Arnaques et hameçonnage

Ne soit pas victime de fraude!

Une cyberarnaque est une activité criminelle en ligne conçue pour soutirer des gens de l'argent ou des informations personnelles.

Les types de fraudes les plus communs

L'hameçonnage (aussi connu comme du «phishing» ou «smishing») est une technique visant à récolter (ou «pêcher») des noms d'utilisatrice ou d'utilisateur, des mots de passe et d'autres renseignements confidentiels auprès de plusieurs (ou dans une «mer») d'utilisa-trices et utilisateurs – par courriel ou texto. Ces courriels et textos frauduleux semblent provenir d'une personne ou d'une entreprise connue ou fiable.

- Ces messages incitent la destinatrice ou le destinataire à cliquer sur un lien, ouvrir un fichier, composer un numéro ou correspondre à une adresse courriel.
- On piège ensuite la victime afin qu'elle fournisse ses renseignements personnels et données d'authentification.

Les fausses applications sont des applications créées par des cybercriminels pour causer du tort aux utilisatrices et utilisateurs et à leurs appareils. Elles sont conçues pour ressembler à de vraies applications, mais contrairement, elles suivent tes activités, installent un logiciel malveillant ou soutirent tes informations.

Les sites web qui vendent de faux produits. Ces sites offrent des produits en forte demande à rabais que la personne qui achète ne recevra jamais.

Le détournement de formulaire est le piratage d'un site web commercial légitime qui redirige les clientes et clients vers une fausse page de paiement. De cette page le fraudeur peut soutirer les renseignements personnels et les numéros de carte de crédit.

Comment éviter la fraude en ligne:

- Ne pas ouvrir les pièces jointes, cliquer sur les liens ou répondre à un message suspect – pose-toi des questions, consulte des personnes en qui tu as confiance ou communique avec l'expéditrice ou l'expéditeur en utilisant une autre méthode de communication.
- Éviter les applications suspectes et ne pas accorder la permission à une application de faire quelque chose qu'elle n'est pas censée faire.
- Toujours utiliser des sites sécurisés **(doit contenir le «s» dans https://)** lorsque tu magasines ou que tu dois te connecter à un compte en ligne.
- Acheter des produits de commerces connus seulement.
- Ne pas publier d'informations personnelles sur les médias sociaux.

Si tu penses être victime d'une arnaque:

- Cesse toute communication avec la personne frauduleuse.
- Demande de l'aide à une ou un adulte de confiance.
- Signale la fraude à la police.

CYBER HÉROS RÉUNIS

/{MOI} NUMÉRIQUE

Financé par :

Ontario

Pour plus d'informations : www.ecno.org/cyber-sensibilisation