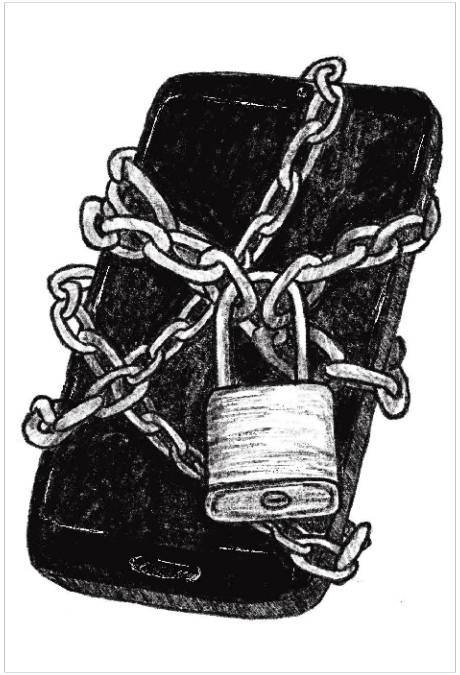


En sécurité

Quelques conseils simples
pour sécuriser ton cellulaire

https://distro.f-91w.club

Nous utilisons tous des téléphones intelligents. Ils sont pratiques et amusants, mais ils contiennent également beaucoup d'information sur nous et notre réseau social. Si quelqu'un qui te veut du mal arrive à mettre la main sur ton cellulaire, ton téléphone intelligent peut s'avérer très dangereux. Il se peut que ton cellulaire soit volé (ou « confisqué ») par de telles personnes en de multiples circonstances.

Le chiffrement généralisé des messages veut dire que c'est plus difficile d'accéder à des communications privées – souvent, la manière la plus facile de le faire c'est d'avoir un accès physique à l'appareil. Si de mauvaises personnes veulent accéder aux informations ou aux messages sur ton cellulaire, ils vont probablement essayer de t'arrêter et de te détenir pour le confisquer – s'ils ont les ressources pour le faire.

Par exemple, lors de la récente vague d'arrestations à Toronto ciblant des militants et des militantes solidaires avec la Palestine, la police a mené des perquisitions au domicile afin d'effectuer des arrestations et confisquer des cellulaires et d'autres appareils. Ils pourraient utiliser ce qu'ils trouvent dans ces cellulaires pour criminaliser d'autres personnes.

C'est une situation inquiétante, mais on n'est pas impuissants. ***Ne te laisse pas intimider, n'aie pas peur d'afficher tes idées et d'organiser de manière publique.*** Il faut juste connaître les risques pour te protéger toi et les personnes autour de toi en réfléchissant à ces simples mesures technologiques et comportementales.

Ce n'est pas tout ou rien – il ne faut pas faire tout ce que nous suggérons ici, mais plus c'est mieux.

Nous nous gardons en sécurité

Alors on t'a pris ton portable...

Une fois que tu es libre et en mesure de le faire, tu peux agir pour atténuer les préjudices :

- Sur un autre appareil, tu peux révoquer toutes les sessions des services comme Google et iCloud.
- Le plus rapidement possible, il faut obtenir une nouvelle carte SIM puis transférer ton numéro et, sur un nouveau cellulaire, t'inscrire à toutes les applis que tu utilises d'habitude. Pour Signal, ceci fera en sorte que ton ancien cellulaire ne reçoit plus les nouveaux messages qui te sont destinés.
- Pour WhatsApp, une fois que tu auras configuré un nouveau cellulaire primaire, tu peux déconnecter les autres appareils.
- Il faut ensuite changer tous ses mots de passe, y compris pour les réseaux sociaux.

Cependant, il y a des limites à ce qu'on peut faire. Toutes les données sur ton portable sont susceptibles d'être copiées et analysées et on ne peut pas changer ce qui était présent au moment de la confiscation du cellulaire (à moins que tu n'arrives à effectuer un effacement à distance très rapidement, ce qui peut te causer encore plus d'ennuis). ***C'est pour cette raison que les mesures préventives énumérées ici sont si importantes!***

Si on te rend ton cellulaire après l'avoir pris, il ne faut pas continuer à l'utiliser, car il y a toutes les chances qu'il ait été compromis. Il faut considérer toutes les données là-dessus comme étant perdues et se contenter de remplacer l'appareil (ce qui est beaucoup plus facile à faire si tu as des sauvegardes accessibles et à jour!).

