10 recommandations pour une utilisation sÃ©curisÃ©e des appareils mobiles
MobilitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 20/12/2012 13:30:00

Les appareils mobiles sont de plus en plus rÃ©pandus et les offres de nouvelles applications, tant pour les affaires que pour les loisirs, inondent le marchÃ©. Les Smartphones et les tablettes, cadeaux de NoÃ«l plÃ©biscitÃ©s, servent Ã jouer, faire des achats, payer les factures et partager des rÃ©flexions sur les mÃ©dias sociaux.

L'entreprise de sÃ©curitÃ© rÃ©seau Stonesoft prodigue **dix conseils pour assurer une utilisation cyber-sÃ©curisÃ©e** de nos dispositifs mobiles.

Â«*Presque toutes les fonctions sont disponibles sur Internet de nos jours, et la criminalitÃ© organisÃ©e y a malheureusement aussi trouvÃ© sa place.Pour le consommateur, la cybercriminalitÃ© peut reprÃ©senter une menace lointaine, principalement liÃ©e Ã l'espionnage entre les Etats-nations ou au piratage de donnÃ©es des grandes entreprises. Toutefois, mÃªme les achats en ligne peuvent Ãªtre impactÃ©s. Avec un appareil mobile, on vÃ©hicule Ã chaque moment une importante masse d'informations personnelles, y compris numÃ©ro de carte de crÃ©dit,* "dit **Joona Airamo**, le RSSI de Stonesoft.

STONESOFT

Secure Information Flow

Quelques prÃ©cautions de base valent la peine dâ□□Ãªtre appliquÃ©es, notamment lorsquâ□□on sait quâ□□il existe de logiciels malveillants nocifs et que les appareils sont faciles Ã voler.

Voici les conseils Stonesoft pour une utilisation sÃ»re des tÃ©lÃ©phones mobiles.

1. Mettre les programmes et le systÃ¨me d'exploitation de l'appareil mobile rÃ©guliÃ¨rement Ã jour. Les mises Ã jour sont fournies automatiquement en gÃ©nÃ©ral. Lorsque vous optez pour un nouvel appareil mobile, assurez-vous que les mises Ã jour sont disponibles pour le systÃ¨me d'exploitation du modÃ¨le en question.

2. Installer des programmes venant de sources fiables et bien connus tels que App Store, Google Play ou Nokia Store. Un jeu Ã un euro peut Ãªtre disponible gratuitement ailleurs, mais il est tout Ã fait susceptible de contenir des logiciels malveillants.

3. Soyez prudent avec des achats Â« in-apps Â» - ils peuvent devenir coÃ»teux. Par exemple, les jeunes peuvent acheter des superpuissances pour leurs personnages de jeu sans comprendre les coÃ»ts supplÃ©mentaires attachÃ©s. Dans de nombreux appareils mobiles, les achats Â« in-apps Â» peuvent Ãªtre dÃ©sactivÃ©s.

4. Surveiller les droits que vous avez accordÃ©s Ã diffÃ©rentes applications. De temps en temps, passer en revue tous les droits d'utilisation et politiques de confidentialitÃ© que vous avez acceptÃ©s. Par exemple, le droit Ã l'information de localisation et le droit Ã la connexion rÃ©seau pour la mÃªme application permettent le suivi de votre emplacement Ã distance. De nombreuses applications vidÃ©o et de mÃ©dias sociaux nÃ©cessitent des droits d'utilisateur aux images tÃ©lÃ©chargÃ©es vers leurs plates-formes.

5. Changer le code d'accÃ¨s par dÃ©faut et le code PIN de la carte SIM. Ne pas utiliser votre annÃ©e de naissance ou d'autres combinaisons de chiffres trop faciles Ã deviner. RÃ©gler votre appareil pour quâ□□il sollicite le mot de passe ou un motif secret chaque fois que vous l'utilisez.

6. Si votre appareil prend en charge le cryptage des donnÃ©es, activer cette fonctionnalitÃ©.

7. Vous pouvez connecter vos appareils mobiles Ã un service en ligne qui permet Ã distance de localiser un appareil perdu ou volÃ© et, si nÃ©cessaire, effectuer une opÃ©ration Ã distance pour effacer toutes les donnÃ©es.

8. Si votre appareil mobile est volÃ©, en informer votre opÃ©rateur immÃ©diatement afin que l'utilisation de votre carte SIM puisse Ãªtre dÃ©sactivÃ©e et votre abonnement transfÃ©rÃ© sur une nouvelle carte.

9. Lorsque vous renoncez Ã votre ancien appareil, effacer tous les renseignements personnels en rÃ©initialisant l'appareil aux paramÃ¨tres dâ□□origine. Supprimer toutes les informations aussi dans les anciennes cartes SIM et les cartes mÃ©moire.

10. Effectuez des sauvegardes rÃ©guliÃ¨res de toutes les donnÃ©es de votre appareil mobile. Les services Cloud sont pratiques pour ces opÃ©rations, cependant il faut veiller Ã ne pas envoyer les informations de votre employeur vers ces derniers sans autorisation.

En complÃ©ment aux conseils de base Ã©numÃ©rÃ©s ci-dessus, **M. Airamo** rappelle que les employÃ©s ont des obligations envers leur employeur.

Â«*Quand vous utilisez un Ã©quipement fourni par votre employeur, vous devriez toujours suivre les instructions donnÃ©es par rapport Ã la sÃ©curitÃ©. Eviter dâ□□enregistrer des donnÃ©es venant du travail sur vos Ã©quipements personnels, sauf accord contraire.* "