Trousse pour le mois de la prévention de la fraude

Mars 2019

Entreprises

#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

Canadian Anti-Fraud Centre
CAFC
Centre antifraude du Canada
FRAUD: RECOGNIZE IT. REPORT IT. STOP IT. LA FRAUDE: IDENTIFIEZ-LA. SIGNALEZ-LA. ENRAYEZ-LA.

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 5 sera consacrée aux fraudes ciblant les entreprises.

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 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 entreprises les plus signalées au cours de cette période figurent dans la liste ci-dessous.

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

Type de plainte	N^bre de plaintes	N^bre de victimes	Pertes (en $)
Extorsion	347	28	105 865,00 $
Vente de marchandise	277	177	875 989,08 $
Fraudes électroniques	273	70	11 121 222,70 $
Annuaires d'entreprises	211	18	12 759,09 $
Hameçonnage	181	6	1 369,40 $
Escroqueries de services	141	38	398 764,08 $
Marchandises	92	54	629 832,07 $
Mystification téléphonique	80	42	0,00
Renseignements personnels	79	26	0,00
Harponnage	78	34	263 219,79 $

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

Type de plainte	N^bre de plaintes	N^bre de victimes	Pertes (en $)
Fraudes électroniques	273	70	11 121 222,70 $
Vente de marchandise	277	177	875 989,08 $
Emplois	71	13	746 570,19 $
Marchandises	92	54	629 832,07 $
Escroqueries de services	141	38	398 764,08 $
Harponnage	78	34	263 219,79 $
Extorsion	347	28	105 865,00 $
Paiement non autorisé	6	5	65 269,40 $
Chèque frauduleux	6	3	43 132,47 $
Prêt	16	5	15 990,03 $

➔ 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 entreprises, fraudes auxquelles sera consacrée la cinquième semaine du mois de la prévention de la fraude (du 25 au 29 mars).

Lundi 25 mars 2019 – **Fraudes ciblant les entreprises**
Bulletin : **Fraude sans carte**

Fraudes électroniques

Les entreprises canadiennes sont visées par deux types de fraudes électroniques : l'arnaque des faux dirigeants d'entreprise et l'escroquerie du fournisseur.

Dans l'arnaque des faux dirigeants d'entreprise, aussi appelée la fraude du compte courriel d'entreprise compromis, la victime potentielle reçoit un courriel qui semble provenir d'un dirigeant de l'entreprise qui est autorisé à demander des virements électroniques. Dans certains cas, les fraudeurs créent des adresses de courriel qui ressemblent à celles du président-directeur général ou du directeur financier. Dans d'autres cas, les fraudeurs compromettent et utilisent leurs comptes courriel. Un employé autorisé à faire des virements électroniques recevra le courriel frauduleux. Souvent, le message indiquera que le « dirigeant » travaille à l'extérieur et qu'il a remarqué un paiement en souffrance qui doit être effectué dans les plus brefs délais. Le « dirigeant » ordonne le versement d'un montant généralement élevé à une personne nommée dans un certain compte bancaire. Les pertes se chiffrent habituellement à plus de 100 000 $.

Dans l'escroquerie du fournisseur, les entreprises canadiennes sont ciblées par des fraudeurs qui prétendent représenter leur fournisseur régulier. Cette fraude cible des entreprises qui ont des relations et des comptes avec des fournisseurs et des grossistes. Elle consiste habituellement à envoyer un faux courriel informant les acheteurs d'un changement touchant les modalités de paiement. Dans ce message, on communique de nouveaux renseignements bancaires et on demande au destinataire de verser les prochains paiements dans le « nouveau » compte.

Signes d'avertissement – Comment vous protéger

- Méfiez-vous des demandes inhabituelles urgentes de virement de fonds reçues par courriel.
- Avant d'envoyer des fonds ou un produit, parlez aux clients, en personne ou au téléphone, pour confirmer que la demande est légitime.
- Vérifiez si le courriel renferme des fautes d'orthographe et des erreurs de mise en forme et abstenez-vous de cliquer sur les pièces jointes, car elles peuvent contenir des virus et des logiciels espions.

Fraude sans carte

Par fraude sans carte, on entend la collecte, l'échange et l'utilisation non autorisés ou frauduleux des données de cartes de paiement (numéro de la carte, date d'expiration et mot de passe). Il est question de fraude sans carte lorsque ces données sont utilisées dans des situations où la carte et le détenteur de la carte ne sont pas présents (au téléphone, par courriel, par télécopieur ou sur un site Web).

