Trousse de prévention de la fraude 2020 :

Entreprises

#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 entreprises 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 pour 13 heures** **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 entreprises les plus signalées en 2019 :

Type de fraude	N^bre de rapports	N^bre de victimes	Pertes (en $)
Harponnage	452	204	20 131 958,34 $
Extorsion	285	55	91 656,81 $
Vente de marchandises	277	170	1 268 287,68 $
Service	143	41	381 026,04 $
Répertoire	85	7	4 964,56 $
Mystification	74	38	
Renseignements personnels	58	15	
Fausse facture	32	5	8 515,70 $
Marchandise	28	21	125 430,15 $
Chèques frauduleux	26	16	43 070,04 $

Les 10 fraudes touchant les entreprises les plus signalées d'après les pertes financières en 2019 :

Type de fraude	N^bre de rapports	N^bre de victimes	Pertes (en $)
Harponnage	452	204	$20,131,958.34
Vente de marchandises	277	170	$1,268,287.68
Services	143	41	$381,026.04
Marchandise	28	21	$125,430.15
Extorsion	285	55	$91,656.81
Chèques frauduleux	26	16	$43,070.04
Marchandise contrefaite	9	3	$21,703.80
Fausse facture	32	5	$8,515.70
Répertoire	85	7	$4,964.56
Prêts	13	3	$4,675.00

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

8) Signalement de la fraude

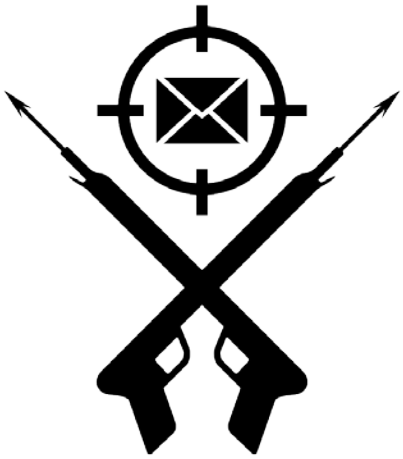
Dans le but d'atténuer les répercussions de la fraude, le CAFC recommande de prendre les six mesures suivantes :

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 entreprises :

Harponnage



Le harponnage est l'une des cyberattaques les plus courantes et les plus dangereuses actuellement employées pour frauder des entreprises et des organisations. Au moment de planifier une telle attaque, les fraudeurs prennent le temps de recueillir des renseignements sur leurs cibles afin d'envoyer des courriels convaincants qui semblent provenir d'une source fiable. Les fraudeurs s'infiltrent dans le compte de courriel d'une entreprise ou le mystifient. Ils créent une règle pour qu'une copie des courriels entrants soit transmise à l'un de leurs comptes et épluchent ces courriels pour étudier le niveau de langue utilisé par l'expéditeur et trouver des caractéristiques liées à des personnes, à des dates et à des paiements importants.

La cyberattaque a lieu lorsque le titulaire du compte de courriel est difficilement joignable par courriel ou téléphone. Si le compte de courriel du haut dirigeant n'a pas été compromis, les fraudeurs peuvent créer un domaine semblable à celui de l'entreprise et utiliser le nom du titulaire. Les coordonnées dont ils ont besoin se trouvent souvent sur le site Web de l'entreprise ou dans les médias sociaux.

Variantes courantes

- Un haut dirigeant envoie un courriel au service des comptes créditeurs de son entreprise afin de demander un paiement urgent pour conclure un marché privé.
- Une entreprise reçoit une copie d'une facture contenant des données de paiement à jour provenant apparemment d'un fournisseur ou d'un entrepreneur.
- Un comptable ou un planificateur financier reçoit une demande de retrait d'une somme importante qui semble provenir du compte de courriel d'un client.
- Le service de la paye reçoit un courriel semblant provenir d'un employé qui veut mettre à jour ses renseignements bancaires.
- Les membres d'une église, d'une synagogue, d'un temple ou d'une mosquée reçoivent une demande de don par courriel provenant prétendument de leur chef religieux.
- Un courriel semblant provenir d'une source fiable vous demande de télécharger une pièce jointe, mais celle-ci renferme un maliciel servant à infiltrer un réseau ou une infrastructure.

