Trousse de prévention de la fraude 2020 :

Personnes d'âge moyen

#DÉNONCERLAFRAUDE
#MONTREMOILAFRAUDE
La fraude : Identifiez-la, signalez-la, enrayez-la.

Table des matières

Introduction

Le Centre antifraude du Canada (CAFC) a préparé une trousse destinée aux Canadiens d'âge moyen (de 30 à 59 ans) 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 invitons nos partenaires à se servir aussi de ces mots-clics, en plus de #Prendre5 et #ParlerA2, protéger plusieurs. #Prendre5 est une campagne nationale lancée par UK Finance (un regroupement de banques et d'institutions financières du Royaume-Uni) qui a connu du succès; elle encourage les consommateurs à s'arrêter, à réfléchir et à ne pas réagir sous la pression des fraudeurs. #ParlerA2 est une initiative entreprise par l'agent-détective Tony Murray, enquêteur sur la fraude à Durham (R.-U.), où l'on invite les consommateurs à prévenir la fraude en envoyant des messages de sensibilisation à au moins deux personnes et en demandant à ces personnes à faire de même. Une chaîne ininterrompue de 25 personnes participant à l'initiative #ParlerA2 permettrait de rejoindre toute la population du Canada.

Pendant le Mois de la prévention de la fraude (mars), le CAFC diffusera chaque jour des messages sur Facebook et Twitter (#MPF2020). 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.

Le CAFC est le dépôt central des données, des renseignements et de la documentation sur la fraude au Canada. 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. Les victimes qui signalent une fraude au CAFC devraient aussi faire un signalement directement au service de police local compétent. Les renseignements fournis peuvent être la pièce manquante du casse-tête.

Les consommateurs et les entreprises peuvent signaler une fraude directement au CAFC au moyen du Système de signalement des fraudes (SSF) en ligne ou en composant le numéro sans frais 1-888-495-8501.

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 Gendarmerie royale du Canada (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 personnes âgées
  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 tous les lundis et tiendra une discussion #ParlonsFraude sur Twitter tous les mercredis à 13 h (heure de l'Est). Les bulletins et les discussions porteront sur les thèmes suivants :

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. Consultez le calendrier ci-dessous pour en savoir plus.

Le **2 mars 2020** – 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 2020

Dimanche	Lundi	Mardi	Mercredi	Jeudi	Vendredi	Samedi
1 Outils utilisés par les fraudeurs	2 **LANCEMENT EN DIRECT** **Bulletin**	3 Renseignements personnels	4 Organismes de bienfaisance **#ParlonsFraude**	5 Méthodes de paiement	6 Prix	7 Vacances
8 Hameçonnage	9 Vol et fraude d'identité **Bulletin**	10 Harponnage	11 Extorsion **#ParlonsFraude**	12 Rançongiciel	13 Échange de carte SIM	14 Besoin urgent d'argent
15 Abonnements piégés	16 Emplois **Bulletin**	17 Vente de marchandises	18 Marchandises **#ParlonsFraude**	19 Fraude sans carte	20 Investissements	21 Location immobilière
22 Se protéger en ligne	23 Chiots **Bulletin**	24 Services	25 Vente pyramidale **#ParlonsFraude**	26 Subventions	27 Stratagème de rencontre	28 Extorsion sexuelle
29 Héritage	30 Paiements en trop **Bulletin**	31 Protection des marques de commerce	1er avril La fraude, ce n'est pas une blague **#ParlonsFraude**	**Facebook : Centre antifraude du Canada** **Twitter : @antifraudecan**		

7) Statistiques

En 2019, le CAFC a reçu 46 465 plaintes de fraude d'entreprises et de consommateurs canadiens. Les pertes financières totales se chiffraient à 96 163 328,64 $. Les dix fraudes les plus signalées au cours de cette période figurent dans la liste ci-dessous.

