CENTRE ANTIFRAUDE DU CANADA

Gendarmerie royale du Canada | Royal Canadian Mounted Police | Bureau de la concurrence Canada | Competition Bureau Canada | Police Provinciale de l'Ontario | Canada


# MONTRE-MOI LA FRAUDE

Trousse de prévention de la fraude 2022

Royal Canadian Mounted Police | Gendarmerie royale du Canada | Competition Bureau Canada | Bureau de la concurrence Canada | Ontario Provincial Police | Canada

# 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 (#MPF2022). Nous publierons notre bulletin chaque semaine sur Facebook et Twitter.

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

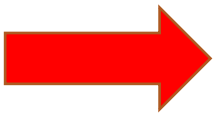
Merci,

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**
Tout au long du mois de Mars, le CAFC publiera un bulletin à chaque semaine qui mettra en vedette les fraudes les plus signalées au CAFC en 2021 reliées à l'usurpation d'identité.

**Bulletins :**
**Semaine 1** : Investissements
**Semaine 2** : Extorsion et Besoin urgent d'argent
**Semaine 3** : Hameçonnage
**Semaine 4** : Harponnage

Le CAFC attirera l'attention des abonnés de ses comptes de réseaux sociaux en discutant chaque bulletin durant la semaine.

**Facebook : Centre antifraude du Canada**
**Twitter : @antifraudecan**

**Mars 2022** – Un vidéo de lancement du #MPF2022 sera partagé sur les médias sociaux pour mettre en vedette les façons de vous protéger contre être victime.

## Mars 2022

| | | | | |
|---|---|---|---|---|
| | **Mardi 1er mars**<br>Facebook et Twitter : #MPF2022 Introduction et lancement | **Mercredi 2 mars**<br>Facebook et Twitter #MPF2022 Vidéo de lancement | **Jeudi 3 mars**<br>Bulletin Facebook et Twitter – Arnaques d'investissement | **Vendredi 4 mars**<br>Facebook et Twitter Médias sociaux Usurpation d'identité Arnaques d'investissement |
| **Lundi 7 mars**<br>Facebook et Twitter Faux sites Web d'investissement dans la cryptomonnaie | **Mardi 8 mars**<br>Facebook et Twitter Diffusion de messages #MPF2022 de partenaires | **Mercredi 9 mars**<br>Facebook et Twitter Demande de transfert d'investissements de cryptomonnaie vers des plateformes frauduleuses | **Jeudi 10 mars**<br>Facebook et Twitter Diffusion de messages #MPF2022 de partenaires | **Vendredi 11 mars**<br>Facebook et Twitter Fraude pyramidale liée à l'emploi et arnaques d'investissement |
| **Lundi 14 mars**<br>Facebook et Twitter Bulletin : Stratagèmes d'extorsion | **Mardi 15 mars**<br>Facebook et Twitter Appels téléphoniques de l'ASFC automatisés et menaçants | **Mercredi 16 mars**<br>Facebook et Twitter Diffusion de messages #MPF2022 de partenaires | **Jeudi 17 mars**<br>Facebook et Twitter Diffusion de messages #MPF2022 de partenaires | **Vendredi 18 mars**<br>Facebook et Twitter Lettres de menaces faussement attribuées à la GRC |
| **Lundi 21 mars**<br>Facebook et Twitter Bulletin : Hameçonnage | **Mardi 22 mars**<br>Facebook et Twitter Diffusion de messages #MPF2022 de partenaires | **Mercredi 23 mars**<br>Facebook et Twitter Messages d'hameçonnage faussement attribués à des organismes gouvernementaux | **Jeudi 24 mars**<br>Facebook et Twitter Diffusion de messages #MPF2022 de partenaires | **Vendredi 25 mars**<br>Facebook et Twitter Messages d'hameçonnage faussement attribués à des institutions financières |
| **Lundi 28 mars**<br>Facebook et Twitter Bulletin : Harponnage | **Mardi 29 mars**<br>Facebook et Twitter Statistiques et indices de harponnage | **Mercredi 30 mars**<br>Facebook et Twitter Diffusion de messages #MPF2022 de partenaires | **Jeudi 31 mars**<br>Facebook et Twitter Comment vous protéger contre les stratagèmes de harponnage | |

## 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 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 2021, le CAFC a reçu 104,295 signalements de fraude représentant des pertes totales de plus de 379 millions de dollars.

