MONTRE-MOI LA FRAUDE

Trousse de prévention de la fraude 2021

Table des matières

Introduction

Le taux de fraude continue d'augmenter au Canada et le monde entier est aux prises avec une pandémie. La COVID-19 a créé un contexte propice à la fraude et aux activités criminelles en ligne. En raison de la pandémie, plus de personnes que jamais se tournent vers Internet pour faire l'épicerie et des courses, effectuer des opérations bancaires et avoir de la compagnie. Si l'on ajoute à cela les profondes répercussions sociales, psychologiques et émotionnelles de la COVID-19 sur les gens, on peut supposer que le nombre de victimes potentielles a augmenté de façon spectaculaire.
Mars est le mois de la prévention de la fraude. Cette année, les efforts seront axés sur l'économie numérique des fraudes et des escroqueries. Le Centre antifraude du Canada (CAFC) a préparé la présente trousse afin de mieux sensibiliser et renseigner le public. Nous vous encourageons tous à ajouter les documents de référence contenus dans la présente trousse à votre site Web, à vos publications écrites et à vos plateformes de médias sociaux.

Tout au long de l'année, le CAFC liera les messages de prévention de la fraude au moyen des mots-clics #déNONcerlafraude et #montremoilaFRAUDE. Nous continuerons également d'utiliser le slogan « La fraude : Identifiez-la, signalez-la, enrayez-la ».

Pendant le Mois de la prévention de la fraude, le CAFC diffusera chaque jour des messages sur Facebook et Twitter (#MPF2021). Nous publierons notre bulletin hebdomadaire tous les lundis et tiendrons une discussion #ParlonsFraude sur Twitter à 13 h (heure de l'Est) chaque mercredi. Tous sont invités à participer à la discussion.

Les questions et les commentaires sur la prévention de la fraude sont toujours les bienvenus.

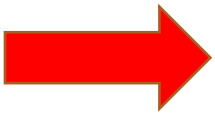
Merci,

L'équipe de prévention de la fraude du CAFC

Twitter : @antifraudecan
Facebook : Centre antifraude du Canada

La présente trousse comprend :

1) **Logo du CAFC**



2) **Bibliothèque graphique**
https://www.facebook.com/pg/canantifraud/photos/?tab=album&album_id=2840141142692133

3) **Vidéothèque**
https://www.youtube.com/channel/UCnvTfqttCb4K6wyVC6rMJkw/playlists

4) **Le petit livre noir de la fraude, 2e édition**
Le Bureau de la concurrence continuera de promouvoir le petit livre noir de la fraude, 2e édition, une ressource en ligne sur 12 fraudes courantes avec des conseils pour les reconnaître, les rejeter et les signaler. Le petit livre noir de la fraude est disponible sur le site Web du Bureau en anglais, français, mandarin, cantonais, pendjabi, tagalog, arabe et espagnol. D'autres ressources sont disponibles sur le site Web du Bureau de la concurrence, y compris un quiz pour tester les connaissances des Canadiens sur les fraudes courantes.

5) **Présentation**
Les présentations PowerPoint du CAFC sont disponibles sur demande en faisant parvenir un courriel à partners@antifraudcentre.ca.

6) **Calendrier des activités**

Tous les lundis en mars, le CAFC publiera un bulletin pour mieux faire connaître la fraude et présenter les thèmes prévus chaque semaine en lien avec l'économie numérique des fraudes et des escroqueries. Les mercredis, nous tiendrons une discussion #ParlonsFraude sur Twitter à 13 h (heure de l'Est) pour donner des conseils sur la façon de rompre tout contact avec les fraudeurs.

Bulletins
Semaine 1 : Achat et vente en ligne
Semaine 2 : Fraudes financières en ligne
Semaine 3 : Protection de vos comptes et de votre identité
Semaine 4 : Courriels frauduleux
Semaine 5 : Fraudes en ligne

Parlons fraude
Semaine 1 : Fraude téléphonique
Semaine 2 : Fraude par courriel ou message texte
Semaine 3 : Fraude en ligne
Semaine 4 : Fraude sur les médias sociaux
Semaine 5 : Fraude par la poste ou en personne

Tous les jours, le CAFC attirera l'attention des abonnés de ses comptes de réseaux sociaux sur une fraude en particulier.
Twitter : @antifraudecan **Facebook : Centre antifraude du Canada**

Le **2 mars 2021** – Joignez-vous à nous sur Facebook pour le lancement en direct (étalé sur 13 heures) à l'échelle du pays du Mois de la prévention de la fraude.

Mars 2021

Lundi 1er mars Facebook et Twitter Bulletin – Achat et vente en ligne	**Mardi 2 mars** Facebook **LANCEMENT EN DIRECT**	**Mercredi 3 mars** Facebook et Twitter Escroquerie de chiots **13 h (HNE)** #ParlonsFraude	**Jeudi 4 mars** Facebook et Twitter Fraudes à la location immobilière	**Vendredi 5 mars** Facebook et Twitter Escroqueries liées à la vente de marchandises et à la contrefaçon
Lundi 8 mars Facebook et Twitter Bulletin – Fraudes financières	**Mardi 9 mars** Facebook et Twitter Arnaques d'investissement	**Mercredi 10 mars** Facebook et Twitter Prêts frauduleux **13 h (HNE)** #ParlonsFraude	**Jeudi 11 mars** Facebook et Twitter Fraudes liées à des subventions	**Vendredi 12 mars** Facebook et Twitter Escroqueries d'emploi
Lundi 15 mars Facebook et Twitter Bulletin – Protection de vos renseignements	**Mardi 16 mars** Facebook et Twitter Vol d'identité et fraude à l'identité	**Mercredi 17 mars** Facebook et Twitter Stratagèmes liés aux médias sociaux **13 h (HNE)** #ParlonsFraude	**Jeudi 18 mars** Facebook et Twitter Protection de vos comptes	**Vendredi 19 mars** Facebook et Twitter Rançongiciels
Lundi 22 mars Facebook et Twitter Bulletin – Fraudes par courriel et par texto	**Mardi 23 mars** Facebook et Twitter Hameçonnage	**Mercredi 24 mars** Facebook et Twitter Harponnage **13 h (HNE)** #ParlonsFraude	**Jeudi 25 mars** Facebook et Twitter Stratagèmes d'extorsion	**Vendredi 26 mars** Facebook et Twitter Escroqueries de prix gagnés
Lundi 29 mars Facebook et Twitter Fraudes courantes en ligne	**Mardi 30 mars** Facebook et Twitter Stratagèmes de rencontre	**Mercredi 31 mars** Facebook et Twitter Fraudes liées à l'immigration **13 h (HNE)** #ParlonsFraude	**Jeudi 1er avril** Facebook et Twitter La fraude, ce n'est pas une blague	

7) Au sujet du CAFC

Le Centre antifraude du Canada (CAFC) est le dépôt central des données sur la fraude. Nous aidons les citoyens et les entreprises :

- à signaler la fraude;
- à se renseigner sur différents types de fraude;
- à reconnaître les indices de fraude;
- à se protéger contre la fraude.

Le CAFC ne mène pas d'enquêtes, mais il apporte une aide précieuse aux organismes d'application de la loi en faisant des rapprochements dans des affaires de fraude partout dans le monde. Nos objectifs comprennent notamment ce qui suit :

- perturber les activités criminelles;
- renforcer le partenariat entre les secteurs privé et public;
- préserver l'économie canadienne.

Le CAFC est géré conjointement par la Gendarmerie royale du Canada, le Bureau de la concurrence et la Police provinciale de l'Ontario.

8) Statistiques

En 2020, le CAFC a reçu 101 483 signalements de fraude représentant des pertes totales de près de 160 millions de dollars. De plus, 67 294 signalements ont été faits par des entreprises et des consommateurs canadiens, dont les pertes déclarées s'élèvent à plus de 104,2 millions de dollars.

Les 10 formes de fraude touchant les Canadiens les plus signalées en 2020 :

Type de fraude	N^{bre} de signalements	N^{bre} de victimes	Pertes (en $)
Extorsion	17 390	6 689	12,5 millions
Fraude à l'identité	16 970	16 970	S.O.
Renseignements personnels	6 649	4 386	S.O.
Hameçonnage	3 672	1 167	S.O.
Marchandises	3 354	2 728	8,7 millions
Fraude liée à la vente	2 320	1 478	4,2 millions
Emploi	2 297	1 035	2,5 millions
Service	2 009	1 241	8,5 millions
Harponnage	1 049	525	14,4 millions
Besoin urgent d'argent	924	310	1,0 million

Les 10 formes de fraude ayant entraîné les plus importantes pertes financières pour les Canadiens en 2020 :

Type de fraude	N^bre de signalements	N^bre de victimes	Pertes (en $)
Stratagème de rencontre	899	620	18,5 millions
Investissements	501	428	16,5 millions
Harponnage	1 049	525	14,4 millions
Extorsion	17 390	6 689	12,5 millions
Marchandises	3 354	2 728	8,7 millions
Service	2 009	1 241	8,5 millions
Fraude liée à la vente	2 320	1 478	4,2 millions
Prix gagné	754	240	3,5 millions
Enquêteur bancaire	835	340	3,0 millions
Emploi	2 297	1 035	2,6 millions

➔ On estime que moins de **5 %** des victimes de fraude font un signalement au CAFC.

9) Signalement de la fraude

La fraude évolue. Elle peut souvent se poursuivre sur une longue période de temps et constitue un crime qui est difficile à déceler et à signaler. Pour vous faciliter la tâche, le CAFC recommande de prendre les six mesures suivantes :

1 : Rassemblez toute l'information sur la fraude.
2 : Consignez les événements en ordre chronologique.
3 : Signalez l'incident au service de police local.
4 : Signalez l'incident au CAFC au moyen du Système de signalement des fraudes (SSF) ou en composant le 1-888-495-8501 (sans frais).
5 : Signalez l'incident à l'institution financière ou au fournisseur de services de paiement utilisé pour envoyer l'argent.
6 : Si la fraude a été commise en ligne, assurez-vous de signaler l'incident directement au site Web.

