CENTRE ANTIFRAUDE DU CANADA

Gendarmerie royale du Canada | Royal Canadian Mounted Police | Bureau de la concurrence Canada | Competition Bureau Canada | Police Provinciale de l'Ontario | Canada

ENTREPRISES

Trousse de prévention de la fraude 2022

Royal Canadian Mounted Police | Gendarmerie royale du Canada | Competition Bureau Canada | Bureau de la concurrence Canada | Ontario Provincial Police | Canada

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. Cette année, les efforts seront axés sur l'économie numérique des fraudes et des escroqueries. 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 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 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 (#MPF2022). Nous publierons notre bulletin chaque semaine sur Facebook et Twitter.

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

Tout au long du mois de Mars, le CAFC publiera un bulletin à chaque semaine qui mettra en vedette les fraudes les plus signalées au CAFC en 2021 reliées à l'usurpation d'identité.

Bulletins
Semaine 1 : Investissements
Semaine 2 : Extorsion et Urgence
Semaine 3 : Hameçonnage
Semaine 4 : Harponnage

Le CAFC attirera l'attention des abonnés de ses comptes de réseaux sociaux en discutant chaque bulletin durant la semaine.

Facebook : Centre antifraude du Canada
Twitter : @antifraudecan

Mars 2022 – Un vidéo #MPF2022 sera partagé sur les médias sociaux pour mettre en vedette les façons de vous protéger contre être victime.

Mars 2022

	Mardi 1er mars Facebook et Twitter : #MPF2022 Introduction et lancement	**Mercredi 2 mars** Facebook et Twitter Diffusion de messages #MPF2022 de partenaires	**Jeudi 3 mars** Bulletin Facebook et Twitter – Arnaques d'investissement	**Vendredi 4 mars** Facebook et Twitter Médias sociaux Usurpation d'identité Arnaques d'investissement
Lundi 7 mars Facebook et Twitter Faux sites Web d'investissement dans la cryptomonnaie	**Mardi 8 mars** Facebook et Twitter Diffusion de messages #MPF2022 de partenaires	**Mercredi 9 mars** Facebook et Twitter Demande de transfert d'investissements de cryptomonnaie vers des plateformes frauduleuses	**Jeudi 10 mars** Facebook et Twitter Diffusion de messages #MPF2022 de partenaires	**Vendredi 11 mars** Facebook et Twitter Fraude pyramidale liée à l'emploi et arnaques d'investissement
Lundi 14 mars Facebook et Twitter Bulletin : Stratagèmes d'extorsion	**Mardi 15 mars** Facebook et Twitter Appels téléphoniques de l'ASFC automatisés et menaçants	**Mercredi 16 mars** Facebook et Twitter Diffusion de messages #MPF2022 de partenaires	**Jeudi 17 mars** Facebook et Twitter Diffusion de messages #MPF2022 de partenaires	**Vendredi 18 mars** Facebook et Twitter Lettres de menaces faussement attribuées à la GRC
Lundi 21 mars Facebook et Twitter Bulletin : Hameçonnage	**Mardi 22 mars** Facebook et Twitter Diffusion de messages #MPF2022 de partenaires	**Mercredi 23 mars** Facebook et Twitter Messages d'hameçonnage faussement attribués à des organismes gouvernementaux	**Jeudi 24 mars** Facebook et Twitter Diffusion de messages #MPF2022 de partenaires	**Vendredi 25 mars** Facebook et Twitter Messages d'hameçonnage faussement attribués à des institutions financières
Lundi 28 mars Facebook et Twitter Bulletin : Harponnage	**Mardi 29 mars** Facebook et Twitter Statistiques et indices de harponnage	**Mercredi 30 mars** Facebook et Twitter Diffusion de messages #MPF2022 de partenaires	**Jeudi 31 mars** Facebook et Twitter Comment vous protéger contre les stratagèmes de harponnage	

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 2021, le CAFC a reçu 104,295 signalements de fraude représentant des pertes totales plus de 379 millions de dollars. De plus, 2,368 signalements ont été faits par des entreprises canadiennes, dont les pertes déclarées s'élèvent à plus de 72.2 millions de dollars.

Voici les dix fraudes les plus courantes dont ont été victimes les entreprises en 2021, selon le nombre de signalements :

Type de fraude	N^{bre} de signalements	N^{bre} de victimes	Pertes (en $)
Harponnage	531	239	49,3 millions
Extorsion	309	99	0.4 millions
Fraude liée à la vente	301	209	3 millions
Service	150	72	1,1 million
Emploi	109	33	5,3 millions
Marchandise	108	77	4,5 millions
Renseignements personnels	96	40	S.O.
Hameçonnage	66	10	S.O.
Fausse Facture	45	9	70 000$
Investissements	29	16	1,7 million

Voici les dix fraudes ayant entraîné les plus importantes pertes financières pour les entreprises en 2021 :

Type de fraude	Nbre de signalements	Nbre de victimes	Pertes (en $)
Harponnage	531	239	$49.3 M
Prêt	21	17	$5.6 M
Emploi	109	33	$5.3 M
Marchandise	108	77	$4.5 M
Fraude liée à la vente	301	209	$3.0 M
Investissements	29	16	$1.7 M
Service	150	72	$1.1 M
Extorsion	309	99	$0.4 M
Stratagème de récupération d'argent	2	2	$0.3 M
Prix gagné	13	3	$0.1 M

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

9) Signalement de la fraude

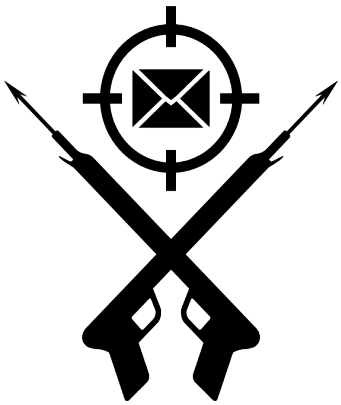
La fraude évolue. Elle peut souvent se poursuivre sur une longue période de temps et constitue un crime qui est difficile à déceler et à signaler. Pour vous faciliter la tâche, le CAFC recommande de prendre les six mesures suivantes :

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 entreprises canadiennes :

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. Les fraudeurs épluchent les courriels pour étudier le niveau de langue utilisé par l'expéditeur et cherchent 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 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 votre réseau.

