CYBERSECURITY AWARENESS MONTH

S'INVESTIR DANS LA CYBERSÉCURITÉ (SEE YOURSELF IN CYBER)

Tout le monde contribue à la cybersécurité, peu importe le rôle.

Le thème du mois de la sensibilisation à la cybersécurité de 2022, « S'INVESTIR DANS LA CYBERSÉCURITÉ » (s'investir dans la cybersécurité), indique que, même si la cybersécurité semble être un sujet complexe, fondamentalement, c'est avant tout une question de personnes. Faites votre part pour assurer la cybersécurité de vous-même et de votre entreprise en prenant quatre mesures clés.

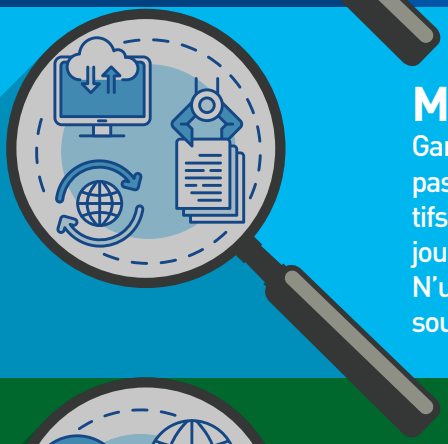
ACTIVER L'AUTHENTIFICATION MULTIFACTEUR

Aussi connue sous le terme « authentification à deux facteurs » et « vérification en deux étapes », l'authentification multifacteur est une mesure de sécurité qui exige que quiconque ouvre une session dans un compte suive un processus en deux étapes pour prouver son identité. Elle rend deux fois plus difficile l'accès à un compte en ligne par les criminels. Par l'ajout d'une simple étape supplémentaire pendant l'ouverture d'une session dans un compte, l'authentification multifacteur augmente grandement la sécurité de votre compte.

UTILISER DES MOTS DE PASSE ROBUSTES

Les mots de passe sont importants pour assurer la sécurité de vos renseignements. Voici quelques moyens simples de sécuriser vos comptes grâce à de meilleurs mots de passe. Peu importe le compte, tous les mots de passe devraient être créés en gardant les trois mots suivants à l'esprit.

- Long : au moins 12 caractères
- Unique : chaque compte doit avoir son mot de passe unique
- Complexe : composé d'une combinaison de lettres majuscules et minuscules, de chiffres et de caractères spéciaux. Certains sites Web vous permettent même d'inclure des espaces.



METTRE LES LOGICIELS À JOUR

Gardez toujours vos logiciels à jour quand les mises à jour sont disponibles. N'attendez pas. Ces mises à jour corrigent certains problèmes logiciels et offrent de nouveaux correctifs de sécurité où les criminels pourraient s'infiltrer. Quand vous téléchargez une mise à jour logicielle, faites-le uniquement auprès de l'entreprise qui a créé le logiciel en question. N'utilisez jamais de versions logicielles piratées ou sans licence, car celles-ci contiennent souvent des logiciels malveillants qui causent plus de problèmes qu'ils n'en résolvent.

RECONNAÎTRE ET SIGNALER L'HAMEÇONNAGE

Les signes peuvent être subtils, mais une fois que vous avez reconnu une tentative d'hameçonnage, vous pouvez éviter de vous faire prendre. Voici quelques conseils simples pour repérer clairement un courriel hameçon imposteur. Il contient une offre trop belle pour être vraie; il est écrit dans un langage urgent, alarmant ou menaçant; il est mal écrit et contient des fautes d'orthographe et de grammaire; la salutation est ambiguë ou très générique; il contient des demandes d'envoi de renseignements personnels; on insiste de cliquer sur des hyperliens inconnus ou des pièces jointes; il contient des propositions d'affaires étranges ou soudaines; l'adresse de courriel de l'expéditeur ne correspond pas à l'entreprise qui l'aurait envoyé.

MAUSER
Packaging Solutions