10) Messages clés et slogans

A) La fraude : Identifiez-la, signalez-la, enrayez-la.

De nos jours, bon nombre de fraudes sont conçues pour jouer sur les émotions des victimes potentielles et les inciter à agir sans réfléchir. Les fraudeurs cherchent à faire réagir les victimes sous l'effet de la panique, de la peur, du désespoir, de l'exaltation

et de l'amour, souvent en leur présentant des situations urgentes qui exigent une action immédiate. Le slogan pour la prévention de la fraude vise à amener les citoyens canadiens à se raisonner et à ne pas réagir aux sollicitations qui pourraient être frauduleuses. Nous encourageons les gens à **reconnaître** que les fraudeurs utilisent tous les moyens à leur disposition pour les cibler : téléphone, courriel, textos, médias sociaux, Internet et courrier. Nous leur demandons de changer la façon dont ils réagissent aux offres ou aux demandes non sollicitées.

Enrayer la fraude consister à protéger ses renseignements personnels et son argent. Parmi les pratiques courantes à adopter : vérifier ses profils de crédit, surveiller ses comptes pour toute activité non autorisée, mettre à jour ses systèmes d'exploitation et logiciels antivirus, et ne pas effectuer de transactions par téléphone. Nous voulons que les gens se raisonnent et qu'ils réfléchissent à la situation et l'évaluent avant de réagir. Ils peuvent notamment dire non, faire une vérification approfondie, effectuer des recherches, confirmer l'information et parler de la situation à des membres de leur famille et à des amis. Nous voulons que les gens prennent leur temps et examinent soigneusement toutes les offres et les demandes.

Signaler la fraude signifie la dénoncer, même quand il n'y a aucune perte d'argent. À l'instar d'autres crimes, si la fraude n'est pas signalée, nous ne savons pas ce qui se passe et nous ne pouvons pas avertir les autres. L'information provenant du signalement d'une fraude (compte bancaire, adresse de courriel, adresse liée à une devise virtuelle, numéro de téléphone, etc.) peut faire l'objet d'une enquête et se révéler utile pour établir des liens avec d'autres incidents. Le signalement offre aussi d'autres moyens de perturbation. En transmettant l'information aux banques, aux entreprises de transfert de fonds, aux fournisseurs de services de courriel, aux compagnies de téléphone et aux responsables des sites de rencontre et des réseaux de médias sociaux, des mesures peuvent être prises pour bloquer ou supprimer ces comptes frauduleux et leur contenu.

- <u>Liste de contrôle pour prévenir la fraude</u> : Voici quelques questions que vous devez vous poser chaque fois qu'on communique avec vous pour obtenir des renseignements personnels. Si vous répondez par l'affirmative à l'une de ces questions, ne fournissez pas vos renseignements et demandez conseil.
    - Est-ce qu'il s'agit d'un appel non sollicité? Était-il prévu ou inattendu?
    - Est-ce qu'on vous demande de confirmer des renseignements personnels comme votre nom, votre adresse ou des renseignements liés à votre compte?

- Est-ce qu'on s'attend à une réponse rapide ou immédiate?
- Est-ce qu'on vous demande de l'argent?
- L'appelant évite-t-il de préciser le nom de l'entreprise ou de l'institution financière?
- Est-ce qu'on vous offre un prix, un essai ou un cadeau gratuit?
- Est-ce qu'on prétend être la police ou mener une enquête?
- Est-ce que l'adresse de courriel est bizarre?
- Est-ce que la mise en forme est étrange? Est-ce que le message renferme des fautes d'orthographe?
- Est-ce qu'on vous demande de modifier votre mot de passe sans que vous en ayez fait la demande?

B) La fraude en 3D – Détecter, dénoncer, décourager

Élaborée par des services de police du Québec en partenariat avec la Banque du Canada, la fraude en 3D est un slogan ou une campagne qui vise à inciter les gens à être vigilants pour éviter les effets dévastateurs de la fraude. Pour en savoir plus, consultez le site : https://www.sq.gouv.qc.ca/services/campagnes/mpf/. Pour le livret en PDF : https://www.banqueducanada.ca/wp-content/uploads/2020/02/fraude-3d.pdf.

C) Prendre5 pour mettre fin à la fraude

Prendre5 est une campagne nationale lancée par UK Finance (un regroupement de banques et d'institutions financières du Royaume-Uni) et le gouvernement britannique qui offre des conseils simples et impartiaux pour aider tout le monde à se protéger contre la fraude pouvant être prévenue. Cela comprend la tromperie par courriel et la fraude téléphonique et en ligne – surtout lorsque les fraudeurs se font passer pour des représentants d'organisations dignes de confiance.

Prendre5 incite les consommateurs à :

S'ARRÊTER : Prendre un temps d'arrêt pour réfléchir avant de fournir vos renseignements personnels ou de donner votre argent pourrait vous protéger.
DOUTER : Est-ce qu'il pourrait s'agir d'une fausse demande? Il n'y a rien de mal à rejeter, refuser ou ignorer des demandes. Seuls les fraudeurs tenteront de vous bousculer ou de vous faire paniquer.

SE PROTÉGER : Si vous croyez être victime d'une fraude, communiquez immédiatement avec votre service de police local, le Centre antifraude du Canada et votre institution financière.

Pour en savoir plus sur Prendre5 : https://takefive-stopfraud.org.uk/.

D) Parler À2

Créée au Royaume-Uni par l'agent-détective Tony Murray, la campagne #ParlerA2 est née d'un fort désir de protéger les consommateurs contre la fraude. Il s'est servi d'une approche axée sur la résolution de problèmes pour déconstruire la fraude et il s'attaque au problème du point de vue des consommateurs. Sa stratégie de communication invite les gens à diffuser les messages de prévention, qui portent sur les cinq principales méthodes utilisées (téléphone résidentiel, Internet, cellulaire, courrier et porte-à-porte) par les fraudeurs pour s'ingérer dans la vie des consommateurs. Cette stratégie fonctionne; elle a remporté des prix et gagne du terrain partout dans le monde.

La campagne vise principalement à faire en sorte que les consommateurs envoient des messages de prévention de la fraude à deux personnes et invitent ensuite celles-ci à faire de même. Une chaîne ininterrompue de 20 personnes permettrait de rejoindre plus d'un million de personnes et une chaîne ininterrompue de 25 personnes, plus de 33,5 millions de personnes, soit un peu moins que toute la population du Canada.

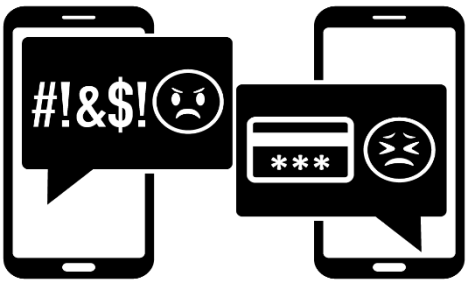
Nous encourageons nos partenaires à diffuser les messages suivants accompagnés du mot-clic **#ParlerA2, protéger plusieurs**.

- Savez-vous vraiment qui appelle? Les fraudeurs mentent et prétendent représenter des entreprises légitimes. Ils falsifient aussi l'information que vous voyez sur l'afficheur pour vous donner l'impression que l'appel est légitime.
- Pour certains, la ligne terrestre est vitale. Pour les fraudeurs, il s'agit d'une ligne directe. Vous ne reconnaissez pas le numéro? Ne répondez pas. Le ton n'est pas amical au bout du fil? Raccrochez.
- De qui provient vraiment le courriel? Les fraudeurs mentent et se font passer pour des entreprises légitimes. Passez le curseur de votre souris sur l'adresse de courriel pour voir si c'est la vraie adresse.
- On vous dit que vous avez gagné un prix par la poste? Sachez que vous ne pouvez pas remporter un concours ou une loterie si vous n'y avez pas participé.
- Vous n'attendez pas de visiteurs? N'ouvrez pas la porte.
- Ne présumez pas que tout le monde est bien renseigné. Parlez directement à deux personnes pour veiller à la sécurité de tous.
- Parlez à deux personnes autour d'un verre ou d'un café.

11) Fraudes courantes et moyens de vous protéger

Vous trouverez ci-dessous quelques fraudes courantes touchant les Canadiens :

Extorsion
Il y a extorsion lorsqu'une personne obtient illégalement de l'argent, des biens ou des services d'une personne, d'une entité ou d'une institution par la coercition.

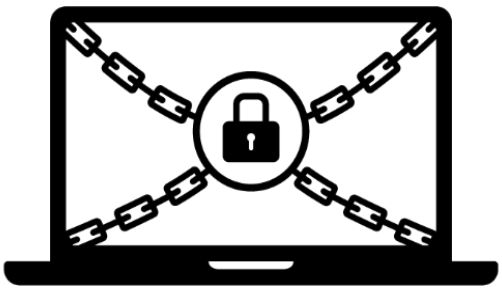


Fraude au numéro d'assurance sociale (NAS) : Les consommateurs reçoivent des messages préenregistrés les informant que leur NAS est lié à une activité frauduleuse ou criminelle. Les fraudeurs se font passer pour des employés d'organismes fédéraux et prétendent que le NAS de la personne est bloqué, compromis ou annulé. Si les victimes ne coopèrent pas, les fraudeurs peuvent menacer d'émettre un mandat d'arrestation contre elles ou de les emprisonner. Ils peuvent leur demander de fournir des renseignements personnels (NAS, date de naissance, adresse, etc.) ou de vider leurs comptes bancaires et de déposer les fonds ailleurs. Les fraudeurs affirment vouloir

s’assurer que l’argent ne sert pas à commettre des activités illégales et qu’il leur sera remis une fois l’enquête terminée.

