Bureau de la concurrence Canada

Competition Bureau Canada

LE PETIT LIVRE NOIR DE LA FRAUDE

Canada

Publié pour la première fois par le Bureau de la concurrence Canada en 2012

Cette publication n'est pas un document juridique. Elle renferme, à titre de référence, des renseignements d'ordre général.

Pour obtenir des renseignements sur les activités du Bureau de la concurrence, veuillez vous adresser au :

Centre des renseignements
Bureau de la concurrence
50, rue Victoria
Gatineau (Québec) K1A 0C9

Téléphone : 819-997-4282
Numéro sans frais : 1-800-348-5358
ATS (pour les malentendants) : 1-866-694-8389
Télécopieur : 819-997-0324
Site Web : www.bureaudelaconcurrence.gc.ca

Pour obtenir un exemplaire de cette publication ou un format substitut (Braille, gros caractères, etc.), veuillez communiquer avec le Centre des renseignements du Bureau de la concurrence aux numéros indiqués ci-dessus.

Cette publication est également offerte sur Internet en version HTML à l'adresse suivante :
http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/04333.html

Autorisation de reproduire

Nº de cat. lu54-42/2018
ISBN 978-0-660-24817-2

2018-03-01

Also available in English under the title The Little Black Book of Scams 2nd edition.

Dans cette publication, la forme masculine désigne tant les femmes que les hommes.

LE PETIT LIVRE NOIR DE LA FRAUDE

2E ÉDITION

PRÉFACE

Les fraudeurs sont sournois et malins. Nous sommes tous leur cible, des plus jeunes aux plus âgés. Ils s'en prennent même aux entreprises. Personne n'est à l'abri de la fraude.

Notre groupe de superhéros a trouvé des moyens de détecter les arnaques. Leur secret? Savoir, c'est avoir le pouvoir.

Lisez ce livre pour apprendre comment devenir à votre tour un superhéros de la fraude. Partagez-le avec vos amis et vos proches et commencez à gagner en puissance!

TABLE DES MATIÈRES

CONTRER LA FRAUDE : UN ABC

Devenez un réel superhéros en vous munissant des renseignements dont vous avez besoin pour lutter contre la fraude. Protégez vos proches, vous-même et votre argent.

Vous travaillez fort pour votre argent. Vous voulez le dépenser pour des choses qui vous tiennent à cœur : l'éducation de vos enfants, un voyage excitant ou le plus récent téléphone intelligent.

Les fraudeurs existent. Tous les jours, ils sont à la recherche de leur prochaine victime. Ils vous ciblent en ligne, au téléphone, par courrier ou en personne.

Vous êtes une cible. Des milliers de Canadiens perdent chaque année des millions de dollars à cause de fraudeurs. L'impact de la fraude peut s'avérer dévastateur pour les familles et les entreprises.

Apprenez à lutter contre la fraude. Ce livre présente 12 des fraudes les plus courantes visant les Canadiens de nos jours, ainsi que des trucs et des astuces sur la façon de vous protéger ou de procéder si vous vous faites prendre.

Signalez-la! Tout le monde peut se faire piéger, des adolescents aux grands-parents et aux dirigeants d'entreprise. Le mieux, c'est de signaler la fraude aux organismes adéquats, peu importe le montant. Ne soyez pas gêné, car cela contribuera à éviter que d'autres personnes tombent dans le panneau.

Savoir, c'est avoir le pouvoir. Protégez-vous en vous renseignant. En plus de ce livre, nombre de sites Web fiables offrent de plus amples renseignements.

Le Centre antifraude du Canada, géré par la Gendarmerie royale du Canada, le Bureau de la concurrence et la Police provinciale de l'Ontario, offre de nombreux renseignements sur la fraude. Gagnez en puissance dès aujourd'hui en visitant le site www.centreantifraude.ca!

ABONNEMENTS PIÉGÉS

De belles offres peuvent être en fait des pièges dispendieux!

Un abonnement piégé peut vous attraper en offrant des essais « gratuits » ou « à faible coût » de produits ou de services : pilules pour maigrir, nourriture santé, produits pharmaceutiques ou soins anti-âge, et bien d'autres.

Lorsque vous fournissez votre information de carte de crédit pour couvrir les frais de transport, vous embarquez sans le savoir dans un abonnement mensuel. La livraison et la facturation sont parfois difficiles ou impossibles à arrêter.

