
GUIDE POUR AUGMENTER LA SÉCURITÉ DE SON SMARTPHONE

1 CHOISIR UN VERROUILLAGE COMPLEXE

Le verrouillage est la première barrière de sécurité contre une utilisation frauduleuse de notre smartphone. Il peut s'agir d'un code de verrouillage, d'un modèle à tracer, d'une lecture d'empreintes digitales ou même d'une lecture de l'iris. Ces méthodes ont leurs avantages et leurs inconvénients. Chacune de ces options présentent des failles qu'il est plus ou moins facile de corriger. Sans même parler de failles techniques, certaines présentent un niveau de complexité peu élevé (un modèle ou un mot de passe trivial par exemple).

L'un des problèmes typiques de sécurité informatique se pose : **sécurité ou facilité d'utilisation ?**

Ces deux critères sont souvent opposés : utiliser un mot de passe long et compliqué protège bien le smartphone mais demande de prendre le temps de le rédiger à chaque ouverture.

L'idéal est donc de bien doser. Concernant l'option de verrouillage à choisir, **on conseille habituellement le mot de passe ou l'empreinte.**

Deux méthodes simples peuvent vous aider à définir vos mots de passe :

- la méthode phonétique : « J'ai acheté 5 CDs pour cent euros cet après-midi » :
ght5CDs%E7am ;
- la méthode des premières lettres : « Allons enfants de la patrie, le jour de gloire est arrivé » :
aE2lP,lJ2Géa!

2 INSTALLER UN ANTIVIRUS

Installer un antivirus pour smartphone. Certaines choses sont à savoir concernant les antivirus pour smartphones :

- oui ils n'arrêtent **pas toutes les applications malveillantes**, tout comme l'ordinateur avec les malwares ;
- oui ils demandent un peu plus de consommation RAM/Processeur sur votre smartphone, comme d'autres applications.

Un antivirus est tout de même une sécurité supplémentaire et recommandée.

Tous les antivirus n'ont pas les mêmes fonctionnalités. Dans l'ensemble un antivirus permet de :

- verrouiller des applications sensibles par modèle ou code PIN ;
- scanner les fichiers et applications du mobile et de la carte SD ;
- nettoyer l'historique de navigation et les fichiers indésirables ;
- optimiser l'appareil ;
- bloquer des appels ;
- sauvegarder les contacts, les SMS ;
- protéger la navigation Internet ;
- etc...

On ajoutera également qu'il existe de nombreuses applications utilitaires permettant le nettoyage, l'optimisation et la sécurité.

À noter qu'il est inutile et contreproductif d'en **installer plusieurs à la fois.**

3 BLOQUER LES SOURCES NON SÛRES

Le vecteur d'infection numéro 1 des appareils mobiles est l'installation d'applications venant **de sources non sûres**.

Les applications terminent typiquement par l'extension ".apk" et rien n'empêche de partager une telle application via un site web donné hors du *Play Store (pour Android)*. Le blocage est habituellement mis en place par défaut sur la plupart des appareils. Vous pouvez tout de même vérifier sur le vôtre.



Votre smartphone peut également se connecter automatiquement à **un réseau Wi-Fi non sûr**, mais aussi **via Bluetooth ou encore NFC**. Garder ces options activées en permanence n'est pas recommandé. Vous pouvez donc les activer au besoin via les paramètres du smartphone et non pas en permanence.

4 CHIFFRER SES DONNÉES

Il s'agit aussi de fonctionnalités plus ou moins par défaut, mais si votre téléphone n'est pas doté de cette option, vous pouvez utiliser des applications spécialement conçues pour cela.

Ce type d'application permet de :

- stocker et gérer ses mots de passe ;
- chiffrer des messages au format texte ;
- chiffrer des fichiers ou dossiers ;
- créer des coffres-forts numériques (dossiers protégés par mots de passe) ;
- permet de visionner/traiter les fichiers au sein du coffre-fort ;
- etc...

5 PENSER A LA PERTE OU AU VOL DU SMARTPHONE

Perdre son smartphone arrive souvent, parfois même dans notre propre chambre. Mais se faire voler son téléphone pose un plus gros problème et effectuer un appel ne suffira pas forcément à retrouver le voleur.

Il existe pour cela des applications permettant de :

- faire sonner votre téléphone à distance ;
- recevoir les coordonnées GPS du téléphone à distance ;
- verrouiller le téléphone à distance ;
- réinitialiser entièrement le téléphone (carte SD et SIM) à distance ;
- prendre des photos à distance.

En plus de cela, certaines applications permettent également de **cacher l'icône de l'application** et **empêcher sa désinstallation**.

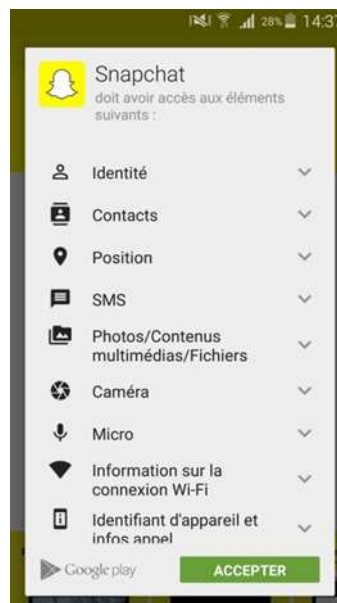
6 VEILLER A L'UTILISATION DE NOS DONNÉES

Lors de l'installation de toutes applications, des informations sont affichées quant à nos données que l'application pourra traiter : ici le cas de l'application Snapchat.

Certaines applications ont besoin de certaines données pour de raisons évidentes, alors que d'autres demandent l'autorisation de les utiliser sans vraiment que l'on sache pourquoi.

L'idéal est ici de bien prendre conscience que ces données seront **accessibles à l'application qui pourra en faire ce qu'elle veut**.

C'est notamment pour cela que l'on conseille de ne pas installer des applications sans en avoir absolument besoin.



7 SAUVEGARDER TOUT

Un mobile volé, des données supprimées par mégarde ou un crash irrécupérable et vos données se sont vaporisées pour de bon. Sauf si vous avez fait des sauvegardes auparavant. Certaines applications permettent de faire des sauvegardes de vos fichiers, votre mobile lui-même peut proposer ce type de fonctionnalité par défaut.

La sauvegarde est à faire non seulement via les applications mais également par vous-même. Par exemple le numéro IMEI et autres codes sont à garder dans un endroit sûr (et en dehors du téléphone).

8 METTRE A JOUR

Il s'agit de l'un des points les plus **importants**. Mettre à jour son téléphone et les applications permet de corriger les vulnérabilités. On imagine trop souvent que mise à jour rime avec "nouvelle fonctionnalité" alors qu'il s'agit également (et surtout !) de **patcher le mobile ou l'application contre des failles**.

La mise à jour **nous concerne également**, se tenir informé des menaces est un excellent moyen pour ne pas tomber dans un piège à l'avenir. 90% des piratages réussis exploitent en fait la faiblesse de l'être humain.

À ce propos, saviez-vous que :

- des malwares peuvent vous espionner même avec votre téléphone **éteint** ;
- d'autres malwares peuvent effectuer des appels depuis votre téléphone **sans permissions** ;
- encore d'autres sont extrêmement **sophistiqués** (contrôle à distance, blocage des désinstallations, ransomware...etc) ;
- des **milliards** de périphériques mobiles se retrouvent régulièrement vulnérables à **des failles critiques** (élévation de privilèges, exécution de code à distance...etc).