SOYEZ CYBER SMART
#CyberMonth

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

PROTEGER VOTRE MAISON NUMERIQUE

Un plus grand nombre de nos appareils domestiques, y compris les thermostats, les serrures de porte, les machines à café et les détecteurs de fumée, sont désormais connectés à Internet. Cela nous permet de contrôler les appareils sur nos smartphones, ce qui peut nous faire gagner du temps et de l'argent tout en offrant commodité et même sécurité. Ces avancées technologiques sont innovantes et intrigantes, mais elles posent également un nouvel ensemble de risques pour la sécurité. #BeCyberSmart pour vous connecter en toute confiance et protéger votre maison numérique.

DES CONSEILS SIMPLES

- **Sécurisez vos réseaux.** Le routeur sans fil de votre maison est la principale entrée des cybercriminels pour accéder à tous vos appareils connectés. Sécurisez le Wi-Fi et les appareils numériques en modifiant le mot de passe et le nom d'utilisateur par défaut. Pour plus d'informations sur la protection de votre réseau domestique, consultez la page Sécurisation des réseaux sans fil de CISA.
- **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.
- **Si vous vous connectez, vous devez protéger.** 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. Si vous avez la possibilité d'activer les mises à jour automatiques pour vous défendre contre les derniers risques, activez-la. Et, si vous insérez quelque chose dans votre appareil, comme une clé USB pour un disque dur externe, assurez-vous que le logiciel de sécurité de votre appareil recherche les virus et les logiciels malveillants. Enfin, protégez vos appareils avec un logiciel antivirus et assurez-vous de sauvegarder périodiquement toutes les données qui ne peuvent pas être recréées telles que des photos ou des documents personnels.
- **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.

- **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 le Fiche de conseils sur la cybersécurité des médias sociaux pour plus d'informations.
- **Utilisez le partage de fichiers avec prudence.** Le partage de fichiers entre les appareils doit être désactivé lorsqu'il n'est pas nécessaire. Vous devez toujours choisir de n'autoriser le partage de fichiers que sur les réseaux domestiques ou professionnels, jamais sur les réseaux publics. Vous pouvez envisager de créer un répertoire dédié pour le partage de fichiers et restreindre l'accès à tous les autres répertoires. De plus, vous devez protéger par mot de passe tout ce que vous partagez.
- **Vérifiez les options de sécurité sans fil de votre fournisseur d'accès Internet ou du fabricant de votre routeur.** Votre fournisseur de services Internet et le fabricant de votre routeur peuvent fournir des informations ou des ressources pour vous aider à sécuriser votre réseau sans fil. Consultez la zone de support client de leurs sites Web pour des suggestions ou des instructions spécifiques.
- **Connectez-vous à l'aide d'un réseau privé virtuel (VPN).** De nombreuses entreprises et organisations ont un VPN. Les VPN permettent aux employés de se connecter en toute sécurité à leur réseau lorsqu'ils ne sont pas au bureau. Les VPN cryptent les connexions aux extrémités de l'envoi et de la réception et bloquent le trafic qui n'est pas correctement crypté. Si un VPN est disponible, assurez-vous de vous y connecter chaque fois que vous avez besoin d'utiliser un point d'accès sans fil public.
- **Accès restreint.** Autorisez uniquement les utilisateurs autorisés à accéder à votre réseau. Chaque élément matériel connecté à un réseau possède une adresse de contrôle d'accès au support (MAC). Vous pouvez restreindre l'accès à votre réseau en filtrant ces adresses MAC. Consultez votre documentation utilisateur pour obtenir des informations spécifiques sur l'activation de ces fonctionnalités. Vous pouvez également utiliser le compte « invité », qui est une fonctionnalité largement utilisée sur de nombreux routeurs sans fil. Cette fonctionnalité vous permet d'accorder un accès sans fil aux invités sur un canal sans fil distinct avec un mot de passe distinct, tout en préservant la confidentialité de vos informations d'identification principales.

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.