7

Téléphonie mobile : Sensibilisation et Sécurité lors de l'utilisation d'un Smartphone

CENTRE DE RECHERCHE
SUR L'INFORMATION
SCIENTIFIQUE ET TECHNIQUE

cerist

SÉCURITÉ DES SMARTPHONES

La sécurité logicielle des Smartphones est devenue une préoccupation de plus en plus importante de l'informatique liée à la téléphonie mobile. Elle est particulièrement préoccupante car elle concerne la sécurité des informations personnelles disponibles au sein des Smartphones.

Tout comme les ordinateurs, les Smartphones sont des cibles privilégiées d'attaques. Par exemple le risque de phishing existe aussi sur Smartphone. En effet, il ne faut pas cliquer sur n'importe quel lien. L'internet mobile se développe très rapidement et nous allons retrouver sur les terminaux mobiles les mêmes risques que sur un ordinateur classique.

La sécurité de ces terminaux mobiles suscite toujours beaucoup d'interrogations. Les Smartphones intègrent toutes les technologies de communication existantes, du Wifi à la 3G en passant par le Bluetooth. Utilisés par des professionnels, ils contiennent également des données à priori confidentielles et ils sont une porte d'entrée dans le système d'information de l'entreprise. Ils deviennent en outre de plus en plus populaires et attirent donc l'intérêt des pirates vers ces nouvelles plateformes mobiles. Il est à noter qu'Android est actuellement le système d'exploitation mobile le plus utilisé au monde. Le succès de celui-ci fait de la plateforme la cible favorite des pirates. Donc rester prudent et appliquer quelques bonnes pratiques va permettre de profiter pleinement de tous les bienfaits de cette technologie avancée. Le risque se présente quand un inconnu peut consulter nos sms, nos photos, notre agenda… Il en va de même pour les Smartphones à usage professionnel : il est peu probable que votre employeur voit d'un bon œil que n'importe qui puisse avoir accès aux documents, emails de la société, aux serveurs Exchange ou SharePoint, ou encore au réseau Wifi. Aussi, il apparait de plus en plus indispensable de protéger son téléphone contre tous les types de menaces.

A travers ces conseils, nous rappellerons à l'utilisateur quels sont les aspects importants en matière de sécurité et quels sont les moyens de protéger son appareil.

BONNES PRATIQUES POUR AMÉLIORER LA SÉCURITÉ DE SON SMARTPHONE :

1. Evaluer les faiblesses principales de votre Smartphone : représente la première ligne de défense, faire une recherche sur Internet pour en savoir davantage car chaque système d'exploitation a ses propres failles.

2. Les mises à jour : comme pour tout système d'exploitation, les fabricants de Smartphones proposent assez régulièrement des mises à jour faisant évoluer les fonctionnalités de leurs terminaux. Elles permettent par la même occasion de combler certaines vulnérabilités critiques.

3. Contrôler les systèmes de communication : il est fortement conseillé de désactiver les systèmes Bluetooth et Wifi quand ils ne sont pas utilisés. Ils peuvent être utilisés à des fins malveillantes comme porte d'entrée aux données du Smartphone.

4. Surveiller son trafic de données : Sans doute l'un des indicateurs les plus pertinents de l'utilisation d'un mobile par un tiers mal intentionné est une augmentation du trafic de données qui doit éveiller tes soupçons. Une application comme Traffic Monitor Widget sur le système d'exploitation mobile Android s'acquitte parfaitement de cette tâche.

5. Activer le verrouillage automatique de son Smartphone : Réflexe de base, le verrouillage automatique, activer la fonction de verrouillage en cas d'inactivité en l'associant à un mot de passe va permettre de restreindre l'accès aux données de votre téléphone par des personnes malveillantes.

6. Activer, si disponible, le chiffrement des données : C'est intéressant dans l'optique où si un logiciel pompe vos données, il ne pourra pas récupérer grand chose. Le chiffrement protège les informations personnelles, cette fonction existe nativement (ou par application tierce).

- Enregistrer les informations sensibles ou les notes (comme une liste de mots de passe ou des numéros de comptes) à l'aide d'une application de cryptage.
- Avant de faire réparer son appareil, réaliser une sauvegarde des données puis les effacer manuellement ou restaurer les paramètres par défaut.
- Activer la suppression automatique de tous les paramètres et de toutes les données lorsqu'une personne entre plusieurs fois un code ou un mot de passe erroné, en essayant de déverrouiller l'appareil.

7. N'enregistrez pas de données confidentielles sur votre Smartphone : Conseil extrêmement simple à donner mais de plus en plus difficile à appliquer. En effet les Smartphones contiennent aujourd'hui presque par défaut des données sensibles. Votre localisation même approximative, vos emails, le numéro de vos proches, votre adresse, et c'est de plus en plus compliqué de ne laisser filtrer aucune information dite « sensible » et donc qui pourrait vous nuire si elle est interceptée par un tiers, sur votre Smartphone.

8. Le blocage à distance : cette fonction de sécurité va permettre de bloquer son téléphone ou d'effacer les données à distance en cas de vol ou de perte. L'éditeur de logiciel de sécurité F-Secure propose une solution de verrouillage à distance des smartphones tournant sur Symbian et Windows Mobile.

9. Vérifiez quels droits vous donnez à quelle application : si vous avez un mobile Android par exemple, à chaque installation d'application apparaît à l'écran une petite liste des permissions à donner: Localisation, accès au réseau, accès au compte Google... la liste peut être longue et donne beaucoup de pouvoir à l'application en question. Vérifiez donc au moins si les permissions demandées sont logiques : un jeu a-t-il réellement besoin d'accéder et de modifier votre liste de contacts ? Si la réponse est non, donc prudence.

10. Evitez les noms d'applications douteux : les applications qui vous promettent trop ou encore les sources inconnues lors de l'installation d'applications sur votre Smartphone. C'est important car une fois l'application lancée, les droits donnés, il faut quelques minutes au logiciel espion pour envoyer toutes les données nécessaires à vous nuire. Les nouveaux terminaux mobiles de type iPhone ou Android par exemple sont, lors d'un usage normal, protégés via le système de signature et de plateforme « propriétaire » d'Apple et de Google respectivement.

Pour conclure, la meilleure protection reste donc la vigilance car par exemple il est plus raisonnable d'installer les applications approuvées, plutôt que celles qui ont une provenance douteuse, non pas qu'elles soient moins sécurisées, mais leur provenance n'ayant pas été approuvée officiellement, il est difficile d'avoir entièrement confiance.

De ce fait, les pirates exploitent les failles, notamment à l'aide des applications. En effet, il faut savoir que les applications non contrôlées par les plateformes officielles (Android Market, Apple Store, Blackberry App World…) ont plus de chances de contenir des malwares donc lisez les avis des personnes ayant téléchargé le logiciel (signalement de bugs ou de virus) et sachez que vous pouvez également installer un antivirus et Firewall sur le Smartphone si vous possédez des données très confidentielles.