

Workforce Security and Risk Training

La lettre d'information mensuelle sur la sensibilisation à la sécurité pour vous

Votre smartphone : une mine d'or pour les cybercriminels

Un désastre qui rentre dans la poche

Emma profitait de ses vacances bien méritées sur une magnifique île ensoleillée. Une après-midi, après avoir passé de longues heures à la plage, elle s'est arrêtée dans un petit café pour déjeuner avant de rentrer à son hôtel. Distraite par la vue sur l'océan et l'envie de retourner dehors, elle a oublié son téléphone sur la table en partant. Ce n'est que plusieurs heures plus tard qu'elle s'est rendue compte qu'elle n'avait plus son téléphone.

Au début, Emma n'était pas très inquiète. Elle est retournée au café pour chercher son téléphone, mais il n'était plus là. La personne qui avait trouvé son téléphone avait maintenant potentiellement accès à ses e-mails, ses comptes de réseaux sociaux, ses applications bancaires, et même son application d'authentification qu'elle utilisait pour confirmer son identité sur les sites importants.

De plus, comme elle était en voyage, Emma comptait sur son téléphone pour le GPS, les réservations d'hôtel, les informations de vol et la communication avec sa famille. Elle ne pouvait plus accéder à ses cartes d'embarquement, confirmer ses réservations ou recevoir des codes de sécurité sur son appareil.

Heureusement, Emma avait activé le verrouillage de son écran et la localisation à distance avant le départ. De retour dans sa chambre d'hôtel, elle a pris son ordinateur pour se connecter à son compte et s'est rendue compte que l'appareil n'était plus dans le café. Quand elle a compris qu'elle ne le récupérerait pas, elle a verrouillé le téléphone à distance et a effacé tous les contenus pour protéger ses informations. Heureusement, elle allait pouvoir les récupérer rapidement, puisqu'elle avait sauvegardé ses informations.

Cinq étapes pour sécuriser votre appareil mobile

1. Activer un écran de verrouillage fort

La première ligne de défense est d'empêcher l'accès non autorisé à votre appareil. Utilisez un code PIN, un code de verrouillage, une empreinte digitale ou la reconnaissance faciale pour verrouiller votre téléphone ou votre tablette. Si votre appareil est perdu ou volé, un verrouillage d'écran fort peut empêcher quelqu'un d'accéder immédiatement à vos applications, vos comptes et vos informations personnelles. Considérez le verrouillage de votre écran comme la porte d'entrée de votre maison numérique. Activez le verrouillage automatique de votre téléphone pour un temps d'inactivité confortable pour vous. Prenez l'habitude de verrouiller systématiquement votre téléphone lorsque vous le posez.

2. Activez la localisation du téléphone et l'effacement à distance

Que se passe-t-il lorsque votre appareil est perdu ou volé ? La plupart des appareils mobiles modernes intègrent des services qui vous permettent de les localiser sur une carte, de les faire sonner, de les verrouiller à distance ou d'effacer toutes leurs données si leur récupération s'avère impossible.

© SANS Institute 2026

Les utilisateurs d'Apple peuvent activer "Localiser". Les utilisateurs d'Android peuvent activer "Localiser mon appareil". Ces services sont gratuits et sont généralement déjà disponibles sur votre appareil. Prendre quelques minutes pour vérifier que ces fonctionnalités sont bien activées peut vous éviter bien des soucis par la suite. Si votre appareil disparaît, vous pouvez ainsi le localiser rapidement ou effacer vos informations avant que quelqu'un d'autre obtienne l'accès.

3. Activez la mise à jour automatique

Les cyber-criminels recherchent constamment des failles dans les systèmes d'exploitation mobiles et les applications. Lorsque ces faiblesses sont découvertes, les éditeurs de logiciels publient des mises à jour pour régler le problème. Le problème est que beaucoup de gens repoussent ces mises à jour pendant des jours, des semaines, voire des mois. La solution la plus simple consiste à activer la mise à jour automatique, y compris pour vos applications mobiles. Cela garantit que votre appareil bénéficie des correctifs de sécurité dès leur mise à disposition, souvent sans que vous ayez à intervenir.

4. Installez uniquement des applications de sources fiables

L'une des principales causes de compromission des appareils mobiles réside dans les applications malveillantes. Ne téléchargez des applications mobiles qu'à partir de boutiques d'applications officielles, telles que l'App Store d'Apple ou Google Play. Même là, vérifiez les notes, les commentaires et les autorisations avant de procéder à l'installation. Méfiez-vous tout particulièrement des applications qui demandent l'accès à des informations ou à des fonctionnalités dont elles n'ont pas besoin. Par exemple, une application "lampe de poche" ne devrait pas avoir besoin d'accéder à vos contacts, à votre microphone ou à votre position. Si une application vous semble suspecte ou demande des autorisations excessives, optez pour une autre application.

5. Activez les sauvegardes automatiques

Perdre un appareil est très stressant. Si votre téléphone disparaît, est endommagé ou tombe en panne, une sauvegarde récente vous permettra de tout restaurer sur un nouvel appareil en quelques minutes, y compris non seulement toutes les applications que vous aviez installées, mais aussi leurs paramètres de configuration. Assurez-vous que les sauvegardes automatiques sont activées.

Rédacteur invité



Le Dr Khushi Gupta est maîtresse de conférences en cybersécurité à l'Université de Géorgie du Nord. Titulaire d'un doctorat en criminalistique informatique, elle est l'auteure de plus de 30 publications et met à profit dans son travail son expérience en matière de criminalistique au sein des forces de l'ordre. Elle intervient en tant que mentor au sein des associations WiCyS, Women4Cyber et BBWIC.

Ressources

Le danger de télécharger : Comment déjouer les applications mobiles malveillantes : https://www.sans.org/newsletters/ouch/download-danger-how-to-outwit-malicious-mobile-apps
Les attaques par SMS : une saga d'hameçonnage par SMS : https://www.sans.org/newsletters/ouch/text-messaging-attacks-smishing-saga
Comment les cybercriminels volent vos mots de passe : https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords

Traduit pour la communauté par : Juliette Busson

OUCH ! Publié par SANS Security Awareness et distribué sous licence Creative Commons BY-NC-ND 4.0. Vous êtes libre de partager ou de distribuer cette newsletter à condition de ne pas la vendre ni la modifier. Comité de rédaction : Phil Hoffman, Leslie Ridout, Princess Young.

Vous pouvez trouver plus de contenu OUCH! Sur le lien suivant : https://www.sans.org/newsletters/ouch