# MARS, *MOIS DE PRÉVENTION DE LA FRAUDE*

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

Indépendamment de l'âge, du niveau d'éducation ou du lieu de résidence d'une personne, nul n'est à l'abri d'être un jour victime d'escroquerie.

La plupart des fraudes peuvent être évitées. C'est pourquoi il est important d'être 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 et utilise, 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;
- 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.
- 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 créant des sites Web imitant des sites légitimes (p. ex., sites bancaires, d'entreprises commerciales ou de réseaux sociaux) afin de recueillir vos renseignements personnels.
- En trafiquant des guichets automatiques et des terminaux de points de vente.

**Principaux renseignements personnels :**

- nom complet
- date de naissance
- adresse
- 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 partager des renseignements personnels sur des réseaux sociaux. Considérez toute information que vous affichez comme étant publique.
- Désactivez la fonction de géolocalisation automatique de votre téléphone avant de prendre des photos et des vidéos que vous voulez partager en ligne pour empêcher les gens de découvrir où vous habitez ou travaillez.
- Protégez vos données. Verrouillez votre ordinateur et vos appareil 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.

**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 pour réduire le risque de piratage informatique.
- Protégez votre réseau Wi-Fi à la maison avec un mot de passe complexe.
- Utilisez des mots de passe difficiles à percer, composés d'un minimum de 8 caractères (le plus long possible, comportant lettres majuscules, minuscules, chiffres, caractères spéciaux ou les premières lettres de chaque mot d'une phrase). Mémorisez et modifiez-les régulièrement.

**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.

**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'exploitation 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.

- 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. Ne répondez jamais à des courriels où l'on vous demande de valider vos informations personnelles ou encore de confirmer votre nom d'utilisateur ou votre mot de passe. Supprimez les courriels dont la source vous est inconnue.

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

Si vous soupçonnez ou savez avoir été victime d'un vol ou d'une fraude d'identité, signaler l'incident auprès du service de police qui dessert votre municipalité (Sûreté du Québec ou service de police local).

Assurez-vous également de communiquer avec les deux agences nationales d'évaluation du crédit et demander qu'un avis de fraude soit inscrit à votre dossier de crédit.

- Équifax Canada : 1800 465-7166
- TransUnion Canada : 1 877 713-3393

Communiquez avec le Centre antifraude du Canada pour signaler la fraude : 1 888 495-8501 ou au www.antifraudcentre-centreantifraude.ca.

Si vous désirez signaler une fraude ou toute autre activité criminelle **de manière anonyme et confidentielle**:

- Pour la région de Montréal, communiquez avec **Info-Crime**, au 514 393-1133, ou visitez www.infocrimemontreal.ca.
- À l'extérieur de Montréal, communiquez avec **Échec au crime**, au 1 800 711-1800, ou visitez www.echecaucrime.com.

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