SOYEZ CYBER SMART
#CyberMonth

MOIS DE LA SENSIBILISATION À LA CYBERSÉCURITÉ 2021 : FAITES VOTRE PART. #BECYBERSMART

CONFIDENTIALITE EN LIGNE

Internet touche presque tous les aspects de notre vie quotidienne. Nous pouvons faire des achats, effectuer des opérations bancaires, communiquer avec notre famille et nos amis et gérer nos dossiers médicaux en ligne. Ces activités nécessitent que vous fournissiez des informations personnellement identifiables (PII) telles que votre nom, votre date de naissance, vos numéros de compte, vos mots de passe et vos informations de localisation. #BeCyberSmart lors du partage d'informations personnelles en ligne pour réduire le risque de devenir une victime de cybercriminalité.

LE SAVIEZ-VOUS?

- 72 % des Américains pensent que la plupart de ce qu'ils font en ligne est suivi par des annonceurs, des entreprises technologiques et d'autres entreprises.[1]
- Plus de la moitié des Américains (52 %) déclarent avoir décidé de ne pas utiliser un produit ou un service parce qu'ils s'inquiétaient de la quantité d'informations personnelles collectées à leur sujet.[1]
- Les coûts des violations de données sont passés de 3,86 millions USD à 4,24 millions USD en 2021.[2]
- Les identifiants compromis, comme les mots de passe, étaient responsables de 20 % des violations pour un coût moyen de violation de 4,37 millions USD.[2]

DES CONSEILS SIMPLES

- **Doublez votre protection de connexion.** Activez l'authentification multifactorielle (MFA) pour vous assurer que la seule personne ayant accès à votre compte est vous-même. Utilisez-le pour les emails, les opérations bancaires, les réseaux sociaux et tout autre service nécessitant une connexion. Activez MFA en utilisant un appareil mobile de confiance, tel que votre smartphone, une application d'authentification ou un jeton sécurisé, un petit appareil physique qui peut se connecter a votre trousseau de clés. Lisez le Guide pratique de l'authentification multifacteur pour plus d'information.
- **Changez votre protocole de mot de passe.** Utilisez le mot de passe ou la phrase secrète le plus long autorisé. Le fait d'avoir des mots de passe différents pour différents comptes permet d'empêcher les cybercriminels d'accéder à ces comptes et de vous protéger en cas de violation. Utilisez des gestionnaires de mots de passe pour générer et mémoriser des mots de passe différents et complexes pour chacun de vos comptes. Lisez la fiche de conseils sur la cybersécurité des média sociaux pour plus d'information.
- **Restez à jour.** Gardez votre logiciel à jour avec la dernière version disponible. Gérez vos paramètres de sécurité pour protéger vos informations en activant les mises à jour automatiques afin que vous n'ayez pas à y penser et configurez votre logiciel de sécurité pour qu'il exécute des analyses régulières.
- **Si vous le connectez, protégez-le.** Qu'il s'agisse de votre ordinateur, smartphone, console de jeu ou autre périphérique réseau, la meilleure défense contre les virus et les logiciels malveillants consiste à mettre à jour les

derniers logiciels de sécurité, navigateur Web et systèmes d'exploitation. Inscrivez-vous aux mises à jour automatiques, si vous le pouvez, et protégez vos appareils avec un logiciel antivirus. Lisez la fiche de conseils sur la cybersécurité des média sociaux pour plus d'information.

- **Jouez dur pour avoir des inconnus.** Les cybercriminels utilisent des tactiques de phishing dans l'espoir de tromper leurs victimes. Si vous n'êtes pas sûr de l'expéditeur d'un email, même si les détails semblent exacts, ou si l'e-mail semble « hameçonneur », ne répondez pas et ne cliquez sur aucun lien ou pièce jointe trouvé dans cet e-mail. Lorsqu'elles sont disponibles, utilisez l'option « indésirable » ou « bloquer » pour ne plus recevoir de messages d'un expéditeur particulier.
- **Ne jamais cliquer et dire.** Limitez les informations que vous publiez sur les réseaux sociaux, des adresses personnelles aux endroits où vous aimez prendre un café. Ce que beaucoup de gens ne réalisent pas, c'est que ces détails apparemment aléatoires sont tout ce que les criminels doivent savoir pour vous cibler, vos proches et vos biens physiques, en ligne et dans le monde réel. Gardez les numéros de sécurité sociale, les numéros de compte et les mots de passe privés, ainsi que des informations spécifiques vous concernant, telles que votre nom complet, votre adresse, votre anniversaire et même vos projets de vacances. Désactivez les services de localisation qui permettent à n'importe qui de voir où vous êtes et où vous n'êtes pas à tout moment. Lisez la fiche de conseils sur la cybersécurité des média sociaux pour plus d'information.
- **Gardez un œil sur vos applications.** La plupart des appareils, jouets et appareils connectés sont pris en charge par une application mobile. Votre appareil mobile peut être rempli d'applications suspectes s'exécutant en arrière-plan ou utilisant des autorisations par défaut que vous n'aviez jamais réalisé avoir approuvées, rassemblant vos informations personnelles à votre insu tout en mettant votre identité et votre vie privée en danger. Vérifiez les autorisations de votre application et utilisez la « règle du moindre privilège » pour supprimer ce dont vous n'avez pas besoin ou n'utilisez plus. Apprenez à simplement dire « non » aux demandes de privilèges qui n'ont pas de sens. Téléchargez uniquement des applications provenant de fournisseurs et de sources de confiance.
- **Restez protégé lorsque vous êtes connecté.** Avant de vous connecter à un point d'accès sans fil public, comme dans un aéroport, un hôtel ou un café, assurez-vous de confirmer le nom du réseau et les procédures de connexion exactes avec le personnel approprié pour vous assurer que le réseau est légitime. Si vous utilisez un point d'accès public non sécurisé, pratiquez une bonne hygiène Internet en évitant les activités sensibles (par exemple, les opérations bancaires) qui nécessitent des mots de passe ou des cartes de crédit. Votre point d'accès personnel est souvent une alternative plus sûre au Wi-Fi gratuit. N'utilisez que des sites commençant par « https:// » lorsque vous effectuez des achats ou des opérations bancaires en ligne.

CONTACTEZ L'EQUIPE CISA DU MOIS DE SENSIBILISATION A LA CYBERSECURITE

Merci pour votre soutien et votre engagement continus envers le Mois de la sensibilisation à la cybersécurité et pour aider tous les Américains à rester en sécurité en ligne. Veuillez envoyer un courriel à notre équipe à CyberAwareness@cisa.dhs.gov ou visitez le www.cisa.gov/cybersecurity-awareness-month ou même staysafeonline.org/cybersecurity-awareness-month/ pour en savoir plus.

RESSOURCES :

1. Auxier, Brooke, "Comment les Américains voient les problèmes de confidentialité numérique au milieu de l'épidémie de COVID-19." Centre de recherche Pew : Réservoir de faits. Le 04 mai, 2020 https://www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/
2. IMB, « Rapport sur le coût d'une violation de données 2021 ». Sécurité de l'IMB. Juillet 2021. https://www.ibm.com/security/data-breach