Trousse pour le mois de la prévention de la fraude

Mars 2019

Jeunes adultes

#DÉNONCERLAFRAUDE

LA FRAUDE : Identifiez-la. Éliminez-la. Signalez-la.

Table des matières

Introduction

En prévision du mois de la prévention de la fraude en mars, le Centre antifraude du Canada (CAFC) a préparé une trousse destinée au personnel de l'application de la loi qui s'en servira pour mieux sensibiliser le public et empêcher les Canadiens d'être victimes de fraude. Nous encourageons tout le personnel de l'application de la loi à ajouter le logo du CACF, les coordonnées et les documents de référence contenus dans la présente trousse à leur site Web, à leurs publications écrites et à leurs plateformes de médias sociaux. Le CAFC publiera chaque jour des messages sur Facebook et Twitter (#FPM2018, #MPF2018) et participera à des séances de clavardage sur la fraude. Utilisez le mot-clic #fraudchat pour suivre la discussion.

Le CAFC est le dépôt central des données, des renseignements et de la documentation sur la fraude par marketing de masse au Canada. Le CAFC ne mène aucune enquête; en revanche, il apporte une aide précieuse aux organismes d'application de la loi du monde entier en faisant des rapprochements entre des affaires en apparence non liées. Les victimes qui signalent une fraude au CAFC devraient aussi faire un signalement directement au service de police local compétent. Les renseignements que vous fournissez peuvent être la pièce manquante du casse-tête.

En français : http://www.antifraudcentre-centreantifraude.ca/reportincident-signalerincident/index-fra.htm

En anglais : http://www.antifraudcentre-centreantifraude.ca/reportincident-signalerincident/index-eng.htm

Les questions et les commentaires sur le mois de 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
- Le cri du cœur des victimes : Stratagème de rencontre (YouTube)
  https://www.youtube.com/watch?v=blyhHl8rc7g
- Télémarketing frauduleux : L'envers du décor (YouTube)
  https://www.youtube.com/watch?v=t7bhQJkelEg (vidéo en anglais avec sous-titres en français)

2) Vidéos de la Police provinciale de l'Ontario (PPO) sur la prévention de la fraude

Ces vidéos où l'on présente plusieurs types de fraudes mettent en vedette des employés et des bénévoles du CAFC. Les vidéos sont disponibles dans les deux langues officielles.

- Français (YouTube)
  https://www.youtube.com/user/OPPCorpCommfr/search?query=scam
- Anglais (YouTube)
  https://www.youtube.com/user/OPPCorpComm/search?query=scam

3) Vidéos du Bureau de la concurrence du Canada sur la prévention de la fraude

Il y a diverses formes de fraude par marketing de masse. Les vidéos ci-après décrivent leur fonctionnement et la façon d'éviter d'en être victime. Les vidéos sont disponibles dans les deux langues officielles.

- Français : http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/03809.html#tab2
- Anglais : http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03809.html#tab2

4) Logo du CAFC

5) Calendrier des activités : « Fraude de la journée » sur Facebook et Twitter

Chaque jour en mars, le CAFC publiera sur Facebook et Twitter un message sur une fraude en particulier. Le message contiendra un lien direct au site Web du CAFC (l'information est disponible dans les deux langues officielles). Se reporter au calendrier ci-dessous. La semaine 2 sera consacrée aux fraudes touchant les jeunes adultes.

Mars 2019

Dimanche	Lundi	Mardi	Mercredi	Jeudi	Vendredi	Samedi
					1 **Facebook et Twitter** Importance du signalement des fraudes	2
3	4 **Facebook et Twitter** Vente de marchandises **Bulletin** Prêts	5 **Facebook et Twitter** Hameçonnage	6 **Facebook et Twitter** Renseignements personnels	7 **Facebook et Twitter** Prêt	8 **Facebook et Twitter** Emploi	9
10	11 **Facebook et Twitter** Extorsion **Bulletin** Extorsion	12 **Facebook et Twitter** Stratagème de rencontre	13 **Facebook et Twitter** Investissements	14 **Facebook et Twitter** Marchandise (contrefaite)	15 **Facebook et Twitter** Offres de vacances	16
17	18 **Facebook et Twitter** Stratagème du besoin urgent d'argent **Bulletin** Service	19 **Facebook et Twitter** Prix	20 **Facebook et Twitter** Service de soutien	21 **Facebook et Twitter** Faux inspecteur de banque	22 **Facebook et Twitter** Récupération d'argent	23
24	25 **Facebook et Twitter** Fraudes électroniques **Bulletin** Fraude sans de carte	26 **Facebook et Twitter** Fraudes sans carte	27 **Facebook et Twitter** Subvention	28 **Facebook et Twitter** Annuaire	29 **Facebook et Twitter** Harponnage	30

Twitter : @antifraudecan
Facebook : Centre antifraude du Canada

6) Statistiques

En 2018, le CAFC a reçu 59 009 plaintes de fraude d'entreprises et de consommateurs canadiens. Les pertes financières totales se chiffraient à 97 654 160,35 $. Les dix fraudes touchant les jeunes adultes les plus signalées au cours de cette période figurent dans la liste ci-dessous.

