OUCH! Juillet 2021

Votre publication mensuelle de conscientisation à propos de la Sécurité

Sécuriser vos appareils mobiles

Aperçu

Les appareils mobiles sont un moyen étonnant et facile de communiquer avec des amis, de faire des achats ou d'effectuer des opérations bancaires en ligne, de regarder des films, de jouer à des jeux et d'effectuer une myriade d'autres activités. Étant donné que ces appareils sont une partie si importante de votre vie, il est essentiel de vous protéger, vous et vos appareils..

Protéger vos appareils

Cela peut vous surprendre d'apprendre que le plus grand risque pour vos appareils mobiles n'est probablement pas les cybercriminels mais vous. Vous êtes beaucoup plus susceptible de perdre ou d'oublier un appareil mobile que de vous le faire pirater. La première des choses que vous devez faire pour protéger votre appareil mobile est d'activer le verrouillage d'écran automatique lorsqu'il est inutilisé. Cela signifie que pour utiliser votre appareil mobile, vous aurez à le déverrouiller avec un mot de passe complexe, votre visage, ou votre empreinte digitale. Cela permet de s'assurer qu'il est beaucoup plus difficile pour quiconque d'accéder à vos informations si votre appareil mobile est perdu ou volé. En prime, pour la plupart des appareils mobiles, l'activation du verrouillage de l'écran permet également le cryptage, aidant à protéger les données stockées sur l'appareil.

Voici plusieurs autres conseils pour vous aider à protéger vos appareils:

1. **Mises à jour**: Activez la mise à jour automatique sur vos appareils, afin qu'ils exécutent toujours la dernière version du système d'exploitation et des applications. Les attaquants sont toujours à la recherche de nouvelles faiblesses dans les logiciels, et les fournisseurs publient constamment des mises à jour et des correctifs pour les corriger. Gardez vos appareils à jour les rend beaucoup plus difficiles à pirater. Lorsque vous choisissez un nouvel appareil Android, examinez l'engagement du fournisseur à maintenir l'appareil à jour. Les appareils Apple iOS sont mis à jour par l'entreprise elle-même, tandis que les appareils mobiles Android sont mis à jour par le fournisseur qui vous a vendu l'appareil, et tous les fournisseurs ne mettent pas activement à jour leurs appareils. Si vous utilisez un ancien appareil qui n'est plus pris en charge ou ne peut pas être mis à jour, envisagez d'acheter un nouvel appareil entièrement pris en charge.

2. **Suivi**: Installez ou activez un logiciel de confiance pour suivre à distance votre appareil mobile sur Internet. De cette façon, vous pouvez vous y connecter via Internet et trouver son emplacement si votre appareil est perdu ou volé ou effacer à distance toutes vos informations dans le pire des cas.

3. **Applications Mobiles de confiance**: Installez uniquement les applications dont vous avez besoin et respectez les sources fiables. Pour les appareils Apple iOS tels que les iPad ou les iPhone, cela signifie l'App Store d'Apple. Pour les appareils Android, utilisez Google Play; pour les tablettes Amazon, utilisez l'Amazon App Store. Bien que vous puissiez installer des applications à partir d'autres sites, celles-ci ne sont pas contrôlées et sont beaucoup plus susceptibles d'être infectées ou carrément malveillantes, ce qui pourrait compromettre votre vie privée. Assurez-vous également que l'application a de nombreuses critiques positives et qu'elle est activement mise à jour par le fournisseur avant de la télécharger. Évitez les nouvelles applications, les applications avec peu d'avis ou les applications rarement mises à jour.

4. **Options de confidentialité**: Les appareils mobiles collectent de nombreuses informations sur vous, d'autant plus que vous les emportez partout où vous allez. Examinez attentivement les paramètres de confidentialité de votre appareil, y compris le suivi de la localisation, et assurez-vous que les notifications sensibles (telles que les codes de vérification) n'apparaissent pas à l'écran lorsque l'appareil est verrouillé.
5. **Travail**: Assurez-vous que tout appareil mobile que vous utilisez pour le travail est autorisé pour une utilisation professionnelle. Au travail, soyez très prudent et ne prenez jamais de photos ou de vidéos qui pourraient accidentellement contenir des informations sensibles, telles que des images de tableaux blancs ou d'écrans d'ordinateur.

Vos appareils mobiles sont un outil puissant – un outil que nous souhaitons que vous appréciez et utilisiez. Le simple fait de suivre ces quelques étapes simples peut grandement contribuer à votre sécurité et à celle de vos appareils.

Rédacteur invité

Jeroen Beckers est un expert en sécurité mobile chez NVISO, co-auteur de l'OWASP MASVS et du MSTG, instructeur pour l'institut SANS et auteur du SEC575: Cours sur la sécurité des appareils mobiles et le piratage éthique. Vous pouvez trouver Jeroen via LinkedIn auhttps://www.linkedin.com/in/beckersjeroen/.

Ressources

Mises à jour: https://www.sans.org/newsletters/ouch/the-power-of-updating
Utilisation sécurisée des applications mobiles: https://www.sans.org/newsletters/ouch/securely-using-mobile-apps/
Attaques de messagerie/messages textes: https://www.sans.org/newsletters/ouch/messaging-smishing-attacks
Gestionnaire de mots de passe: https://www.sans.org/newsletters/ouch/making-passwords-simple
Vishing - Attaques et escroqueries par appel téléphonique: https://www.sans.org/newsletters/ouch/vishing

Traduit pour la communauté par: Jérôme Boutin et Sebastien Kierszka