Continuons à organiser

Assurons notre sécurité

Protégeons et défendons les uns les autres

Préparons-nous à gagner

également le moment de faire une sauvegarde chiffrée des fichiers que tu veux conserver, mais que tu n'as pas besoin de porter avec toi dans ton cellulaire!

8. Ne pas afficher les messages sur l'écran de verouillage

Si ton cellulaire est confisqué sans avoir été éteint (il n'est donc pas chiffré), c'est plutôt grave. Mais c'est encore pire s'il ne faut même pas le déverrouiller pour voir les messages qui arrivent! Imagine tous les messages qu'on envoie dans tes groupes de discussion en raison de la confiscation de ton cellulaire et la personne qui l'a pris qui lit tous ces messages en temps réel sur ton écran de verrouillage! Tu peux régler Signal pour ne pas afficher le nom de l'expéditeur et le contenu du message dans les notifications. Ceci se trouve dans Paramètres -> Notifications -> Afficher.

9. Laisser le cellulaire à la maison

Les perquisitions au domicile coûtent cher et ne sont pas faciles. C'est bien plus facile de prendre le cellulaire à quelqu'un arrêté dans la rue ou lors d'une manifestation ou d'une action. Si tu comptes participer à quelque chose avec ce risque, il vaut mieux laisser ton cellulaire *à la maison.* Soyons prudents. La vie est imprévisible et on ne sait jamais ce qui pourrait se produire quand on sort de chez soi. Si ton cellulaire est chez toi (chiffré et éteint), on ne peut pas te le prendre lors d'une action. Il faut un certain temps pour s'y habituer, mais t'es plus en sécurité sans ton cellulaire. Cela implique de faire des plans qui ne demandent pas de cellulaire (ou prendre le temps de configurer un téléphone jetable). Fais des plans avec tes amis en avance. Mémorise les numéros importants ou note-les sur ton bras. Porte une montre. Achète une carte en papier.

1. Chiffrer ton cellulaire

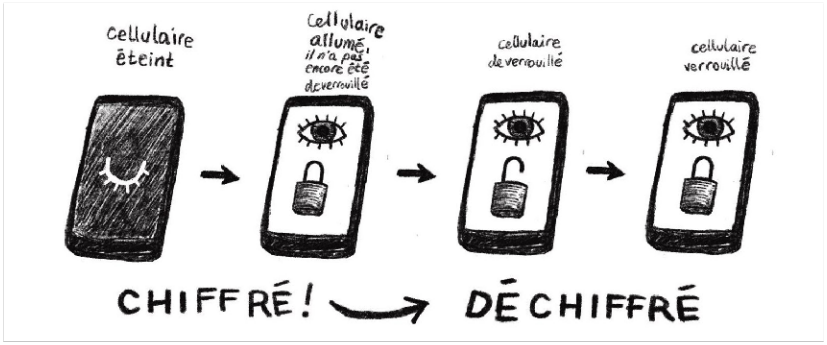
Le chiffrement signifie que les données sur ton appareil sont encodées de telle sorte qu'on ne peut pas les lire sans les avoir décodées à l'aide d'une clé.

iPhone : le chiffrement est activé automatiquement si tu utilises une phrase de passe
Android : tu peux activer le chiffrement dans les paramètres de sécurité

Si ton cellulaire n'est pas chiffré, n'importe qui qui y a accès peut voir son contenu en le copiant sur un ordinateur *même s'il ne connaît pas ta phrase de passe.*

2. Garder ton cellulaire éteint

La plupart des cellulaires ne sont chiffrés *qu'avant que tu ne saisisses ta phrase de passe pour la première fois après avoir allumé le cellulaire.* Après, les données sur le cellulaire sont, en fait, déchiffrées et l'écran de verrouillage ne sert qu'à empêcher quelqu'un de prendre ton cellulaire et de se mettre immédiatement à l'utiliser. Si un cellulaire est confisqué après avoir été allumé et déverrouillé pour la première fois (déchiffré), un hacker avec un peu de talent peut accéder à toutes les données en connectant le cellulaire à un ordinateur.
Donc c'est une bonne idée de garder ton cellulaire éteint le plus



possible! Certains cellulaires disposent d'une option pour planifier quand le cellulaire va s'éteindre – sur Android, ça se trouve au plus souvent dans les paramètres du système ou d'alimentation. D'autres te permettent de faire en sorte que le cellulaire redémarre après une

durée donnée. De tels réglages aident à sécuriser tes données, car redémarrer un portable remet en place le chiffrement.

