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.

FRAUDE PAR CARTES DE PAIEMENT (CRÉDIT OU DÉBIT)

La fraude par carte de paiement englobe les fraudes commises en utilisant des cartes de crédit et débit, ou les informations de celles-ci, afin d'obtenir des fonds ou se procurer des biens.

Comment font les fraudeurs ?

- En obtenant votre numéro de carte de crédit, sa date d'expiration et le numéro de vérification (code CVV) et en se servant de cette information pour faire des achats par téléphone ou en ligne.
- En obtenant le numéro d'identification personnel (NIP) de votre carte de débit pour effectuer des retraits et dérober votre épargne.
- En obtenant l'information de la bande magnétique se trouvant au version d'une carte de paiement pour ainsi cloner celle-ci.

Comment se protéger ?

- Gardez sur vous uniquement les cartes dont vous avez vraiment besoin et assurez-vous que les autres sont en sécurité.
- Signalez la perte ou le vol d'une carte dès que vous vous en rendez compte.
- Effectuez vos transactions au guichet à l'endroit et au moment où vous vous sentez le plus en sécurité. Si quelque chose semble inhabituel, signalez la situation à la police, au marchand ou à votre institution financière.
- Ne prêtez jamais votre carte de paiement ni ne divulguez le NIP.
- Protégez votre NIP, c'est votre signature électronique.
    - Mémorisez-le et assurez-vous qu'il ne figure sur aucun document.
    - Choisissez un NIP qui ne peut être facilement deviné. N'utilisez pas votre date de naissance, votre numéro de téléphone ou votre adresse.
    - Changez-le régulièrement.
    - Prenez soin de le cacher des regards des autres lors de transactions.
- Vérifiez vos relevés de compte bancaire et de carte de crédit régulièrement. Contestez immédiatement tout achat qui vous est inconnu.
- Méfiez-vous des courriels ou textos qui prétendent provenir de votre institution financière ou d'une agence gouvernementale. Ces institutions ne transmettent jamais de courriels ou textos à leurs clients afin d'obtenir des renseignements bancaires ou personnels.

POUR OBTENIR DE L'AIDE OU SIGNALER UNE FRAUDE

Si vous soupçonnez ou savez avoir été victime d'une fraude par carte de paiement, signaler l'incident auprès du service de police qui dessert votre municipalité (Sûreté du Québec ou service de police local) et communiquez rapidement avec votre institution financière et avec la compagnie émettrice de votre carte de paiement.

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 : 1 800 465-7166
- 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!

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.

LA CONTREFAÇON DES BILLETS DE BANQUE

La vérification des billets de banque, c'est monnaie courante!

L'argent comptant est un moyen commode et rapide de payer ses achats. Comme il s'agit d'un mode de paiement utilisé par tous, celui-ci intéresse les faussaires. Chaque fois que vous acceptez un billet de banque sans le vérifier, vous risquez d'être victime de contrefaçon.

Que vous soyez caissier ou client, vous pouvez aider à empêcher les faux billets d'entrer en circulation. Les commerçants victimes de fraude subissent des pertes dont ils répercutent souvent le coût sur les consommateurs – en l'occurrence, vous !

Les billets de banque canadiens sont pourvus d'éléments de sécurité qui sont faciles à vérifier et difficiles à contrefaire. Toutefois, les billets de banque ne sont sûrs que si vous les vérifiez. Si vous connaissez bien vos billets, vous pourrez détecter un faux en un coup d'œil.

Pour détecter une fausse coupure, il faut vous familiariser avec les éléments de sécurité des billets. C'est la meilleure ligne de défense contre la contrefaçon. Voici quelques conseils :

- Comparez un billet douteux à un billet que vous savez authentique.
- Vérifiez au moins deux éléments de sécurité.
- Cherchez les différences et non les similitudes.
- Si vous ne savez pas comment vérifier un billet en papier, refusez-le et demandez qu'on vous remette un billet en polymère.

Comment vérifier les billets en polymère ?

Touchez le billet, examinez-le et regardez au verso :

- Touchez la texture lisse et unique du billet. Celui-ci est fait d'un seul morceau de polymère dont certaines parties sont transparentes.
- Touchez le billet pour sentir l'encre en relief sur le grand chiffre, les épaules du grand portrait et les mots « Banque du Canada » et « Bank of Canada ».
- Examiner la bande transparente contenant un portrait et un édifice à reflets métalliques, le mot « Canada » qui est transparent et légèrement en relief, et les petits chiffres qui correspondent à la valeur du billet.
- Regardez au verso du billet pour vous assurer que ces images ont les mêmes couleurs et détails qu'au recto.

Source : https://flic.kr/p/c6T94S

Sachez qu'aucune loi ne vous oblige à accepter un billet de banque si vous doutez de son authenticité.

Si, **AU COURS** d'une transaction, vous soupçonnez qu'on vous remet un faux billet :

- Refusez le billet poliment et expliquez que vous soupçonnez qu'il s'agit d'un faux.
- Demandez qu'on vous donne un autre billet (que vous vérifierez également).
- Conseillez à la personne d'apporter le billet suspect au service de police local pour le faire vérifier.
- Informez le service de police local qu'on a possiblement tenté de vous remettre un faux billet.

Si par mégarde vous soupçonnez qu'on vous a remis un billet suspect **APRÈS** une transaction, remettez-le à votre service de police local pour le faire vérifier. S'il s'avère authentique, on vous le rendra.

Séries de billets de banque

Pour en savoir davantage sur les éléments de sécurité de toutes les séries billets de banque, visitez le site http://www.banqueducanada.ca/billets/series-de-billets-de-banque/.

