



FRAUDES SUR INTERNET

De quoi s'agit-il?

Qu'il s'agisse de gains financiers, de produit ou service miracle ou même de sentiment amoureux, les différentes approches autrefois utilisées par les fraudeurs sont toujours d'actualité et se sont adaptées au monde virtuel. Les mises en scène peuvent provenir de n'importe où dans le monde, par courriel, des sites Web et, souvent des deux à la fois.

Comment font-ils?

Les fraudeurs misent sur la méconnaissance et la vulnérabilité des gens et ont recours à une panoplie de moyens afin de mettre la main sur vos données personnelles. Ils peuvent :

- vous inciter à installer une application ou télécharger un logiciel malveillant qui peuvent endommager votre ordinateur de même que voler vos renseignements personnels ou financiers;
- utiliser la connexion Bluetooth dont sont équipés la plupart des appareils mobiles et ordinateurs portables pour s'introduire dans ceux-ci;
- vous envoyer des messages non sollicités par courriel ou messagerie instantanée dans le but de vous soutirer des informations confidentielles;

- créer des sites Web imitant des sites légitimes tels que des sites bancaires, des sites commerciaux et même des sites de réseaux sociaux afin de recueillir vos renseignements personnels;
- vous annoncer par courriel que vous avez gagné un prix ou que vous avez un héritage inattendu mais que, pour avoir accès à ce prix ou cette somme, vous devez d'abord payer des frais quelconques;
- faire appel à votre compassion et à vos sentiments amoureux pour obtenir de l'argent sous divers prétextes (frais de voyage, droits d'immigration, enfant malade, besoin de nourriture). Ils peuvent également tenter d'obtenir des photos intimes pour vous extorquer de l'argent par la suite.

Comment se protéger

Faites preuve de prudence et de scepticisme.

- Utilisez des mots de passe difficiles à percer composés de lettres majuscules, minuscules, de chiffres et de caractères spéciaux et dont la longueur devrait être au minimum de 8 caractères. N'utilisez pas le nom de votre animal de compagnie ou la date de naissance de votre enfant : ceux-ci peuvent être facilement déchiffrés.
- Protégez votre ordinateur à l'aide d'un pare-feu, d'un logiciel anti-virus et d'un programme anti-espions, et assurez-vous de les maintenir à jour.
- Soyez prudent lorsque vous utilisez les médias sociaux : vérifiez les paramètres de confidentialité et de sécurité des sites que vous fréquentez et soyez prudent avec l'information que vous y affichez.
- Méfiez-vous des logiciels ou applications gratuits, prenez toujours connaissance du contenu des licences d'exploitation et de la politique de confidentialité avant de les installer afin d'éviter de donner un accès pratiquement illimité à vos informations personnelles.

- Protégez vos données, chiffrez vos documents de nature délicate, faites des sauvegardes régulières de toutes vos données importantes. Prenez soin de verrouiller votre ordinateur et vos appareils mobiles lorsque vous ne les utilisez pas.
- Protégez votre réseau sans fil (Wi-Fi) à la maison car il peut être vulnérable aux intrusions. Les réseaux Wi-Fi publics sont également vulnérables. Évitez de faire des transactions financières ou des achats sur ces réseaux.
- Recherchez le symbole du cadenas sur le site Web ou le préfixe « https:// » au début de l'adresse du site (le « s » signifie « sécurisé ») pour vous assurer que le site est chiffré ou encodé lorsque vous devez transférer des informations personnelles ou financières, ou des mots de passe.
- Interrogez-vous toujours avant de cliquer sur un lien ou un fichier d'origine inconnue. Ne répondez jamais à des courriels où l'on vous demande de vérifier votre information ou encore de confirmer votre nom d'utilisateur ou votre mot de passe.

Si vous découvrez du contenu douteux sur Internet, si vous soupçonnez un délit informatique ou une fraude commerciale, si vous croyez avoir été victime de ce genre de fraude, portez plainte auprès du service de police qui dessert votre municipalité (Sûreté du Québec ou service de police local) et signalez le cas au Centre antifraude du Canada (1-888-495-8501).