Votre publication mensuelle de conscientisation à propos de la Sécurité

Utilisation sécurisée des applications mobiles

Aperçu

Les appareils mobiles, tels que les tablettes, les smartphones et les montres intelligentes, sont devenus l'une des principales technologies que nous utilisons dans notre vie personnelle et professionnelle. Ce qui rend ces appareils si puissants, ce sont les milliers d'applications parmi lesquelles nous pouvons choisir. Ces applications nous permettent d'être plus productifs, de communiquer et de partager avec les autres, de nous former et d'éduquer, ou tout simplement de nous amuser. Voici les étapes que vous pouvez suivre pour utiliser en toute sécurité et tirer le meilleur parti des applications mobiles actuelles.

Obtenir des applications mobiles sûres

Les cybercriminels ont maîtrisé leurs compétences en matière de création et de distribution d'applications malveillantes qui semblent légitimes. Si vous installez l'une de ces applications, les criminels peuvent souvent prendre le contrôle total de votre appareil mobile ou de vos données. C'est pourquoi vous voulez vous assurer de ne télécharger que des applications mobiles sûres à partir de sources fiables. Ce que vous ne réalisez peut-être pas, c'est que la marque d'appareil mobile que vous utilisez détermine vos options de téléchargement d'applications.

Pour les appareils Apple, téléchargez uniquement des applications mobiles depuis l'App Store d'Apple. L'avantage ici est qu'Apple effectue un contrôle de sécurité de toutes les applications mobiles avant qu'elles ne soient mises à la disposition des clients. Bien qu'Apple ne puisse pas attraper toutes les applications malveillantes, cet environnement géré réduit considérablement le risque d'en télécharger une. De plus, si Apple trouve une application qu'il juge malveillante, il la supprimera rapidement.

Pour les appareils Android, téléchargez uniquement des applications mobiles à partir de Google Play, qui est géré par Google. Semblable à Apple, Google effectue un contrôle de sécurité de toutes les applications avant qu'elles ne soient mises à la disposition des clients. La différence avec les appareils Android est que vous pouvez également activer certaines options qui vous permettent de télécharger des applications mobiles à partir d'autres sources. Nous vous déconseillons vivement cela, car tout le monde, y compris les cybercriminels, peuvent facilement créer et distribuer des applications mobiles malveillantes et vous inciter à infecter votre appareil mobile.
Quelle que soit la marque que vous utilisez, faites vos recherches à propos de l'application avant de la télécharger. Regardez depuis combien de temps l'application mobile est disponible, combien de personnes l'ont utilisée et qui est le fournisseur.

Plus une application est accessible au public depuis longtemps, plus il y a de personnes qui l'ont utilisée et ont laissé des commentaires positifs à son sujet, et plus fréquemment les fournisseurs d'applications la mettent à jour, plus grande est la probabilité que l'application peut être considéré fiable. De plus, installez uniquement les applications dont vous avez besoin et que vous utilisez. Demandez-vous: "Ai-je vraiment besoin de cette application?" Non seulement chaque application apporte potentiellement de nouvelles vulnérabilités, mais également de nouveaux problèmes de confidentialité. Si vous arrêtez d'utiliser une application ou ne la trouvez plus utile, supprimez-la de votre appareil mobile (vous pouvez toujours la rajouter plus tard si vous en avez vraiment besoin).

Confidentialité et autorisations des applications

Une fois installée, assurez-vous que l'application protège votre vie privée. Cette application a-t-elle vraiment besoin d'accéder à votre position, à votre microphone ou à vos contacts? Lorsque vous activez les autorisations, vous autorisez peut-être le créateur de cette application à vous suivre, lui permettant même de partager ou de vendre vos informations à d'autres. Si vous ne souhaitez pas accorder ces autorisations, refusez simplement la demande d'autorisation, accordez l'autorisation à l'application uniquement lorsqu'elle est activement utilisée ou recherchez une autre application qui répond à vos besoins. Rappelez-vous, vous avez beaucoup de choix disponible.

Mise à jour des applications

Les applications mobiles, tout comme votre ordinateur et le système d'exploitation de votre appareil mobile, doivent être mises à jour. Les criminels recherchent et découvrent constamment de nouvelles faiblesses dans les applications et développent des moyens d'exploiter ces faiblesses. Les développeurs de l'application créent et publient des mises à jour pour corriger ces faiblesses et protéger vos appareils. Plus vous recherchez et installez des mises à jour fréquemment, mieux c'est. La plupart des appareils vous permettent de configurer votre système pour mettre à jour automatiquement les applications mobiles. Nous vous recommandons vivement d'activer ce paramètre.

Les applications mobiles sont essentielles pour tirer le meilleur parti de vos appareils. Faites juste attention à ceux que vous sélectionnez et assurez-vous de les utiliser en toute sécurité.

Rédacteur invité

Domenica Crognale est ingénieure en assurance qualité et formatrice certifiée au SANS Institute. Elle est co-auteure de FOR585: Smartphone Analysis In-Depth. Rejoignez Domenica sur Twitter @domenicacrognal.

Ressources

La puissance des mises à jour: https://www.sans.org/security-awareness-training/resources/power-updating/
Intimité: https://www.sans.org/newsletters/ouch/privacy/
Traduit pour la communauté par: Jérôme Boutin et Sebastien Kierszka