PROTÉGEZ-VOUS CONTRE LES ARNAQUES LIÉES À LA COVID-19

Les arnaques liées à la COVID-19 ne cessent d'augmenter. Dans certains cas, les cybercriminels se servent de la Prestation canadienne d'urgence (PCU) ou d'annonces d'équipement de protection pour vous inciter à cliquer sur des liens dans le but de vous voler de l'argent ou de verrouiller l'accès à votre information.

Protégez-vous en apprenant comment vous pourriez être ciblé et en adoptant des mesures simples pour renforcer votre sécurité. Voici cinq mesures que vous pouvez prendre dès maintenant pour vous protéger, peu importe l'appareil que vous utilisez.

VISITEZ LE SITE WWW.CYBER.GC.CA POUR EN SAVOIR PLUS.

SOYEZ À L'AFFÛT DES ARNAQUES

Vous êtes une cible attrayante pour les cybercriminels.

Sachez reconnaître les messages d'hameçonnage et de harponnage.

Méfiez-vous des liens suspects – ne cliquez jamais dessus. Le gouvernement du Canada ne vous enverra jamais de remboursement par message texte ni de transfert électronique de fonds. En cas de doute, consultez les sites Web officiels du gouvernement en tapant l'adresse URL dans votre navigateur. Visitez le site de l'***Agence du revenu du Canada*** (ARC) pour en savoir plus sur des arnaques courantes.

SÉCURISEZ VOS COMPTES DE MÉDIAS SOCIAUX ET DE COURRIEL

Passez en revue tous les paramètres de confidentialité et de sécurité dans vos comptes de médias sociaux et de courriel, et activez le plus de fonctions de protection que possible.

Choisissez des questions de sécurité auxquelles peu de gens connaissent les réponses. Par exemple, au lieu de « Comment s'appelle votre animal de compagnie? », choisissez plutôt « Qui était votre meilleur ami à la maternelle? », ou, mieux encore, donnez une réponse fictive que vous seul connaissez. Et ne dévoilez jamais cette information sur vos médias sociaux.

METTEZ À JOUR VOS APPAREILS MOBILES, VOS ORDINATEURS ET VOS APPLICATIONS

Les mises à jour sont essentielles pour votre protection, car elles peuvent contenir les correctifs de sécurité. Ne les ignorez jamais.

Assurez-vous d'appliquer les mises à jour aux systèmes d'exploitation de vos appareils ainsi qu'aux applications mobiles, et optez pour les mises à jour automatiques.

STOCKEZ VOS DONNÉES DE FAÇON SÉCURITAIRE ET SACHEZ COMMENT RÉCUPÉRER LES COPIES DE SAUVEGARDE

Utilisez un logiciel antivirus ou antimaliciel sur vos ordinateurs.

Créez des copies de sauvegarde pour vos fichiers importants et votre information personnelle essentielle. Pour ce faire, vous pouvez utiliser des services infonuagiques, mais n'oubliez pas de passer en revue les mesures de protection contre les rançongiciels offerts par votre fournisseur de services infonuagiques et d'activer toutes les fonctions de sécurité disponibles.

Exercez-vous au moins une fois à récupérer vos copies de sauvegarde. Vous saurez ainsi quoi faire si jamais vous êtes victime d'une attaque par rançongiciel.

ASSUREZ LA SÉCURITÉ DE VOS MOTS DE PASSE

Optez pour des phrases de passe uniques ou des mots de passe complexes, surtout pour les sites qui renferment des renseignements sensibles ou importants, comme vos comptes bancaires en ligne et vos comptes de l'ARC.

Ne dévoilez jamais vos mots de passe. N'utilisez pas le même mot de passe pour différents comptes, sites Web ou appareils.

Utilisez l'authentification à deux facteurs (A2F) lorsqu'elle est offerte.

Centre de la sécurité des télécommunications
Communications Security Establishment
Canada