Le billet de banque commémoratif Canada 150

En 2017, à l'occasion du 150e anniversaire de la Confédération, la Banque a émis un billet commémoratif de 10 $. Pour en savoir plus au sujet de ce billet et ses éléments de sécurité, visitez http://www.banqueducanada.ca/billet150.

Un nouveau billet de banque de 10 $ en 2018

Le prochain billet de 10 $ destiné à la circulation courante sera émis à la fin de 2018. Il sera orné du portrait de Viola Desmond, une militante pour la justice sociale. C'est la première fois que le portrait d'une femme canadienne emblématique figurera sur un billet de circulation courante de la Banque du Canada. Pour en apprendre davantage sur Viola Desmond et sur ce billet, visitez http://www.banqueducanada.ca/billets/.

Les billets de banque américains

Pour vous familiariser avec les éléments de sécurité des billets de banque américains, consultez le site internet www.uscurrency.gov.

POUR OBTENIR DE L'AIDE OU SIGNALER UNE FRAUDE

Pour des informations sur la prévention de la contrefaçon de monnaie, communiquez avec la Banque du Canada au 1 800 303-1282, info@banqueducanada.ca ou visitez www.banqueducanada.ca/billets.

Si vous croyez avoir été victime de fraude, communiquez avec votre service de police local.

Pour signaler une fraude auprès du Centre antifraude du Canada : 1 888 495-8501 ou 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 !

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.

FRAUDE DU « PAIEMENT EN TROP » ET FRAUDE DU « PAIEMENT URGENT »

QU'EST-CE QUE LA FRAUDE DU « PAIEMENT EN TROP » ?

La fraude du « paiement en trop » consiste en différents stratagèmes s'accompagnant généralement de chèques frauduleux (falsifiés, contrefaits ou volés) ou de faux avis de virement.

Il s'agit de stratagèmes visant, par exemple, à :

- Vous offrir un faux emploi.
- Payer un article que vous vendez à un prix plus élevé (p. ex., sur un site de petites annonces).
- Vous offrir le remboursement d'un solde payé en trop en vous invitant à cliquer sur un lien d'un fournisseur (p. ex., de téléphonie, d'Internet, etc.) ou d'un service public (p. ex., municipalité, agence gouvernementale).

Comment font les fraudeurs ?

Fraude liée à l'emploi

- En vous envoyant un message texte ou un courriel proposant une opportunité alléchante de faire de l'argent (par exemple pour agir comme représentant d'une société outre-mer, comme client mystère ou afficher un logo sur votre véhicule).
- Une fois l'offre acceptée, en vous incitant à déposer un chèque, à transférer un certain montant vers un autre compte et à garder une partie du montant à titre de rémunération ou de commission. Le chèque s'avère frauduleux et vous devez assumer la perte.
- En virant une somme d'argent vers votre compte et en vous demandant de transférer ensuite un certain montant vers un autre compte. La transaction initiale s'avère frauduleuse et vous devez assumer la perte.

Fraude liée aux petites annonces

En vous offrant un montant plus élevé que le prix affiché en vous indiquant d'encaisser le chèque, de conserver une partie du montant à titre de paiement de l'article et de remettre la balance de l'argent à une tierce personne, un complice du fraudeur. Le chèque déposé s'avère frauduleux et vous devez assumer la perte.

Comment se protéger ?

- Ne répondez jamais à un texto ou un courriel non sollicité.
- Soyez prudent lorsqu'une « compagnie » utilise une simple adresse de courriel sur le Web pour faire des affaires. Vérifiez son existence, recherchez ses coordonnées complètes (nom de l'entreprise, adresse civique, numéro de téléphone) et validez ces informations.

- N’effectuez aucun virement de fonds tant que vous n’avez pas confirmé la légitimité d’un chèque ou d’un dépôt électronique.
- N’acceptez jamais un chèque libellé au nom d’un tiers qui vous le transfère en guise de paiement.
- Si un emploi semble trop beau pour être vrai, il s’agit d’une arnaque.

Dans le cadre d’une transaction de vente

- N’acceptez jamais un chèque dont le montant est supérieur au montant de la vente.
- En cas de doute, n’effectuez simplement pas la transaction.

QU’EST-CE QUE LA FRAUDE DU « PAIEMENT URGENT » ?

Il s’agit d’une fraude où la victime est sollicitée par téléphone, par messagerie texte ou par courriel par des gens se faisant passer pour un agent gouvernemental (souvent du revenu ou de l’immigration). Les fraudeurs invoqueront, par exemple, des impôts non payés ou un dossier administratif incomplet afin d’inciter la victime à payer un montant d’argent.

Comment font les fraudeurs ?

- En créant un sentiment de panique ou d’urgence au moyen de menaces (amende, poursuite, déportation, mandat d’arrestation), par l’emploi d’un ton agressif ou le recours à de fortes pressions, afin d’effrayer les victimes et exiger un paiement immédiat.
- En vous demandant d’acheter des cartes prépayées et de leur communiquer les codes d’activation au verso de la carte.
- En vous exigeant d’effectuer un paiement par téléphone ou via un site Internet donné.

Comment se protéger ?

- Ne cédez pas à la pression, faites preuve de prudence et de scepticisme.
- Méfiez-vous, aucun organisme gouvernemental :
    - n’emploie de ton menaçant ou n’effectue une pression indue auprès des citoyens;
    - n’exige le remboursement immédiat d’impôts, l’obtention d’un service ou le traitement d’une demande d’immigration à l’aide d’une carte prépayée ou d’un transfert d’argent.
- Retrouvez le numéro de téléphone officiel de l’organisme qui vous a contacté, appelez et vérifiez la validité de la demande qui vous est adressée.

POUR OBTENIR DE L’AIDE OU SIGNALER UNE FRAUDE

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

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!

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!