Indices

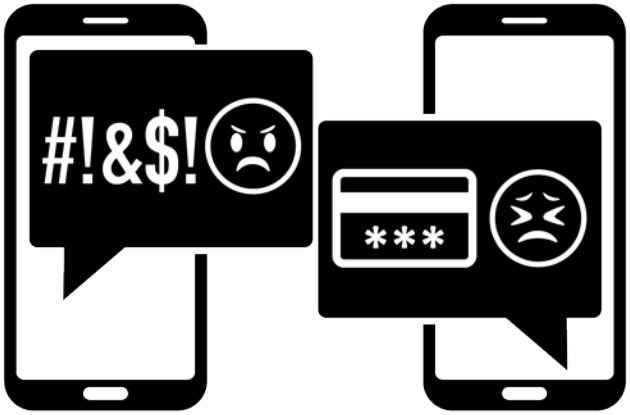
- Courriels non sollicités
- Courriel provenant directement d'un haut responsable avec qui vous ne communiquez pas d'habitude
- Demandes de confidentialité absolue
- Pression exercée ou impression d'urgence
- Demandes inhabituelles qui ne respectent pas les procédures internes
- Menace ou promesse de récompense

Comment vous protéger

- Tenez-vous au courant des fraudes ciblant les entreprises et sensibilisez tous les employés. Offrez une formation sur la fraude aux nouveaux employés.
- Mettez en place des modalités de paiement détaillées. Exigez la vérification des demandes inhabituelles.
- Établissez des mesures d'identification, de gestion et de signalement des fraudes.
- N'ouvrez pas les courriels non sollicités et ne cliquez pas sur les pièces jointes ou les liens suspects.
- Passez le curseur de votre souris sur une adresse de courriel ou un lien pour confirmer qu'ils sont corrects.
- Limitez la quantité d'information diffusée publiquement et faites preuve de prudence dans les médias sociaux.
- Mettez à niveau et à jour vos logiciels de sécurité.

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.

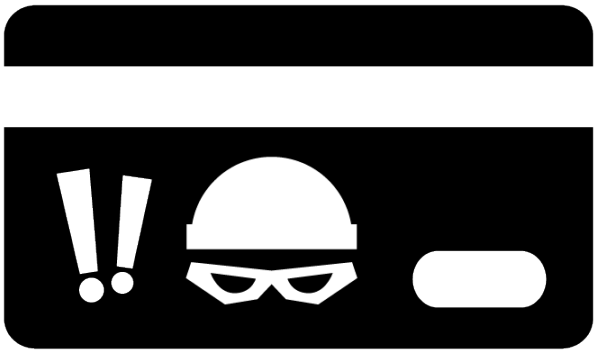
Rançongiciel : Un type de maliciel conçu pour infecter ou bloquer l'accès à un système ou à des données. Il existe plusieurs façons d'infecter un dispositif au moyen d'un maliciel, mais généralement, cela se produit lorsqu'une victime clique sur un lien malveillant ou une pièce jointe. À l'heure actuelle, 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.

Vente de marchandises ou de services

Les entreprises qui vendent de la marchandise ou offrent leurs services en ligne peuvent recevoir des paiements frauduleux. Dans bien des cas, les victimes reçoivent un montant plus élevé que le prix demandé, et on leur demande de rembourser la différence à une tierce partie pour conclure la transaction (souvent, une entreprise d'expédition). Les victimes qui se plient à la demande ne se font pas payer et perdent leur marchandise.



