Fraudes

Ce document a été préparé de bonne foi et est présenté comme guide général. Beaucoup d'efforts ont été déployés afin de s'assurer que les informations qui s'y trouvent sont exactes. Même si des efforts sont faits pour maintenir le document à jour, des modifications ont pu être apportées aux informations utilisées en vue de sa préparation. Par conséquent, l'auteur n'assume aucune responsabilité pour les erreurs qui pourraient s'y trouver ou les omissions. Il est donc conseillé d'effectuer les vérifications nécessaires pour s'assurer que l'information fournie est à jour.

Pourquoi certaines personnes tentent-elles de frauder les personnes âgées ?

Plusieurs personnes âgées sont particulièrement vulnérables à la fraude téléphonique parce qu'elles ont tendance à faire davantage confiance aux gens et sont moins susceptibles de raccrocher si la personne qui les appelle paraît sympathique.

Les personnes âgées sont ciblées pour maintes raisons, par exemple : l'isolement, le manque d'appui familial, l'âge, la vulnérabilité, les raisons liées à la santé (comme l'Alzheimer).

Quelles sont les tentatives de fraude les plus courantes ?

1. La fraude par cartes de paiement se produit lorsque quelqu'un utilise vos cartes de crédit ou de débit dans le but d'en faire une copie ou de les utiliser pour obtenir frauduleusement un bien, un service ou de l'argent.

   Soyez-donc vigilant et avisez les autorités concernées dès que vous vous apercevez que vous avez perdu vos cartes.

2. L'hameçonnage est un envoi massif de courriels par des fraudeurs qui utilisent une fausse identité (par exemple une institution financière) dans le but de recueillir des renseignements personnels et bancaires pour ensuite les utiliser afin de détourner des fonds.

   Les renseignements demandés peuvent comprendre vos numéros de compte, mots de passe, numéros de carte de crédit ou numéro d'assurance sociale.

   Sachez que les institutions financières n'envoient jamais de courriel pour faire la mise à jour de vos renseignements personnels. Si vous en recevez un, ne cliquez pas sur le lien contenu dans le courriel, ignorez-le ou contactez votre institution financière.

3. Le vol d'identité est l'utilisation non autorisée de vos renseignements personnels en vue de commettre une fraude ou un autre type de crime. Soyez vigilant et protégez vos renseignements personnels.

4. La vente itinérante est aussi un moyen utilisé par certains fraudeurs. Par exemple, une personne se présente chez vous pour faire des travaux d'entretien de votre maison à des coûts peu élevés. Si vous acceptez, la personne vous dit qu'elle reviendra dans une semaine, mais que vous devez la payer maintenant. Finalement, vous ne la revoyez jamais.

5. La fraude appelée nigériane est une forme de sollicitation par courriel promettant une importante somme d'argent en échange d'une aide financière.

6. La fraude par chèque. On vous demande de rembourser un paiement en trop. Par exemple, vous vendez votre vieille voiture pour 1000 $, mais l'acheteur vous envoie un chèque de 2000 $. Ce dernier vous dit d'encaisser le chèque et de lui retourner la différence. Toutefois, le chèque est un faux ou est sans provisions. Vous avez donc déboursé 1000 $, mais n'avez rien reçu pour votre voiture.

7. L'emprunt privé. Avant de prêter de l'argent à un ami, à une connaissance ou même à un membre de votre famille, sachez que cela comporte habituellement un risque que les paiements d'intérêt ne seront pas faits et même que le montant prêté ne vous sera pas remis.

8. Frais à payer pour bénéficier d'un prix. Par exemple, ces appels qui nous disent que nous avons gagné une croisière et qui nous demandent de payer certains frais connexes comme la taxe, etc.

Quels sont les moyens souvent utilisés par les fraudeurs ?

Les appels téléphoniques et les courriels sont souvent utilisés par les fraudeurs.

Les courriels non sollicités et les messages incitant leurs destinataires à «agir maintenant» et à «vérifier leur nom d'utilisateur et leur mot de passe» sont des tactiques régulièrement utilisées par les fraudeurs. Ceux-ci souhaitent ainsi mettre de la pression sur les destinataires des messages et les inciter à répondre sans prendre le temps de bien réfléchir.

Méfiez-vous d'appels téléphoniques ou des courriels provenant d'un organisme familier comme une banque et qui vous demande des renseignements comme votre nom d'utilisateur, votre mot de passe, votre numéro de carte de crédit ou votre date de naissance. Il s'agit très probablement d'une tentative de fraude. Les banques et la majorité des entreprises ne communiquent pas avec leurs clients par courriel et ne demandent pas ce genre de renseignements par téléphone.

Souvent, les courriels malveillants font référence à des problèmes. Par exemple, on indiquera que «votre compte a été suspendu pour des raisons de sécurité» ou que «vous devez réactiver votre compte bancaire en ligne». Cette technique est utilisée par les fraudeurs pour vous inciter à donner vos informations personnelles spontanément, sous le coup de l'émotion.

Une bonne règle à appliquer est de ne pas donner suite à tout ce qui semble bizarre.

Les personnes âgées en ligne

Comme pour tous les utilisateurs d'Internet, il est important que les personnes âgées demeurent informées des mesures de sécurité à prendre pour utiliser des ordinateurs et naviguer sur Internet.

Voici les principales précautions à prendre :

- Tenez à jour vos logiciels, c'est-à-dire le logiciel de sécurité et tout autre programme installé dans votre ordinateur. La plupart des logiciels de sécurité fournissent des avis de mise à jour ou, mieux encore, procèdent automatiquement à la mise à jour ou à l'installation de la plus récente version dans votre système.

- Si un message vous semble trop beau pour être vrai, ou bizarre, ignorez-le.

- Ne partagez pas vos mots de passe sauf avec des personnes à qui vous faites vraiment confiance.

- N'agissez pas trop vite. En cas de doute, parlez-en avec un membre de votre famille ou avec une personne en qui vous avez confiance.

Que pouvez-vous faire d'autre si vous croyez être victime d'une arnaque ou d'une fraude ?

Si vous croyez être victime ou faire la cible d'une arnaque ou d'une fraude, vous pouvez aider à mettre fin à l'arnaque ou à la fraude en la rapportant.

- En premier lieu, vous pouvez signaler le problème à la police.

- Vous pouvez aussi communiquer avec le *Centre antifraude du Canada* en composant le 1-888-495-8501 (sans frais). Ses bureaux sont normalement ouverts du lundi au vendredi de 9 h à 17 h (heure normale de l'Est).

Document préparé par André Lépine le 15 février 2016