Les dix fraudes touchant les jeunes adultes les plus signalées d'après les plaintes reçues en 2018 :

Type de plainte	N^{bre} de plaintes	N^{bre} de victimes	Pertes (en $)
Extorsion	3 299	470	2 182 166,9 $
Fraude d'identité	1 711	1 620	2 119 557,81 $
Hameçonnage	1 327	821	23 166,96 $
Renseignements personnels	922	625	39 030,14 $
Vente de marchandises	911	797	474 977,09 $
Marchandises	583	462	415 595,62 $
Emploi	519	209	566 749,84 $
Escroqueries de services	372	211	300 827,92 $
Marchandises contrefaites	105	103	33 756,57 $
Offres de prêt frauduleuses	99	76	129 215,21 $

Les dix fraudes touchant les jeunes adultes les plus signalées d'après les pertes financières en 2018 :

	N^{bre} de plaintes	N^{bre} de victimes	Pertes (en $)
Extorsion	3 299	470	2 182 166,9 $
Fraude d'identité	1 711	1 620	2 119 557,81 $
Investissements	42	30	804 031,48 $
Emploi	519	209	566 749 84 $
Vente de marchandises	911	797	474 977,09 $
Marchandises	583	462	415 595,62 $
Escroqueries de services	372	211	300 827,92 $
Stratagème de rencontre	60	43	154 190,37 $
Héritage	10	4	136 067,00 $
Offres de prêt frauduleuses	99	76	129 215,21 $

➔ Moins de **5 %** des victimes de fraude font un signalement au CAFC.

7) Avis de fraude/Bulletins

Vous trouverez ci-dessous quelques fraudes courantes ciblant les jeunes adultes, fraudes auxquelles sera consacrée la deuxième semaine du mois de la prévention de la fraude (du 4 au 8 mars).

Lundi 4 mars 2019 – **Fraudes ciblant les jeunes adultes**
Bulletin : **Prêts**

Vente de marchandise

Au moment de vendre des produits en ligne, vous devez savoir que ce ne sont pas toutes les offres qui sont dignes de confiance. Les consommateurs qui offrent un service ou vendent de la marchandise peuvent recevoir un paiement frauduleux, souvent d'un montant plus élevé que le prix demandé, et on leur demandera de rembourser la différence à une tierce partie pour conclure la transaction (souvent, une entreprise d'expédition). Les consommateurs qui se plient à la demande peuvent perdre la marchandise expédiée et devoir rembourser les fonds perdus à l'institution financière.

Le fraudeur effectue une transaction en ligne et propose de payer par PayPal. Il offre aussi de verser un supplément pour que la victime lui expédie la marchandise. La victime qui accepte de le faire reçoit un faux courriel indiquant que les fonds sont disponibles, mais qu'ils ne seront débloqués que lorsque celle-ci confirmera un numéro de repérage. La victime expédie la marchandise, mais elle ne se fait pas payer et perd la marchandise vendue.

Indices – Comment vous protéger

- Authentifiez les paiements avant d'expédier la marchandise.
- Les fraudeurs utilisent le mot « article » (*item*) plutôt que de renvoyer à la marchandise vendue.
- Méfiez-vous lorsqu'un acheteur essaie de changer l'adresse d'expédition à la dernière minute.
- Méfiez-vous des paiements en trop et des acheteurs qui demandent d'envoyer le montant excédentaire à un agent d'expédition.

Hameçonnage

Les courriels d'hameçonnage traditionnels visent à faire croire à la victime qu'elle fait affaire avec une entreprise de renom. Ils sont envoyés en vue de recueillir des renseignements personnels et financiers pouvant être utilisés pour commettre une fraude d'identité. À l'heure actuelle, les courriels les plus répandus sont ceux envoyés par des fraudeurs qui prétendent représenter PayPal, l'Agence du revenu du Canada, des institutions financières et des fournisseurs de services de courriel. On encourage les victimes qui répondent à ces courriels à prendre les mesures appropriées pour protéger leur identité – en communiquant avec Equifax, TransUnion, leurs institutions financières, le service de police local et le CAFC.

Indices – Comment vous protéger

- Vérifiez si le courriel renferme des fautes d'orthographe et des erreurs de mise en forme.
- Vérifiez l'hyperlien contenu dans le courriel suspect en plaçant le pointeur de la souris sur le lien pour vérifier l'adresse.
- Ne cliquez pas sur les pièces jointes; elles peuvent contenir des virus et des logiciels espions.
- N'ouvrez pas les hyperliens contenus dans des courriels non sollicités et douteux.
- Méfiez-vous des courriels non sollicités d'organisations qui demandent des renseignements personnels ou financiers.