Les fraudeurs utilisent les sites Web, les courriels, les médias sociaux et le téléphone pour rouler les gens. Les stratégies de vente sous pression, comme « pour un temps limité », visent souvent à vous faire prendre une décision hâtive.

Pour vous protéger :

- Fiez-vous à votre instinct. Si c'est trop beau pour être vrai, ne vous abonnez pas.
- Avant de vous décider, renseignez-vous sur l'entreprise et lisez les commentaires, surtout les négatifs. Les bureaux d'éthique commerciale sont une bonne source d'information.
- Ne vous abonnez pas si les conditions sont introuvables ou incompréhensibles. Attention aux cases déjà cochées, aux clauses d'annulation ou de retour des produits et aux frais imprécis!
- Si vous vous abonnez, gardez tous les documents, les factures, les courriels et les textos.
- Vérifiez régulièrement votre relevé de carte de crédit pour repérer les frais récurrents ou inhabituels.
- Si vous n'arrivez pas à annuler l'abonnement, communiquez avec votre fournisseur de carte de crédit, votre organisme de protection des consommateurs local ou un organisme d'application de la loi.

Si vous soupçonnez une fraude, signalez-la immédiatement.

Allez aux pages 34 et 36 pour obtenir plus de renseignements.

VOL D'IDENTITÉ

Assurez-vous de ne pas « partager » votre identité!

Les fraudeurs sont toujours à l'affût de vos renseignements personnels pour les utiliser à leurs fins : faire des achats, obtenir un passeport, recevoir des prestations gouvernementales, demander un prêt, etc. Votre vie pourrait s'en trouver chamboulée.

Les techniques vont de simplistes à élaborées. Les fraudeurs peuvent fouiller les poubelles ou voler le courrier. En ligne, ils utilisent des logiciels espions et des virus, en plus du piratage ou de l'hameçonnage (voir p. 22).

Voici ce que les fraudeurs recherchent : renseignements de carte de crédit et de compte bancaire, nom complet et signature, date de naissance, numéro d'assurance sociale, adresse complète, nom de jeune fille de votre mère, identifiants en ligne et mots de passe, numéro de permis de conduire et de passeport.

Le vol d'identité est un crime grave!

Pour vous protéger :

- Ne donnez jamais de renseignements personnels au téléphone, par texto, par courriel ou sur Internet.
- Ne consultez pas vos renseignements personnels sur un ordinateur ou un réseau Wi-Fi public.
- Créez un mot de passe fort et unique pour chaque compte en ligne, appareil et réseau Wi-Fi.
- Utilisez un service de paiement en ligne sécuritaire (adresse URL en « https » et symbole de cadenas verrouillé).
- Ne donnez pas vos renseignements personnels sur les médias sociaux. Jumelés à vos photos, ils peuvent servir à des fins frauduleuses.
- Cachez toujours le NIP de votre carte. Ne perdez jamais de vue votre carte si vous la donnez au caissier.
- Déchiquetez ou détruisez les documents contenant des renseignements personnels.

Si vous soupçonnez une fraude, signalez-la immédiatement.

Allez aux pages 34 et 36 pour obtenir plus de renseignements.

FRAUDE DU FAUX PDG

Votre PDG demande un transfert d'argent urgent. Le courriel est-il légitime?

Vous travaillez en comptabilité ou en finances? Vous avez les autorisations requises pour transférer de l'argent? Votre patron est un haut dirigeant, comme un président-directeur général (PDG)? Si c'est le cas, soyez prudent. Vous êtes la cible de cette fraude.

En général, les fraudeurs se font passer pour un dirigeant, soit en obtenant l'accès à son courriel ou en l'imitant. Ils envoient des courriels qui semblent réalistes pour vous faire transférer de l'argent à un tiers.

Les courriels vous font croire que la demande est urgente et confidentielle. Par exemple, on vous dit que l'argent servira à obtenir un contrat important, à finaliser une transaction confidentielle ou à modifier les renseignements d'un fournisseur.

Les fraudeurs envoient ces courriels à des moments stratégiques : quand le haut dirigeant est en voyage ou difficile à joindre. Cette arnaque peut coûter des millions aux entreprises.