Les 10 formes de fraude les plus signalées en 2021 :

| Type de fraude | N$^{bre}$ de signalements | N$^{bre}$ de victimes | Pertes (en $) |
|---|---|---|---|
| Extorsion | 14202 | 3160 | $18 M |
| Renseignements personnels | 7566 | 4730 | S.O. |
| Hameçonnage | 7190 | 1597 | S.O. |
| Marchandise contrefait | 5200 | 5151 | $1.1 M |
| Service | 5106 | 3223 | $11.6 M |
| Marchandise | 4994 | 4051 | $12.3 M |
| Fraude liees à la vente | 4038 | 2431 | $7.8 M |
| Emploi | 3796 | 1880 | $9.4 M |
| Investissements | 3442 | 3077 | $163.9 M |
| Enquêteur bancaire | 2212 | 734 | $4.6 M |

Les 10 formes de fraude ayant entraîné les plus importantes pertes financières en 2021 :

| Type de fraude | N^bre de signalements | N^bre de victimes | Pertes (en $) |
|---|---|---|---|
| Investissements | 3442 | 3077 | $163.9M |
| Stratagèmes de rencontre | 1928 | 1365 | $64.6 M |
| Harponnage | 1817 | 871 | $54 M |
| Extorsion | 14202 | 3160 | $18 M |
| Marchandises | 4994 | 4051 | $12.3 M |
| Service | 5106 | 3223 | $11.6 M |
| Emploi | 3796 | 1880 | $9.4 M |
| Fraude liées à la vente | 4038 | 2431 | $7.7 M |
| Prêt | 570 | 434 | $6.9 M |
| Enquêteur bancaire | 2212 | 734 | $4.6 M |

➔ 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.

- Liste de contrôle pour prévenir la fraude : 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**.

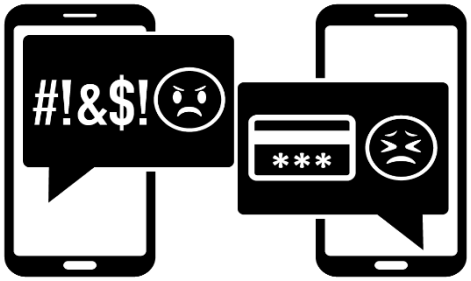
- Savez-vous vraiment qui appelle? Les fraudeurs mentent et prétendent représenter des entreprises légitimes. Ils falsifient aussi l'information que vous voyez sur l'afficheur pour vous donner l'impression que l'appel est légitime.
- Pour certains, la ligne terrestre est vitale. Pour les fraudeurs, il 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**

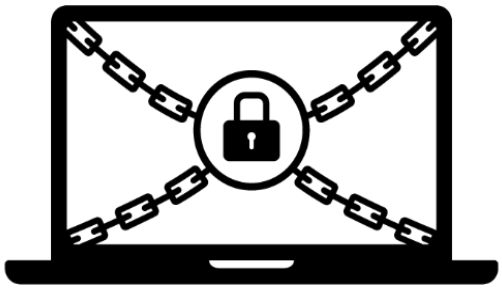
Il y a extorsion lorsqu'une personne obtient illégalement de l'argent, des biens ou des services d'une personne, d'une entité ou d'une institution par la coercition.




*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

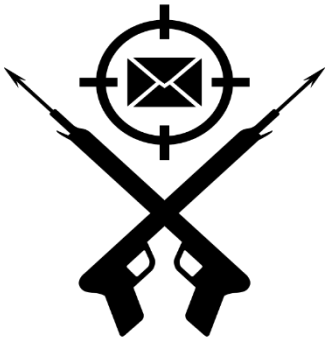
renseignements personnels et financiers pouvant être utilisés pour commettre une fraude d'identité.

**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.).

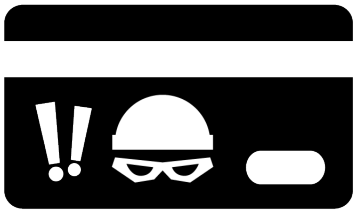
*Location immobilière* : Les fraudeurs se servent de sites de petites annonces en ligne et des réseaux de médias sociaux pour afficher des logements à louer. La propriété se situe habituellement dans un quartier recherché et le loyer demandé est inférieur aux loyers moyens sur le marché. Les personnes 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**

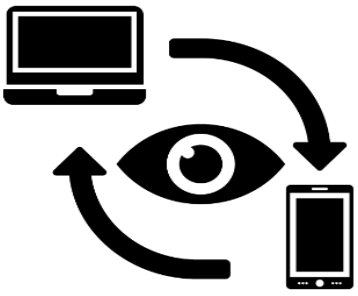
- Connaissez les indices et vérifiez toutes les commandes reçues.
- Avant d'envoyer la marchandise, vérifiez l'information fournie par le client (numéro de téléphone, adresse de courriel, adresse d'expédition, etc.).

- 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.