Un fraudeur commande un produit ou un service sans carte auprès d'un commerçant (au téléphone, par courriel, par télécopieur ou sur un site Web) dans l'intention d'utiliser une carte volée pour faire le paiement. Le commerçant, qui croit qu'il s'agit d'un achat légitime, impute le montant à la carte volée et livre le produit ou le service. Tôt ou tard, le véritable détenteur de la carte relève les frais non autorisés et les conteste. Le commerçant reçoit alors une rétrofacturation et doit rembourser le montant payé sur la carte volée. Il est important de se rappeler que tout commerçant qui accepte des commandes sans carte peut être victime de fraude.

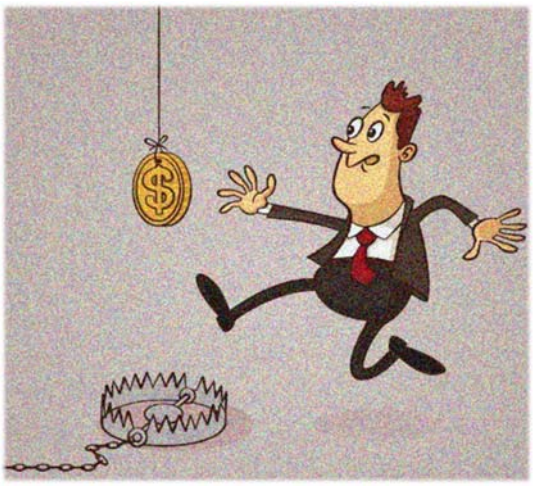
Il arrive aussi qu'un fraudeur demande un paiement en trop dans une transaction sans carte. Il demande au commerçant de prélever un montant plus élevé que le prix du produit ou du service et d'envoyer la différence à une tierce partie, souvent une compagnie de déménagement pour faciliter l'expédition. Les fraudeurs transforment ainsi des cartes de crédit volées en argent comptant.

Une autre méthode de fraude sans carte a été observée dans le secteur de l'aviation commerciale : les fraudeurs achètent des billets d'avion au moyen de cartes de crédit volées et vendent les billets à un prix inférieur en ligne, sur des sites de petites annonces. Dans ces situations, tout comme le commerçant, la personne qui achète les billets revendus est victime. Dans la plupart des cas, l'acheteur ne peut pas utiliser les billets, car le commerçant les annule une fois que la fraude a été confirmée.

Signes d'avertissement – Comment vous protéger

- Avant d'expédier les articles, appelez le client au numéro qu'il vous a donné et vérifiez les renseignements relatifs à la transaction.
- Soyez attentif aux expéditions prioritaires de biens faciles à falsifier : il pourrait s'agir de transactions frauduleuses.
- Méfiez-vous des commandes que l'on demande d'expédier immédiatement, surtout si l'adresse d'expédition n'est pas la même que celle qui est liée à la carte de crédit utilisée pour faire l'achat.
- Faites attention aux commandes de clients réguliers qui diffèrent des habitudes d'achat de ces derniers.
- Communiquez avec vos fournisseurs de services et assurez-vous que des mesures de sécurité sont mises en place pour éviter d'être victime de fraude et réduire les rétrofacturations indésirables.
- Pour les commerçants qui acceptent les commandes sans carte, la meilleure façon d'éviter les fraudes est d'avoir recours aux outils de vérification automatisés préconisés par les acquéreurs et les associations de paiement.

Subvention



Il s'agit de toute sollicitation fausse, trompeuse ou frauduleuse impliquant la promotion d'une subvention. Habituellement, ces annonces se trouvent dans diverses publications, comme les journaux, les petites annonces, des revues ou dans des publicités en ligne et sur des sites Web. D'autres fois, elles découlent d'un appel téléphonique de fraudeurs se faisant passer pour une organisation gouvernementale ou une autre organisation dont le nom sonne officiel. Lorsqu'une victime répond à l'annonce ou à l'appel téléphonique, on lui demande de fournir les données sur son compte chèque pour que la

subvention soit directement versée dans son compte ou pour payer des « frais de traitement ». Les paiements sont souvent demandés sous forme de chèques-cadeaux iTunes, par l'intermédiaire d'entreprises de transferts de fonds, de transferts télégraphiques, de cartes de paiement ou de virement bancaire par courriel. En fin de compte, aucune subvention n'est versée, et si les données bancaires ont été fournies, les fraudeurs ont l'occasion de se sauver avec votre argent.

