OUCH! | Mars, 2017

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, les smartphones et les montres connectées sont devenus les principales technologies que nous utilisons dans le cadre de notre vie personnelle et 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, 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

Joshua Wright est le directeur technique de Counter Hack. Instructeur sénior à l'institut SANS, il est également l'auteur de SEC575: Mobile Device Security and Ethical Hacking, and Hacking Exposed: Wireless. Rejoignez Josh sur Twitter **@ joswr1ght**.

Téléchargement d'applications

La première étape consiste à vous assurer de toujours télécharger des applications mobiles à partir d'une source sûre et fiable. Les cybercriminels ont développé leurs compétences pour créer et distribuer des applications mobiles infectées qui semblent légitimes. Si vous installez une de ces applications infectées, les criminels peuvent prendre le contrôle complet de votre appareil mobile. En téléchargeant des applications uniquement à partir de sources bien connues et fiables, vous réduisez les chances d'installer une application infectée. Ce que vous ne savez peut-être pas, c'est que la marque de l'appareil mobile que vous utilisez détermine vos options pour télécharger des applications.

Pour les appareils Apple tels qu'un iPad ou un iPhone, vous ne pouvez télécharger uniquement les applications mobiles qu'à partir de l'App Store d'Apple. L'avantage est qu'Apple vérifie au préalable la sécurité des applications et leurs provenances avant qu'elles ne soient mises à disposition. Bien sûr, Apple ne peut pas intercepter tous les criminels ou toutes les applications infectées, cependant, 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.

Utiliser les applications mobiles de manière sécurisée

Les appareils mobiles 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 en effet faire attention à quelles applications vous téléchargez et installez puisque pas toutes ne sont vérifiées. Cependant, 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 à partir de Google Play ont passé quelques contrôles de sécurité de base. De ce fait, nous vous conseillons de ne télécharger vos applications pour Android que sur Google Play. Évitez de télécharger des applications mobiles Android depuis d'autres sites Web, car quiconque, y compris les cybercriminels, peut facilement créer et distribuer des applications mobiles malveillantes et vous inciter à infecter votre appareil mobile. Considérez une protection supplémentaire en installant un anti-virus sur vos appareils mobiles.

La clé pour utiliser en toute sécurité les applications mobiles consiste à installer des applications uniquement à partir de sources fiables, à installer des mises à jour lorsqu'elles sont disponibles et à n'accorder que les autorisations d'applications requises.

Quel que soit le périphérique que vous utilisez, essayez d'éviter les applications qui sont flambant neuves, que peu de gens ont téléchargé, ou qui ont très peu de commentaires positifs. Plus une application est disponible, plus il y a de personnes qui l'utilisent, plus les commentaires sont positifs, plus l'application sera fiable. En outre, installez uniquement les applications dont vous avez besoin et utilisez-les. Demandez-vous si vous avez un réel besoin de cette application? Non seulement chaque application apporte potentiellement de nouvelles vulnérabilités, mais aussi de nouveaux problèmes de confidentialité. Si vous cessez d'utiliser une application, supprimez-la de votre appareil mobile (vous pouvez toujours l'ajouter ultérieurement si vous en avez besoin). Enfin, ne jailbreakez ou ne rootez pas votre appareil mobile. Il s'agit d'un processus pour pirater et pour installer des applications non approuvées ou pour modifier les fonctionnalités intégrées existantes. Cela contourne ou élimine non seulement beaucoup de contrôles de sécurité intégrés à votre appareil mobile, mais annule souvent aussi les garanties et les contrats de support.

Autorisations

Une fois que vous avez installé une application mobile à partir d'une source de confiance, assurez-vous qu'elle soit configurée et protégée en toute sécurité. Pensez toujours avant d'autoriser un accès à une application mobile: voulez-vous accorder à l'application l'autorisation demandée, l'application en a-t-elle réellement besoin? Par exemple, certaines applications

Utiliser les applications mobiles de manière sécurisée

utilisent des services de géolocalisation. Si vous autorisez une application à toujours connaître votre emplacement, vous pouvez autoriser le créateur de cette application à suivre vos mouvements, en permettant même à l'auteur de l'application de vendre cette information à d'autres. Si vous ne souhaitez pas accorder les autorisations, refusez la demande d'autorisation ou achetez une autre application qui réponde à vos besoins. Rappelez-vous que vous avez beaucoup de choix à disposition.

Mise à jour des applications

Les applications mobiles, tout comme votre ordinateur et votre système d'exploitation, doivent être mises à jour pour rester à jour. Les criminels sont constamment à la recherche de faiblesses dans les applications. Ils développent alors des attaques pour exploiter ces failles. Les développeurs qui ont créé votre application ont également créé et publié des mises à jour pour corriger ces faiblesses et protéger vos périphériques. Le plus souvent vous rechercherez et installerez des mises à jour, mieux cela sera. La plupart des périphériques vous permettent de configurer votre système pour mettre à jour automatiquement les applications mobiles. Nous recommandons ce réglage. Si cela n'est pas possible, nous vous recommandons de vérifier au moins toutes les deux semaines les mises à jour de vos applications mobiles. Enfin, lorsque vos applications sont mises à jour, assurez-vous toujours de vérifier les nouvelles autorisations dont elles pourraient avoir besoin.

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.answer.ch et http://answersecurity.com/

Sources

Ingénierie sociale : https://securingthehuman.sans.org/ouch/2017#january2017

Comment se séparer de votre appareil mobile de façon sécurisée? :
https://securingthehuman.sans.org/ouch/2016#december2016

Sécuriser votre nouvelle tablette : https://securingthehuman.sans.org/ouch/2016#january2016

Archives OUCH ! & traductions : https://securingthehuman.sans.org/ouch/archives

Cours de sécurité pour les appareils mobiles : https://sans.org/sec575

Comité de rédaction : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Traduit par : Marilyn Combet