Investissez dans votre cybersécurité

Comment sécuriser facilement vos données financières

Les services bancaires en ligne sont un moyen pratique de gérer vos finances et vos investissements, mais un accès instantané peut aussi signifier un accès plus facile pour les cybercriminels. En adoptant des mesures et des comportements simples en matière de cybersécurité, vous pouvez aider à garder en sécurité vos comptes en ligne et vos finances.

La population canadienne travaille fort pour son argent.

Mais elle ne sait pas toujours comment le protéger en ligne.

60 % de la population canadienne s'inquiète des pertes financières causées par la cybercriminalité[1]

mais

seulement **22 %** de la population se sent en mesure de faire face aux cybermenaces qui pèsent sur leurs finances[1]

Et quand les comptes ne sont pas protégés, cela peut s'additionner.

531 000 000 $

ont été perdus à cause d'arnaques financières en 2022[2]

Diminuez le risque d'arnaques financières grâce à ces conseils :

Sécurisez votre profil bancaire en ligne

Utilisez un mot de passe robuste

Les mots de passe robustes se composent d'au moins 12 caractères, incluant des lettres majuscules et minuscules, des chiffres et des symboles.

79 % de la population canadienne utilise des mots de passe complexes comprenant des lettres, des chiffres et des symboles[1]

Activez l'authentification multifactorielle

L'authentification multifactorielle ajoute une couche de sécurité supplémentaire, comme un code de vérification par message texte, pour garder les utilisateurs non autorisés hors de votre compte.

69 % de la population canadienne utilise l'authentification multifactorielle[1]

Utilisez un réseau sécurisé

Utilisez seulement un réseau Wi-Fi sécurisé ou vos données cellulaires pour accéder à vos informations bancaires, jamais un réseau Wi-Fi public.

Si vous avez à vous connecter à un réseau Wi-Fi public, utilisez toujours un réseau privé virtuel (RPV) pour garder vos informations sécurisées!

88 % de la population canadienne a pris des précautions pour protéger ses comptes en ligne, appareils et réseaux[1]

Restez en sécurité tout en naviguant

26 % de la population canadienne a été victime de virus informatiques, de malciels ou de logiciels espions[1]

Accéder à vos comptes

- Ne vous connectez pas à des comptes confidentiels sur un réseau Wi-Fi public
- Utilisez un RPV si vous utilisez un réseau externe
- Ne cliquez jamais sur un lien pour accéder à votre compte.
- Désactivez la sauvegarde automatique et les fonctionnalités « se souvenir de moi » quand vous entrez des renseignements sur votre compte

Magasiner en ligne

- Achetez seulement sur des sites vérifiés que vous connaissez bien
- Apprenez à repérer les signes de mystification
- Vérifiez toujours que le site est chiffré en vérifiant que son URL commence par https et que l'icône d'un cadenas verrouillé apparaît

Effectuer des virements d'argent

- Acceptez seulement les virements électroniques provenant de personnes que vous connaissez
- Ninclusez jamais de renseignements personnels dans vos mots de passe de virement électronique
- Mainvoyez pas de mots de passe de virement électronique par le biais de la notification de virement, du courriel ou de la messagerie texte

Soyez à l'affût

Hameçonnage

Messages déguisés en source légitime pour vous inciter à fournir des informations personnelles ou à cliquer sur un lien malveillant

Rançongiciel

Malciel qui, quand il est téléchargé, verrouille l'accès à vos fichiers jusqu'à ce que vous payiez une rançon

Sites usurpés

Sites Web susceptibles de ressembler à des détaillants de bonne réputation, souvent avec un design et une URL similaires

OBTENEZ PLUS DE CONSEILS POUR PROTÉGER VOS DONNÉES PERSONNELLES ET FINANCIÈRES À

PENSEZCYBERSECURITE.CA

Centre de la sécurité des télécommunications | Communications Security Establishment

Canada

Sources :

1. Sondage de suivi sur la connaissance de la campagne Pensez cybersécurité, ERDS, 2022
2. Centre antifraude du Canada (CAFC), 2022
3. Sondage de suivi sur la connaissance de la campagne Pensez cybersécurité, ERDS, 2020

Numéro de catalogue : D90-100/2023F-PDF | ISSN : 978-0-660-48651-2