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

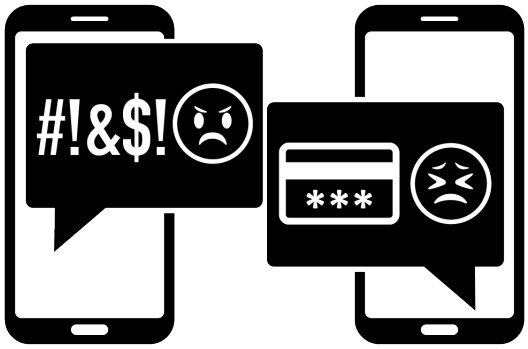
- Tenez-vous au courant des fraudes ciblant les entreprises et sensibilisez tous les employés. Offrez une formation sur la fraude aux nouveaux employés.
- Mettez en place des modalités de paiement détaillées. Exigez la vérification des demandes inhabituelles.
- Établissez des mesures d'identification, 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.



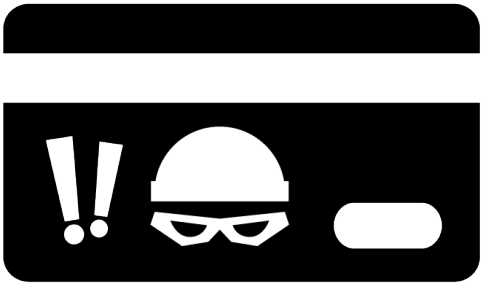
Indices – Comment vous protéger

- 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.

Fraude liée à la vente

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 aussi 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, 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.

Prêts frauduleux

De nombreux Canadiens connaissent des difficultés financières en raison de la pandémie. Le gouvernement du Canada offre diverses formes de soutien financier, mais des Canadiens cherchent malgré tout à obtenir des prêts. Malheureusement, il y a augmentation des signalements de sites Web de prêts frauduleux.

Ces sites Web ressemblent à ceux d'établissements de prêt légitimes. Les demandes frauduleuses de prêt que les victimes remplissent servent à recueillir leurs renseignements personnels. Vol d'identité et fraude peuvent s'ensuivre. Une fois le prêt rapidement approuvé, les fraudeurs exigeront des frais pour le garantir. La victime ne reçoit jamais d'argent.

Indices – Comment vous protéger

- Dans la plupart des provinces, il est illégal pour une entreprise d'exiger des frais initiaux avant l'obtention de votre prêt. Vous ne devriez jamais envoyer d'argent en premier.
- Méfiez-vous des entreprises qui offrent des prêts garantis même si vous avez un mauvais crédit ou aucun crédit.
- Méfiez-vous des prêts approuvés instantanément.
- Faites des recherches avant de fournir vos renseignements personnels.
- Communiquez avec l'agence de protection des consommateurs ou l'organisme de réglementation financière de votre province pour confirmer qu'une entreprise est un prêteur légitime.
- Cessez tout contact avec l'entreprise si celle-ci demande un paiement par virement de fonds par courriel, par l'intermédiaire d'une entreprise de transfert de fonds ou par cartes de crédit prépayées

Liste pour se protéger votre entreprise contre la fraude et la cybercriminalité

- ✓ Renseignez vos employés au sujet de la fraude et de la cybercriminalité.
- ✓ Ayez des politiques ou un plan en place pour aider les employés.
- ✓ Sachez à qui vous avez affaire. Dressez une liste des entreprises auxquelles vous faites généralement appel pour aider les employés à distinguer les vrais contacts des faux.
- ✓ Gare aux factures sur lesquelles figurent le nom d'entreprises légitimes. Les fraudeurs utilisent des noms de véritables entreprises comme les Pages jaunes pour que les factures semblent authentiques. Assurez-vous de bien examiner les factures avant d'effectuer un paiement.
- ✓ Ne donnez pas de renseignements si vous recevez un appel ou un courriel non sollicité.
- ✓ Apprenez aux employés de tous les échelons à se méfier des appels non sollicités. S'ils ne sont pas l'auteur de l'appel, ils ne devraient pas fournir ni confirmer :
    - l'adresse de l'entreprise;
    - le numéro de téléphone de l'entreprise;
    - des numéros de compte;

- des renseignements au sujet du matériel de bureau (p. ex. marque et modèle de l'imprimante).

✓ Limitez les pouvoirs de vos employés en autorisant seulement quelques employés à approuver les achats et à régler les factures.

✓ Méfiez-vous du harponnage. Ayez des politiques en place pour confirmer verbalement les demandes urgentes de virement électronique ou d'achat.

✓ Examinez les commandes potentiellement frauduleuses. Méfiez-vous :

- des commandes plus grosses que la normale;
- des commandes multiples du même produit;
- des commandes de gros achats;
- des commandes payées au moyen de plusieurs cartes de crédit.

✓ Consultez le Guide Pensez cybersécurité pour les entreprises.