MARS, *MOIS DE PRÉVENTION DE LA FRAUDE*

Tout au long du mois de mars, à l'occasion du *Mois de prévention de la fraude*, la Sûreté du Québec et plusieurs partenaires des forces policières, en collaboration avec la Banque du Canada, mènent une campagne afin de sensibiliser les citoyens aux différents types de fraudes les plus courantes.

Personne n'est à l'abri de la fraude, peu importe son âge, son niveau d'éducation ou son lieu de résidence. Cependant, la plupart des fraudes peuvent être évitées en étant informé et vigilant afin de les identifier et se protéger efficacement.

LE VOL ET LA FRAUDE D'IDENTITÉ

C'est quoi ?

Le **vol d'identité** se produit lorsqu'une personne obtient, à votre insu et sans votre consentement, vos renseignements personnels à des fins criminelles. La **fraude d'identité** est l'usage frauduleux de ces renseignements pour :

- accéder à vos comptes bancaires, faire des demandes de prêt, de cartes de crédit ou d'ouverture de comptes (bancaires, client);
- vendre votre propriété à votre insu;
- obtenir un passeport ou toucher des prestations du gouvernement;
- obtenir des services médicaux.

Comment font les fraudeurs ?

- En volant votre portefeuille, votre sac à main ou votre courrier résidentiel.
- En fouillant dans vos poubelles ou bacs de recyclage pour récupérer vos factures, relevés bancaires et autres documents.
- En remplissant un formulaire de changement d'adresse pour rediriger votre courrier.
- En se faisant passer pour votre créancier, propriétaire, employeur, un agent gouvernemental ou un enquêteur.
- En envoyant des courriels non sollicités qui semblent légitimes afin de recueillir vos renseignements personnels.
- En créant des imitations de sites Web ou d'applications légitimes (p. ex., sites bancaires, d'entreprises commerciales ou de médias sociaux).
- En piratant vos appareils électroniques (ordinateur, téléphone ou tablette) ou en vous incitant à leur donner accès à ceux-ci au moyen de supercheries.
- En trafiquant des guichets automatiques et des terminaux de points de vente.
- En faisant des achats à votre insu.

Principaux renseignements personnels :

- nom complet
- date de naissance
- adresse résidentielle
- adresse électronique
- numéro de téléphone
- mots de passe
- numéro d'assurance sociale (NAS)
- signature (manuscrite ou numérique)
- numéro de passeport
- numéro de permis de conduire
- numéro d'assurance-maladie
- données de cartes de paiement

Comment se protéger ?

Transmission des informations personnelles

- Soyez vigilant, ne donnez vos renseignements personnels que lorsque cela est absolument nécessaire, à condition de connaître la personne ou l'organisation avec qui vous faites affaire et d'avoir pris vous-mêmes contact avec elle.

Paramètres de sécurité et de confidentialité

- Vérifiez vos paramètres de confidentialité et de sécurité avant de télécharger des applications, de s'enregistrer sur un site Web ou de partager des renseignements personnels sur des médias sociaux. Considérez toute information que vous affichez comme étant publique.
- Désactivez la fonction de géolocalisation automatique de votre téléphone. Bien se renseigner sur l'utilisation et les engagements de confidentialité avant d'activer un service de localisation.
- Protégez vos données. Verrouillez votre ordinateur et vos appareils mobiles lorsque vous ne les utilisez pas.
- Utilisez des sites sécurisés (débutant par « https:// ») lorsque vous devez transmettre des informations personnelles ou financières.
- Évitez de faire des transactions financières ou des achats à partir de réseaux sans fil (Wi-Fi) publics (p. ex., dans un café).
- Ne gardez jamais de photo de permis de conduire, de passeport ou de carte d'assurance-maladie dans votre cellulaire.

Antivirus et mots de passe

- Installez sur vos appareils électroniques un antivirus, un filtre anti-pourriel, un pare-feu ainsi qu'un logiciel anti-espion. Activez le filtre anti-pourriel de votre boite courriel. Ces mesures permettront de réduire votre vulnérabilité face au piratage informatique.
- Protégez votre réseau Wi-Fi à la maison avec un mot de passe complexe, composé d'un minimum de dix caractères. Évitez les mots du dictionnaire. Insérez des caractères spéciaux au milieu du mot (évitez la majuscule au début et le chiffre ou caractère spécial à la fin du mot). Évitez les caractères spéciaux en remplacement (p. ex. a = @).
- Mémorisez et modifiez-les régulièrement (incluant le mot de passe de votre routeur). N'utilisez pas le même mot de passe pour plusieurs sites. N'acceptez jamais qu'un site Internet se « souvienne de votre mot de passe ».

Numéro d'identification personnel (NIP)

- Mémorisez vos NIP afin de ne pas en conserver de trace écrite. Lorsque vous composez votre NIP, assurez-vous que personne autour de vous ne puisse le voir, incluant le commis.

Numéro d'assurance sociale (NAS)

- Ne divulguez jamais votre NAS. En vertu de la loi, seuls les organismes gouvernementaux, votre employeur (au moment de l'embauche) ou votre institution financière peuvent l'exiger.

Relevés officiels

- Vérifiez vos relevés de compte bancaire et de carte de crédit régulièrement. Contestez immédiatement tout achat qui vous est inconnu.
- Déchiquetez tout document contenant des renseignements personnels avant d'en disposer.

Logiciels et applications gratuits

- Consultez la licence d'utilisation et la politique de confidentialité des logiciels ou applications gratuits avant de les installer afin d'éviter de donner un accès pratiquement illimité à vos informations personnelles.

Courriels

- Validez l'adresse courriel de l'expéditeur dans toutes vos communications. Interrogez-vous toujours avant de cliquer sur un lien ou d'ouvrir un fichier d'origine inconnue. Supprimez les courriels dont l'expéditeur vous est inconnu. Ne confirmez ni ne validez aucune information personnelle par courriel.

Une fois par année, demandez une copie de votre dossier de crédit auprès de TransUnion ou d'Équifax et assurez-vous qu'il ne comporte aucune erreur.

POUR OBTENIR DE L'AIDE OU SIGNALER UNE FRAUDE

- Communiquez rapidement avec votre institution financière et avec la compagnie émettrice de votre carte de crédit.
- Signalez l'incident auprès de votre service de police local.
- Communiquez avec les deux agences nationales d'évaluation du crédit et demandez qu'un avis de fraude soit inscrit à votre dossier de crédit.
  Équifax Canada : 1 800 465-7166
  TransUnion Canada : 1 877 713-3393
- Signalez l'incident au Centre antifraude du Canada au 1 888 495-8501 ou au www.antifraudcentre-centreantifraude.ca

Mars, Mois de prévention de la fraude.
Un mois de prévention, douze mois de vigilance!