



CENTRE ANTIFRAUDE DU CANADA

Trousse de prévention de la fraude 2021 – Personnes d'âge moyen 2021-02-15

LA FRAUDE : IDENTIFIEZ-LA, SIGNALEZ-LA, ENRAYEZ-LA

PERSONNES D'ÂGE MOYEN

Trousse de prévention de la fraude 2021



Royal Canadian Mounted Police
Gendarmerie royale du Canada



Competition Bureau
Canada
Bureau de la concurrence
Canada



Ontario Provincial Police

Canada

Table des matières

Introduction	---	3
Vidéos de la GRC	---	4
Vidéos de l'OPP	---	4
Vidéos du Bureau de la concurrence Canada	---	4
Vidéos sur la prévention de la fraude du CAFC	---	4
Logo du CAFC	---	5
Calendrier des activités	---	5
Au sujet du CAFC	---	7
Statistiques	---	7
Signalement de la fraude	---	8
Fraudes les plus courantes ciblant les personnes d'âge moyen	---	9
• Vol et fraude d'identité	---	9
• Extorsion	---	10
• Stratagème de rencontre	---	11
• Investissements	---	12
• Marchandise	---	13

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-clés #dÉNONcerlafraude et #montremoilaFRAUDE. Nous continuerons également d'utiliser le slogan « La fraude : Identifiez-la, signalez-la, enrayer-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](https://twitter.com/antifraudecan)

Facebook : [Centre antifraude du Canada](https://www.facebook.com/CentreAntifraudeCanada)

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=0rIWUcc57dM> (anglais)

Le cri du cœur des victimes

<https://www.youtube.com/watch?v=cHZfvpH2YW8>

<https://www.youtube.com/watch?v=blyhHI8rc7g> (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=PLbecW3cjtFJ6jyMpBlS Y1NQkrj0-59Kp2>

(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.

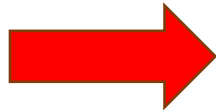
<https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04272.html>

<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.

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

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

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 2020, le CAFC a reçu 101 483 signalements de fraude représentant des pertes totales de près de 160 millions de dollars. De plus, 24 271 signalements ont été faits par des Canadiens d'âge moyen, dont les pertes déclarées s'élèvent à plus de 36,3 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 \$)
Fraude à l'identité	7 951	7 951	S.O.
Extorsion	6 189	2 169	3,0 millions
Renseignements personnels	2 173	1 497	S.O.
Marchandise	1 246	1 029	2,7 millions
Hameçonnage	1 180	360	S.O.
Emploi	651	267	0,7 million
Fraude liée à la vente	595	320	0,4 million
Service	587	379	0,8 million
Stratagème de rencontre	334	226	7,5 millions
Harponnage	226	132	0,4 million

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 \$)
Stratagème de rencontre	334	226	7,5 millions
Investissements	186	159	3,9 millions
Extorsion	6 189	2 169	3,0 millions
Marchandise	1 246	1 029	2,7 millions
Service	587	379	0,8 million
Emploi	651	267	0,7 million
Prêt	193	151	0,6 million
Harponnage	226	132	0,4 million
Fraude liée à la vente	595	320	0,4 million
Enquêteur bancaire	168	63	0,3 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 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.

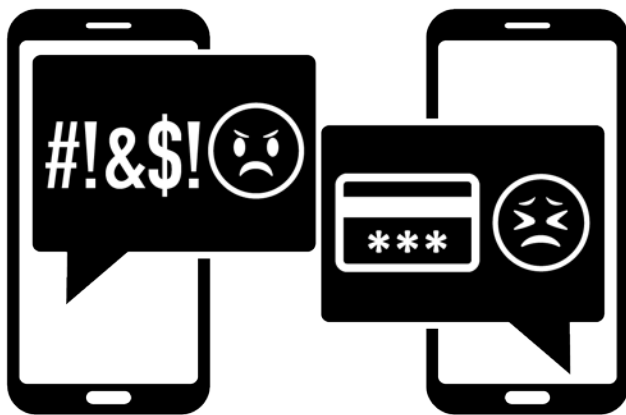
Si vous êtes victime de vol ou de fraude d'identité, prenez immédiatement les mesures suivantes :

- **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

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 inexistantes.

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/>).

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.