Services d’électricité : L’entreprise reçoit un appel provenant prétendument de son fournisseur d’hydroélectricité. Le fraudeur demande un paiement immédiat, habituellement par bitcoin, à défaut de quoi il coupera le courant.

Rançongiciel : Un type de maliciel conçu pour infecter ou bloquer l’accès à un système ou à des données. Il existe plusieurs façons d'infecter un dispositif au moyen d'un maliciel, mais généralement, cela se produit lorsqu'une victime clique sur un lien malveillant ou une pièce jointe. À l’heure actuelle, le rançongiciel le plus répandu chiffre les données. Une fois que le système est infecté ou que les données sont chiffrées, la victime reçoit une demande de rançon. Le fraudeur peut aussi menacer la victime de rendre les données publiques.



Indices – Comment vous protéger

- Les fraudeurs utilisent la technique de « falsification des données de l’appelant », qui est facilement accessible, pour induire les victimes en erreur. Ne présumez jamais que les numéros de téléphone qui apparaissent sur votre afficheur sont authentiques.
- Aucun organisme gouvernemental ne communiquera avec vous pour signaler le blocage ou l’annulation de votre NAS ou pour vous menacer de poursuites judiciaires.
- Ne divulguez jamais de renseignements personnels au téléphone à un inconnu.
- Aucun organisme gouvernemental ou d’application de la loi n’exigera que vous fassiez un paiement immédiatement ou que vous remettiez toutes vos économies aux fins d’enquête.
- Aucun organisme gouvernemental ou d’application de la loi n’exigera un paiement par bitcoin, par l’entremise d’une entreprise de transfert de fonds ou par cartes-cadeaux (p. ex. iTunes, Google Play, Steam).
- Comment reconnaître la fraude liée à l’Agence du revenu du Canada : https://www.canada.ca/fr/agence-revenu/organisation/securite/protegez-vous-contre-fraude.html

- Familiarisez-vous avec les conditions d'utilisation de votre fournisseur de services.
- Communiquez directement avec votre fournisseur de services et vérifiez que votre compte est en règle.
- N'ouvrez pas les courriels et les messages textes non sollicités.
- Ne cliquez pas sur des pièces jointes ou des liens suspects.
- Faites régulièrement des copies de sauvegarde des fichiers importants.
- Gardez votre système d'exploitation et vos logiciels à jour.
- Le paiement d'une rançon ne garantit pas la restauration de vos fichiers et dispositifs. Les fraudeurs pourraient continuer à demander de l'argent.
- Faites inspecter vos systèmes par des techniciens locaux.
- Signalez toute intrusion dans des bases de données conformément à la *Loi sur la protection des renseignements personnels et les documents électroniques*, qui s'applique au secteur privé au Canada.

Stratagème de rencontre

Les fraudeurs utilisent tous les types de sites de rencontre et de réseautage social pour communiquer avec leurs victimes. Ils créent leurs comptes au moyen de photos volées d'autres personnes. Leurs antécédents sont souvent semblables à ceux de la victime et il n'est pas rare qu'ils affirment être dans l'armée, travailler à l'étranger ou être des gens d'affaires prospères. Ils ne tardent pas à déclarer leur amour pour gagner la confiance, l'affection et l'argent de leur victime. Ce type de fraude mise beaucoup sur les émotions des victimes et peut durer des mois, des années ou jusqu'à ce que la victime n'ait plus rien à donner. Les fraudeurs éprouveront toujours des ennuis financiers et ne pourront jamais rembourser leurs victimes, mais ils continueront de faire des promesses vides et de demander plus d'argent.

Indices – Comment vous protéger

- Méfiez-vous lorsqu'une personne ne tarde pas à vous déclarer son amour.
- Méfiez-vous des personnes qui prétendent être riches, mais qui ont besoin d'emprunter de l'argent.
- Quand vous tentez d'organiser une rencontre, méfiez-vous si la personne vous donne toujours des excuses pour annuler. Si vous finissez par vous rencontrer, faites-le dans un endroit public et donnez les détails de votre rendez-vous à quelqu'un.

- N’envoyez jamais de photos ou de vidéos intimes de vous-même car celles-ci pourraient être utilisées pour vous faire du chantage.
- Il ne faut jamais, sous aucun prétexte, envoyer ou accepter de l’argent. Vous pourriez, sans le savoir, participer à des activités de blanchiment d’argent, ce qui constitue une infraction criminelle.

Hameçonnage par courriel et par texto

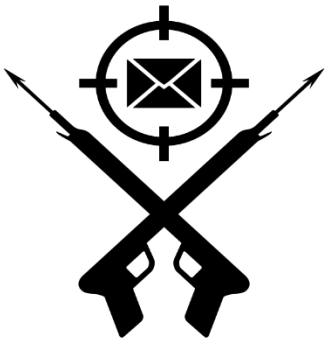
Les courriels et les textos d’hameçonnage visent à faire croire à la victime qu’elle fait affaire avec une entreprise de renom (p. ex. institution financière, fournisseur de services, organisme du gouvernement). Dans ces messages, on vous invite à cliquer sur un lien pour diverses raisons : mettre à jour les renseignements de votre compte, déverrouiller celui-ci ou accepter un remboursement. Le but est de recueillir des renseignements personnels et financiers pouvant être utilisés pour commettre une fraude d’identité.

Indices – Comment vous protéger

- Ne cliquez pas les liens dans des courriels ou des textos non sollicités.
- Examinez le courriel ou le message pour voir s’il renferme des fautes d’orthographe et des erreurs de mise en forme.
- Vérifiez l’hyperlien derrière le texte ou le bouton du lien en passant le curseur sur le texte.
- Ne cliquez pas sur des liens suspects puisqu’ils peuvent contenir un maliciel.

Harponnage

Le harponnage est l’une des cyberattaques les plus courantes et les plus dangereuses actuellement employées pour frauder des entreprises et des organisations. Au moment de planifier une telle attaque, les fraudeurs prennent le temps de recueillir des renseignements sur leurs cibles afin d’envoyer des courriels convaincants qui semblent provenir d’une source fiable. Les fraudeurs s’infiltrent dans le compte de courriel d’une entreprise ou le mystifient. Ils créent une règle pour qu’une copie des courriels entrants soit transmise à l’un de leurs comptes et épluchent ces courriels pour étudier le niveau de langue utilisé par l’expéditeur et trouver des caractéristiques liées à des personnes, à des dates et à des paiements importants.



La cyberattaque a lieu lorsque le titulaire du compte de courriel est difficilement joignable par courriel ou téléphone. Si le compte de courriel du haut dirigeant n'a pas été compromis, les fraudeurs peuvent créer un domaine semblable à celui de l'entreprise et utiliser le nom du titulaire. Les coordonnées dont ils ont besoin se trouvent souvent sur le site Web de l'entreprise ou dans les médias sociaux.

Variantes courantes

- Un haut dirigeant envoie un courriel au service des comptes créditeurs de son entreprise afin de demander un paiement urgent pour conclure un marché privé.
- Une entreprise reçoit une copie d'une facture contenant des données de paiement à jour provenant apparemment d'un fournisseur ou d'un entrepreneur.
- Un comptable ou un planificateur financier reçoit une demande de retrait d'une somme importante qui semble provenir du compte de courriel d'un client.
- Le service de la paye reçoit un courriel semblant provenir d'un employé qui veut mettre à jour ses renseignements bancaires.
- Les membres d'une église, d'une synagogue, d'un temple ou d'une mosquée reçoivent une demande de don par courriel provenant prétendument de leur chef religieux.
- Un courriel semblant provenir d'une source fiable vous demande de télécharger une pièce jointe, mais celle-ci renferme un maliciel servant à infiltrer votre réseau.

Indices

- Courriels non sollicités
- Courriel provenant directement d'un haut responsable avec qui vous ne communiquez pas d'habitude
- Demandes de confidentialité absolue
- Pression exercée ou impression d'urgence
- Demandes inhabituelles qui ne respectent pas les procédures internes
- Menace ou promesse de récompense

Comment vous protéger

- Tenez-vous au courant des fraudes ciblant les entreprises et sensibilisez tous les employés. Offrez une formation sur la fraude aux nouveaux employés.

- Mettez en place des modalités de paiement détaillées. Exigez la vérification des demandes inhabituelles.
- Établissez des mesures d'identification, de gestion et de signalement des fraudes.
- N'ouvrez pas les courriels non sollicités et ne cliquez pas sur les pièces jointes ou les liens suspects.
- Passez le curseur de votre souris sur une adresse de courriel ou un lien pour confirmer qu'ils sont corrects.
- Limitez la quantité d'information diffusée publiquement et faites preuve de prudence dans les médias sociaux.
- Mettez à niveau et à jour vos logiciels de sécurité.

Achat de marchandises

Les fraudeurs peuvent publier des annonces dans des sites populaires ou de réseautage social. Ils peuvent aussi créer des sites Web qui ressemblent fidèlement à ceux des fabricants légitimes. Les fraudeurs attirent les acheteurs vers leurs sites en faisant la publicité de leurs produits à très bas prix. Les acheteurs peuvent recevoir des produits contrefaits, des biens de valeur inférieure et différents de ce qu'ils ont commandé ou ne rien recevoir du tout. Les entreprises doivent faire preuve de diligence raisonnable avant d'acheter des produits ou des services de fournisseurs nouveaux et inconnus.

Véhicules à vendre : Les véhicules sont affichés à un prix inférieur à la moyenne. Les fraudeurs prétendent se trouver à l'étranger et indiquent qu'un tiers s'occupera de livrer le véhicule. Ils demandent à la victime de payer le véhicule et la livraison, mais celle-ci ne le reçoit jamais.