Renseignements personnels

Il s'agit de toute sollicitation où l'on demande à une personne de fournir ou de confirmer des renseignements privés et personnels. Qu'ils aient recours à de faux sites Web ou à des appels impromptus pour obtenir des renseignements personnels et financiers, les fraudeurs emploient plusieurs tactiques pour commettre des vols d'identité.

Indices – Comment vous protéger

- Ne donnez jamais vos renseignements personnels par téléphone, sauf si vous avez fait l'appel.
- Conservez vos documents financiers et personnels dans un endroit sûr et verrouillé à la maison et placez votre porte-monnaie ou votre sac à main dans un lieu sûr.

- Déchiquetez vos reçus, les offres de cartes de crédit, les demandes de carte de crédit, les formulaires d'assurance, les chèques, les relevés bancaires et tout autre document semblable lorsque vous n'en avez plus besoin.

Prêts

Les offres de prêt frauduleuses se trouvent souvent dans des publicités en ligne ou des sites Web trompeurs conçus pour ressembler à celui d'institutions financières légitimes. La victime qui présente une demande doit fournir des renseignements personnels, ce qui peut mener à un vol d'identité. Comme toutes les demandes de prêt sont approuvées, le fraudeur exige que la victime paie des frais initiaux pour obtenir le prêt. On lui promet que le prêt sera déposé dans son compte dans les 24 heures qui suivent le paiement des frais. Une fois que la victime envoie l'argent, le fraudeur cesse habituellement de communiquer avec elle et celle-ci ne reçoit jamais l'argent du prêt.

Indices – Comment vous protéger

- Si on vous demande de faire des paiements au moyen d'un virement bancaire par courriel, par l'intermédiaire d'une entreprise de transferts de fonds ou au moyen d'une carte de crédit prépayée, cessez de communiquer avec le prêteur immédiatement.
- Il est illégal pour une entreprise de demander des frais initiaux avant l'obtention de votre prêt.
- Méfiez-vous des entreprises qui vous garantissent un prêt même si vous avez une mauvaise cote de crédit ou si vous n'avez aucun dossier de crédit.
- Communiquez avec des organisations de protection des consommateurs et des organismes de réglementation pour confirmer qu'il s'agit bien d'un prêteur légitime.
- Ce n'est pas parce qu'une annonce est publiée par une organisation médiatique reconnue qu'elle est nécessairement légitime.

Offres d'emploi

Les fraudeurs se servent de sites bien connus comme Kijiji, Craigslist, Monster, Indeed et Workopolis pour recruter des victimes potentielles. Les fraudes les plus répandues sont celles liées à l'habillage de voiture et à des emplois administratifs, dans les RH ou de clients mystères.

Client mystère : La victime se fait offrir un emploi de client mystère après avoir répondu à une annonce en ligne ou à un message texte. Elle reçoit par la poste un chèque et des directives précisant qu'elle doit faire des achats dans des magasins locaux et envoyer des fonds par MoneyGram ou Western Union. Elle se fait dire de prendre note de son expérience et d'évaluer le service à la clientèle. Elle découvre par la suite que le chèque était faux et doit payer elle-même les fonds qu'elle a virés.

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 le logo d'une « entreprise » sur sa voiture. La victime qui accepte de le faire reçoit un chèque avec des directives précisant qu'elle doit le déposer et virer une partie des fonds à une entreprise de graphisme. La victime apprend ensuite que le chèque original est faux. Les fraudeurs se feront passer pour des entreprises légitimes pour que l'emploi semble réel.

Emploi administratif ou dans les RH : Dans une autre fraude courante, la victime agit à titre de mandataire ou d'agent financier. On lui demande d'accepter un paiement dans son compte personnel (souvent reçu par virement électronique ou par chèque), de garder une partie du montant et de transférer le reste à des « employés » de la tierce partie ou à de tierces « entreprises ». La victime découvre par la suite que le paiement était faux ou frauduleux et que le montant viré doit être remboursé à ses frais. Les fraudeurs tenteront de traiter autant de paiements que possible avant que les victimes soient prévenues de l'escroquerie par leurs institutions financières.

Indices – Comment vous protéger

- Méfiez-vous des sites où vous affichez votre curriculum vitæ; les fraudeurs se servent de sites Web légitimes pour trouver des victimes.
- Un employeur légitime ne vous demandera jamais de lui remettre une partie des fonds qu'il vous a versés.
- Faites des vérifications; une simple recherche dans Internet peut vous éviter de perdre des milliers de dollars.
- N'utilisez jamais votre compte personnel pour traiter des paiements versés par des inconnus.
- Méfiez-vous des offres d'emploi reçues dans un message texte non sollicité.
- Méfiez-vous d'une « entreprise » qui utilise une adresse courriel Web personnelle pour faire des affaires.

Si vous croyez être victime de fraude ou si vous connaissez une personne qui a été victime de fraude, veuillez communiquer avec le Centre antifraude du Canada au 1-888-495-8501 ou signalez une fraude en utilisant le Système de signalement des fraudes (SSF) en ligne au http://www.antifraudcentre-centreantifraude.ca/reportincident-signalerincident/index-fra.htm