AÎNÉS

Trousse de prévention de la fraude 2021

Table des matières

Introduction

Le taux de fraude continue d'augmenter au Canada et le monde entier est aux prises avec une pandémie. La COVID-19 a créé un contexte propice à la fraude et aux activités criminelles en ligne. En raison de la pandémie, plus de personnes que jamais se tournent vers Internet pour faire l'épicerie et des courses, effectuer des opérations bancaires et avoir de la compagnie. Si l'on ajoute à cela les profondes répercussions sociales, psychologiques et émotionnelles de la COVID-19 sur les gens, on peut supposer que le nombre de victimes potentielles a augmenté de façon spectaculaire.

Mars est le mois de la prévention de la fraude. Cette année, les efforts seront axés sur l'économie numérique des fraudes et des escroqueries.

Le Centre antifraude du Canada (CAFC) a préparé une trousse destinée aux aînés canadiens (âgés de 60 ans et plus) 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 (#MPF2021). Nous publierons notre bulletin hebdomadaire tous les lundis et tiendrons une discussion #ParlonsFraude sur Twitter à 13 h (heure de l'Est) chaque mercredi. Tous sont invités à participer à la discussion.

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

Merci,

L'équipe de prévention de la fraude du CAFC

Twitter : @antifraudecan
Facebook : Centre antifraude du Canada

La présente trousse comprend :

1) 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)

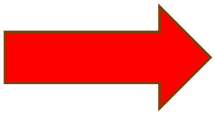
3) Vidéos du Bureau de la concurrence Canada

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

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

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

Séances de clavardage sur la fraude
Semaine 1 : Fraude téléphonique
Semaine 2 : Fraude par courriel ou par texto
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.
Facebook : Centre antifraude du Canada
Twitter : @antifraudecan

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

Mars 2021

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

7) Au sujet du CAFC

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

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

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

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

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

8) Statistiques

En 2020, le CAFC a reçu 101 483 signalements de fraude représentant des pertes totales de près de 160 millions de dollars. De plus, 11 447 signalements ont été faits par des aînés canadiens, dont les pertes déclarées s'élèvent à plus de 31,8 millions de dollars.

Voici les dix fraudes les plus courantes dont ont été victimes les aînés canadiens en 2020, selon le nombre de signalements :

Type de fraude	N^{bre} de signalements	N^{bre} de victimes	Pertes (en $)
Extorsion	3 651	1 207	1,1 million
Renseignements personnels	1 350	804	S.O.
Hameçonnage	1 047	268	S.O.
Service	692	419	6,5 millions
Enquêteur bancaire	524	228	2,5 millions
Besoin urgent d'argent	501	172	0,6 million
Marchandise	425	328	0,4 million
Escroquerie du prix gagné	408	133	2,5 millions
Fraude liée à la vente	279	105	0,2 million
Stratagème de rencontre	251	169	7,3 millions

Voici les dix fraudes ayant entraîné les plus importantes pertes financières pour les aînés canadiens en 2020 :

Type de fraude	N^bre de signalements	N^bre de victimes	Pertes (en $)
Stratagème de rencontre	251	169	7,3 millions
Service	692	419	6,5 millions
Investissements	96	86	6,1 millions
Escroquerie du prix gagné	408	133	2,5 millions
Enquêteur bancaire	524	228	2,5 millions
Harponnage	183	84	1,1 million
Extorsion	3 651	1 207	1,1 million
Héritage	86	8	0,8 million
Besoin urgent d'argent	501	172	0,7 million
Prêt	55	35	0,5 million

➔ 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 :

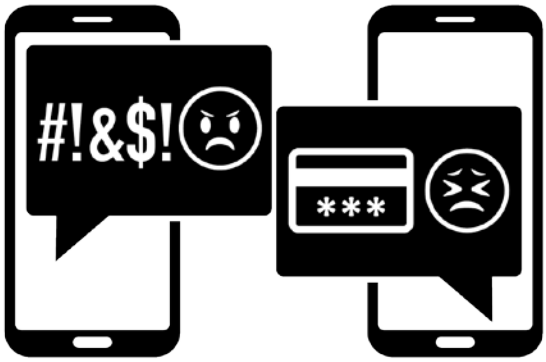
1 : Rassemblez toute l'information sur la fraude.
2 : Consignez les événements en ordre chronologique.
3 : Signalez l'incident au service de police local.
4 : Signalez l'incident au CAFC au moyen du Système de signalement des fraudes (SSF) ou en composant le 1-888-495-8501 (sans frais).
5 : Signalez 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 quelques fraudes courantes touchant les aînés 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.



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.

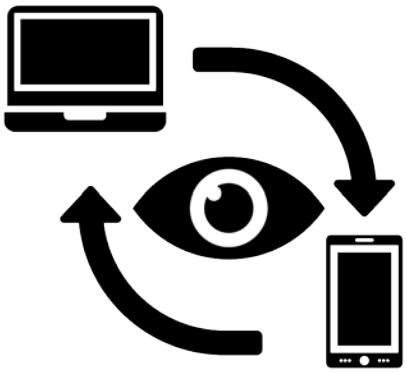
Service

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 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.

Enquêteur bancaire

Les fraudeurs téléphonent aux victimes et se font passer pour un employé d'une institution bancaire ou d'un fournisseur d'une carte de crédit reconnue. Pour prouver la légitimité de l'appel, ils demandent souvent à la victime de raccrocher et de composer immédiatement le numéro inscrit au dos de sa carte de crédit. Les fraudeurs informent ensuite la victime qu'ils font enquête sur des transactions non autorisées effectuées dans son compte et lui demandent de l'aide pour appréhender

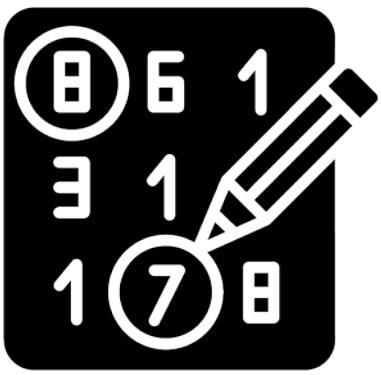
les criminels. Si la victime leur donne un accès à distance à son appareil, les fraudeurs prétendront déposer dans son compte de l'argent qui sera utilisé comme « appât ». Malheureusement, les fonds versés dans le compte de la victime viennent de leurs autres comptes et l'argent envoyé va directement aux fraudeurs.

Indices – Comment vous protéger

- En général, les fraudeurs ont tendance à téléphoner tôt le matin. Assurez-vous toujours d'être vigilant lorsqu'il est question de finances.
- Si vous mettez fin à un appel sur une ligne terrestre et composez immédiatement un autre numéro, il est possible que l'appel original ne soit pas complètement déconnecté. Attendez quelques minutes ou utilisez un autre téléphone pour effectuer un autre appel.
- Ne transmettez jamais de renseignements personnels ou financiers au téléphone à moins d'avoir appelé vous-même votre institution financière.
- Les institutions financières ne demanderont jamais l'aide du public pour des enquêtes internes et elles ne vous demanderont jamais de transférer des fonds dans un compte externe pour des raisons de sécurité.
- Ne permettez jamais à des appelants inconnus d'accéder à votre appareil à distance.

Escroquerie du prix gagné

Les consommateurs se font annoncer qu'ils ont remporté un gros lot ou un prix important même 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. Leur prix ne leur est 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.