Animaux à donner : Les fraudeurs annoncent souvent des animaux à donner, surtout des chiots et des chatons. Ils disent que l'animal est gratuit, mais la victime doit payer le transport. Une fois le paiement reçu, les fraudeurs demandent des paiements supplémentaires pour couvrir divers coûts (cage de transport, vaccins, médicaments, assurance, frais de douanes et de courtage, etc.).

Location immobilière : Les fraudeurs se servent de sites de petites annonces en ligne et des réseaux de médias sociaux pour afficher des logements à louer. La propriété se situe habituellement dans un quartier recherché et le loyer demandé est inférieur aux loyers moyens sur le marché. Les personnes intéressées doivent remplir une demande dans laquelle elles doivent fournir des renseignements personnels. Souvent, le soi-disant propriétaire dit être à l'étranger et souhaite louer rapidement la propriété à la bonne personne. Il demande à la victime de verser un dépôt pour visiter l'endroit ou pour recevoir les clés. Les fonds sont souvent envoyés par voie électronique ou par l'intermédiaire d'entreprises de transfert de fonds. Malheureusement pour la victime, la propriété n'est pas à louer et il est possible qu'elle n'existe même pas. Les annonces frauduleuses sont souvent créées à partir d'annonces de propriétés qui sont à vendre ou qui ont récemment été vendues.

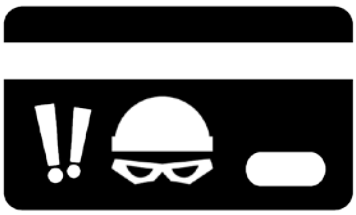
Indices – Comment vous protéger

- Si c'est trop beau pour être vrai, il s'agit probablement d'une escroquerie.
- Méfiez-vous des messages qui s'affichent et vous redirigent vers d'autres pages Web.
- Vérifiez l'URL et les coordonnées du vendeur.
- Cherchez des mises en garde en ligne et lisez bien les commentaires avant de faire un achat.
- Les erreurs de grammaire et d'orthographe indiquent également qu'il pourrait s'agir d'un faux site Web.
- Utilisez une carte de crédit lorsque vous achetez en ligne, car une protection est offerte aux clients et ils pourraient même être remboursés. Si vous avez reçu un produit différent de celui commandé, communiquez avec la compagnie émettrice de votre carte de crédit pour contester le paiement des frais.
- Faites des recherches pour connaître la valeur marchande des propriétés locales.
- Vérifiez l'adresse de la propriété sur une carte interactive et faites des recherches pour vous assurer qu'il ne s'agit pas d'une annonce copiée.
- S'il est possible de le faire, rendez-vous sur place pour visiter la propriété.
- Exigez un bail et lisez-le attentivement.
- N'envoyez pas d'argent avant d'avoir visité la propriété et signé une entente.
- Vérifiez la légitimité de l'URL et des coordonnées du vendeur.

- Renseignez vos employés sur les fraudes courantes qui touchent les entreprises.
- Ne fournissez aucune information concernant la marque ou le modèle de l'équipement de bureau à toute organisation autre que votre fournisseur habituel.
- Examinez les factures suspectes; les fraudeurs envoient de fausses factures pour des produits ou des services jamais achetés.

Fraude liée à la vente

Les entreprises qui vendent de la marchandise ou offrent leurs services en ligne peuvent recevoir des paiements frauduleux. Dans bien des cas, les victimes reçoivent un montant plus élevé que le prix demandé, et on leur demande de rembourser la différence à une tierce partie pour conclure la transaction (souvent, une entreprise d'expédition). Les victimes qui se plient à la demande ne se font pas payer et perdent leur marchandise.



Fraude sans carte : La fraude sans carte peut survenir lorsqu'une entreprise accepte des commandes et des paiements par téléphone, Internet ou courriel. Le fraudeur utilise une carte de crédit volée pour payer les produits ou les services. Il demande la livraison urgente pour s'assurer de recevoir la commande avant que le titulaire de la carte ne découvre les frais. Si le titulaire de la carte conteste les frais, l'entreprise doit rembourser le montant payé avec la carte volée.

Indices

Indices liés au client

- Commandes effectuées à partir d'une seule adresse IP, mais au moyen de différents noms, adresses et cartes de paiement
- Adresses de courriel d'un service de courriel gratuit
- Plusieurs numéros de carte utilisés pour une même commande (les cartes sont toujours refusées)
- L'acheteur n'est pas le titulaire de la carte

Indices liés au produit ou à la commande

- Commandes plus grosses que la normale
- Commandes multiples du même produit, surtout s'il s'agit de gros achats

- Commandes de clients réguliers qui diffèrent des habitudes d'achat de ces derniers
- Commandes par le même client ou liées aux mêmes données de paiement, mais plusieurs adresses IP différentes

Indices liés à la livraison

- Client qui demande une livraison urgente, par exemple dans les 24 heures
- Plusieurs adresses d'expédition associées à une même carte
- Adresse de facturation différente de l'adresse de livraison
- Demande d'envoyer le montant versé en trop à une tierce partie

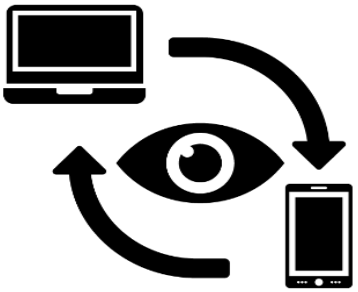
Comment vous protéger

- Connaissez les indices et vérifiez toutes les commandes reçues.
- Avant d'envoyer la marchandise, vérifiez l'information fournie par le client (numéro de téléphone, adresse de courriel, adresse d'expédition, etc.).
- Méfiez-vous des demandes d'expédition prioritaire de biens convoités par les fraudeurs.
- Vérifiez les demandes d'expédition prioritaire lorsque les adresses de facturation et d'expédition ne sont pas les mêmes.
- Pour toute commande douteuse, communiquez avec votre chargé du traitement des paiements. Assurez-vous que des mesures de sécurité sont en place pour éviter d'être victime de fraude et réduire les rétrofacturations indésirables.
- N'acceptez jamais de prélever un montant plus élevé que le prix du produit ou du service et d'envoyer la différence à une tierce partie.

Service

Ces fraudes comportent souvent des offres de services financiers, médicaux ou liés aux télécommunications, à Internet et à l'énergie. De plus, cette catégorie comprend notamment des offres de garanties prolongées, d'assurances et de services de vente.

Soutien technique : La victime reçoit un message ou un appel d'un soi-disant représentant d'une entreprise technologique comme Microsoft ou Windows, qui lui dit qu'un maliciel ou un virus a infecté son ordinateur, ou qu'une personne tente de pirater celui-ci. Le fraudeur offre de régler le problème en accédant à l'ordinateur à distance. Il peut ainsi voler les renseignements personnels de la victime.



Offre de faible taux d'intérêt : Les fraudeurs téléphonent aux victimes pour leur offrir de réduire le taux d'intérêt de leur carte de crédit. Cette fraude vise à obtenir leurs renseignements personnels et les données de leur carte de crédit.

Réparations au domicile et produits : Les propriétaires de résidence se font offrir des services à moindre coût. Il peut s'agir de services de nettoyage de conduits, de réparation de fournaise ou de systèmes de traitement d'eau, ou de rénovations domiciliaires. Si les travaux sont effectués, ils sont de piètre qualité, sont assortis de garanties difficilement applicables ou peuvent causer d'autres dommages.

Indices – Comment vous protéger

- Ne permettez jamais à quiconque d'accéder à distance à votre ordinateur. Si vous éprouvez des problèmes avec votre système d'exploitation, apportez-le à un technicien de votre région.
- Vérifiez la légitimité des appels en composant le numéro de téléphone qui figure au dos de votre carte de crédit. Assurez-vous d'attendre quelques minutes après l'appel original avant de composer le numéro.
- Ne donnez jamais de renseignements personnels ou bancaires au téléphone à moins d'être l'auteur de l'appel.
- Seule une société émettrice de cartes de crédit peut ajuster les taux d'intérêt sur ses produits.
- Effectuez des recherches sur les entreprises et les entrepreneurs qui offrent des services avant de les embaucher.

Emploi

Les fraudeurs se servent de sites Web d'offres d'emploi pour recruter des victimes potentielles. Les offres d'emploi frauduleuses les plus courantes sont les suivantes : adjoint personnel ou client mystère, agent financier ou percepteur de dettes, et habillage de voiture. Dans bien des cas, les fraudeurs se font passer pour des entreprises légitimes.

Adjoint personnel ou client mystère : La victime reçoit un paiement (sans savoir qu'il est faux) accompagné d'instructions lui demandant d'effectuer des retraits en argent et d'autres transactions par l'entremise d'une institution financière, d'une entreprise de transfert de fonds ou d'un guichet automatique de bitcoins. On lui demande de prendre note de son expérience et d'évaluer le service à la clientèle. Le faux paiement finit par être signalé comme étant frauduleux et la victime est responsable de l'argent dépensé.

Agent financier, adjoint administratif ou percepteur de dettes : La victime se fait offrir un emploi où elle doit agir à titre de mandataire ou d'agent financier. On lui demande d'accepter un paiement dans son compte bancaire personnel, de garder une partie du montant et de transférer le reste à des tiers. Elle finit par apprendre que le paiement original était frauduleux et qu'elle est responsable de toute dette contractée. Les fraudeurs tenteront de traiter autant de paiements que possible avant que les victimes soient prévenues de l'escroquerie par leurs institutions financières.

