OUCH! | Janvier 2015

La Newsletter mensuelle de Sensibilisation à la Sécurité destinée aux utilisateurs informatiques

OUCH!

Dans ce numéro...

Utiliser les applications mobiles de manière sécurisée

Vue d'ensemble

Les appareils mobiles tels que les tablettes et les smartphones sont devenus les principales technologies que nous utilisons aussi bien dans notre vie privée que professionnelle. Ce qui rend ces appareils aussi polyvalents s'explique par les millions d'applications disponibles. Ces applications nous permettent d'être plus productifs, de communiquer de manière instantanée et de partager avec les autres, de former et d'éduquer ou simplement de s'amuser davantage. Toutefois, le pouvoir de ces applications s'accompagne de risques. Voici quelques étapes à suivre afin d'utiliser ces applications en toute sécurité.

Editeur invité

Chris Crowley est un consultant indépendant, certifié instructeur SANS également auteur de cours. Il est actif sur Twitter à **@CCrowMontance** et sur Google plus: **+ChrisCrowley**.

Téléchargement d'applications

La première étape consiste à vous assurer que vous téléchargez toujours à partir de sources sûres et fiables. Imaginez, à peu près n'importe qui peut créer une application, alors méfiez-vous d'où elle provient. Les cybers criminels ont développé leurs compétences afin de créer et distribuer des applications infectées qui apparaissent comme légitimes. Si vous installez une de ces applications infectées, ces criminels peuvent prendre le contrôle sur vos appareils mobiles, à savoir lire vos mails, écouter vos conversations et pirater vos contacts. En ne téléchargeant que depuis des sources sûres et fiables, vous limitez les risques d'installer une application infectée. Ce que vous ne savez peut-être pas, c'est que la marque de votre appareil mobile détermine vos options.

Pour les appareils Apple, par exemple, tels qu'un iPad ou un iPhone, vous ne pouvez télécharger vos applications qu'à partir d'une plateforme fiable, l'Apple App Store. L'avantage est qu'Apple vérifie au préalable la sécurité des applications et leurs provenances. Bien sûr, Apple ne peut pas intercepter tous les criminels ou toutes les applications infectées, mais ce fonctionnement contribue à réduire considérablement les risques de télécharger une application infectée. De plus, si Apple découvre une application éventuellement infectée dans son App Store, il la retire immédiatement. Windows Phone utilise un procédé semblable pour gérer ses applications.

Les appareils Android sont différents. Android permet une plus grande flexibilité et la possibilité de télécharger une application mobile d'où vous le souhaitez, sur internet. Toutefois, cette flexibilité s'accompagne de davantage de responsabilités. Vous devez faire attention à quelles applications vous téléchargez et installez puisque pas toutes sont vérifiées. Cependant,

Utiliser les applications mobiles de manière sécurisée

Google gère tout de même une boutique d'applications mobiles en ligne, similaire à celle d'Apple, appelée Google Play. Les applications mobiles que vous téléchargez sur Google Play ont subi des contrôles basiques. De ce fait, nous vous conseillons de ne télécharger vos applications pour Android que sur Google Play. Evitez de télécharger des applications mobiles à partir d'autres sites internet, puisque n'importe qui, les cybers criminels inclus, peut facilement créer et redistribuer des applications malveillantes pour infecter vos appareils mobiles malgré vous. Considérez une protection supplémentaire en installant un anti-virus sur vos appareils mobiles.

La clé pour utiliser en toute sécurité des applications mobiles est d'installer des applications uniquement à partir de sources de confiance et de vous assurer que vos applications sont mises à jour et que vous avez vérifié les autorisations.

Pour réduire encore davantage les risques, évitez les toutes nouvelles applications que peu de gens ont encore téléchargées et pour lesquelles il n'y a que peu de retours positifs. Plus l'application est ancienne, ou plus les commentaires sont positifs, plus vous pouvez vraisemblablement faire confiance à cette application. De plus, n'installez que les applications dont vous avez besoin ou que vous utilisez. Demandez-vous, ai-je réellement besoin de cette application ? Non seulement chaque nouvelle application apporte potentiellement de nouvelles vulnérabilités, mais elle comporte également des risques concernant vos données privées. Si vous n'utilisez pas une application, supprimez-la de votre appareil mobile (vous pourrez toujours la réinstaller plus tard si vous en avez besoin).

