HAMEÇONNAGE : NE VOUS LAISSEZ PAS PRENDRE AU PIÈGE!

Les policiers du Service de police de la Ville de Montréal (SPVM) souhaitent sensibiliser les personnes aînées sur un stratagème frauduleux utilisé par les criminels, appelé hameçonnage.

BUT ET MÉTHODES UTILISÉES

Le but de l'hameçonnage est de subtiliser vos renseignements personnels et financiers afin de vous frauder ou de voler votre identité. Les méthodes utilisées **peuvent prendre la forme d'un appel téléphonique, d'un courriel, d'un texto ou encore d'un faux site Internet.**

Le fraudeur procède de la façon suivante :

- Il prend l'apparence d'une source crédible, par exemple, un représentant d'une agence gouvernementale, d'une institution financière, d'un fournisseur de services (téléphone, télévision, électricité, etc.), ou même d'une entreprise.
- Il envoie un message par courriel ou texto dans lequel il demande à la personne de cliquer sur un hyperlien dans le but, par exemple, de mettre à jour ses informations personnelles, confirmer un achat, éviter la fermeture de son compte, recevoir un héritage ou un gain à une loterie, etc.
- Il incite la personne à le faire rapidement et fait pression sur elle pour qu'elle agisse sans réfléchir, dans un court délai, en stipulant par exemple qu'il s'agit d'un dernier rappel, que son compte sera fermé, qu'elle sera poursuivie, perdra un remboursement, etc.

Le SPVM souhaite rappeler certains conseils de prévention aux personnes aînées ou à leur proche, pour assurer leur protection et les recours possibles en cas de fraude.

CONSEILS DE PRÉVENTION

- Soyez à l'affût de ces stratagèmes frauduleux en consultant la page *Fraudes par index A-Z*, disponible sur le site Internet du Centre antifraude du Canada, sur les sujets *Hameçonnage* et *Vol d'identité et fraude à l'identité*.
- **Ignorez et supprimez les messages** (courriels, textos ou autres) **non sollicités**, **ou provenant de personnes inconnues,** et surtout, **n'ouvrez jamais de pièce jointe ou ne cliquez jamais sur un hyperlien** joint dans ces messages.
- Surveillez les indices vous permettant d'identifier un message frauduleux, soit :
  - Message impersonnel, par exemple, *Madame*, *Monsieur, Cher contribuable*, etc.;
  - Message comportant des fautes d'orthographe, de grammaire ou de syntaxe;
  - Message qui semble provenir d'une source crédible, mais dont l'adresse courriel ou les coordonnées ne sont pas les mêmes que sur le site Internet officiel de l'organisme.
- Méfiez-vous des messages qui vous demandent d'agir rapidement, ou qui semblent trop beaux pour être vrais. Prenez le temps de vérifier auprès de l'organisme concerné, au numéro de téléphone figurant sur un relevé ou son site Internet officiel. N'hésitez pas également à consulter un membre de votre famille, un proche aidant, ou votre service de police local pour valider leur authenticité.
- Rappelez-vous qu'**aucune agence gouvernementale, institution financière, fournisseur de services ou même une entreprise ne vous demandera jamais d'informations personnelles par courriel ou par texto.**

POUR OBTENIR DE L'AIDE OU SIGNALER UNE FRAUDE

En cas de fraude, communiquez avec votre institution financière et la compagnie émettrice de votre carte de crédit.

Vous pouvez également communiquer avec les deux agences nationales d'évaluation du crédit et demander qu'un avis de fraude soit inscrit à votre dossier de crédit. Pour communiquer avec Equifax Canada, composez le 1 800 465 - 7166, et pour communiquer avec TransUnion Canada, composez le 1 877 713-3393.

Vous pouvez aussi porter plainte à votre service de police local. Pour communiquer avec votre poste de quartier (PDQ), composez le **514 280 - 01XX** (XX correspondant au numéro de votre PDQ). Pour toute urgence, faites le **9-1-1**.

Pour signaler une fraude, vous pouvez communiquer avec le Centre antifraude du Canada en composant le 1 888 495 - 8501 ou directement sur leur site Internet à antifraudcentre-centreantifraude.ca.

Montréal