OUCH! Octobre 2024

OUCH!

SANS SECURITY AWARENESS

Votre bulletin mensuel sur la sensibilisation à la sécurité

Télécharger Danger : comment déjouer les applications mobiles malveillantes

L'application mystérieuse : un court récit d'avertissement

Durant un dimanche tranquille, alors qu'elle scrollait ses réseaux sociaux, Sarah est tombée sur une publicité pour une application pour modifier les photos, « PiksPerfect ». Intriguée par les filtres incroyables, elle a téléchargé l'application sans se poser de questions. Au début, l'application marchait très bien, mais rapidement, son téléphone est devenu lent et des publicités ont commencé à apparaître sur son écran. Quelques jours plus tard, Sarah a reçu un appel de sa banque à propos de prélèvements allant jusqu'à des milliers de dollars. Elle a ouvert l'application de sa banque en panique et a découvert que ses économies étaient quasiment vides. Après avoir signalé la fraude et bloqué son compte, elle s'est retrouvée seule et désemparée.

Son amie, experte en technologie, a découvert la vérité : l'application mobile était fausse et volait ses informations personnelles, y compris ses informations bancaires. Il lui a fallu des mois pour s'en remettre, mais Sarah est devenue plus prudente, et elle fait des recherches sur les applications mobiles avant de les installer maintenant. Elle partage aujourd'hui son histoire pour mettre en garde les autres, comprenant qu'un moment d'inattention peut avoir de lourdes conséquences.

Comment savoir si les applications sont sûres ?

Les applications mobiles sont pratiques et puissantes, elles nous permettent de faire à peu près tout ce que nous faisons dans notre vie en appuyant sur un bouton. Cependant, les cybercriminels en profitent pour créer de fausses applications mobiles ou des applications malveillantes. Si vous téléchargez l'une de ces applications, elle peut prendre le contrôle de votre téléphone et surveiller tout ce que vous faites. Pour se protéger, il faut s'assurer que les applications mobiles que l'on installe sur son appareil sont légitimes et sûres.

Tout d'abord, ne téléchargez les applications mobiles qu'à partir des magasins officiels où les vendeurs examinent les applications mobiles, comme l'App Store d'Apple ou le Play Store de Google. Cela permet de réduire le risque de télécharger une mauvaise application mobile. Les boutiques d'applications tierces ne sont souvent pas fiables et peuvent même être gérées par des cybercriminels. Mais même si vous utilisez un magasin d'applications mobiles de confiance, vous devez être prudent. Voici quelques mesures supplémentaires que vous pouvez prendre pour vous assurer que vous téléchargez des applications mobiles légitimes et sûres.

1. **Vérifier le nom du développeur**: Lorsque vous recherchez une application mobile spécifique créée par une certaine entreprise, assurez-vous que l'application que vous téléchargez est bien créée par cette entreprise. Une astuce courante des escrocs consiste à créer des applications mobiles qui ressemblent à s'y méprendre à des applications connues. Vérifiez le nom du développeur : s'agit-il de la même entreprise ou d'un développeur connu, ou l'application a-t-elle été développée par quelqu'un dont vous n'avez jamais entendu parler ? Une autre option consiste à visiter le site web officiel de l'application ou du développeur pour trouver des liens directs vers l'application mobile dans le magasin d'applications. Cela permet de s'assurer que vous téléchargez l'application officielle.

2. **Lire les commentaires et les évaluations**: consultez les avis et les évaluations des utilisateurs. Une application légitime dispose d'un nombre important d'avis positifs et d'évaluations élevées. Méfiez-vous des applications qui ont peu d'avis, beaucoup d'avis négatifs ou des avis trop positifs qui semblent faux.

3. **Examiner le nombre de téléchargements**. Les applications légitimes ont généralement un nombre élevé de téléchargements. Une application peu téléchargée peut être un signal d'alarme.

4. **Examiner les permissions**: Vérifiez les autorisations demandées par l'application avant de la télécharger. Les applications légitimes ne demandent que les autorisations nécessaires à leur fonctionnement. Méfiez-vous des applications qui demandent des autorisations excessives ou non pertinentes. Par exemple, l'application a-t-elle vraiment besoin d'accéder à vos contacts ou de connaître en permanence votre position ?

5. **Vérifier les mises à jour régulières**: Les applications légitimes sont régulièrement mises à jour pour corriger les bugs et améliorer les performances. Vérifier l'historique des mises à jour de l'application pour s'assurer qu'elle reçoit des mises à jour fréquentes.

6. **Soyez prudent avec les nouvelles applications**: Les nouvelles applications qui ne font l'objet d'aucun commentaire ou d'aucune évaluation doivent être considérées avec prudence. Les nouvelles applications qui ne font l'objet d'aucun commentaire ou d'aucune évaluation doivent être considérées avec prudence.

Une fois que vous avez téléchargé une application mobile, activez la mise à jour automatique. De nouvelles erreurs et vulnérabilités sont constamment découvertes dans le code et les configurations des applications mobiles. En veillant à toujours utiliser la dernière version de vos applications mobiles, vous pouvez vous assurer que ces vulnérabilités ont été corrigées et que vous disposez des dernières fonctions de sécurité. De même, si vous n'utilisez plus une application mobile, supprimez-la de votre téléphone.

Rédacteur Invité

Danielle Strimbu est chef de projet technique à l'agence numérique Travel Minds, avec une expérience en technologie et en gestion des opérations. En tant que présidente des événements pour l'affilié WiCyS Colorado, elle cherche à organiser des événements attrayants pour aider à faire progresser les femmes dans le domaine de la cybersécurité. Elle est titulaire d'une maîtrise en sécurité des systèmes d'information et d'un certificat d'études supérieures en gestion de la cybersécurité.

Ressources

Les trois principaux moyens utilisés par les cyberattaquants pour vous cibler :
https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you/
Déclencheurs émotionnels, comment les cyber-attaquants vous piègent-ils ? :
https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
Tout ce que vous devez savoir sur les données d'arrière-plan : https://www.avast.com/c-what-is-background-data#

Traduit pour la communauté par : Juliette Busson