

**S curit  : 10 astuces pour am liorer la s curit  de son appareil mobile**  
**S curit **

Post  par : JPilo

Publi e le : 11/12/2013 11:30:00

L'expert en s curit  Avira a r uni des astuces visant   am liorer la **s curit  des appareils mobiles en 10  tapes** faciles   r aliser.

1. D 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  quip s d'une solution pr install e, d'autres pas (l'iPhone dispose de  « Localiser mon iPhone  », Andro d les services Google). Avira propose  galement une solution gratuite, Avira Free Mobile Security (Android et iOS).

3. Installez les derni res **mises   jour** du syst me d'exploitation

Peu importe qu'il s'agisse d'iOS, Android, Windows mobile, etc., car ils seront tous mis   jour s'ils sont pris en charge par le fournisseur. Souvent, la derni re version du syst me d'exploitation n'apporte pas seulement de nouvelles fonctionnalit s mais s'accompagne  galement de mises   jour de s curit  essentielles.

 



 

#### 4. Installez les derni res **mises   jour** de vos applications

Comme ci-dessus, non seulement le syst me d'exploitation est vuln rable, mais ce sont aussi les applications qui posent des probl mes de s curit  la plupart du temps.

#### 5. Installez une **solution de s curit **

M me si les logiciels malveillants ne sont pas aussi r pandus sur les plateformes mobiles qu'ils le sont sous Windows, les menaces sont bien pr 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 r v 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 v rifi es mettant en danger la s curit  de votre appareil.

#### 7. **Ne rootez pas votre appareil**

Rooter un appareil peut rendre la garantie prot geant votre appareil nulle et non avenue et peut engendrer  galement d'autres failles de s curit . Concernant iOS, cela peut permettre d'installer des applications issues de boutiques non officielles et donc de compromettre la s curit  de votre mobile.

#### 8. **Chiffrez le stockage**

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

#### 9. N'utilisez que des **connexions de r seau Wi-Fi s curis es**

En vous connectant   des r seaux Wi-Fi non s curis s, vous envoyez toutes les donn es en texte brut. Mots de passe compris ...

#### 10. Utilisez votre appareil **en vous souciant de la s curit **

M me si vous utilisez un syst me d'exploitation autre que Windows, ceci ne signifie pas que vous  tes   l'abri de toute infection. Faites preuve de pr caution quand vous naviguez sur des sites Web suspects, quand vous ouvrez des pi ces jointes   des e-mails, quand vous autorisez des applications   acc der   vos donn es ou quand elles demandent des **privil ges sp ciaux** dont elles n'ont pas besoin pour fonctionner.