Habillage de voiture : Un consommateur reçoit un message texte non sollicité l'avisant qu'il peut gagner de 300 $ à 500 $ par semaine en apposant des annonces publicitaires sur sa voiture. La victime qui accepte de le faire reçoit un paiement (sans savoir qu'il est faux) avec des instructions lui demandant de déposer et de virer une partie des fonds à une entreprise de graphisme. Le paiement finit par être signalé comme étant frauduleux et la victime apprend qu'elle est responsable des fonds envoyés à l'entreprise.

Indices – Comment vous protéger

- Faites attention aux sites où vous affichez votre curriculum vitæ.
- Méfiez-vous des offres d'emploi reçues dans un message texte non sollicité.
- Peu d'employeurs utiliseront des adresses de courriel gratuites sur le Web pour faire des affaires.
- Prenez le temps de faire des recherches sur un employeur potentiel.
- N'utilisez jamais votre compte bancaire personnel pour déposer des paiements versés par des inconnus.
- Jamais un employeur légitime ne vous enverra de l'argent pour ensuite vous demander de lui en retourner une partie ou d'en envoyer une partie à un tiers.

Investissements

Il s'agit de possibilités d'investissement fausses, trompeuses ou frauduleuses, souvent assorties d'un rendement monétaire plus élevé que la normale, et dans lesquelles les

victimes perdent une bonne partie ou la totalité de leur argent. Les investisseurs risquent aussi d'être victimes de vol d'identité et de retraits non autorisés d'argent sur leur carte de crédit, puis devoir payer des intérêts élevés pour des investissements inexistants.

Offre initiale de jetons : Le marché de devises virtuelles évolue constamment. De nouvelles devises virtuelles voient le jour chaque mois. Comme un premier appel public à l'épargne, une offre initiale de jetons vise à recueillir des fonds pour aider une entreprise à lancer une nouvelle devise virtuelle. Dans cette fraude, le fraudeur envoie un courriel à des investisseurs potentiels à qui il cherche à vendre des jetons frauduleux. Il fournit des documents qui ont l'air officiels, utilise du jargon et peut même offrir un vrai « jeton », mais tout finit par être faux et vous perdez votre investissement.

Vente pyramidale : Comparable à une combine à la Ponzi, la fraude liée à la vente pyramidale vise principalement à générer des profits en recrutant de nouveaux investisseurs. De nos jours, un des stratagèmes courants de vente pyramidale prend la forme d'un « cercle de dons ». Les participants donnent une somme d'argent pour joindre le cercle puis doivent recruter d'autres personnes pour récupérer leur argent. Dans ces stratagèmes, on peut vous offrir des produits, mais ils ont habituellement très peu de valeur.

Au Canada, la vente pyramidale est une infraction criminelle. La loi interdit de mettre sur pied, d'exploiter, de promouvoir un système de vente pyramidale ou d'en faire la publicité.

Indices – Comment vous protéger

- Méfiez-vous lorsqu'on vous demande de fournir des renseignements personnels ou financiers pour récupérer les profits de vos investissements.
- Méfiez-vous des possibilités de placement qui offrent un rendement supérieur à la normale.
- Faites attention lorsqu'une personne insiste pour que vous investissiez immédiatement pour ne pas rater cette occasion.
- Avant d'investir, renseignez-vous sur l'investissement. Faites des recherches sur l'équipe responsable de l'offre et analysez la faisabilité du projet. Vérifiez l'inscription et les antécédents disciplinaires de la société.

- Les Autorités canadiennes en valeurs mobilières (ACVM) encouragent tous les investisseurs à visiter leur moteur de recherche national (http://www.sontilsinscrits.ca/).

Prix

Les consommateurs se font annoncer qu'ils ont remporté un gros lot ou un prix important mêmes s'ils n'ont jamais acheté de billet ou participé à un concours. Ils doivent d'abord payer des frais initiaux pour récolter leur prix, qui ne leur sera jamais remis.

Autre variante de cette fraude : le consommateur reçoit un message d'un ami sur les médias sociaux. Celui-ci lui dit avoir gagné un prix et lui demande s'il a déjà reçu le sien puisque son nom figure aussi sur la liste des gagnants. L'ami l'encourage à communiquer avec la personne responsable de la remise des prix. Malheureusement, ce que la victime ne sait pas, c'est que le compte de son ami a été compromis et qu'elle communique avec le fraudeur depuis le début.

Indices – Comment vous protéger

- Ne divulguez jamais de renseignements personnels ou financiers à des inconnus.
- La seule façon de participer à une loterie à l'étranger est de vous rendre au pays visé et d'acheter un billet en personne. Un billet de loterie ne peut pas être acheté en votre nom.
- Au Canada, si vous gagnez à une loterie, vous n'avez aucune taxe et aucuns frais à payer.
- Il ne faut jamais, sous aucun prétexte, envoyer ou accepter de l'argent. Vous pourriez, sans le savoir, participer à des activités de blanchiment d'argent, ce qui constitue une infraction criminelle.

12) Vol et fraude d'identité

Une personne victime de fraude d'identité a aussi déjà été victime de vol d'identité.

Il y a vol d'identité lorsque les renseignements personnels d'une personne sont volés ou compromis. Cela peut se produire si la personne donne volontairement des renseignements personnels ou financiers, si elle est victime d'hameçonnage, si elle se fait voler son portefeuille, s'il y a intrusion dans une base de données, etc.

La fraude d'identité survient lorsque le fraudeur utilise les renseignements de la victime à des fins frauduleuses. Il peut créer de faux documents d'identité, présenter des demandes de crédit non autorisées et ouvrir des comptes bancaires sous son nom, rediriger son courrier, acheter des cellulaires, prendre le contrôle de ses comptes financiers et de médias sociaux, etc.

Si vous êtes victime de vol ou de fraude d'identité, prenez immédiatement les mesures suivantes :

- **1** : Rassemblez toute l'information sur la fraude.
- **2** : Communiquez avec les deux principales agences d'évaluation du crédit pour obtenir une copie de votre rapport de solvabilité et examinez-le.
    - **Equifax Canada** : https://www.consumer.equifax.ca/personnel/, 1-800-465-7166
    - **TransUnion Canada** : https://www.transunion.ca/fr, 1-877-525-3823
- **3** : Signalez l'incident au service de police local.
- **4** : Signalez l'incident au CAFC au moyen du Système de signalement des fraudes (SSF) ou en composant le 1-888-495-8501 (sans frais).
- **5** : Examinez vos relevés de compte et signalez toute activité suspecte à l'organisme visé.
- **6** : Informez votre institution financière et la société émettrice de votre carte de crédit et modifiez le mot de passe de vos comptes en ligne.
- **7** : Si vous soupçonnez que votre courrier a été redirigé, communiquez avec Postes Canada (https://www.canadapost.ca/cpc/fr/home.page, 1-866-607-6301) et vos fournisseurs de services.
- **8** : Informez les organismes fédéraux qui délivrent des pièces d'identité :
    - **Service Canada** : www.servicecanada.gc.ca, 1-800-622-6232
    - **Passeport Canada** : https://www.canada.ca/fr/immigration-refugies-citoyennete/services/passeports-canadiens.html, 1-800-567-6868
    - **Immigration, Réfugiés et Citoyenneté Canada** : www.cic.gc.ca, 1-888-242-2100
- **9** : Informez les organismes provinciaux qui délivrent des pièces d'identité.

13) Principales méthodes de communication utilisées par les fraudeurs

Les fraudeurs utilisent tous divers outils pour parvenir à leurs fins. Pour commettre une fraude, ils ont besoin d'un moyen de communiquer avec leurs victimes potentielles et d'un système leur permettant de recevoir des paiements de celles-ci.

Pour vous aider à mieux prévenir la fraude dès le début, voici les principales méthodes de communication employées par les fraudeurs et les pratiques exemplaires à adopter.

Fraude téléphonique

Le téléphone a été inventé pour permettre aux gens de communiquer instantanément les uns avec les autres sans avoir à se trouver dans la même pièce. Au cours des 150 dernières années, le téléphone a évolué pour devenir le dispositif mobile actuel qui tient dans votre poche et vous permet d'effectuer des appels partout dans le monde. En 2019, en bonne partie en raison des avancées technologiques, les appels téléphoniques étaient la principale méthode de communication utilisée par les fraudeurs.

Appels à composition automatique : Un appeleur automatique est un dispositif ou un logiciel qui compose automatiquement des numéros de téléphone. Ces numéros proviennent habituellement de grandes listes. Dès qu'une personne répond à l'appel, l'appeleur automatique fait jouer un message enregistré ou achemine l'appel à un « agent ». Ces systèmes peuvent être utilisés par des centres d'appels légitimes ou frauduleux. Les fraudeurs peuvent se servir de listes de numéros de téléphone (obtenues légalement ou non) ou régler l'appeleur pour qu'il compose toutes les configurations possibles de numéros de téléphone dans une région donnée.

Appels automatisés : Il s'agit d'un appel qui s'effectue au moyen d'un appeleur automatique pour diffuser un message préenregistré. Dans ce message, on peut entendre une voix informatisée/robotisée ou la voix d'une vraie personne. Au Canada, il n'y a pas de lois qui interdisent les appels automatisés, mais ceux-ci sont assujettis aux règlements du Conseil de la radiodiffusion et des télécommunications canadiennes. Si vous êtes inscrit sur la **Liste nationale des numéros de télécommunication exclus** (LNNTE), cela devrait éliminer beaucoup d'appels non sollicités. Les consommateurs qui s'inscrivent sur la LNNTE peuvent décider s'ils veulent recevoir des appels de télémarketing ou non. Voici les organismes qui bénéficient d'exemptions et peuvent toujours faire des appels impromptus : organismes de bienfaisance canadiens enregistrés, partis politiques, personnes qui recueillent de l'information dans le cadre d'un sondage, journaux pour des sollicitations d'abonnements et organisations avec lesquelles vous avez déjà une

relation d'affaires. Si le message enregistré que vous entendez ne provient pas d'organismes exemptés, il s'agit fort probablement d'un appel frauduleux.

