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

PERSONNES D'ÂGE MOYEN

Trousse de prévention de la fraude 2022

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 une trousse destinée aux Canadiens d'âge moyen (nés entre 1962 à 1986) afin de mieux sensibiliser le public et de réduire le nombre de victimes. Nous encourageons tous les partenaires à ajouter les documents de référence contenus dans la présente trousse à leur site Web, à leurs publications écrites et à leurs 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) Vidéos de la GRC

Le visage de la fraude (YouTube) https://www.youtube.com/watch?v=cXXP35rICQY
https://www.youtube.com/watch?v=0rlWUcc57dM (anglais)
Le cri du cœur des victimes
https://www.youtube.com/watch?v=cHZfvpH2YW8
https://www.youtube.com/watch?v=blyhHl8rc7g (anglais)
Télémarketing frauduleux : L'envers du décor
https://www.youtube.com/watch?v=XteG_fdasdw
https://www.youtube.com/watch?v=t7bhQJkelEg (anglais)

2) Vidéos de la Police provinciale de l'Ontario (OPP)

Vidéos pour le Mois de la prévention de la fraude
https://www.youtube.com/playlist?list=PLbecW3cjtFJ4gxFvi9vuGlh8hJR13y1-c
Vidéos sur les fraudes touchant les aînés
https://www.youtube.com/user/OPPCorpCommFR/search?query=fraude
https://www.youtube.com/playlist?list=PLbecW3cjtFJ6jyMpBlsY1NQkrj0-59Kp2
(anglais)

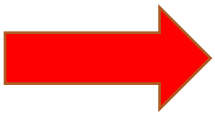
3) Vidéos du Bureau de la concurrence Canada

Il y a diverses formes de fraude par marketing de masse. Ces vidéos présentent comment ces fraudes fonctionnent et ce qu'il faut faire pour éviter d'en être victime. Les vidéos sont disponibles dans les deux langues officielles.
https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04272.html
https://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/04272.html

4) Vidéos sur la prévention de la fraude du CAFC

https://www.youtube.com/channel/UCnvTfqttCb4K6wyVC6rMJkw/playlists

5) Logo du CAFC



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

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

Mars 2022 – Un vidéo #MPF2022 sera partagé qui aura comme but de vous informer sur les moyens de vous protéger contre la fraude.

Mars 2022

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

7) Au sujet du CAFC

Le 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 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. De plus, 12,897 signalements ont été faits par la population d'âge moyen, dont les pertes déclarées s'élèvent à plus de 77.5 millions de dollars.

Voici les dix fraudes les plus courantes dont ont été victimes les Canadiens d'âge moyen en 2020, selon le nombre de signalements :

Type de fraude	N^bre de signalements	N^bre de victimes	Pertes (en $)
Extorsion	2448	536	$3.3 M
Renseignements personnels	1,662	1,203	N/A
Hameçonnage	1,276	341	N/A
Marchandise	1,111	948	$2.5 M
Service	878	595	$1.1 M
Investissement	807	739	$43.2 M
Fraude liée à la vente	750	406	$0.5 M
Emploi	561	286	$1.1 M
Stratagème de rencontre	459	321	$20.2 M
Enqueteur bancaire	346	129	$1.0 M

Voici les dix fraudes ayant entraîné les plus importantes pertes financières pour les Canadiens d'âge moyen :

Type de fraude	N^bre de signalements	N^bre de victimes	Pertes (en $)
Investissements	807	739	$43.2 M
Stratagème de rencontre	459	321	$20.2 M
Extorsion	2,448	536	$3.3 M
Marchandise	1,111	948	$2.5 M
Service	878	595	$1.1 M
Emploi	561	286	$1.1 M
Enquêteur bancaire	346	129	$1.0 M
Fraude liée a la vente	750	406	$0.5 M
Fraude de multipropriété	7	5	$0.4 M
Prêt frauduleux	151	131	$0.4 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) Fraudes les plus courantes et moyens de vous protéger

Vous trouverez ci-dessous les fraudes les plus courantes touchant les Canadiens d'âge moyen :

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.

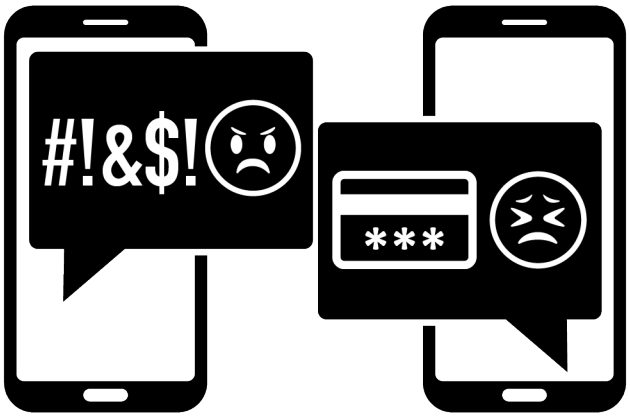
La fraude d'identité survient lorsque le fraudeur utilise les renseignements de la victime à des fins frauduleuses. Il peut créer de faux documents d'identité, présenter des demandes de crédit non autorisées et ouvrir des comptes bancaires sous son nom, rediriger son courrier, acheter des cellulaires, 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** : https://www.canada.ca/fr/services/immigration-citoyennete.html, 1-888-242-2100
- **9** : Informez les organismes provinciaux qui délivrent des pièces d'identité.

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.



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

- 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.

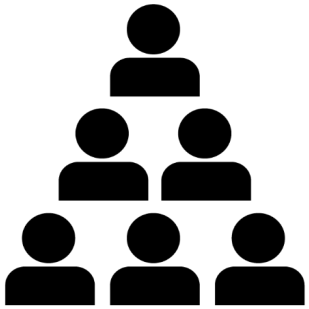
Investissements

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.

Marchandise

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.

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.).

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.

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 :
  - l'adresse de l'entreprise;
  - le numéro de téléphone de l'entreprise;
  - des numéros de compte;
  - 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.