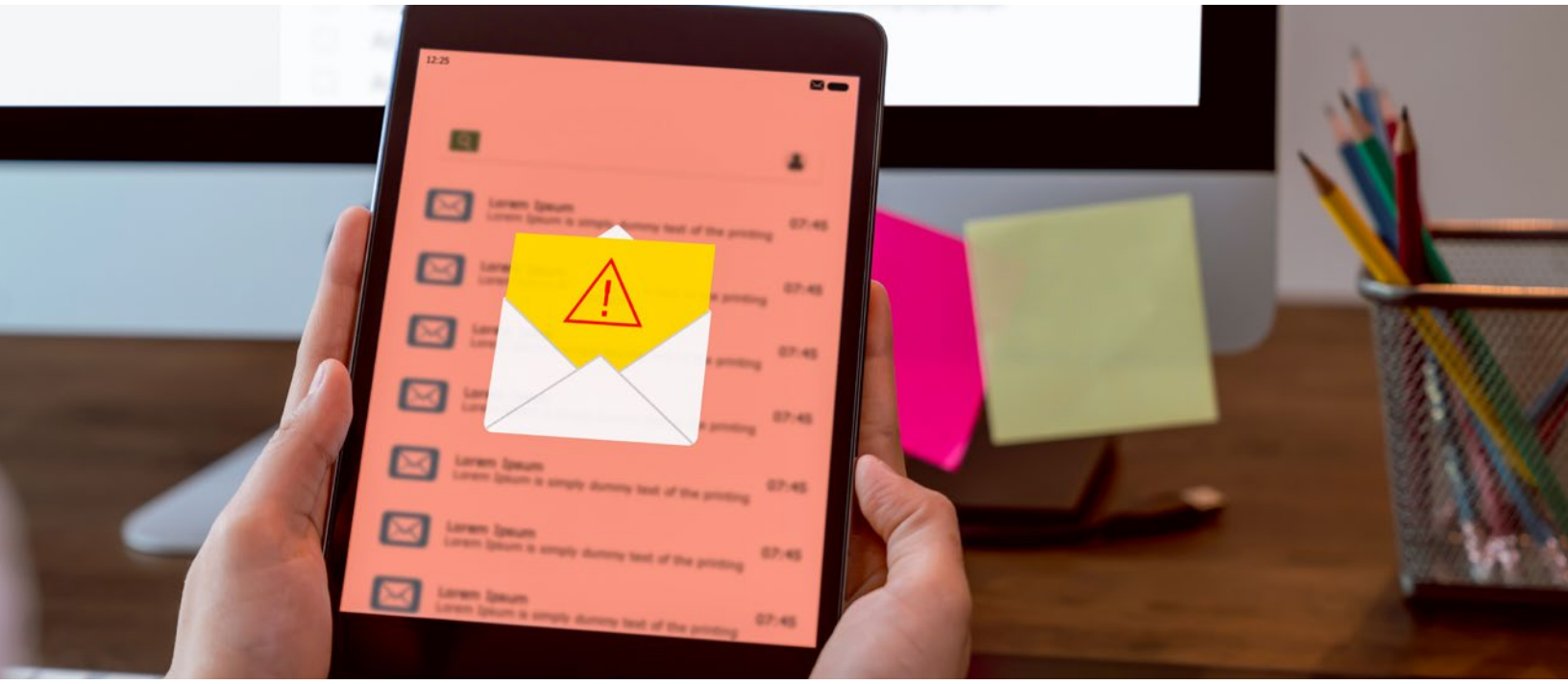
AJOUTER AU PANIER : VACCIN CONTRE LA FRAUDE



Alors que la pandémie se poursuit, les criminels exploitent le climat de peur et d'incertitude pour créer de nouvelles arnaques. Ils ont tendance à exploiter ceux qui ont désespérément besoin d'un soutien financier ou d'aide en matière de santé. Il est important d'apprendre comment vous protéger, vous et vos proches, contre la fraude. Jetons un coup d'œil à quelques arnaques courantes.

Cliquez ici pour acheter un vaccin contre la COVID-19

Il n'est pas étonnant que des arnaques liées aux vaccins contre la COVID-19 soient apparues[1]. Certaines sources en ligne et certains distributeurs non autorisés affirment avoir des vaccins et des trousses de test à vendre. N'oubliez pas que la seule façon d'avoir accès à des vaccins et à des tests légitimes est par l'intermédiaire de cliniques organisées par les autorités de santé publique de votre région en collaboration avec le gouvernement fédéral et les gouvernements provinciaux et territoriaux du Canada. Votre médecin de famille ou les professionnels de la santé de votre région sont d'excellentes ressources si vous avez des questions ou des préoccupations. Vous trouverez également d'autres ressources sur le site Web officiel du gouvernement du Canada.