Falsification des données de l'appelant : L'afficheur ou le dispositif d'identification de l'appelant indique habituellement le numéro de téléphone et le nom de la personne associée à la ligne utilisée pour vous téléphoner. Il existe plusieurs raisons légitimes de modifier l'information qui figure sur l'afficheur. Malheureusement, il y a autant de raisons illégitimes pour lesquelles les fraudeurs manipulent l'information affichée. Voici l'information trompeuse la plus souvent utilisée pour amener les Canadiens à répondre à des appels : indicatif régional identique à celui de la personne appelée pour donner l'impression qu'il s'agit d'un appel local, numéro de téléphone correspondant à celui de la personne appelée, numéro de téléphone reconnu d'un organisme précis (p. ex. service de police ou organisme gouvernemental) ou un numéro de téléphone qui ne peut être composé.

Déconnexion retardée : (Ne s'applique qu'aux lignes terrestres.) Pour tenter de légitimer leur appel, les fraudeurs vous demandent parfois de raccrocher et de composer immédiatement le numéro inscrit au dos de votre carte ou un autre numéro qu'ils vous fournissent. Lorsque vous composez ce numéro, la personne à qui vous parliez vous répond presque instantanément parce que la communication initiale n'a jamais été rompue.

Comment vous protéger contre la fraude téléphonique

- Inscrivez gratuitement votre numéro de téléphone sur la Liste nationale des numéros de télécommunication exclus du Canada au https://lnnte-dncl.gc.ca/fr.
- Si vous n'attendez pas d'appel ou ne reconnaissez pas le numéro affiché, laissez votre boîte vocale répondre à l'appel.
- L'identification de l'appelant peut être falsifiée. Ne présumez pas que l'information est authentique.
- Si vous répondez au téléphone et qu'il s'agit d'un message enregistré, raccrochez. N'appuyez pas sur le 1 et ne rappelez pas.
- Lorsqu'on vous demande de faire un autre appel, attendez quelques minutes après avoir raccroché ou utilisez un autre téléphone pour effectuer l'appel.
- Ne fournissez jamais de renseignements personnels ou financiers au téléphone à moins d'être l'auteur de l'appel.
- Il ne faut jamais se sentir obligé de transmettre des renseignements personnels ou financiers au téléphone.

- Posez des questions. Si l'appelant ne peut pas ou ne veut pas y répondre, raccrochez.
- Si vous avez encore des doutes quant à l'appel, parlez-en à quelqu'un.

Fraude par courriel ou message texte

Les consommateurs sont de plus en plus accessibles aux fraudeurs parce qu'ils reçoivent des courriels et des messages textes sur leurs cellulaires, appareils qu'ils ont toujours avec eux. Même si les appels téléphoniques demeurent la méthode de communication la plus utilisée par les fraudeurs, les consommateurs sont beaucoup plus souvent victimes de fraudes par courriel et messages textes.

Falsification des données de l'expéditeur : En plus de pouvoir falsifier les données de l'appelant, les fraudeurs peuvent aussi modifier l'information de l'expéditeur de courriels et de messages textes. Ils utilisent des tactiques pour afficher le nom, le numéro de téléphone ou l'adresse de courriel qu'ils veulent vous montrer. Dans les courriels, vous devriez pouvoir placer le curseur sur le nom de l'expéditeur, cliquer sur répondre ou voir les propriétés du courriel pour découvrir l'adresse de courriel réelle.

Automatisation : Les courriels et messages textes automatisés ou programmés visent à aider les entreprises à gagner du temps en communiquant rapidement et simultanément avec leurs contacts. Les fraudeurs utilisent les mêmes applications et services pour envoyer instantanément un message à une liste de contacts. Ils peuvent choisir les destinataires, décider du moment pour envoyer les messages et même les personnaliser en fonction de l'information recueillie auparavant. Les fraudeurs peuvent aussi créer des courriels de réponse automatique pour l'envoi différé de messages lorsque les consommateurs donnent suite à leur message initial.

Compte de courriel compromis : Lorsque les fraudeurs accèdent à des comptes de courriel, ils peuvent se faire passer pour la victime pour tenter de commettre une fraude. S'ils ont accès à des comptes de consommateurs, ils peuvent envoyer un courriel à tous leurs contacts et prétexter une urgence pour leur demander de l'argent. S'ils ont accès à des comptes d'entreprises, ils peuvent créer une règle pour qu'une copie de tous les courriels entrants soit transmise à leur propre compte de courriel. Ils examinent l'information et se font passer pour l'entreprise au moment voulu. Ils peuvent envoyer de nouveau une facture à des clients et leur demander d'effectuer le paiement dans un « nouveau » compte bancaire. Les fraudeurs peuvent

aussi se faire passer pour un cadre et demander à des employés d'effectuer un paiement pour diverses raisons. La réussite de ces fraudes dépend de la capacité des fraudeurs de tromper les victimes.

Comment vous protéger contre la fraude par courriel et message texte

- La *Loi canadienne anti-pourriel* (LCAP) protège les consommateurs et les entreprises contre le mauvais usage de la technologie numérique, ce qui comprend les pourriels et d'autres menaces électroniques. Vous pouvez signaler un pourriel à l'adresse suivante : https://www.fightspam.gc.ca/eic/site/030.nsf/frm-fra/MMCN-9EZV6S.
- Méfiez-vous des courriels et des messages textes non sollicités. Supprimez-les.
- N'ouvrez pas les messages qui semblent provenir d'entreprises ou d'organisations avec lesquelles vous ne faites pas déjà affaire.
- La majorité des entreprises et des organisations utilisent des domaines personnalisés dans leurs adresses de courriel, tandis que celles des fraudeurs renferment des domaines facilement accessibles et gratuits (p. ex. @outlook, @hotmail, @gmail, @yahoo, @me, etc.).
- Prenez le temps de vérifier l'adresse de courriel de l'expéditeur en passant le curseur sur son nom ou sur l'adresse de courriel visible. Les fraudeurs achètent parfois des domaines très semblables à des domaines légitimes. Ce peut être aussi simple qu'un « m » qui est changé pour « rn ».
- Les courriels ou messages textes ayant un caractère urgent sont une bonne indication de fraude.
- Vérifiez si le message renferme des fautes d'orthographe et de grammaire, des expressions qui clochent ou des éléments associés à l'image de marque qui ne sont pas tout à fait exacts.
- Ne cliquez pas sur des liens ou des pièces jointes si vous n'êtes pas certain de l'identité de l'expéditeur.
- Si vous avez cliqué sur un lien et qu'on vous demande des renseignements personnels ou financiers, ne le faites pas. Fermez la page et effectuez un balayage rigoureux sur votre appareil.
- Les institutions financières et organismes gouvernementaux ne demandent jamais des renseignements personnels ou financiers par courriel ou message texte.
- Si le message semble provenir de l'un de vos contacts, mais que quelque chose cloche ou semble trop beau pour être vrai, communiquez avec cette personne en utilisant un autre moyen de communication.

Fraude en ligne

Internet est un réseau de dispositifs électroniques qui s'étend dans le monde entier. Il est facile de s'y brancher et, une fois en ligne, il est possible d'accéder à presque n'importe quel renseignement ou de communiquer avec n'importe qui qui utilise Internet. Il s'agit du lieu de travail idéal pour les fraudeurs.

Référencement naturel : Au moment de chercher de l'information, bien des consommateurs utilisent un moteur de recherche populaire pour trouver rapidement des réponses. Il arrive souvent que les fraudeurs paient pour que leur information ou leurs sites Web figurent parmi les premiers résultats obtenus.

Fenêtres contextuelles : Les fenêtres contextuelles sont utilisées pour attirer votre attention et sont considérées comme étant des sources de distraction et d'irritation. Il existe quelques variantes : celles qui apparaissent par-dessus votre page actuelle (*pop-overs*), celles qui vous redirigent vers une nouvelle fenêtre ou un nouvel onglet, et celles qui ouvrent une nouvelle fenêtre ou un nouvel onglet sans vous sortir de votre page actuelle (*pop-unders*). Il y a trois facteurs qui entraînent l'ouverture d'une fenêtre contextuelle : le temps (fenêtre conçue pour apparaître lorsque vous cliquez sur un élément et que la minuterie réglée en arrière-plan s'est écoulée); le comportement (fenêtre qui s'affiche lorsque des conditions précises sont remplies); et la fermeture d'un navigateur ou la consultation d'un site Web différent.

Petites annonces en ligne : Bien des fraudeurs sont présents sur ces sites populaires pour la chasse aux aubaines. Ils créent diverses annonces (pour des animaux, des logements à louer, des véhicules, etc.) dans lesquelles tout est offert à prix réduit. Ils peuvent aussi communiquer avec des consommateurs pour leur indiquer qu'ils sont intéressés à acheter leur *article* et offrent de payer plus que le prix demandé. Dans certains cas, ils peuvent prendre le contrôle du compte de la victime ou offrir de faux emplois pour que d'autres personnes publient des annonces pour eux.

Faux sites Web : Il peut être rapide et facile de créer un site Web, mais celui-ci pourrait ne pas être en ligne longtemps s'il est signalé comme étant frauduleux. Les fraudeurs créent des sites Web pour bon nombre de fraudes. Ceux-ci sont conçus pour inspirer confiance et donner de la légitimité à l'information fournie. Les fraudeurs achètent parfois un certificat pour passer leur site en https, ce qui indique qu'il est sécurisé lors de la transmission d'information. Ils peuvent aussi acheter des noms de domaines qui

ressemblent beaucoup à des marques légitimes, surtout s'ils prétendent être affiliés à une entreprise ou s'ils cherchent à vendre des marchandises contrefaites.

Fausse information : Les fraudeurs créent des comptes et des sites Web en se servant d'information, de photos de personnes ou de marchandises et de logos volés.

