Sécuriser son Smartphone sous Android en 8 étapes

Android représente environ 70% de part du marché des systèmes d'exploitation pour smartphone contre 15 à 20% pour iOS. C'est un OS moderne qui permet non seulement l'envoi de SMS/MMS mais aussi d'installer toutes sortes d'applications pour nous **localiser,** traiter des données **médicales** et bien d'autres.

Tout le monde peut, à l'aide d'un tutoriel, créer une application Android. Et ensuite tout le monde peut la télécharger **facilement et gratuitement**. Cette facilité de création combinée à une utilisation massive par des personnes non sensibilisées est un point d'entrée idéal pour les pirates informatiques.

Voici donc les 8 étapes pour sécuriser son mobile sous Android

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. Chaque option possède également des failles, plus ou moins patchées. Lorsqu'il ne s'agit pas de failles, il s'agit d'un problème de complexité permettant de débloquer le téléphone en devinant par exemple le modèle ou le mot de passe.

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

Ces deux critères sont souvent opposés. Faut-il utiliser un mot de passe long et compliqué qui protège bien le smartphone en contrepartie de prendre 30 secondes à débloquer le téléphone, ou un modèle simple à tracer mais facile à deviner ?

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

2. Installer un antivirus

Installer un antivirus pour smartphone : Pour ou contre ? Cette question est souvent au centre des débats.

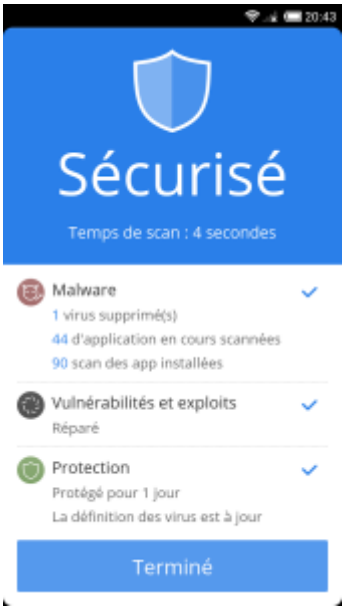
Certaines choses sont à savoir concernant les antivirus pour smartphones :

- 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.

Voici les antivirus parmi les meilleurs pour Android. À noter qu'il est inutile et contreproductif d'en **installer plusieurs à la fois** :

CM Security AppLock & Antivirus Installer



CM Security est l'une des applications antivirus Android les mieux notées avec plus de 8 000 000 d'avis positifs.

Cette application 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
- etc…

Avast! Mobile Security & Antivirus Installer

Il s'agit de la version Android du fameux logiciel antivirus Avast!

Cette application permet de :

- Scanner en temps réel les applications, les fichiers sur carte SD…etc
- Verrouiller des applications avec modèle ou code
- Sauvegarder les contacts, les SMS…etc
- Bloquer des applications via le pare-feu
- Retrouver son téléphone en cas de vol
- etc…

Lookout Antivirus & Securité Installer

Cette application permet de :

- Scanner en continu les applications contre des programmes malveillants et autres adwares
- Retrouver l'appareil et déclencher une alarme en cas de vol (avec photo du voleur)
- Enregistrer automatiquement la position dès que la batterie est faible
- Sauvegarder et transférer des contacts
- Protéger la navigation Internet
- etc…

On ajoutera également ici les applications utilitaires (nettoyage, optimisation, sécurité) suivantes :

- Ccleaner
- Clean Master
- Malwarebytes Anti-Malwares

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 Android terminent typiquement par l'extension ".apk" et rien n'empêche de partager une telle application via un site web donné hors du *Play Store*.

Le blocage est habituellement mis en place par défaut sur la plupart des appareils. Vous pouvez tout de même vérifier sur le vôtre.

