Votre bulletin mensuel sur la sensibilisation à la sécurité

Quatre étapes simples pour rester en sécurité

Aperçu

Profiter pleinement de la technologie en toute sécurité peut paraître insurmontable et déroutant. Cependant, qu'importe la technologie que vous utilisez ou comment vous l'utilisez, voici quatre étapes simples qui vous aideront à rester en sécurité.

1. Vous : pour commencer, la technologie seule ne peut vous protéger entièrement : vous êtes votre meilleure défense. Les cybercriminels savent que la manière la plus simple d'obtenir ce qu'ils veulent est de vous cibler vous, plutôt que votre ordinateur ou autres appareils. S'ils veulent votre mot de passe, carte de crédit ou le contrôle de votre ordinateur, ils vous inciteront à le leur donner, souvent en créant un sentiment d'urgence. Par exemple, ils peuvent vous appeler, prétendant être l'équipe technique Microsoft, pour vous dire que votre ordinateur est infecté, alors qu'en fait se sont des cybercriminels qui veulent que vous leur donniez accès à votre ordinateur. Ou peut-être vont-ils vous envoyer un e-mail vous prévenant que votre colis ne peut être livré et vont vous pousser à cliquer sur un lien pour confirmer votre adresse, quand en réalité ils vous invitent à visiter un site malveillant qui piratera votre ordinateur. Au final, la meilleure défense contre les cybercriminels, c'est vous. En utilisant du bon sens, vous pouvez repérer et arrêter ces attaques.

2. Phrases de passe : la vitesse des ordinateurs actuels rendent les anciens mots de passe à 8 caractères vulnérables. Quand un site vous demande de créer un mot de passe, créez à la place une phrase de passe longue et unique. Une phrase de passe est une sorte de mot de passe utilisant une série de mots facile à se souvenir, comme « abeilles miel bourbon pluie ». Plus la phrase de passe est longue, plus elle est forte. Une phrase de passe unique signifie une différente pour chaque appareil ou compte. Ainsi, si une phrase de passe est compromise, vos autres comptes ou appareils restent sécurisés. Vous ne pouvez pas vous souvenir de toutes ces phrases de passe ? Utilisez un gestionnaire de mots de passe : c'est un programme spécial qui store toutes vos phrases de passe dans un format chiffré (et vous offre d'autres services intéressants).

Enfin, activez la vérification à deux étapes (aussi appelée vérification à deux facteurs). Cela requiert votre mot de passe mais aussi une seconde étape, comme entrer un code envoyé par sms ou généré d'une application. La vérification à deux étapes est probablement l'étape la plus importante pour protéger vos comptes en ligne et c'est bien plus simple que vous ne le pensez.

3. Mise à jour : assurez-vous que vos ordinateurs, appareils mobiles, programmes et applications utilisent la dernière version de leurs logiciels. Les cybercriminels recherchent constamment de nouvelles vulnérabilités dans les logiciels utilisés par vos appareils. Quand ils en découvrent, ils utilisent des programmes spéciaux pour les exploiter et pirater vos appareils. Pendant ce temps, les entreprises qui créent ces logiciels travaillent dur pour corriger les vulnérabilités en publiant des mises à jour. En vous assurant que vos ordinateurs et appareils mobiles installent ces mises à jour rapidement, vous rendez la tâche plus difficile aux cybercriminels. Pour rester à jour, autorisez simplement la mise à jour automatique quand c'est possible. Cela fonctionne avec pratiquement toutes les technologies connectées à un réseau, comme les télés connectées, moniteurs pour bébé, caméras de sécurité, routeurs, consoles ou même votre voiture.

4. Sauvegardes et restaurations : Des fois, peu importe votre vigilance, vous pouvez vous faire pirater. Souvent, si c'est le cas, la seule façon de restaurer vos données personnelles vient de vos sauvegardes. Assurez-vous de faire des sauvegardes fréquentes de vos informations et vérifiez que vous pouvez restaurer ces données. La plupart des systèmes d'exploitation, portables inclus, supportent les sauvegardes automatiques, soit vers un disque externe, soit vers un Cloud.

Rédacteur Invité

*Instructeur certifiée SANS **Steve Anson** conseille les équipes de sécurité informatique et gouvernements à travers le monde pour améliorer la sécurité. Steve est l'auteur d'un prochain livre intitulé « Réponse aux incidents appliquée » et propose des ressources gratuites pour les praticien de la cyber sécurité sur* AppliedIncidentResponse.com.

Ressources

Ingénierie sociale :	https://www.sans.org/u/W3G
Attaques personnalisées :	https://www.sans.org/u/W3Q
Simplifier les mots de passe :	https://www.sans.org/u/W3V
Sauvegardez-vous ? :	https://www.sans.org/u/W40