Cartes de crédit volées : Les fraudeurs font des achats en ligne au moyen de cartes de crédit volées.

Comment vous protéger en ligne

- Avant de vous connecter à Internet, assurez-vous d'activer les paramètres de sécurité de base sur votre appareil.
- N'accédez pas à des comptes protégés par un mot de passe et ne transmettez pas de renseignements personnels et financiers lorsque vous êtes connecté à un réseau Wi-Fi public.
- La navigation privée ou incognito devrait désactiver l'historique de navigation, l'historique de recherche, l'historique de téléchargement, les témoins et les fichiers Internet temporaires.
- Désactivez les témoins et supprimez votre historique de navigation lorsqu'ils ne sont pas nécessaires.
- Utilisez un moteur de recherche qui ne recueillent pas vos renseignements personnels, n'enregistre pas votre historique de recherche et n'effectue pas le suivi de vos activités de navigation privée.
- Évitez de sélectionner des résultats commandités (payés) après avoir effectué une recherche en ligne.
- Vérifiez si les coordonnées que vous avez trouvées sont valables en menant une autre recherche sur l'information elle-même.
- Aucune entreprise de technologie ou de sécurité ne vous mettra en garde contre un virus ou un maliciel et ne vous demandera de communiquer avec elle pour la solution.
- La façon la plus sécuritaire de fermer une fenêtre contextuelle est de le faire dans votre gestionnaire de tâches. À l'ordinateur, appuyez sur les touches Ctrl + Alt + Del, sélectionnez Ouvrir le Gestionnaire des tâches, trouvez l'application voulue puis cliquez sur Fin de tâche.
- Si vous êtes incapable de fermer la fenêtre contextuelle, forcez la fermeture de votre appareil.
- Faites régulièrement une recherche de virus ou de maliciel sur vos appareils.
- Gardez vos logiciels à jour.

- Si vous faites un achat en ligne, rencontrez le vendeur en personne pour bien inspecter le produit avant d'effectuer votre paiement.
- Si un site d'achats et de ventes offre des options de clavardage et de paiement sécuritaires, n'hésitez pas à les utiliser pour tirer profit des programmes de protection disponibles. Si on vous demande de poursuivre la conversation ailleurs ou d'utiliser un autre mode de paiement pour éviter des frais, soyez prudent.
- Méfiez-vous des messages non sollicités qui vous demandent de confirmer les renseignements de votre compte, votre mot de passe et des renseignements personnels ou financiers.
- Renseignez-vous sur les fraudes courantes dans les petites annonces.
- Signalez toute annonce ou message frauduleux au propriétaire du site Web.
- Si c'est trop beau pour être vrai, il s'agit probablement d'une escroquerie.
- Lorsque vous visitez un site Web, portez attention à la barre d'adresse.
- Il n'est pas garanti qu'un site Web dont l'adresse débute par « https:// » n'est pas frauduleux, mais il s'agit tout de même de quelque chose qu'il faut surveiller.
- Consultez le site https://www.whois.net pour trouver de l'information sur l'enregistrement d'un domaine. Méfiez-vous des sites Web récents, car les faux sites Web ont tendance à être actifs seulement pour peu de temps.
- Il faut se méfier des sites qui renferment des erreurs de grammaire et d'orthographe.
- Cherchez des coordonnées fiables (numéro de téléphone, adresse de courriel, adresse physique).
- Lisez bien les commentaires avant de faire un achat.
- Utilisez une carte de crédit reconnue lorsque vous achetez en ligne, car les sociétés qui émettent ces cartes offrent les meilleurs programmes de protection contre la fraude.
- Méfiez-vous des commandes en ligne pour lesquelles on demande la livraison urgente et dont l'adresse postale diffère de l'adresse d'expédition.
- N'acceptez jamais de prélever un montant plus élevé que le prix demandé et d'envoyer la différence à une tierce partie.

Fraude sur les médias sociaux

Les médias sociaux ont été créés pour permettre aux utilisateurs de produire et d'échanger du contenu, et de faire du réseautage social. Au Canada, les dix sites Web ou applications les plus utilisés sont Facebook, YouTube, Instagram, Pinterest, Twitter, Snapchat, LinkedIn, Reddit, Twitch et Tumblr. Les sites Web et applications de rencontre font aussi partie de cette méthode de communication.

Faux comptes : Les fraudeurs créent habituellement leurs comptes au moyen d'information et de photos volées d'autres personnes. Tout récemment, Facebook a annoncé avoir supprimé 2,19 milliards de faux comptes de sa plateforme entre janvier et mars 2019[1].

Robots sur les médias sociaux : Ce type de robot utilise de faux comptes pour générer automatiquement des messages précis et amplifier ceux-ci, comme des publicités et de fausses critiques (ce qu'on appelle aussi l'*astroturfing*, ou la désinformation populaire planifiée). Ces robots servent surtout à créer des profils de personnes capables d'influencer les gens. Puisqu'ils sont automatisés, ces robots fonctionnent jour et nuit.

Comptes compromis : Lorsqu'un fraudeur accède à un compte de médias sociaux, il obtient aussi toute l'information qui y est associée. S'il découvre de l'information ou des photos compromettantes de la victime, il peut lui faire du chantage. Il y a des chances qu'il se fasse passer pour elle pour tenter de commettre des fraudes. Il peut envoyer des messages aux contacts de la victime pour les informer qu'il a repéré leur nom sur une liste de gagnants d'un concours ou pour leur demander de l'argent en prétextant une urgence. Il peut aussi se servir de ce compte pour publier de fausses annonces.

Annonces : Les fraudeurs savent que les gens passent beaucoup de temps sur les médias sociaux et placent des annonces pour des essais gratuits, de la marchandise à prix réduit ou de fausses possibilités d'emploi. Ils peuvent aussi utiliser des noms et des photos de personnes ou d'entreprises bien connues pour falsifier des témoignages publicitaires.

[1] https://fbnewsroomus.files.wordpress.com/2019/05/cser-press-call-5.23.19.pdf

Comment vous protéger contre la fraude sur les réseaux sociaux

- N'acceptez pas de demandes d'abonnement de personnes que vous ne connaissez pas. Vous ne savez pas si elles ont des intentions malveillantes.
- Méfiez-vous des personnes dont les photos de profil semblent parfaites.
- Faites une recherche inversée d'images pour voir si la même photo est utilisée ailleurs en ligne. https://images.google.com et https://tineye.com sont d'excellentes options.
- Posez des questions précises et recherchez les incohérences dans les réponses.
- Méfiez-vous des personnes qui ont toujours une excuse pour ne pas pouvoir vous rencontrer en personne.
- N'envoyez jamais d'argent à une personne que vous n'avez jamais rencontrée.
- Méfiez-vous des profils qui n'ont pas beaucoup d'abonnés ou d'amis.
- Si une personne vous harcèle ou vous menace, supprimez-la de vos abonnés, bloquez-la et signalez son compte.
- Voici quelques indices pour repérer d'autres faux comptes : ils comptent un grand nombre d'abonnés mais l'engagement est faible, le taux d'engagement augmente trop rapidement, ils ont un grand nombre d'abonnés mais très peu de publications, ils ont atteint le nombre maximal d'abonnés, ou ils ne diffusent que du contenu indésirable.
- Si un compte ne fait que fournir de l'information et ne participe à aucun échange, c'est probablement un robot qui est à l'origine de celui-ci.
- Faites attention aux formulations ou aux messages qui semblent artificiels.
- Ne cliquez pas sur des liens suspects.
- Réglez les paramètres de sécurité de vos comptes sociaux à une option plus restreinte.
- N'échangez pas trop d'information de nature délicate (renseignements personnels ou financiers, absences prévues, etc.).
- Sachez que ce que vous publiez en ligne restera toujours en ligne.
- Ne donnez pas vos identifiants de connexion à personne.
- Utilisez une phrase passe ou un mot de passe fort pour protéger votre compte.
- N'oubliez pas de fermer votre session quand vous avez terminé.
- Protégez votre compte et votre appareil en mettant régulièrement à jour vos logiciels et vos applications.

Fraude par courrier ou en personne

La fraude par courrier ou en personne est probablement la forme la plus ancienne de fraude puisque ces méthodes de communication existent depuis des milliers d'années.

Modèles personnalisés : Les fraudeurs utilisent des modèles de lettres depuis longtemps; ils ne font que modifier le nom de famille dans l'appel et quelques autres petits détails. Dans un message type, le fraudeur informe le destinataire qu'une personne ayant le même nom de famille est décédée et a laissé des millions dans un compte bancaire. Si l'expéditeur et le destinataire collaborent, ils peuvent se partager l'argent. Dans un autre message type, le fraudeur annonce au destinataire qu'il a remporté un gros lot ou un prix important.

Timbres : Les fraudeurs doivent trouver une façon de livrer leurs lettres. Chaque année, les faux timbres coûtent jusqu'à 10 millions de dollars à Postes Canada. Les fraudeurs achètent des rouleaux de timbres légitimes de Postes Canada, mais ils les paient au moyen de cartes de crédit volées.

Vignettes frauduleuses : Les fraudeurs ont aussi recours à des vignettes postales d'entreprises pour la livraison de leur courrier. Ces vignettes *prépayées* indiquent le nom du service et le numéro du client.

Employés : Les fraudeurs qui font du porte-à-porte prétendent souvent être des employés ou des étudiants. Ils portent parfois un uniforme et ont fréquemment une carte d'identité et une planchette à pince.

Vente sous pression : Les fraudeurs offrent souvent des produits et des services dont vous n'avez pas besoin. Ils peuvent vous dire que selon leur inspection, il y a un danger pour votre santé. Ils prétendent vous pourrez vous faire rembourser la majeure partie du montant du devis qu'ils vous ont présenté dans le cadre d'un programme gouvernemental. Lorsqu'ils vous donnent leur prix final, ils vous disent que celui-ci est fortement réduit et que l'offre est valable que tant qu'ils sont là.