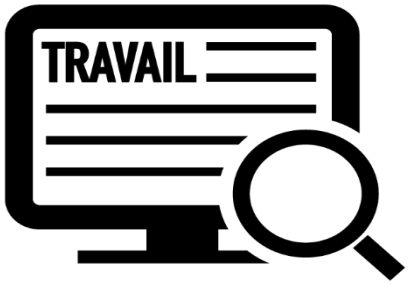
*Réparations au domicile et produits* : Les propriétaires de résidence se font offrir des services à moindre coût. Il peut s'agir de services de nettoyage de conduits, de réparation de fournaise ou de systèmes de traitement d'eau, ou de rénovations domiciliaires. Si les travaux sont effectués, ils sont 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.

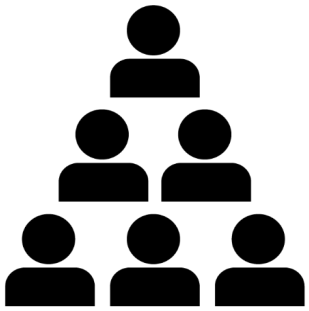
**Investissements**

Les fraudes liées à l'investissement sont les escroqueries les plus signalées, en fonction des pertes en dollars déclarées en 2021. Les victimes de ce type de fraude ont signalé des pertes totales de 169,9 millions de dollars au CAFC. 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.

*Cryptoplacements :* La majorité des fraudes liées à l'investissement qui sont signalées comprennent des placements en cryptomonnaie effectués par des Canadiens qui ont vu des annonces trompeuses. Habituellement, les victimes téléchargent une plateforme de négociation et virent de la cryptomonnaie dans leur compte de négociation. Dans la plupart des cas, les victimes sont incapables de retirer leur argent. Il est très probable que de nombreuses plateformes de négociation sont frauduleuses ou contrôlées par des fraudeurs. En plus des fraudes liées à la cryptonégociation, on signale aussi au CAFC des premières émissions de cryptomonnaie présumées frauduleuses.

*Variante des fraudes liées aux cryptoplacements :*

- On aborde la victime sur des sites de rencontre ou dans les médias sociaux. Dans certains cas, l'escroquerie commence par un stratagème de rencontre qui se transforme rapidement en une occasion de placement. Comme les suspects ont gagné la confiance de la victime, cela peut entraîner de grosses pertes financières pour la victime.
- Les victimes signalent parfois que les suspects ont compromis les comptes de leurs amis dans les médias sociaux. Comme la victime croit qu'elle

communique avec un ami ou une personne de confiance, elle se laisse facilement convaincre de profiter de l'« occasion d'investissement ».

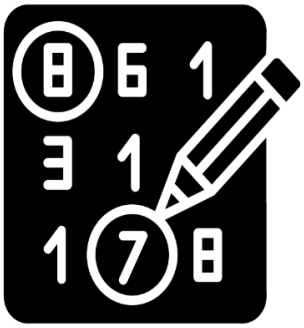
- Le suspect appelle directement la victime et la convainc d'investir dans de la cryptomonnaie. Dans bien des cas, le suspect demande à accéder à distance à l'ordinateur de la victime. Le suspect montre à la victime un site Web de cryptoplacements frauduleux, et convainc la victime d'effectuer un placement axé sur la croissance exponentielle potentielle du placement. Dans bien des cas, la victime effectue un placement à très long terme, pour finalement se rendre compte qu'elle ne peut pas retirer son argent.
- La victime reçoit un courriel qui lui offre une occasion d'investissement en cryptomonnaie.
- La victime tombe sur une annonce dans les médias sociaux. Lorsque la victime clique sur l'annonce et fournit ses coordonnées, les suspects téléphonent à la victime et la convainquent d'investir.

**Indices – Comment vous protéger**

- Soyez vigilant au moment d'envoyer de la cryptomonnaie. Une fois la transaction effectuée, il est peu probable de pouvoir l'annuler.
- Comme les produits de la criminalité et les régimes de lutte contre le blanchiment d'argent de partout dans le monde créent des cadres de réglementation qui traitent les entreprises faisant le commerce de cryptomonnaies comme des entreprises de transfert de fonds, les Canadiens doivent faire leurs recherches pour s'assurer de faire appel à des services conformes et de bonne réputation.
- Si vous recevez un message suspect d'un ami de confiance, confirmez l'envoi du message auprès de cette personne en communiquant avec elle par un autre moyen.
- Vérifiez si les entreprises de placement sont enregistrées auprès de l'agence des valeurs mobilières de votre province ou à l'aide du moteur de recherche national (http://www.sontilsinscrits.ca/).
- Avant d'investir, demandez de l'information sur l'investissement. Faites des recherches sur l'équipe responsable de l'offre et analysez la faisabilité du projet.

