournent sous iOS 4-iOS 7 :

1. Ouvrir le menu 'Général' dans l'application 'Réglages' et choisir 'Code' (ou iTouch et code)
2. Suivre les instructions pour créer un mot de passe.

Pour les appareils qui tournent sous iOS 8-iOS 11:

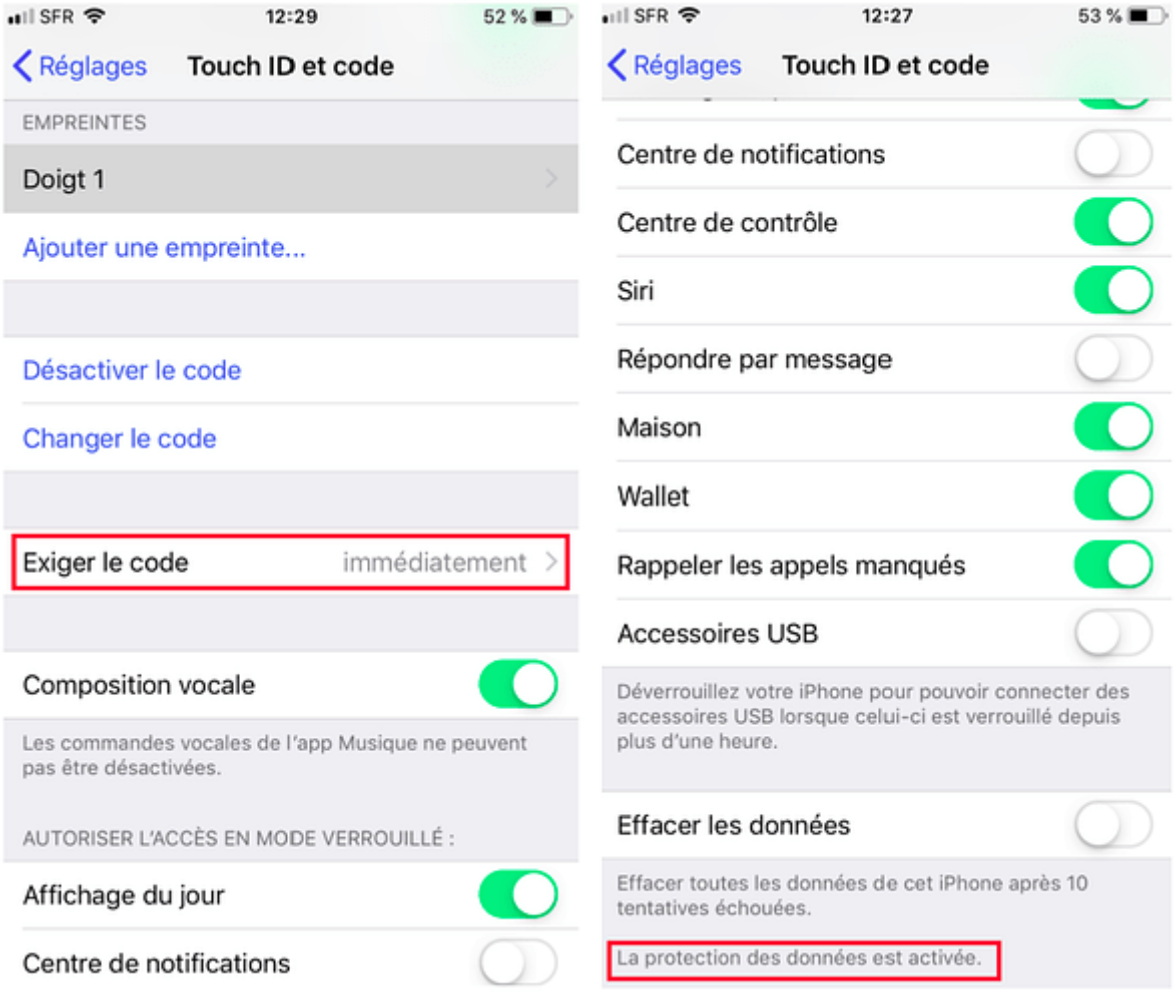
1. Ouvrir l'application 'Réglages'.
2. Appuyer sur 'Touch ID et code'.
3. Suivre les instructions pour créer un mot de passe.

Si votre appareil est sous iOS 8, désactiver l'option "mot de passe simple" pour créer un code de plus de quatre caractères. Avec la mise à jour sur iOS 9, Apple a mis par défaut un mot de passe à six caractères.

i Si vous choisissez un mot de passe avec seulement des chiffres, vous aurez un clavier numérique quand vous devrez déverrouiller votre téléphone, ce qui peut être plus simple que de taper une série de lettres et de symboles sur un tout petit clavier. Cependant, même si le logiciel Apple est conçu pour ralentir les outils de 'craquement' de mot de passe, nous vous suggérons de choisir un mot de passe de six caractères ou plus, qui contient des chiffres et des lettres. C'est tout simplement plus compliqué à 'craquer'.

