Votre bulletin mensuel sur la sensibilisation à la sécurité

Navigateurs

Aperçu

Les navigateurs tels que Google Chrome, Microsoft Edge, Safari ou Mozilla Firefox sont l'un des moyens les plus courants d'utiliser internet. Nous les utilisons pour lire les actualités, consulter nos e-mails, faire des achats en ligne, regarder des vidéos et jouer à des jeux. Par conséquent, les navigateurs sont également une cible pour les cyberattaquants.

Nombreux sont ceux qui pensent que la navigation en ligne est sûre si vous ne visitez que des sites Web connus et fiables. Cependant, il est assez facile de cliquer accidentellement sur une page web dangereuse ou de la visiter, parfois sans même le savoir. En outre, les sites web que vous connaissez et auxquels vous faites confiance peuvent être piratés par les cyber-criminels qui ont installé des logiciels malveillants. Enfin, les navigateurs d'aujourd'hui offrent de nombreuses nouvelles fonctionnalités, qui peuvent souvent être difficiles à utiliser et, en cas de mauvaise configuration, vous exposer à encore plus de dangers.

Exploiter votre navigateur en toute sécurité

Voici les étapes clés pour vous protéger :

Mise à jour : Utilisez toujours la dernière version de votre navigateur. Les navigateurs mis à jour disposent des derniers correctifs de sécurité et sont beaucoup plus sûrs. Avec les ordinateurs d'aujourd'hui, cela est devenu beaucoup plus facile, car il suffit d'activer la mise à jour automatique sur votre système. Ou, pour certains navigateurs, il suffit de redémarrer le navigateur chaque fois qu'il vous indique qu'il y a une nouvelle mise à jour. Après une mise à jour, vérifiez les nouvelles fonctions de sécurité dont vous pouvez bénéficier.

Avertissements : Les navigateurs actuels peuvent souvent reconnaître certains sites web malveillants conçus pour vous nuire. Si votre navigateur vous avertit que le site que vous êtes sur le point de visiter est dangereux, fermez l'onglet de votre navigateur et trouvez ce dont vous avez besoin sur un autre site.

Synchronisation : Ne synchronisez jamais votre navigateur professionnel avec votre navigateur personnel ou vos comptes personnels. La synchronisation consiste à permettre aux navigateurs de différents appareils de communiquer entre eux et de partager vos informations de navigation, telles que votre historique de navigation, vos signets et le contenu enregistré.

Mots de passe : De nombreux navigateurs offrent la possibilité d'enregistrer vos mots de passe sur différents sites. Au lieu de stocker vos mots de passe dans votre navigateur, nous vous recommandons d'utiliser un gestionnaire de mots de passe dédié. Les gestionnaires de mots de passe sont une application de sécurité à part qui possède beaucoup plus de caractéristiques et de fonctionnalités de sécurité.

Plug-ins : Les plug-ins ou les extensions sont de petits logiciels ajoutés aux navigateurs qui peuvent ajouter des fonctionnalités. Cependant, chaque nouveau plug-in que vous ajoutez peut également ajouter des dangers supplémentaires. Sur votre ordinateur de travail, n'ajoutez que des plug-ins autorisés et approuvés, et tout comme votre navigateur, tenez-les à jour. Supprimez les plug-ins dont vous n'avez plus besoin ou que vous n'utilisez plus.

La fonction navigation privée : La plupart des navigateurs proposent une option de confidentialité (également appelée « navigation privée »). Cela signifie que lorsque vous ouvrez un onglet du navigateur en mode « navigation privée », vous limitez les informations recueillies à votre sujet. Par exemple, votre navigateur ne collecte pas de cookies, ne suit pas l'historique de navigation et ne stocke ni ne distribue aucune information sensible vous concernant.

Les applications de messages en ligne : Certains sites Web proposent désormais une fonction de discussion en direct où vous pouvez poser des questions. Ne participez à ces discussions en ligne qu'avec des sites Web connus et fiables. En outre, limitez les informations que vous partagez au cours d'une session de chat en direct, car vous n'avez aucune idée de qui collecte vos informations, de ce qu'il en fait et à qui il peut les vendre ou les partager.

Vous avez le contrôle : Les sites Web frauduleux tentent de pirater votre ordinateur en affichant une fausse fenêtre contextuelle de sécurité dans votre navigateur, indiquant que votre ordinateur est infecté, et en vous incitant à participer à une session de discussion en ligne pour réparer votre ordinateur. Il vous demandera alors instamment de l'autoriser à installer un agent distant pour lui permettre de réparer votre ordinateur. En réalité, votre ordinateur va très bien. Au lieu de cela, ils tentent de vous inciter à installer un logiciel malveillant afin de voler vos mots de passe et vos données, et de suivre toute votre activité en ligne.

Se déconnecter : Lorsque vous avez terminé de naviguer sur un site web, veillez à vous déconnecter pour supprimer les informations sensibles de connexion et de mot de passe avant de fermer le navigateur.

Rédacteur Invité

Dean Parsons est le PDG d'ICS Defense Force, avec plus de 20 ans d'expérience en matière de cyberdéfense IT/ICS. Il est également instructeur certifié SANS pour ICS515 et co-auteur / instructeur de ICS418, enseignant la cyberdéfense active, la réponse aux incidents, le leadership et la gestion des risques pour les systèmes de contrôle industriels. www.linkedin.com/in/dean-parsons-cybersecurity.

Ressources

Gestionnaires de mots de passe : https://www.sans.org/newsletters/ouch/password-managers/
Attaques personnalisées : https://www.sans.org/security-awareness-training/resources/power-updating
Ingénierie sociale : https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Confidentialité : https://www.sans.org/newsletters/ouch/privacy/

Traduit pour la communauté par : Juliette Busson