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 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, 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.
- Faire des achats à votre insu.

COMMENT FONT LES FRAUDEURS?

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

PRINCIPAUX RENSEIGNEMENTS PERSONNELS

- nom complet	- numéro d'assurance sociale (NAS)
- date de naissance	- signature (manuscrite ou numérique)
- adresse résidentielle	- adresse électronique
- numéro de téléphone	- numéro de passeport
- mots de passe	- 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 et à condition de connaître la personne ou l'organisation qui vous les demande et d'avoir pris vous- même contact avec elle.

Paramètres de sécurité et de confidentialité

- Vérifiez vos paramètres de confidentialité et de sécurité avant de télécharger des applications, de vous enregistrer sur un site Web ou de partager des renseignements personnels sur des médias sociaux. Considérez toute information que vous affichez comme étant publique.
- Si cela est possible, optez pour l'authentification à deux facteurs (ou facteurs multiples). Cette mesure de protection supplémentaire permet d'associer une information que vous connaissez (votre mot de passe) à une information que vous possédez (un code envoyé par SMS, un jeton, une empreinte digitale, etc.).
- Désactivez la fonction de géolocalisation automatique de votre télé- phone. Renseignez-vous bien 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 (commençant 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).
- Assurez-vous de réaliser vos transactions sur des sites légaux.
- Déconnectez-vous avant de quitter votre poste.
- Ne gardez jamais de photo de permis de conduire, de passeport ou de carte d'assurance maladie dans vos appareils mobiles à moins de verrouiller les pièces d'identité avec un mot de passe.

Antivirus et mots de passe

- Installez sur vos appareils électroniques un antivirus, un filtre antipourriel, un pare-feu ainsi qu'un logiciel anti-espion. Activez le filtre antipourriel de votre boîte courriel. Ces mesures permettront de réduire votre vulnérabilité 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-les 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 peut le voir, incluant le commis.

Numéro d'assurance sociale (NAS)

- Protégez votre numéro d'assurance sociale (NAS). Le NAS est émis par le gouvernement fédéral à des fins d'emploi, d'accès aux prestations et aux programmes gouvernementaux, ainsi que pour des fins d'impôts. Référez-vous à Service Canada pour connaître la liste des organismes publics justifiant la

cueillette du NAS par une loi ou un règlement.

Relevés officiels

- Vérifiez vos relevés de comptes bancaires et de cartes 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

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

Courriels / Textos

- 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 aucune information personnelle par courriel.
- Signalez gratuitement un message texte frauduleux en le transférant auprès de votre fournisseur de téléphonie mobile au numéro 7726 (SPAM).

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

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.

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 !