La cybersécurité bancaire

Comment protéger votre argent

Ouvrir un premier compte bancaire et être responsable de son propre argent est une étape excitante de grandir. Mais comme beaucoup de choses de la vie adulte, il y a des responsabilités et des risques supplémentaires. Si vous consultez vos données bancaires en ligne ou par le biais d'une application, vous devez prendre des mesures simples pour protéger votre argent des cybercriminels.

Les enfants et les ados travaillent fort pour gagner de l'argent.

Qu'il s'agisse de l'argent que vous avez reçu à votre anniversaire ou gagné grâce à votre emploi à temps partiel, vous travaillez fort pour économiser vos sous.

Mais

Si vous n'êtes pas en sécurité

en ligne,

votre argent

n'est l'est peut-être pas non plus.

Effectuez vos opérations bancaires en ligne en toute sécurité grâce à ces conseils :

Vous ouvrez votre premier compte bancaire en ligne?

Avec l'aide d'un parent ou d'un tuteur, suivez ces étapes de cybersécurité lorsque vous ouvrez un ou des comptes 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.

Activez l'authentification multifactorielle

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

Utilisez un réseau sécurisé

N'utilisez pas un réseau Wi-Fi public pour vous connecter à votre compte en banque.Utilisez uniquement **un réseau Wi-Fi sécurisé** (pas un réseau gratuit ou dans un centre commercial ou un restaurant) ou utilisez des données cellulaires sur un téléphone de confiance.

Restez en sécurité en ligne

Lorsque vous consultez votre compte bancaire :

- n'utilisez pas le réseau Wi-Fi public pour vous connecter à des comptes contenant des informations bancaires – accédez à ces comptes par le biais d'un réseau Wi-Fi sécurisé ou avec les données cellulaires de votre propre téléphone ou celui d'une personne de confiance
- ne cliquez jamais sur un lien pour accéder à votre compte – accédez-y par le biais de l'application ou du site Web officiel
- désactivez la sauvegarde automatique et les fonctionnalités « se souvenir de moi » lorsque vous entrez des renseignements sur votre compte

Lorsque vous magasinez en ligne, par le biais d'une application ou d'un jeu :

- achetez seulement par le biais des applications et de sites Web vérifiés que vous connaissez bien
- apprenez à repérer les signes de mystification
- vérifiez toujours si le site Web est chiffré en vérifiant que son URL commence par https et que l'icône d'un cadenas verrouillé apparaît

Lorsque vous envoyez ou recevez des virements électroniques :

- acceptez seulement les virements électroniques provenant de personnes que vous connaissez
- n'incluez jamais de renseignements personnels dans vos mots de passe de virement électronique
- n'envoyez pas de mots de passe de virement électronique par le biais d'un message texte, d'un courriel ou d'une notification de virement

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, lorsqu'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

PENSEZCYBERSECURITE.CA

Centre de la sécurité des télécommunications
Communications Security Establishment
Canada