Stratagèmes en ligne

Dans cette section...

- Faux sites de cybercommerce
- Hameçonnage
- Ventes aux enchères frauduleuses
- Lettres frauduleuses
- Logiciel malveillant

De nos jours, il est possible de faire des achats, des opérations bancaires ou une recherche d'emploi par Internet, à partir de chez soi. Le Web permet aussi, entre autres choses, de faire des recherches, de consulter les petites annonces, de communiquer et de participer à des ventes aux enchères ou à des jeux. Cependant, les progrès technologiques donnent lieu à des crimes d'un genre nouveau. Voici des informations qui vous aideront à les repérer.

Faux sites de cybercommerce

Ces sites sur lesquels on essaie de vous vendre quelque chose présentent des offres trop belles pour être vraies. En fait, ils sont créés dans le but de recueillir vos renseignements personnels; ils resteront accessibles quelques semaines, puis ils disparaîtront.

Hameçonnage

L'hameçonnage est un terme général utilisé pour décrire la production, par des criminels, de courriels, de messages texte et de sites Web qui sont conçus pour avoir l'air de provenir d'entreprises, d'institutions financières et d'organismes gouvernementaux légitimes et bien connus, mais qui visent à obtenir frauduleusement des renseignements personnels, financiers ou de nature délicate. On parle aussi d'« usurpation de marque » ou de « détournement de domaine ».

Ventes aux enchères frauduleuses

Une vente aux enchères en ligne consiste à utiliser Internet pour mettre des articles en vente au plus offrant. Elle devient frauduleuse lorsque les informations sur un article sont trompeuses ou qu'il y a défaut de livraison ou de paiement des biens ou des services achetés.

Lettres frauduleuses provenant du nigeria ou d'afrique occidentale

C'est une escroquerie connue de bien des gens partout dans le monde. Elle est maintenant perpétrée par courriel et peut prendre différentes formes. En général, cela commence par une lettre émanant d'un représentant officiel ou d'un agent du gouvernement du Nigeria qui dit être entré en possession de millions de dollars et chercher à faire sortir cette somme de son pays. Il affirme ne pas pouvoir utiliser son propre compte en banque et vous demande d'utiliser le vôtre, en échange de quoi il vous versera de 10 à 35 % de l'argent. Une fois qu'il est en possession de votre numéro de compte, le fraudeur puise dans vos fonds.

Il existe de nombreuses variantes de cette escroquerie. On peut vous faire miroiter un rendement extraordinaire si vous envoyez de l'argent au compte à l'étranger que l'on vous indique. Une fois votre premier placement fait, on vous demande d'envoyer toujours plus d'argent, pour éviter de perdre ce que vous avez déjà investi. Tous les scénarios ont une chose en commun : vous ne reverrez jamais l'argent que vous envoyez. De nos jours, ce type d'escroquerie ne se limite plus à des lettres ou à des courriels venant du Nigeria, mais on retrouve toujours les mêmes éléments. Soit l'escroc demande que vous envoyiez de l'argent à l'avance, soit il accède lui-même à votre compte en banque.

Logiciel malveillant

Également connu sous le nom de maliciel, il se présente sous différentes formes, comme des virus, des vers informatiques, des programmes de cheval de Troie, des logiciels espions ou des logiciels publicitaires. Un ordinateur peut être infecté lorsque son utilisateur ouvre un courriel, accède à un site Web, utilise un support contaminé ou télécharge des programmes infectés, par exemple des jeux.

Conseils de prévention

- Prenez le temps de faire des recherches lorsque vous souhaitez acheter quelque chose en ligne.
- Laissez passer une bonne affaire si vous ne pouvez pas l'authentifier.
- Effacez immédiatement les messages électroniques.
- Méfiez-vous de tout ce qui est inhabituel et soyez à l'affût de toute anomalie dans l'adresse ou les pages d'un site Web.
- Souvenez-vous qu'au Canada, vous ne devez payer ni taxes ni frais pour recevoir un prix légitime.
- Lorsque vous participez à des enchères en direct, lisez le guide d'utilisateur et les conseils de sécurité qui peuvent vous être donnés en ligne pour éviter d'être victime d'une fraude.
- Protégez votre ordinateur en gardant votre système d'exploitation et vos progiciels à jour et munissez-vous de logiciels de protection : antivirus, pare-feu, antiespiogiciel et antipubliciel.