Abus financiers numériques et ressources sur les fraudes par hameçonnage

On parle de fraude par hameçonnage lorsque des criminels utilisent des tactiques trompeuses pour inciter des personnes à révéler des informations personnelles ou financières ou à cliquer sur des liens malveillants. Les fraudes sont souvent reçues par SMS, par courriel ou par téléphone.

Les tactiques les plus courantes comprennent:

- Envoi d'un courriel en se faisant passer pour une personne ou un site web.
- Dire à une personne qu'elle doit envoyer de l'argent ou fournir des informations financières immédiatement sinon un de ses proches sera blessé, qu'elle risque de perdre tout son argent ou que son compte sera fermé.
- Proposer des remboursements ou de l'argent à vous verser en cryptomonnaie.
- Demande apparemment inoffensive de cliquer sur des liens, de numériser des codes QR, de télécharger des pièces jointes ou de remplir des formulaires en ligne.

Les messages frauduleux semblent souvent provenir d'institutions légitimes, telles que des banques, des services d'abonnement, des entreprises ou des agences gouvernementales, et incitent généralement les destinataires à prendre des mesures immédiates sous de faux prétextes, comme la mise à jour d'informations de compte ou la demande de remboursement. Les variantes des fraudes par hameçonnage peuvent comporter un minimum de texte et se présenter sous la forme de reçus, de notifications de livraison ou d'avis urgents; elles sont conçues pour infecter un appareil avec des logiciels malveillants ou des virus lorsque l'on clique sur des liens ou des pièces jointes.

Il peut être difficile d'identifier ce type d'escroquerie. Voici quelques ressources qui peuvent être utiles aux survivantes d'autres formes d'abus financiers numériques.

Fraudes locatives

En raison du manque de logements abordables, les escroqueries aux fausses locations sont fréquentes. Consultez la page web de la GRC sur les fraudes locatives pour obtenir de plus amples renseignements et des conseils pour vous aider.

Fraudes par courriel

Nous recevons tous des courriels affirmant que nous avons hérité d'une somme d'argent, que quelqu'un a tenté d'accéder à nos comptes ou qu'un tiers possède des images intimes de nous. Voici quelques ressources permettant d'identifier les fraudes et de savoir ce qu'il faut faire dans un tel cas:

- Comment repérer les fraudes et les escroqueries par courriel
- What to do if a scammer has your email address - 8 tips
- Ne mordez pas à l'hameçon: Reconnaitre et prévenir les attaques par hameçonnage

Fraudes par SMS

Les fraudes par hameçonnage par le biais de SMS et d'applis comme WhatsApp commencent généralement par une tentative d'engager la conversation. Il se peut que vous receviez des messages d'un numéro inconnu disant:

- « Est-ce que c'est le bon moment? »
- « Le paiement de votre facture n'a pas été effectué. »
- « Nous n'avons pas pu livrer votre colis. »
- « L'ARC a besoin de plus d'informations. »

Les escrocs peuvent également se faire passer pour des représentants d'une entreprise ou d'une administration et vous demander d'assurer le suivi d'un colis ou d'un document.

Les ressources suivantes expliquent comment identifier les fraudes et ce qu'il faut faire dans un tel cas.

- What to do if you receive a spam text
- How to stop spam tests: An easy 4-step guide
- Mettre fin aux pourriels sur appareils mobiles

Fraudes par appel téléphonique (Robo Call)

Les fraudes par appel téléphonique tentent de vous faire croire que vous avez un problème urgent dont il faut discuter afin de vous garder au téléphone. Les fraudes courantes par appel téléphonique consistent souvent à raconter des histoires d'enlèvement et à demander des informations bancaires.

- Comment vous protéger contre les arnaqueurs
- Protégez-vous contre les arnaques de télémarketing et les fraudes liées à la vente par téléphone
- Liste nationale de numéros de télécommunication exclus du Canada
- Blocage et filtrage des appels indésirables

Fraudeurs se faisant passer pour le gouvernement canadien

Voici un lien vers un document du gouvernement du Canada sur la manière de reconnaitre les fraudes de la part des services et sur ce qu'il faut faire si l'on en reçoit.

- Arnaques et fraudes: gouvernement du Canada

Pour plus de conseils en matière de sécurité technologique, consultez nos ressources:

- Que faire si vous êtes victime d'une fraude?
- 6 conseils pour sécuriser vos informations financières en ligne

La violence fondée sur le genre facilitée par la technologie (VFGFT) fait partie d'un continuum de violence qui peut se produire à la fois en ligne et en personne. Si vous ou une personne de votre entourage êtes victime de VFGFT, vous n'êtes pas seule. Vous pouvez consulter https://hébergementfemmes.ca/ pour trouver une MH près de chez vous afin de discuter de vos options et élaborer un plan de sécurité. Il n'est pas nécessaire de résider dans une MH pour avoir accès à des services et à un soutien gratuits et confidentiels. Pour plus d'informations sur les abus financiers numériques, consultez notre trousse.

Ce projet a été financé par le Groupe Banque TD, par l'entremise de sa plateforme de citoyenneté d'entreprise, La promesse TD Prêts à agir.