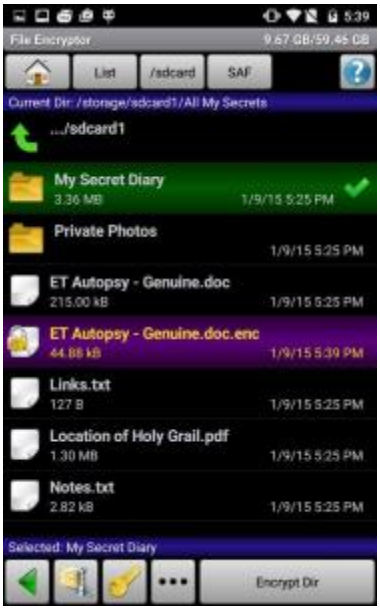
Votre smartphone peut également se connecter automatiquement à un réseau Wi-Fi non sûr, mais aussi via Bluetooth ou encore NFC.

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 (cf image précédente), mais si votre téléphone n'est pas doté de cette option, vous pouvez utiliser des applications spécialement conçues pour cela. En voici parmi les mieux notées :

SSE Universal Encryption App 



Cette application permet de :

- Stocker et gérer ses mots de passe
- Chiffrer des messages au format texte
- Chiffrer des fichiers ou dossiers
- etc…

Cybersafe Chiffrement Installer

Cette application permet de :

- Créer des coffres-forts numériques (dossiers protégés par mots de passe)
- Chiffrer des dossiers via le réseau
- Permet de visionner/traiter les fichiers au sein du coffre-fort
- etc…

5. Penser à 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. C'est pour cela qu'il existe l'application suivante :

Where's My Droid Installer

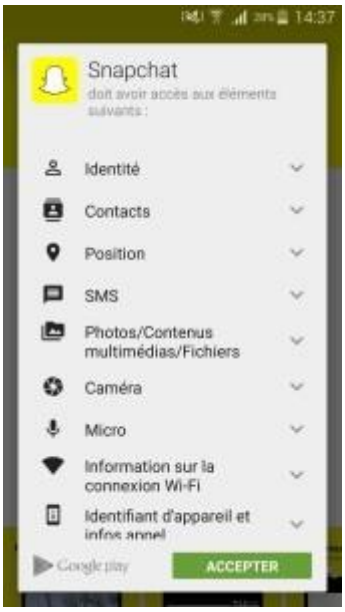
Where’is My Droid permet de :

- 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

Le tout en envoyant des SMS personnalisés au téléphone volé. En plus de cela, Where’s My Droid permet également de **cacher l’icône de l’application** et **empêcher sa désinstallation**.

6. Veiller à l’utilisation faites de nos données

Lors de l’installation de toutes applications Android (via *Play Store*), des informations sont affichées quant à nos données que l’application pourra traiter.



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.

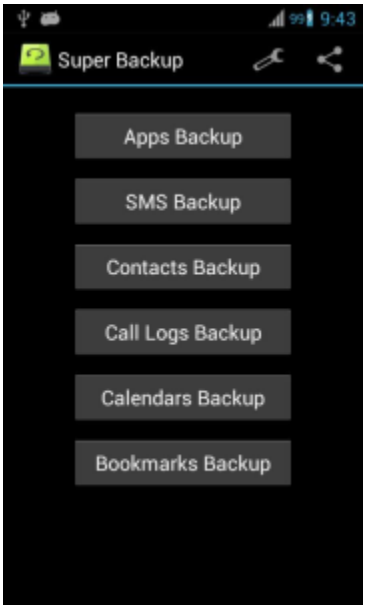
7. Sauvegarder tout

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 citées dans cet article permettent de faire des sauvegardes de vos fichiers, votre mobile lui-même peut proposer ce type de fonctionnalité par défaut.

Mais si une application vous intéresse, voici l’une des plus populaires :

Super Backup SMS & Contacts 



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 à 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(e) 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 Android se retrouvent régulièrement vulnérables à **des failles critiques** (élévation de privilèges, exécution de code à distance…etc)