Fraude sans carte : La fraude sans carte peut survenir lorsqu'une entreprise accepte des commandes et des paiements par téléphone, Internet ou courriel. Le fraudeur utilise une carte de crédit volée pour payer les produits ou les services. Il demande la livraison urgente pour s'assurer de recevoir la commande avant que le titulaire de la carte ne découvre les frais. Si le titulaire de la carte conteste les frais, l'entreprise doit rembourser le montant payé avec la carte volée.

Indices

Indices liés au client

- Commandes effectuées à partir d'une seule adresse IP, mais au moyen de différents noms, adresses et cartes de paiement
- Adresses de courriel d'un service de courriel gratuit
- Plusieurs numéros de carte utilisés pour une même commande (les cartes sont toujours refusées)
- L'acheteur n'est pas le titulaire de la carte

Indices liés au produit ou à la commande

- Commandes plus grosses que la normale
- Commandes multiples du même produit, surtout s'il s'agit de gros achats
- Commandes de clients réguliers qui diffèrent des habitudes d'achat de ces derniers
- Commandes par le même client ou liées aux mêmes données de paiement, mais plusieurs adresses IP différentes

Indices liés à la livraison

- Client qui demande une livraison urgente, par exemple dans les 24 heures
- Plusieurs adresses d'expédition associées à une même carte
- Adresse de facturation différente de l'adresse de livraison
- Demande d'envoyer le montant versé en trop à une tierce partie

Comment vous protéger

- Connaissez les indices et vérifiez toutes les commandes reçues.
- Avant d'envoyer la marchandise, vérifiez l'information fournie par le client (numéro de téléphone, adresse de courriel, adresse d'expédition, etc.).
- Méfiez-vous des demandes d'expédition prioritaire de biens convoités par les fraudeurs.
- Vérifiez les demandes d'expédition prioritaire lorsque les adresses de facturation et d'expédition ne sont pas les mêmes.
- Pour toute commande douteuse, communiquez avec votre chargé du traitement des paiements. Assurez-vous que des mesures de sécurité sont en place pour éviter d'être victime de fraude et réduire les rétrofacturations indésirables.
- N'acceptez jamais de prélever un montant plus élevé que le prix du produit ou du service et d'envoyer la différence à une tierce partie.

Achat de marchandises ou de services

Les entreprises doivent faire preuve de diligence raisonnable avant d'acheter des produits ou des services de fournisseurs nouveaux et inconnus. Les fraudeurs peuvent publier des annonces dans des sites populaires ou les envoyer par la poste ou par télécopieur. Ils peuvent aussi facilement 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.

Les entreprises canadiennes sont ciblées par des fraudeurs qui offrent des services de traitement de paiements par carte de débit et de crédit et des fournitures de bureau à des prix réduits. Dans certains cas, les fraudeurs se présentent comme étant le fournisseur habituel de l'entreprise. Les entreprises peuvent recevoir une facture pour des produits qu'elles n'ont jamais commandés.

Indices – Comment vous protéger

- Si c'est trop beau pour être vrai, il s'agit probablement d'une escroquerie.
- Vérifiez la légitimité de l'URL et des 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.
- Renseignez vos employés sur les fraudes courantes qui touchent les entreprises.
- Ne fournissez aucune information concernant la marque ou le modèle de l'équipement de bureau à toute organisation autre que votre fournisseur habituel.
- Examinez les factures suspectes; les fraudeurs envoient de fausses factures pour des produits ou des services jamais achetés.

Fraudes liées aux annuaires d'entreprises

Les entreprises reçoivent une facture pour une publication ou une inscription non autorisée dans un annuaire. En général, les fraudeurs commencent par appeler l'entreprise pour confirmer ses coordonnées. Ils peuvent enregistrer la conversation initiale et manipuler l'enregistrement pour donner l'impression qu'une commande a été placée.

Indices – Comment vous protéger

- Apprenez aux employés de tous les échelons à se méfier des appels non sollicités.
- Dressez une liste des fournisseurs de services autorisés avec qui votre entreprise fait 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.


Canadian Anti-Fraud Centre
C A F C
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