SÃ©curitÃ© : 10 astuces pour amÃ©liorer la sÃ©curitÃ© de son appareil mobile
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 11/12/2013 11:30:00

L'expert en sÃ©curitÃ© Avira a rÃ©uni des astuces visant Ã amÃ©liorer la **sÃ©curitÃ© des appareils mobiles en 10 Ã©tapes** faciles Ã rÃ©aliser.
1. DÃ©finissez un **mot de passe fiable** pour votre appareil mobile

2. Mettez au point une **solution anti-vol**

Les appareils mobiles se perdent ou se font voler plus facilement que des ordinateurs portables ou de bureau. C'est pourquoi il est primordial de configurer un tel outil. Certains appareils mobiles sont Ã©quipÃ©s d'une solution prÃ©installÃ©e, d'autres pas (l'iPhone dispose de Â« Localiser mon iPhone Â», AndroÃ¯d les services Google). Avira propose Ã©galement une solution gratuite, Avira Free Mobile Security (Android et iOS).

3. Installez les derniÃ¨res **mises Ã jour** du systÃ¨me d'exploitation

Peu importe qu'il s'agisse d'iOS, Android, Windows mobile, etc., car ils seront tous mis Ã jour s'ils sont pris en charge par le fournisseur. Souvent, la derniÃ¨re version du systÃ¨me d'exploitation n'apporte pas seulement de nouvelles fonctionnalitÃ©s mais s'accompagne Ã©galement de mises Ã jour de sÃ©curitÃ© essentielles.

Â

Â

4. Installez les derniÃ¨res **mises Ã jour** de vos applications

Comme ci-dessus, non seulement le systÃ¨me d'exploitation est vulnÃ©rable, mais ce sont aussi les applications qui posent des problÃ¨mes de sÃ©curitÃ© la plupart du temps.

5. Installez une **solution de sÃ©curitÃ©**

MÃªme si les logiciels malveillants ne sont pas aussi rÃ©pandus sur les plateformes mobiles qu'ils le sont sous Windows, les menaces sont bien prÃ©sentes. Nombreuses sont les applications qui ne sont pas ce qu'elles affichent et, plus important, qui ne font pas ce qu'elles affirment. Un antivirus peut donc se rÃ©vÃ©ler essentiel.

6. N'installez **aucune application** ne provenant pas des boutiques d'applications officielles

Il existe des milliers de boutiques non officielles d'applications pour Android, et certaines d'entre elles pourraient installer des applications inconnues et non vÃ©rifiÃ©es mettant en danger la sÃ©curitÃ© de votre appareil.

7. **Ne rootez pas votre appareil**

Rooter un appareil peut rendre la garantie protÃ©geant votre appareil nulle et non avenue et peut engendrer Ã©galement d'autres failles de sÃ©curitÃ©. Concernant iOS, cela peut permettre d'installer des applications issues de boutiques non officielles et donc de compromettre la sÃ©curitÃ© de votre mobile.

8. **Chiffrez le stockage**

Certains appareils mobiles, pour ne pas dire tous Ã l'heure actuelle, autorisent le chiffrement du stockage (externe ou intÃ©grÃ©). Ceci est important si vous stockez tous types d'information sur votre appareil mobile (Ã l'exemple des tablettes).

9. N'utilisez que des **connexions de rÃ©seau Wi-Fi sÃ©curisÃ©es**

En vous connectant Ã des rÃ©seaux Wi-Fi non sÃ©curisÃ©s, vous envoyez toutes les donnÃ©es en texte brut. Mots de passe compris ...

10. Utilisez votre appareil **en vous souciant de la sÃ©curitÃ©**

MÃªme si vous utilisez un systÃ¨me d'exploitation autre que Windows, ceci ne signifie pas que vous Ãªtes Ã l'abri de toute infection. Faites preuve de prÃ©caution quand vous naviguez sur des sites Web suspects, quand vous ouvrez des piÃ¨ces jointes Ã des e-mails, quand vous autorisez des applications Ã accÃ©der Ã vos donnÃ©es ou quand elles demandent des **privilÃ¨ges spÃ©ciaux** dont elles n'ont pas besoin pour fonctionner.