Comment vous protéger contre la fraude par courrier et en personne

- Vous pouvez réduire le montant d'offres de marketing que vous recevez par la poste en vous inscrivant au Service d'interruption de sollicitation de

l'Association canadienne du marketing (https://www.the-cma.org/french/information-des-consommateurs). Votre nom restera sur la liste pendant six ans.

- Vous ne pouvez pas remporter un concours, une loterie ou un tirage si vous n'y avez pas participé.
- Vous ne pouvez pas jouer à la loterie d'un autre pays sans d'abord acheter un billet dans ce pays.
- Ne donnez pas suite aux offres d'essais gratuits, de prix ou d'emplois qui exigent que vous fassiez un paiement à l'avance.
- Les gagnants n'ont jamais à payer des frais pour récolter leur prix. Les frais sont plutôt déduits du montant total des gains.
- Au Canada, les règles qui s'appliquent aux testaments varient d'une province à l'autre; toutefois, il incombe à l'exécuteur testamentaire d'informer les bénéficiaires.
- Une succession légitime ne cherche pas à trouver des héritiers.
- Ne donnez pas suite aux demandes où on vous demande de l'aide pour effectuer des déplacements de fonds importants dans un autre pays.
- Jetez les envois dans lesquels on vous offre un pourcentage d'une soi-disant fortune en échange de renseignements financiers.
- Vérifiez que le chèque reçu n'est pas contrefait avant de le déposer dans votre compte bancaire. Si possible, communiquez avec le titulaire du compte inscrit sur le chèque.
- En Alberta et en Ontario, la vente à domicile non sollicitée de produits énergétiques est interdite. Dans bien d'autres provinces, les vendeurs itinérants ou directs doivent avoir un permis.
- Installez une caméra de surveillance près de votre entrée pour dissuader les criminels.
- Avant d'inviter une personne chez vous ou d'écouter une offre de vente, demandez-lui de produire une pièce d'identité avec photo et de vous donner son nom ainsi que le nom et les coordonnées de l'entreprise qu'elle représente.
- Si vous demandez au vendeur de partir, il doit quitter immédiatement. Si vous ne vous sentez pas en sécurité, appelez votre service de police local.
- Ne vous fiez pas à l'opinion d'une personne vous disant que quelque chose dans votre maison n'est pas sécuritaire ou doit être remplacé. Obtenez un deuxième avis.
- Avant de signer quoi que ce soit, assurez-vous d'avoir toutes les réponses à vos questions par écrit.

- Vous n’êtes jamais obligé de signer un contrat sur-le-champ.
- Les lois provinciales sur la protection des consommateurs comprennent souvent une période de réflexion où les consommateurs peuvent annuler un contrat signé à leur domicile jusqu’à dix jours suivant la réception d’une copie de l’entente signée. Le contrat doit comprendre des renseignements précis sur les biens ou services et vos droits en tant que consommateur. Si ce n’est pas le cas, vous avez jusqu’à un an après avoir signé le contrat pour l’annuler. Vous pouvez aussi l’annuler, peu importe sa valeur, jusqu’à un an après l’avoir signé, si l’entreprise ou le vendeur avec qui vous l’avez signé a délibérément fait une déclaration inexacte ou trompeuse au sujet du contrat.
- Si vous croyez qu’une entreprise a enfreint la loi en ce qui concerne le contrat signé à votre domicile, communiquez avec le bureau de la protection des consommateurs de votre région.

14) Principales méthodes de paiement utilisées par les fraudeurs

En 2020, voici les méthodes de paiements les plus utilisées par les fraudeurs :

Virement télégraphique

Un virement télégraphique est un transfert de fonds par voie électronique entre des institutions financières du monde entier. Pour effectuer un virement, il faut que l'expéditeur et le destinataire aient tous deux un compte bancaire. Les fraudeurs peuvent prendre le contrôle du compte d’une autre personne pendant quelques jours ou ouvrir un compte au moyen de pièces d’identité volées. Les virements télégraphiques sont utiles car l’argent est déplacé en très peu de temps (dans les 72 heures). Le gros risque, c’est que le destinataire retire l’argent que vous envoyez et que vous vous rendez compte que c’est une fraude seulement quand il est trop tard. Vous devez toujours savoir à qui vous envoyez de l’argent. Si vous devez annuler un virement télégraphique, communiquez avec l’institution financière remettante le plus tôt possible.

Cryptomonnaie

La cryptomonnaie est la forme la plus récente de monnaie numérique ou virtuelle. Les opérations de cryptomonnaie fonctionnement indépendamment d'une institution financière centrale et ne sont actuellement pas réglementées au Canada. Il existe de nombreux types de cryptomonnaies, mais le plus reconnu est le bitcoin. Même si de plus en plus de commerces acceptent les cryptomonnaies en guise de paiement, ce

n’est pas le cas pour les organismes gouvernementaux. Si vous déposez de l’argent dans un guichet automatique de bitcoins à la suite d’une demande frauduleuse, retournez au guichet automatique et communiquez immédiatement avec le propriétaire. Dans certains guichets, les dépôts sont différés.

Carte de crédit

Les cartes de crédit peuvent être utilisées frauduleusement de différentes façons. Les fraudeurs peuvent se servir d’une carte de crédit volée pour faire plusieurs petits achats en peu de temps en exploitant la fonction « taper et payer » de la carte physique. Si l’information sur la carte est compromise (nom du titulaire, numéro de la carte, date d’expiration et code CVC), les fraudeurs peuvent se faire passer pour vous afin de réaliser des achats sans carte, ou des commerçants frauduleux peuvent porter des transactions non autorisées à votre compte. Il est important d’utiliser une carte de crédit reconnue lorsque vous achetez de la marchandise en ligne, car les principales cartes de crédit offrent une plus grande protection des achats. Si vous avez reçu un produit contrefait ou de qualité inférieure, un produit autre que celui acheté ou rien du tout, contestez tous les frais qui s’y rapportent auprès de la société émettrice de votre carte de crédit.

Les victimes de fraude d'identité peuvent avoir plusieurs cartes de crédit non autorisées émises à leur nom. Ces victimes ne sont pas responsables des dettes qui sont directement liées à la fraude d’identité.

Chèque/mandat ou traite bancaire

Les fraudeurs demandent aux victimes de faire un chèque et de l’envoyer par la poste. Il est probable que l’argent sera ensuite envoyé à une mule. Celle-ci transfert l’argent à d’autres personnes (autrement elle blanchit l’argent). Une mule peut être un membre d’un réseau de fraude qui agit de son plein gré ou une victime sans méfiance qui suppose qu’elle reçoit de l’argent dans le cadre d’un emploi, d’un prix ou même au nom d’un « ami ».

Carte-cadeau prépayée

Les cartes-cadeaux prépayées sont un moyen populaire et pratique de donner un cadeau à une personne. Elles servent de cadeau et non de paiement. C’est pourquoi toute demande de paiement par carte-cadeau est toujours une fraude. Le plus souvent, les fraudeurs se font passer pour des représentants d’organismes gouvernementaux, de services de police ou de fournisseurs de services lorsqu’ils font ces demandes. Les cartes les plus convoitées sont celles d’Amazon, d’Apple iTunes, de

Google Play et de Steam. Les fraudeurs n'ont pas besoin des cartes physiques pour accéder aux fonds. Ils ont simplement besoin du code à l'arrière de la carte et pour l'obtenir, il suffit de gratter la bande de protection qui le recouvre. Une fois que la carte a été utilisée ou que le code à l'arrière a été gratté, vous ne pouvez plus vous faire rembourser. Pour signaler la fraude ou tenter de récupérer votre argent, composez le numéro à l'arrière de la carte.

Virement de fonds par courriel

Comme pour les virements télégraphiques, les virements de fonds par courriel se font entre deux comptes bancaires. L'expéditeur effectue le transfert dans son compte bancaire en ligne et n'a besoin que du courriel ou du numéro de cellulaire du destinataire. Les fonds sont instantanément prélevés du compte de l'expéditeur et déposés dans le compte du destinataire dès qu'il répond à la question de sécurité. Il est important de créer une réponse difficile à deviner que vous ne donnez qu'au destinataire. Les fonds peuvent être déposés sans délai si le destinataire a la fonction de dépôt direct dans son compte. Les virements de fonds par courriel peuvent être annulés ou renversés, mais seulement avant que les fonds soient déposés.

Argent comptant

Qu'il soit donné en personne ou envoyé par la poste, l'argent comptant remis à un fraudeur n'est pas remboursable. Si vous l'envoyez par la poste, le fraudeur peut vous demander de le cacher dans un livre ou un magazine. Si vous avez envoyé de l'argent par la poste à la suite d'une fraude, communiquez immédiatement avec l'entreprise de messagerie et fournissez-lui le numéro de suivi pour tenter de récupérer le colis.

Entreprise de transfert de fonds

Les entreprises de transfert de fonds (comme MoneyGram et Western Union) facilitent les virements de fonds entre des particuliers ou des organisations en l'espace de quelques minutes. Les expéditeurs peuvent payer pour le virement en ligne ou en magasin, et les fonds peuvent être envoyés dans un compte bancaire ou remis au destinataire en argent comptant à n'importe quel commerce de détail partout dans le monde. Le fraudeur n'a besoin que d'une pièce d'identité pour récupérer l'argent en personne.

Toutes les victimes doivent signaler et contester les transactions frauduleuses auprès du commerce, de l'organisation ou de l'institution financière qui a facilité le paiement. Suivez le processus de résolution approprié le plus tôt possible, car pour certains, les délais sont serrés. Le dédommagement n'est jamais garanti.