- Méfiez-vous d'une personne rencontrée sur un site de rencontre ou les médias sociaux qui tente de vous convaincre d'investir dans de la cryptomonnaie.
- N'envoyez pas vos placements en cryptomonnaie dans des services de négociation légitimes à d'autres adresses de cryptomonnaie.

**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.

**Liste pour se protéger contre la fraude et la cybercriminalité en 2022**

Étant donné le nombre de signalements de fraudes et d'incidents de cybercriminalité est en hausse encore cette année, le Centre antifraude du Canada (CAFC) a créé les listes de vérification suivantes pour aider les Canadiens à mieux se protéger contre la fraude et la cybercriminalité en 2021.

Protégez-vous contre la fraude

- ✓ N'ayez pas peur de dire non.
- ✓ Ne réagissez pas de manière impulsive; prenez le temps d'examiner les demandes urgentes.
- ✓ Ne vous laissez pas intimider par les tactiques de vente sous pression.
- ✓ Posez des questions et parlez de la situation à des membres de votre famille ou à des amis.
- ✓ Demandez l'information par écrit.
- ✓ En cas de doute, raccrochez.
- ✓ Méfiez-vous des demandes urgentes qui jouent sur les émotions.
- ✓ Vérifiez toujours que l'organisation avec laquelle vous faites affaire est légitime.
- ✓ Ne donnez pas de renseignements personnels.
- ✓ Méfiez-vous des appels ou des courriels non sollicités (hameçonnage) où l'on vous demande de confirmer ou de mettre à jour vos renseignements personnels ou financiers.

Protégez-vous contre la cybercriminalité

- ✓ Protégez votre ordinateur en vous assurant que votre système d'exploitation et votre logiciel de sécurité sont à jour.
- ✓ Sécurisez vos comptes en ligne, utilisez des mots de passe difficiles à deviner et, si possible, activez l'authentification à deux facteurs.
- ✓ Sécurisez vos appareils et vos connexions Internet.
- ✓ Sur certains sites Web, comme ceux où il est possible de télécharger de la musique, des jeux, des films ou du contenu réservé aux adultes, des virus ou des programmes malveillants peuvent être installés à votre insu.
- ✓ Méfiez-vous des fenêtres contextuelles ou des courriels qui renferment des fautes d'orthographe et des erreurs de mise en forme.

- ✓ Méfiez-vous des pièces jointes et des liens puisqu'ils peuvent contenir des maliciels ou des espiogiciels.
- ✓ Ne donnez jamais à quiconque accès à votre ordinateur à distance.
- ✓ Désactivez votre caméra Web ou vos dispositifs de stockage lorsque vous ne les utilisez pas.
- ✓ Si vous éprouvez des problèmes avec votre système d'exploitation, apportez-le à un technicien près de chez vous.

**Pour les entreprises**

Protégez-vous contre la fraude et la cybercriminalité

- ✓ Renseignez vos employés au sujet de la fraude et de la cybercriminalité.
- ✓ Ayez des politiques ou un plan en place pour aider les employés.
- ✓ Sachez à qui vous avez affaire. Dressez une liste des entreprises auxquelles vous faites généralement appel pour aider les employés à distinguer les vrais contacts des faux.
- ✓ Gare aux factures sur lesquelles figurent le nom d'entreprises légitimes. Les fraudeurs utilisent des noms de véritables entreprises comme les Pages jaunes pour que les factures semblent authentiques. Assurez-vous de bien examiner les factures avant d'effectuer un paiement.
- ✓ Ne donnez pas de renseignements si vous recevez un appel ou un courriel non sollicité.
- ✓ Apprenez aux employés de tous les échelons à se méfier des appels non sollicités. S'ils ne sont pas l'auteur de l'appel, ils ne devraient pas fournir ni confirmer :
    - o l'adresse de l'entreprise;
    - o le numéro de téléphone de l'entreprise;
    - o des numéros de compte;
    - o des renseignements au sujet du matériel de bureau (p. ex. marque et modèle de l'imprimante).
- ✓ Limitez les pouvoirs de vos employés en autorisant seulement quelques employés à approuver les achats et à régler les factures.
- ✓ Méfiez-vous du harponnage. Ayez des politiques en place pour confirmer verbalement les demandes urgentes de virement électronique ou d'achat.

- ✓ Examinez les commandes potentiellement frauduleuses. Méfiez-vous :
  - des commandes plus grosses que la normale;
  - des commandes multiples du même produit;
  - des commandes de gros achats;
  - des commandes payées au moyen de plusieurs cartes de crédit.
- ✓ Consultez le Guide Pensez cybersécurité pour les entreprises.