Signes d'avertissement – Comment vous protéger?

- Ce n'est pas parce qu'une annonce est publiée dans un journal ou dans un autre média reconnu qu'elle est assurément légitime.
- Ne donnez jamais de renseignements personnels ou bancaires à un inconnu.
- Ne payez jamais d'argent pour recevoir une subvention gouvernementale « gratuite ».
- Méfiez-vous des renseignements que vous donnez à une organisation.

Fraudes liées aux annuaires d'entreprises

Les entreprises reçoivent une facture pour une publication, une inscription ou un annuaire qu'elles n'ont ni commandés ni autorisés. Les fraudeurs appellent l'entreprise et demandent à un employé de confirmer l'adresse, le numéro de téléphone et d'autres renseignements de l'entreprise. Ils lui envoient ensuite une facture que le service de comptabilité règle souvent sans savoir que l'entreprise n'a jamais commandé ni accepté de payer l'annuaire. Le fraudeur peut même enregistrer la conversation initiale et s'en servir contre l'entreprise pour vérifier l'achat de l'annuaire.

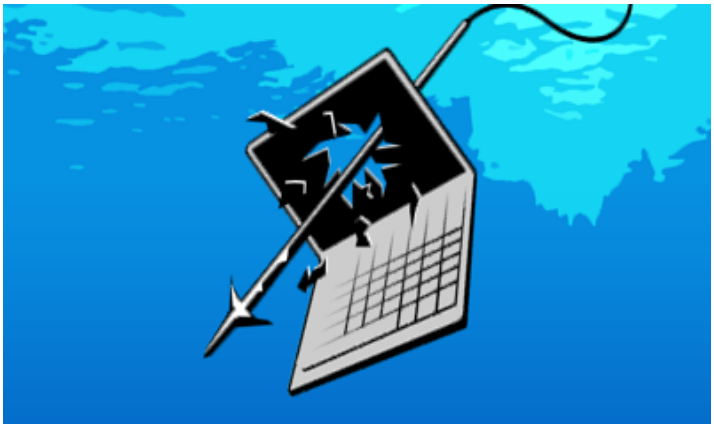
Signes d'avertissement – Comment vous protéger

- Apprenez aux employés de tous les échelons à se méfier des appels non sollicités.
- Dressez une liste des entreprises avec qui vous faites généralement affaire.
- Les fraudeurs utilisent des noms de véritables entreprises comme les Pages jaunes pour que les factures semblent authentiques. Examinez soigneusement les factures avant d'effectuer un paiement.

Harponnage

Le harponnage est une pratique frauduleuse qui consiste à envoyer des courriels qui semblent provenir d'un expéditeur connu, comme un patron, un collègue ou un client. Il s'agit d'une mystification. Les criminels ont recours au harponnage pour faire croire au destinataire qu'il reçoit un courriel d'une source fiable. Cette tactique incite le destinataire à révéler des renseignements confidentiels ou de nature délicate. On demande souvent dans le courriel de cliquer sur un lien malveillant ou une pièce jointe, ce qui peut entraîner la perte de renseignements de nature délicate.

Le harponnage est aussi utilisé dans le cadre de différents stratagèmes pour tromper des travailleurs et les inciter à envoyer de l'argent aux fraudeurs. Une arnaque courante qui cible les entreprises consiste à envoyer à un employé une demande par courriel qui semble provenir d'un gestionnaire, du propriétaire ou du président de l'entreprise. Dans le courriel, on lui demande d'acheter des cartes-cadeaux (iTunes, Google, Amazon, etc.) et d'envoyer les numéros des cartes prépayées par courriel à l'expéditeur. Dans d'autres cas, les fraudeurs peuvent demander aux employés d'envoyer de l'argent par virement électronique.



Signes d'avertissement – Comment vous protéger

- Assurez-vous que le courriel provient d'une source légitime.
- Méfiez-vous des demandes d'achat irrégulières.
- Mettez en œuvre des mesures de précautions accrues pour les achats ou l'envoi de fonds.

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