OUCH! Février 2023

Votre bulletin mensuel sur la sensibilisation à la sécurité

Ai-je besoin d'un logiciel de sécurité ?

Aperçu

Lorsque vous achetiez un nouvel ordinateur il y a quelques années, vous deviez souvent installer un logiciel de sécurité supplémentaire sur votre ordinateur afin de le protéger contre les cyberattaquants. Cependant, la plupart des ordinateurs et des appareils d'aujourd'hui intègrent déjà de nombreuses fonctions de sécurité, telles que la mise à jour automatique, les pare-feu, le cryptage des disques et la protection des fichiers. En outre, Microsoft fournit sur les ordinateurs Windows une fonctionnalité de sécurité appelée Microsoft Defender, qui comprend des fonctions supplémentaires telles qu'un anti-virus. À bien des égards, les systèmes actuels sont beaucoup plus sûrs par défaut. En fait, VOUS êtes très probablement maintenant la plus grande faiblesse. C'est pourquoi les cyberattaquants ciblent continuellement les gens, en essayant de vous inciter à faire des choses que vous ne devriez pas faire, comme donner vos mots de passe, cliquer sur des liens ou ouvrir des pièces jointes d'e-mails qui installent des logiciels malveillants sur vos ordinateurs ou partagent les informations de votre carte de crédit.

Quels outils dois-je envisager ?

Si vous souhaitez prendre des mesures supplémentaires pour sécuriser vos systèmes, il existe des programmes de sécurité supplémentaires que vous pouvez envisager.

Gestionnaire de mots de passe : Les mots de passe peuvent être complexes et fastidieu, surtout s'il faut se souvenir de centaines de mots de passe différents. Un gestionnaire de mots de passe est un coffre-fort sécurisé qui protège et stocke tous vos mots de passe pour vous, de sorte que vous n'ayez à retenir qu'un seul mot de passe principal. En outre, ils peuvent vous connecter à des sites Web, générer des mots de passe pour vous et aider à valider certains sites Web.

Réseaux Privés Virtuels (VPN) Les VPN visent principalement à protéger votre vie privée en cryptant votre connexion à internet et en masquant votre emplacement d'origine.

Suites de sécurité : Il s'agit de paquets de logiciels de sécurité qui fournissent un ensemble de fonctions de sécurité supplémentaires en plus de celles déjà fournies par votre système d'exploitation. Par exemple, le filtrage des sites web dangereux, le contrôle parental et souvent un VPN. Chaque suite a des caractéristiques différentes, alors recherchez celle qui vous semble la meilleure si vous en avez besoin.

Sélection d'un fournisseur de sécurité

Si vous devez acheter des outils ou des logiciels de sécurité supplémentaires, vous pouvez choisir parmi de nombreux fournisseurs. Lequel devriez-vous choisir ? Bien souvent, les caractéristiques offertes par les différents fournisseurs sont plus similaires que différentes. L'essentiel est d'utiliser une solution proposée par un fournisseur de confiance. Vous ne voulez pas acheter et installer accidentellement un produit distribué par des cybercriminels et infecté par des logiciels malveillants.

N'achetez des outils qu'auprès de fournisseurs connus, dont vous avez entendu parler et en qui vous avez confiance. N'achetez jamais un outil d'une entreprise que vous ne connaissez pas, qui est tout nouveau, ou qui n'a pas de commentaires ou beaucoup de commentaires négatifs. Vous voulez être sûr que la solution que vous achetez est légitime et qu'elle est activement mise à jour et entretenue. Vous pouvez même vous demander dans quel pays le vendeur est basé. Il existe de nombreux sites en ligne qui proposent des évaluations de fournisseurs de confiance mettant en évidence les différences de fonctionnalités et de coûts de leurs logiciels de sécurité.

Faites attention aux outils gratuits. Bien qu'il existe d'excellents outils de sécurité gratuits, certains problèmes peuvent se poser. Ces outils peuvent avoir des fonctionnalités limitées, être difficiles à utiliser ou ne pas être mis à jour fréquemment. Dans certains cas, les outils gratuits peuvent être développés par des cyber-attaquants, puis infectés par des logiciels malveillants.

N'oubliez pas que, même si ces outils de sécurité sont utiles, commencez par les fonctions de sécurité intégrées de votre ordinateur, notamment l'activation de la mise à jour automatique. Les systèmes d'exploitation actuels sont très sûrs par défaut. Vous êtes de loin la meilleure défense. Méfiez-vous des appels téléphoniques, des courriels ou des messages texte étranges ou suspects. Aucun logiciel de sécurité au monde ne peut vous protéger contre quelqu'un qui essaie de vous piéger ou de vous tromper en vous faisant faire quelque chose que vous ne devriez pas faire.

Rédacteur Invité

Nico "Dutch_OsintGuy" Dekens est un instructeur certifié SANS et un ancien analyste des renseignements gouvernementaux spécialisé dans les renseignements sur les sources ouvertes (OSINT). Plus d'informations sur Nico ici : https://www.sans.org/profiles/nico-dekens/
Bsides: http://www.securitybsides.com.

Ressources

Gestionnaires de mots de passe : https://www.sans.org/newsletters/ouch/password-managers/
Le pouvoir des mises à jour : https://www.sans.org/security-awareness-training/resources/power-updating
Réseaux privés virtuels : https://www.privacyguides.org/vpn/
Ingénierie sociale : https://www.youtube.com/watch?v=lc7scxvKQOo
Critiques de suite de sécurité : https://www.pcmag.com/picks/the-best-security-suites

Traduit pour la communauté par : Juliette Busson