SOYEZ CYBER SMART
#CyberMonth

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

CYBERSÉCURITÉ TOUT EN VOYAGEANT

Dans un monde où nous sommes constamment connectés, la cybersécurité ne peut se limiter à la maison ou au bureau. Lorsque vous voyagez, qu'il soit national ou international, il est toujours important d'adopter un comportement en ligne sûr et de prendre des mesures proactives pour sécuriser les appareils connectés à Internet. Plus nous voyageons, plus nous risquons de subir des cyberattaques. #BeCyberSmart et utilisez ces conseils pour vous connecter en toute confiance lors de vos déplacements.

DES CONSEILS SIMPLES

AVANT QUE TU PARTES

- **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 Fiche de conseils sur l'hameçonnage pour plus d'information.
- **Sauvegardez vos informations.** Sauvegardez vos contacts, données financières, photos, vidéos et autres données d'appareil mobile sur un autre appareil ou service cloud au cas où votre appareil serait compromis, et vous devez le réinitialiser aux paramètres d'usine.
- **Connectez-vous uniquement avec des personnes de confiance.** Bien que certains réseaux sociaux puissent sembler plus sûrs pour se connecter en raison du nombre limité d'informations personnelles partagées à travers eux, gardez vos liens avec des personnes que vous connaissez et en qui vous avez confiance.
- **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.
- **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 Lisez le Guide pratique de l'authentification multifacteur (MFA) pour plus d'information.

PENDANT VOTRE VOYAGE

- **Arrêtez la connexion automatique.** Certains appareils rechercheront et se connecteront automatiquement aux réseaux sans fil disponibles ou aux appareils Bluetooth. Cette connexion instantanée permet aux cybercriminels d'accéder à distance à vos appareils. Désactivez ces fonctionnalités afin de choisir activement quand vous connecter à un réseau sécurisé.

- **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.
- **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'email semble « hameçonneur », ne répondez pas et ne cliquez sur aucun lien ou pièce jointe trouvé dans cet email. Lorsqu'elles sont disponibles, utilisez l'option « indésirable » ou « bloquer » pour ne plus recevoir de messages d'un expéditeur particulier. Lisez la fiche de conseils Fiche de conseils sur l'hameçonnage pour plus d'information.
- **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.
- **Protégez vos appareils mobiles.** Pour empêcher le vol et l'accès non autorisé ou la perte d'informations sensibles, ne laissez jamais votre équipement, y compris les périphériques de stockage USB ou externes, sans surveillance dans un lieu public. Gardez vos appareils en sécurité dans les taxis, dans les aéroports, dans les avions et dans votre chambre d'hôtel.

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.