SOYEZ CYBER SMART
#CyberMonth

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

CREER UN MOT DE PASSE

La création d'un mot de passe fort est une étape essentielle pour se protéger en ligne. L'utilisation de mots de passe longs et complexes est l'un des moyens les plus simples de se défendre contre la cybercriminalité. Personne n'est à l'abri du cyber-risque, mais #BeCyberSmart et vous pouvez minimiser vos chances de subir un incident

DES CONSEILS SIMPLES

- **Utilisez une phrase de passe longue.** Selon l'orientation Institut national des normes et de la technologie (NIST), vous devriez envisager d'utiliser le plus long mot de passe ou mot de passe admissible. Par exemple, vous pouvez utiliser une phrase secrète telle qu'un titre d'actualité ou même le titre du dernier livre que vous avez lu. Ensuite, ajoutez des signes de ponctuation et des majuscules.
- **Ne rendez pas les mots de passe faciles à deviner.** N'incluez pas d'informations personnelles dans votre mot de passe telles que votre nom ou les noms d'animaux de compagnie. Ces informations sont souvent faciles à trouver sur les réseaux sociaux, ce qui permet aux cybercriminels de pirater plus facilement vos comptes.
- **Évitez d'utiliser des mots courants.** Remplacez les lettres par des chiffres et des signes de ponctuation ou des symboles. Par exemple, @ peut remplacer la lettre "A" et un point d'exclamation (!) peut remplacer les lettres "I" ou "L".
- **Soyez créatif.** Utilisez des remplacements phonétiques, tels que "PH" au lieu de "F". Ou faites des fautes d'orthographe délibérées, mais évidentes, telles que « mauteur » au lieu de « moteur ».
- **Gardez vos mots de passe secrets.** Ne divulguez vos mots de passe à personne et surveillez les attaquants qui essaient de vous inciter à révéler vos mots de passe par e-mail ou par appels. Chaque fois que vous partagez ou réutilisez un mot de passe, il compromet votre sécurité en ouvrant davantage de voies par lesquelles il pourrait être utilisé à mauvais escient ou volé.
- **Compte unique, mot de passe unique.** 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. Il est important de mélanger les choses : trouvez des moyens faciles à retenir pour personnaliser votre mot de passe standard pour différents sites.
- **Doublez votre protection de connexion.** Activez l'authentification multifactorielle (MFA) pour vous assurer que la seule personne ayant accès à votre compte n'est que vous-même. Utilisez-le pour les e-mails, 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.
- **Utilisez un gestionnaire de mots de passe pour mémoriser les mots de passe.** Le moyen le plus sûr de stocker tous vos mots de passe uniques consiste à utiliser un gestionnaire de mots de passe. Avec qu'un seul mot de passe, un ordinateur peut créer et enregistrer des mots de passe pour chaque compte que vous possédez, protégeant vos informations en ligne, y compris les numéros de carte de crédit et leurs codes à trois chiffres, les réponses aux questions de sécurité, etc..

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

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 au CyberAwareness@cisa.dhs.gov ou visitez le www.cisa.gov/cybersecurity-awareness-month ou au staysafeonline.org/cybersecurity-awareness-month/ pour en savoir plus.