Pour modifier votre mot de passe, allez dans Réglages > [votre nom] > Mot de passe et sécurité et sélectionnez 'Modifier le mot de passe'. Vous devrez aussi paramétrer l'option 'Exiger le code' sur 'immédiatement', afin que votre appareil ne soit pas déverrouillé lorsque vous ne l'utilisez pas.

Une fois que vous avez paramétré votre mot de passe, faites défiler vers le bas la page des paramètres du mot de passe. Vous devriez voir un message disant 'La protection de données est activée'. Cela signifie que le chiffrement de votre appareil est maintenant relié à votre mot de passe, et que le mot de passe est nécessaire pour accéder à la majeure partie des données de votre téléphone.



Un point sur les sauvegardes Apple

Les propriétaires d'appareils Apple effectuent généralement des sauvegardes sur iCloud ou iTunes.

⚠ Si vous effectuez des sauvegardes sur l'iCloud, vous devez être conscient·e que toutes ces données peuvent être accessibles à la police d'après la loi. Et quand bien même Apple vous assure que vos données sont cryptées, ils ont les clefs de chiffrement et sont obligés de les donner en cas d'enquête pénale. La police peut donc avoir accès aux données sauvegardées sur l'iCloud. Pour cette raison, nous vous recommandons de ne faire aucune sauvegarde sur ces clouds.

Si vous sauvegardez votre appareil Apple sur votre ordinateur en utilisant iTunes, il est important de savoir que, par défaut, le système de sauvegarde de iTunes ne chiffre pas les données. Vous devez donc choisir l'option 'Chiffrer la sauvegarde' afin que toutes les données soient bien stockées de façon chiffrée sur l'ordinateur. Assurez-vous de bien retenir le mot de passe et de sécuriser votre disque dur entier.