Si tu te trouves dans une situation où tu risques de perdre ton cellulaire, tu peux essayer de l'éteindre avant qu'il soit volé.

Achète-toi un réveil-matin et éteins ton portable la nuit!

3. Utiliser une phrase de passe fiable

Comme le chiffrement cache tes données derrière une phrase de passe, le chiffrement n'est fiable que si tu utilises une bonne phrase de passe. Une bonne phrase de passe est composée de lettres et de chiffres et est aussi longue que tu peux t'en souvenir. Pense à utiliser un mot de passe composé d'au moins cinq mots aléatoires et un chiffre. N'utilise pas le déverrouillage par balayage et n'utilise pas un code de passe composé uniquement de chiffres – ils sont faciles à décoder.

Il n'est pas idéal d'utiliser une empreinte digitale ou la reconnaissance faciale (« la biométrie ») pour sécuriser ton cellulaire, car on peut plus facilement te forcer à déverrouiller ton cellulaire s'il est verrouillé (la police peut te forcer de le faire, par exemple).

Je sais que c'est pas idéal d'avoir à saisir plein de caractères chaque fois que tu veux voir un truc sur ton cellulaire, mais c'est encore moins idéal si le contenu de ton cellulaire permet d'incarcérer des gens que tu aimes!

4. Utiliser des applis chiffrées

Il est important de chiffrer ton cellulaire, mais si tu envoies tous tes messages par SMS, courriel ou des services qui ne respectent pas ta vie privée (comme Instagram, Discord et Facebook Messenger), les gens qui te veulent du mal peuvent encore accéder à tes messages. Signal est probablement l'appli de messagerie la plus sécuritaire qui dispose de toutes les fonctionnalités auxquelles la plupart des utilisateurs s'attendent, mais WhatsApp n'est pas mal. Cela dit, utiliser une appli de messagerie sécuritaire ne va pas *à lui seul* vous protéger si votre cellulaire est capturé!

5. Activer les messages éphémères

Signal et WhatsApp disposent tous les deux d'une fonctionnalité pour détruire les messages après une période donnée. Cela veut dire que même si quelqu'un arrive à accéder aux données sur ton cellulaire, il n'aura accès qu'aux messages du jour précédent (ou de la semaine précédente selon tes réglages). Il y a aussi un paramètre dans Signal pour limiter la longueur des conversations sauvegardées – par exemple, Signal ne conservera que les 30 messages les plus récents dans une conversation et effacera les autres. Ceci se trouve dans Paramètres -> Données et stockage -> Gérer l'espace de stockage.

6. Se méfier des sauvegardes

Alors, tu as chiffré ton cellulaire et tu utilises une appli de messagerie chiffrée… mais si le tout est sauvegardé sur iCloud ou Google Drive où il est stocké sans chiffrement, il est à la portée de n'importe qui qui peut convaincre ces services de le leur donner. Les sauvegardes automatiques et la synchronisation (p. ex. pour WhatsApp et Google) sont utiles, mais elles veulent dire que tes données sont stockées quelque part hors de ton contrôle.

Souvent, la façon la plus facile de contourner le chiffrement d'un cellulaire est d'envoyer une requête pour données à Google ou à Apple qui vont remettre les sauvegardes non chiffrées. Il vaut mieux désactiver ces fonctionnalités (ou au moins, les désactiver pour tes applis de messagerie et ta liste de contacts) et effacer les données sauvegardées si possible. C'est une bonne idée de faire des sauvegardes, mais assure-toi qu'elles sont chiffrées et stockées sur un serveur que *tu* contrôles ou tout simplement sur un disque dur chiffré rangé en toute sécurité.

7. Effacer les vieux contenus

C'est une bonne idée de passer en revue les fichiers sur ton cellulaire de temps en temps pour effacer tout ce dont tu n'as plus besoin. Cela peut comprendre les vieux messages, photos, captures d'écran, notes et calendriers et ton historique de navigation. Comme ça, tu est moins exposé si quelqu'un arrive à pénétrer dans ton cellulaire. Il est