Finalement, vous serez peut-être tentés de jailbreak votre appareil mobile. Ceci est un procédé de piratage par lequel vous pourrez forcer des installations d'applications non approuvées, ou de changer les fonctionnalités de base de votre appareil. Nous vous déconseillons fortement le jailbreak dans la mesure où, non seulement cela contourne ou élimine la plupart des contrôles de sécurité de base sur votre appareil mobile, mais souvent cela annule également la garantie et les contrats de services.

Autorisations

Une fois que vous avez téléchargé l'application depuis une source sûre, l'étape suivante consiste à vous assurer qu'elle est configurée de manière sécurisée et qu'elle protège vos données personnelles. Installer et/ou télécharger une application mobile vous oblige souvent à donner certaines autorisations. Demandez-vous toujours si l'application a réellement besoin d'accéder à certaines de vos données personnelles pour être opérationnelle. Par exemple, certaines applications utilisent la géolocalisation. Si vous autorisez une application à constamment connaître votre localisation, peut-être autorisez-vous le créateur de cette application à suivre vos déplacements, voire même à revendre cette information. Si vous ne souhaitez pas donner les autorisations requises à l'application, faites le tour des applications afin de trouver celle dont les autorisations

Utiliser les applications mobiles de manière sécurisée

requises vous conviennent. N'oubliez pas que le choix est vaste. Les mobiles Apple autorisent parfois des modifications d'autorisations dans les Paramètres, tel que l'accès à la géolocalisation. Windows et Android sont différents, c'est « tout ou rien ». Si vous ne donnez pas toutes les autorisations requises, vous ne pouvez pas installer l'application.

Mise à jour des applications

Tout comme le système d'exploitation de votre ordinateur ou de vos appareils mobiles, les applications mobiles doivent également être mises à jour. Les cybers criminels sont toujours en quête de faiblesses dans les applications et ils finissent par les trouver. Ensuite ils développent des attaques afin d'exploiter ces faiblesses. Les développeurs qui créent ces applications mettent régulièrement des mises à jour à disposition afin de contrer ces faiblesses et protéger vos appareils. Plus vous rechercherez et installerez les mises à jour, mieux ce sera. La plupart des plateformes vous permettent d'ailleurs de configurer votre système afin que les mises à jour se fassent toutes seules. Nous vous recommandons d'activer ce paramètre. Si cela n'est pas possible, nous vous recommandons de vérifier, au moins toutes les deux semaines, les mises à jour disponibles pour vos applications mobiles. Toutefois, lorsque vos applications ont été mises à jour, vérifiez toujours les éventuelles nouvelles autorisations qu'elles demandent.

Version Française

La division sécurité de ANSWER S.A. offre des services de Conseil, d'Audit et d'Architecture en sécurité des systèmes d'information. Ces activités sont accompagnées d'une veille active sur les solutions de sécurité du marché permettant ainsi à ses consultants de répondre efficacement aux problématiques de ses clients.
Pour en savoir plus, veuillez vous référer aux liens suivants :
http://www.answersolutions.ch et http://answersecurity.com/

Ressources

Ingénierie sociale:	http://www.securingthehuman.org/ouch/2014#november2014
Mise au rebut de votre équipement mobile:	http://www.securingthehuman.org/ouch/2014#june2014
Sécurisez votre nouvelle tablette:	http://www.securingthehuman.org/ouch/2013#december2013
Termes communs de sécurité:	http://www.securingthehuman.org/resources/security-terms
SEC575: Cours sur la sécurité des dispositifs mobiles:	http://www.sans.org/sec575

Comité de rédaction : Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Traduit par : Marilyn Combet