Les 10 fraudes touchant les personnes d'âge moyen les plus signalées en 2019 :

Type de fraude	N^bre de rapports	N^bre de victimes	Pertes (en $)
Extorsion	5 198	977	2 399 174,29$
Renseignements personnels	3 665	2 620	
Hameçonnage	2 029	559	
Service	1 333	709	2 261 944,47 $
Marchandises	1 221	867	1 471 023,97 $
Vente de marchandises	755	470	626 691,03 $
Emploi	744	265	762 626,81 $
Stratagème de rencontre	497	334	6 071 048,79 $
Prix	334	87	319 607,69 $
Prêts	327	226	877 878,22 $

Les 10 fraudes touchant les personnes d'âge moyen les plus signalées d'après les pertes financières en 2019 :

Type de fraude	N^bre de rapports	N^bre de victimes	Pertes (en $)
Investissements	191	161	7 092 618,26 $
Stratagème de rencontre	497	334	2 071 048,79 $
Extorsion	5 198	977	2 399 174,29 $
Service	1 333	709	2 261 944,47 $
Marchandises	1 221	867	1 471 023,97 $
Prêts	327	226	877 878,22 $
Emploi	744	265	762 626,81 $
Vente de marchandises	755	470	626 691,03 $
Offre de vacance à temps partagé	32	25	392 721,05 $
Prix	334	87	319 607,69 $

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

8) Signalement de la fraude

Dans le but d'atténuer les répercussions de la fraude, le CAFC recommande de prendre les six mesures suivantes :

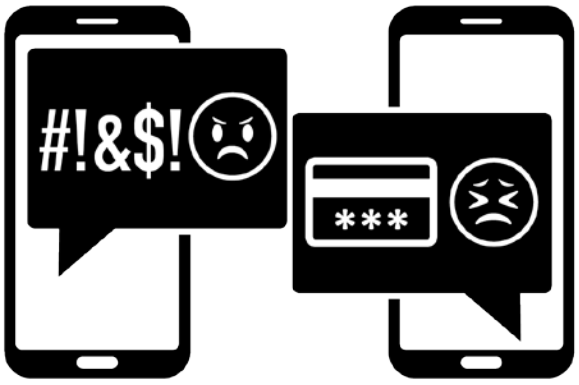
1 : Rassemblez toute l'information sur la fraude.
2 : Signalez l'incident au service de police local.
3 : Signalez l'incident au CAFC au moyen du Système de signalement des fraudes (SSF) ou en composant le 1-888-495-8501 (sans frais).
4 : Signalez l'incident à l'institution financière ou au fournisseur de services de paiement utilisé pour envoyer l'argent.
5 : Si la fraude a été commise en ligne, assurez-vous de signaler l'incident directement au site Web.
6 : Suivez le *Guide pour les victimes de fraude ou vol d'identité* : http://www.rcmp-grc.gc.ca/scams-fraudes/victims-guide-victimes-fra.htm

9) Fraudes courantes et moyens de vous protéger

Vous trouverez ci-dessous quelques fraudes courantes ciblant les personnes d'âge moyen :

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.

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

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.

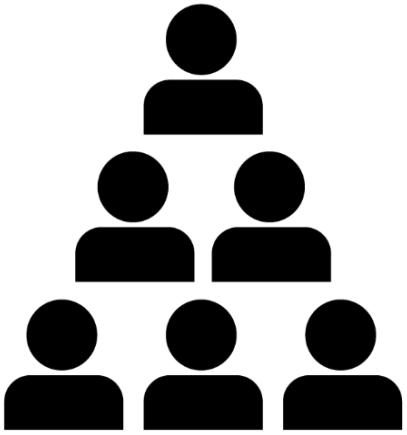
Indices – Comment vous protéger

- 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

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/).

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.

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.

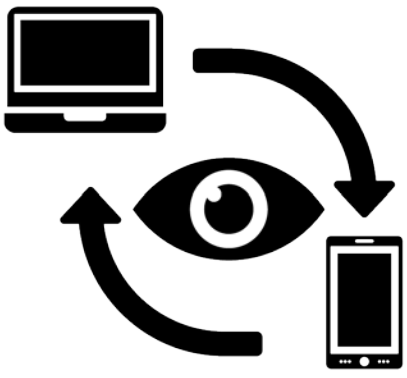
Animaux à donner : Les fraudeurs annoncent souvent des animaux à donner, surtout des chiots et des chatons. Ils disent que l'animal est gratuit, mais la victime doit payer le transport. Une fois le paiement reçu, les fraudeurs demandent des paiements supplémentaires pour couvrir divers coûts (cage de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

Services

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 bien connue 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.

Hameçonnage

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 sur des 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.


Canadian Anti-Fraud Centre
CAFC
Centre antifraude du Canada
FRAUD: RECOGNIZE IT. REPORT IT. STOP IT.
LA FRAUDE : IDENTIFIEZ-LA. SIGNALEZ-LA. ENRAYEZ-LA.
Competition Bureau Canada
Bureau de la concurrence Canada
Royal Canadian Mounted Police
Gendarmerie royale du Canada
Canada