SOYEZ CYBER SMART
#CyberMonth

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

VOL D'IDENTITÉ ET ARNAQUE SUR INTERNET

La technologie d'aujourd'hui nous permet de nous connecter partout dans le monde, d'effectuer des opérations bancaires et de faire des achats en ligne, et de contrôler nos téléviseurs, nos maisons et nos voitures à partir de nos smartphones. Cette commodité supplémentaire s'accompagne d'un risque accru d'usurpation d'identité et d'escroqueries sur Internet. #BeCyberSmart sur Internet—à la maison, à l'école, au travail, sur les appareils mobiles et en déplacement.

LE SAVIEZ-VOUS ?

- Le coût moyen d'une violation de données pour pour une entreprise américaine en 2020 était de 8,84 millions de dollars. [1]. Il s'agit d'une augmentation par rapport au chiffre de 8,64 millions de dollars en 2019.
- 7-10% de la population américaine est victime d'usurpation d'identité chaque année, et 21 % d'entre elles subissent de multiples incidents d'usurpation d'identité[2].
- En 2020, 47% des personnes vivant aux États-Unis ont été victimes d'une usurpation d'identité[3].

ESCARPINS INTERNET COURANTS

À mesure que la technologie continue d'évoluer, les cybercriminels utiliseront des techniques plus sophistiquées pour exploiter des systèmes, des comptes et des appareils afin de voler votre identité, vos informations personnelles et votre argent. Pour vous protéger des menaces en ligne, vous devez savoir quoi rechercher. Voici certaines des escroqueries sur Internet les plus courantes :

- Les escroqueries COVID-19 prennent la forme d'e-mails avec des pièces jointes malveillantes ou des liens vers des sites Web frauduleux pour inciter les victimes à révéler des informations sensibles ou à faire un don à des œuvres caritatives ou à des causes frauduleuses. Faites preuve de prudence dans le traitement de tout e-mail contenant une ligne d'objet, une pièce jointe ou un lien hypertexte lié à COVID-19, et méfiez-vous des appels, SMS ou appels liés à COVID-19 sur les réseaux sociaux.
- Les escroqueries par imposteur se produisent lorsque vous recevez un e-mail ou un appel d'une personne prétendant être un représentant du gouvernement, un membre de votre famille ou un ami vous demandant des informations personnelles ou financières. Par exemple, un imposteur peut vous contacter depuis la Social Security Administration pour vous informer que votre numéro de sécurité sociale (SSN) a été suspendu, dans l'espoir que vous révéliez votre SSN ou que vous payiez pour le réactiver.
- Les escroqueries liées aux paiements économiques du COVID-19 ciblent les paiements de relance des Américains. La CISA exhorte tous les Américains à être à l'affût de la fraude criminelle liée aux paiements à impact économique COVID-19 - en particulier la fraude utilisant des leurres de coronavirus pour voler des informations personnelles et financières, ainsi que les paiements à impact économique eux-mêmes - et pour les adversaires cherchant à perturber les efforts de paiement

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 e-mails, les opérations

bancaires, les réseaux sociaux et tout autre service nécessitant une connexion. Si MFA est une option, activez-la à l'aide d'un appareil mobile de confiance, tel que votre smartphone, une application d'authentification ou un jeton sécurisé, un petit dispositif physique qui peut s'accrocher à votre trousseau de clés.

- **SECOUEZ VOTRE PROTOCOLE DE MOT DE PASSE.** Selon les directives du National Institute of Standards and Technology (NIST), vous devriez envisager d'utiliser le mot de passe ou la phrase secrète le plus long autorisé. Faites preuve de créativité et personnalisez votre mot de passe standard pour différents sites, ce qui peut empêcher les cybercriminels d'accéder à ces comptes et 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 création d'un mot de passe pour plus d'informations.
- **RESTEZ A JOUR.** Gardez votre logiciel à jour avec la dernière version disponible. Conservez 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 exécuter des analyses régulières

PROTÉGEZ-VOUS CONTRE LA FRAUDE EN LIGNE

RESTEZ PROTEGE LORSQUE VOUS ETES CONNECTE : L'essentiel est que chaque fois que vous êtes en ligne, vous êtes vulnérable. Si les appareils de votre réseau sont compromis pour une raison quelconque, ou si des pirates piratent un pare-feu crypté, quelqu'un pourrait vous espionner, même chez vous via un réseau Wi-Fi crypté.

- Naviguez en toute sécurité sur le Web où que vous soyez en recherchant l'icône de « cadenas vert » ou de cadenas dans la barre de votre navigateur, ce qui signifie une connexion sécurisée.
- Lorsque vous vous trouvez dans le grand « Wi-Fi West sauvage », évitez l'accès gratuit à Internet sans cryptage.
- 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.
- Ne révélez pas d'informations personnellement identifiables telles que votre numéro de compte bancaire, votre SSN ou votre date de naissance à des sources inconnues.
- Tapez les URL de sites Web directement dans la barre d'adresse au lieu de cliquer sur des liens ou de copier-coller à partir de l'email.

RESSOURCES À VOTRE DISPOSITION

Si vous découvrez que vous êtes devenu une victime de cybercriminalité, informez immédiatement les autorités pour déposer une plainte. Conservez et enregistrez toutes les preuves de l'incident et de sa source présumée. La liste ci-dessous répertorie les organisations gouvernementales auprès desquelles vous pouvez déposer une plainte si vous êtes victime de cybercriminalité.

- **FTC.gov**: La ressource unique et gratuite de la FTC, www.identitytheft.gov/peut vous aider à signaler et à récupérer du vol d'identité. Signalez la fraude à la FTC à ftc.gov/OnGuardOnline ou www.ftccomplaintassistant.gov.
- **US-CERT.gov**: Signalez les vulnérabilités des ordinateurs ou des réseaux à l'US-CERT via la ligne d'assistance : 1-888-282-0870 ou us-cert.cisa.gov. Transmettez les courriels ou les sites Web de phishing à l'US-CERT à l'adresse suivante phishing-report@us-cert.gov.
- **IC3.gov**: Si vous êtes victime d'un crime en ligne, déposez une plainte auprès du Centre de plainte pour les crimes sur Internet (IC3) à l'adresse suivante www.IC3.gov.
- **SSA.gov**: Si vous pensez que quelqu'un utilise votre SSN, contactez le service d'assistance téléphonique pour les fraudes de la Social Security Administration au 1-800-269-0271.

CONTACTEZ L'EQUIPE CISA DU MOIS DE LA 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 consultez le http://www.cisa.gov/cybersecurity-awareness-month ou même le staysafeonline.org/cybersecurity-awareness-month/ pour en savoir plus.

RESSOURCES

1. Brook, Chris. (Le 18 aout, 2020). *Combien coûte une violation de données en 2020 ?* Digital Guardian. https://digitalguardian.com/blog/what-does-data-breach-cost-2020
2. Ricks, A, Irvin-Erickson, Y, PhD (2021). *Mémoire de recherche : Vol d'identité et fraude.* Centre de recherche sur les victimes. https://ncvc.dspacedirect.org/bitstream/item/1228/CVR Research Syntheses_Identity Theft and Fraud_Brief.pdf
3. GIACT. (2021). *Vol d'identité aux États-Unis : La réalité austère.* GIACT Systems, LLC.https://www.giact.com/aite-report-us-identity-theft-the-stark-reality/