ASSURER SA CYBERSÉCURITÉ DURANT LA COVID-19

Depuis le début de la pandémie de COVID-19, les Canadiens passent plus de temps que jamais en ligne. Or, le nombre de tentatives de fraude attribuables à des cybercriminels qui prétendent représenter un organisme de santé ou le gouvernement du Canada continue d'augmenter. Voilà pourquoi il est essentiel de veiller à notre cybersécurité.

La pandémie de COVID-19 nous a montré que le monde peut changer très rapidement, mais la nécessité d'assurer notre cybersécurité, elle, ne change pas. Si vous savez comment reconnaître une tentative de fraude et protéger vos comptes, vous serez prêt à affronter les menaces auxquelles vous pourriez être exposé.

QUELQUES ÉTAPES SIMPLES POUR VOUS PROTÉGER

NE MORDEZ PAS À L'HAMEÇON

Les tentatives d'hameçonnage sont des messages électroniques ou des appels téléphoniques conçus pour vous amener à croire qu'ils proviennent de personnes ou d'organisations que vous connaissez. Dans certains cas, les cybercriminels connaissent de l'information à votre sujet, ce qui pourrait vous faire penser qu'il s'agit d'un message ou d'un appel légitime.

SI VOUS RECEVEZ UN COURRIEL, UN APPEL TÉLÉPHONIQUE OU UN MESSAGE TEXTE SUSPECT, MÊME S'IL SEMBLE PROVENIR D'UNE ENTREPRISE CONNUE OU D'UN AMI, VOICI CE QUE VOUS DEVEZ FAIRE :

RESPIREZ. Les messages d'hameçonnage sont conçus pour exercer une pression ou même menacer la victime afin de l'amener à répondre rapidement. Si l'on exige que vous répondiez « immédiatement », il s'agit probablement d'une tentative d'escroquerie.

NE CLIQUEZ PAS SUR LES LIENS OU LES PIÈCES JOINTES dont vous n'êtes pas certains. Tentez de joindre l'expéditeur d'une autre manière, par exemple par téléphone, pour confirmer qu'il a bien envoyé le message.

PENSEZ AUX SITES QUE VOUS AVEZ VISITÉS SUR INTERNET. À moins que vous en ayez fait la demande, tous les messages vous demandant de réinitialiser votre mot de passe ou de mettre à jour les renseignements sur votre compte sont probablement faux.

SUPPRIMEZ TOUT MESSAGE QUI SEMBLE TROP BEAU POUR ÊTRE VRAI, comme les messages qui vous annoncent que vous avez gagné un concours auquel vous n'avez pas participé.

CRÉEZ DES MOTS DE PASSE ROBUSTES

Utilisez une **phrase de passe** composée d'au moins 4 mots et 15 caractères.

Ou bien un mot de **passe complexe** :

- Au moins 12 caractères
- Combinaison de majuscules, minuscules, chiffres et symboles
- Aucun renseignement personnel

UTILISEZ UN MOT DE PASSE UNIQUE POUR CHAQUE COMPTE

NE PARTAGEZ JAMAIS VOS MOTS DE PASSE AVEC QUICONQUE

ACTIVEZ L'AUTHENTIFICATION MULTIFACTORIELLE

L'authentification multifactorielle ajoute une couche de sécurité qui permet de mieux protéger vos comptes et vos appareils en utilisant au moins deux facteurs pour vérifier que vous êtes bien la personne que vous prétendez être. C'est ce qu'on appelle les **facteurs d'authentification**.

Il existe différents types de facteurs d'authentification, dont :

- **Qui vous êtes**, comme vos empreintes digitales ou la reconnaissance faciale
- **Ce que vous connaissez**, comme une question de sécurité ou un mot de passe
- **Ce que vous possédez**, comme une application ou une notification sur votre téléphone

POUR D'AUTRES CONSEILS SUR LA FAÇON DE VOUS PROTÉGER ET DE PROTÉGER VOTRE ENTREPRISE ET VOS APPAREILS, CONSULTEZ PENSEZCYBERSECURITE.CA

SUIVEZ-NOUS SUR LES RÉSEAUX SOCIAUX @PENSEZCYBERSÉCURITÉ OU SUR TWITTER @CYBER_SECURITE

Centre de la sécurité des télécommunications
Communications Security Establishment
Canada