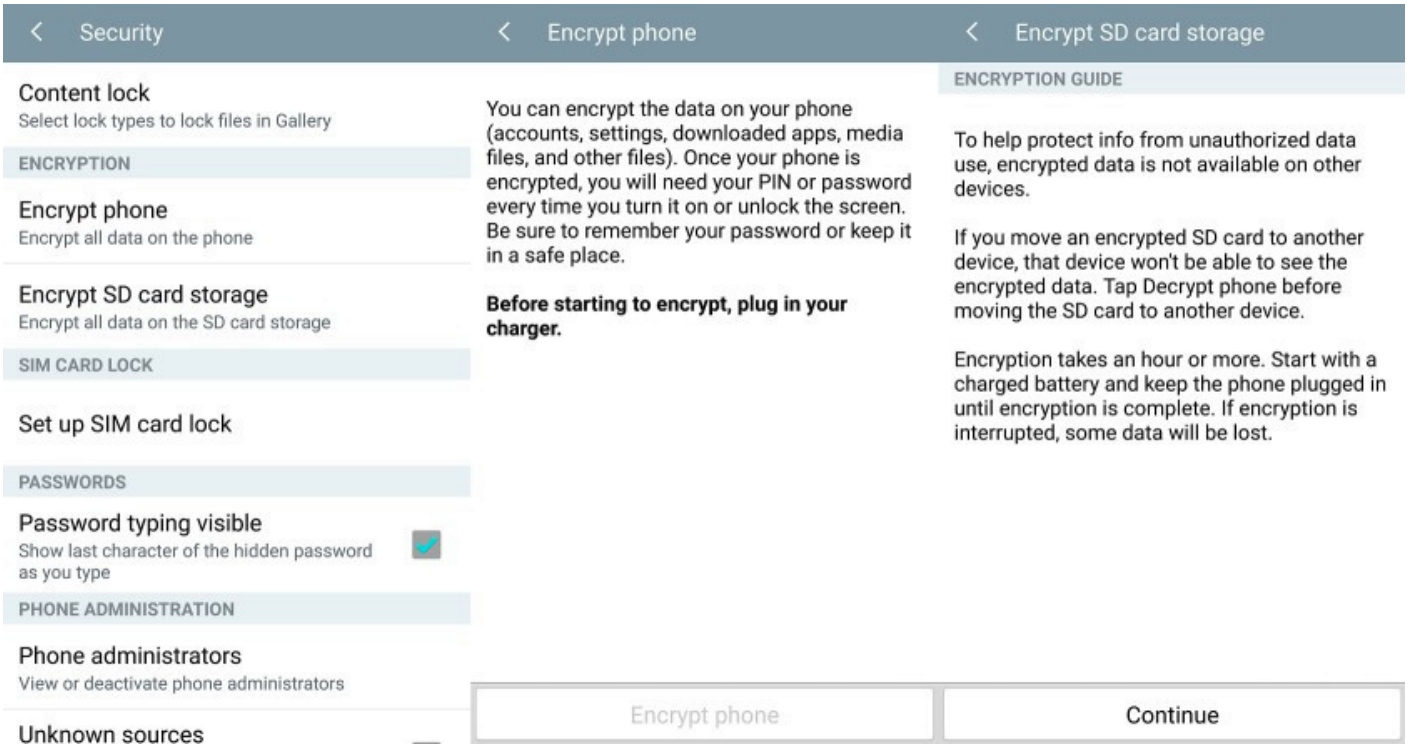
Téléphones Android

Aujourd'hui, par défaut, la plupart des appareils sont cryptés, en particulier les appareils qui fonctionnent sous les dernières versions d'Android. Si jamais ce n'était pas le cas sur votre appareil, il est possible et simple de l'activer.

Pour connaitre quelle version d'android fonctionne sur votre téléphone : https://www.astuces-aide-informatique.info/4826/identifier-version-android

Android 5.0 ou plus

Pour les téléphones et tablettes sous Android 5.0 Lollipop ou plus récent, vous pouvez aller directement dans l'onglet 'Sécurité'. Cela dépend un peu des appareils pour y accéder, mais généralement on y arrive via Paramètres > Personnel > Sécurité.



Vous trouverez ici une option pour chiffrer votre téléphone. Vous devrez brancher celui-ci sur secteur pour être sûr·e que le processus puisse se faire sans encombre. Si vous ne l'avez jamais fait, il vous sera demandé de choisir un code PIN ou mot de passe dont vous aurez besoin pour déverrouiller votre téléphone.

Android 4.4 ou moins

Si vous avez un téléphone avec Android 4.4 KitKat ou moins, vous devrez configurer un mot de passe ou PIN avant de commencer le processus de cryptage. Allez dans Paramètres > Sécurité > Verrouillage de l'écran. Vous pouvez choisir entre un schéma, des chiffres (PIN) ou un mélange de chiffres et lettres. Ce sera votre mot de passe après le chiffrement alors assurez-vous de le retenir.

Une fois que c'est fait, vous pouvez revenir au menu Sécurité et cocher 'Chiffrer le téléphone', ou 'Chiffrer la tablette'. Vous devrez brancher votre téléphone sur secteur et lire les messages d'avertissement, et sûrement confirmer votre mot de passe une dernière fois avant que commence le processus de cryptage.

Le cryptage du téléphone peut durer une heure ou plus, en fonction de la puissance de votre appareil et la quantité de données stockées. Une fois le processus terminé vous pouvez déverrouiller votre appareil et commencer à utiliser votre appareil fraîchement chiffré.

i De retour dans le menu sécurité, vous pourrez aussi chiffrer votre carte microSD. C'est recommandé pour que toutes vos données soient sécurisées. Veuillez noter que dans ce cas, votre carte microSD ne pourra pas être utilisée sur un autre appareil (ordinateur, appareil photo, ...).

ℹ Il peut être assez difficile de se souvenir d'un mot de passe permettant un niveau de chiffrement élevé, c'est une raison pour laquelle les mots de passe choisis sont souvent moins sécurisés, plus courts. Sur tous les appareils Android, il y a une option schéma qui est excellente car des gestes complexes sont souvent plus faciles à retenir qu'un mot de passe complexe. Assurez-vous que le schéma contienne au moins six lignes, et une grille de 4x4 points ou plus.

Un point sur les sauvegardes Android

Les appareils Android sont synchronisés avec différents types de sauvegardes à distance. Toutes ces sauvegardes doivent être désactivées au profit d'une sauvegarde en local sur un appareil (comme un ordinateur par exemple), qui doit lui-même avoir un disque dur entièrement chiffré (cf. Sécurité de l'ordinateur: 1 - Saisie par la police). Avant de faire des sauvegardes, les fonctionnalités telles que 'SideSync' doivent être désactivées.

⚠ Les développeu·r·se·s et passioné·e·s ont souvent des fonctionnalités spéciales pour manipuler leur téléphone en bas niveau, cela peut présenter des risques. Par exemple, activer le 'USB Debugging' présente un risque réel qu'un "attaquant" ayant un accès physique à l'appareil puisse utiliser les outils `adb` d'Android pour accéder à l'appareil. Assurez-vous que le débogage par USB est désactivé avant d'aller sur une action.

Références

How to encrypt your iphone ?

How to encrypt android device ?

▶ Suivant : Sécurité du téléphone 2 - Tracage par gsm et wifi

---

Créé 2023-09-08 20:16:22 CEST par mollusque
Mis à jour 2025-07-29 20:49:15 CEST par Guest