Conseils :

- Ignorez les messages textes et les courriels offrant une aide financière ou une assistance et une indemnisation gouvernementales.
- Raccrochez lorsque vous recevez des appels automatisés (avec un message enregistré plutôt qu'une personne réelle) et n'appuyez pas sur les chiffres de votre clavier; vous pourriez recevoir davantage d'appels par la suite.
- N'oubliez pas que les fraudeurs utilisent des appels automatisés illégaux pour présenter de faux traitements contre la COVID-19 ou des stratagèmes qui promettent un revenu élevé en travaillant à domicile[2].

Faire la distinction entre les vrais et les faux rabais en ligne

Nous utilisons de plus en plus Internet pour magasiner, ce qui n'est pas étonnant. Toutefois, la situation a entraîné une hausse des arnaques liées aux achats en ligne[3]. En voici une répandue : les fraudeurs annoncent des rabais importants sur des produits en forte demande pour inciter les consommateurs à acheter auprès d'eux.

Conseils :

- Magasinez auprès de commerçants connus et vérifiez les offres avant d'effectuer une commande. Si c'est trop beau pour être vrai, c'est sans doute le cas!
- Surveillez les signes suivants pour confirmer qu'un site Web est sécurisé et chiffre vos données :
  1. Une icône de cadenas se trouve dans le haut de la fenêtre de votre navigateur
  2. « HTTPS » s'affiche dans la barre d'adresse
- Usez de prudence lorsque vous ouvrez des pièces jointes dans des courriels d'expéditeurs inconnus, car elles peuvent contenir des logiciels malveillants.
- Si vous repérez des mots mal orthographiés ou des erreurs grammaticales dans un courriel d'aspect officiel, il est probable qu'il provienne d'une source suspecte.

Garder les renseignements sur votre carte hors de portée

Saviez-vous que les fraudeurs peuvent effectuer des opérations non autorisées en ligne sans avoir accès à votre carte? Si vous ne protégez pas vos renseignements de paiement, il pourrait être possible d'obtenir par hameçonnage vos renseignements confidentiels, comme le nom du titulaire de carte, l'adresse de facturation, le numéro de compte et le code de sécurité à trois chiffres.

Conseils :

- Méfiez-vous des courriels, des messages textes, des appels téléphoniques ou du courrier non sollicités vous demandant des renseignements personnels, y compris des NIP, des mots de passe et des numéros de compte.
- Inscrivez-vous pour recevoir des alertes à la fraude en temps réel en cas d'opérations suspectes par carte de débit ou de crédit, et vérifiez régulièrement vos relevés bancaires afin de repérer toute activité inconnue.
- Vérifiez vos rapports d'évaluation du crédit périodiquement et avisez l'agence d'évaluation du crédit de toute irrégularité; déchiquetez les documents personnels et financiers avant de les jeter à la poubelle.

Profiter des caractéristiques de sécurité des virements électroniques

Lorsque vous envoyez des fonds par virement électronique au moyen d'une adresse de courriel ou d'un numéro de téléphone, les fraudeurs peuvent intercepter l'opération en ligne et détourner l'argent vers un autre compte bancaire. Pour ce faire, ils accèdent au compte de courriel du destinataire et devinent ou obtiennent la réponse à la question de sécurité.

Conseils :

- Inscrivez-vous au dépôt automatique de fonds par Virement Interac afin que les fonds soient déposés automatiquement et pour éviter d'avoir à répondre à une question de sécurité.
- Lorsque vous envoyez des fonds, créez des questions de sécurité dont la réponse est unique et difficile à devnier, et auxquelles seuls vous et votre destinataire savez répondre. Communiquez la réponse au destinataire par l'intermédiaire d'un moyen de communication sécurisé, comme un appel téléphonique.
- Ne réutilisez pas la même réponse pour plusieurs destinataires.

Travaillons ensemble pour vous aider à protéger vos renseignements

La Banque CIBC offre des alertes de prévention de la fraude pour vous aider à gérer et à protéger votre compte. Après votre inscription, vous recevrez des alertes en temps réel sur les opérations suspectes par carte de débit et de crédit. Vous pouvez aussi vérifier votre cote de crédit instantanément et gratuitement au moyen de l'application Services bancaires mobiles CIBC, sans aucune incidence sur votre cote. Plus tôt vous serez en mesure de repérer des activités inhabituelles, plus vous serez en mesure d'éviter des préjudices financiers.

Visitez la nouvelle page Confidentialité et sécurité de la Banque CIBC et lisez Le petit livre noir de la fraude pour en savoir davantage. N'oubliez pas que nous avons tous un rôle à jouer pour prévenir la fraude.

[1] https://antifraudcentre-centreantifraude.ca/features-vedette/2020/covid-19-fra.htm
[2] https://www.ftc.gov/coronavirus/scams-consumer-advice
[3] https://www.bbb.org/article/news-releases/23276-bbb-research-shows-spike-in-online-purchase-scams-since-covid-started

736 | 03/2021