L'arnaque du faux PDG, qui est de plus en plus fréquente, touche des entreprises de toutes tailles.

Pour vous protéger :

- Utilisez un antivirus fiable et à jour et des mots de passe forts pour protéger vos systèmes informatiques.
- Confirmez au téléphone ou en personne toute demande de transaction. N'utilisez jamais les coordonnées fournies dans un courriel.
- Validez l'adresse courriel : les fraudeurs créent souvent des adresses qui ressemblent aux véritables, en changeant une ou deux lettres.
- Encouragez votre employeur à mettre en place un processus à plusieurs niveaux d'approbation pour transférer de l'argent.
- Limitez les renseignements que vous rendez publics. Les fraudeurs se servent de l'information disponible en ligne et sur les médias sociaux pour trouver leurs victimes et planifier leur arnaque.

Si vous soupçonnez une fraude, signalez-la immédiatement.

Allez aux pages 34 et 36 pour obtenir plus de renseignements.

FRAUDES MÉDICALES OU LIÉES À LA SANTÉ

Méfiez-vous des soins miracles qui offrent une guérison rapide et facile.

Certains fraudeurs cherchent à profiter de la souffrance des gens. Il y a trois types courants de fraudes médicales : soins miracles, programmes pour maigrir et fausses pharmacies en ligne. Ces fraudes prennent souvent la forme de messages commandités sur les médias sociaux ou de fenêtres publicitaires dans les sites Web.

Les fraudeurs offrent des produits et des services qui semblent légitimes – une médecine non conventionnelle ou un traitement pour soigner rapidement et facilement un trouble médical grave. Ces produits et services sont parfois parrainés par des vedettes ou appuyés par des témoignages de personnes prétendant avoir été guéries.

Les arnaques pour maigrir promettent des résultats exceptionnels sans effort. Les fraudeurs recommandent des régimes inhabituels, des exercices révolutionnaires, des appareils brûlant les calories ou des produits novateurs, comme des pilules, des timbres ou des crèmes.

Les fausses pharmacies en ligne offrent des médicaments peu coûteux ou sans exiger de prescription. Elles font leurs annonces en ligne et dans des pourriels. Si vous recevez le produit promis, rien ne garantit qu'il s'agisse du vrai médicament ni qu'il soit sécuritaire.

Pour vous protéger :

- Sachez qu'il n'existe pas de pilule magique ou de traitement miracle pour maigrir rapidement ou traiter une condition médicale.
- Ne croyez pas tout ce qu'on vous dit au sujet de médicaments, de suppléments ou d'autres traitements. Consultez votre médecin.
- N'acceptez jamais quelque chose sous pression, en particulier si vous devez faire un gros paiement d'avance ou signer un contrat à long terme.
- N'oubliez pas qu'une vraie pharmacie en ligne exige toujours une prescription valide.
- Mettez en doute l'appui de vedettes et les témoignages.

Si vous soupçonnez une fraude, signalez-la immédiatement.

Allez aux pages 34 et 36 pour obtenir plus de renseignements.

FRAUDES RELATIVES AUX SERVICES DE RENCONTRE

Qui se trouve réellement derrière l'écran?

Restez sur vos gardes et faites attention aux fraudeurs qui cherchent à vous faire relâcher votre vigilance en faisant appel à votre côté romantique et compatissant. Ils se cachent non seulement sur les faux sites de rencontre, mais aussi sur les sites populaires légitimes.

Sur un vrai site de rencontre, un fraudeur pourrait vous envoyer quelques messages avec des photos flatteuses de sa personne... ou de celle qu'il dit être. Une fois que vous êtes sous le charme, il vous demande d'envoyer de l'argent pour diverses raisons : un membre de famille malade, ou une situation désespérée pour laquelle il a besoin de votre aide. Après avoir payé, vous ne le reverrez sans doute plus.

Un fraudeur peut aussi créer un faux site de rencontre dans lequel vous payez pour chaque message envoyé et reçu. Pour vous forcer à répondre et payer, le fraudeur vous intriguera par de vagues messages où il déclare son amour.

Dans bien des cas, le fraudeur essaye même d'organiser une rencontre en personne pour rendre l'arnaque plus crédible.

Pour vous protéger :

- N'envoyez jamais d'argent et ne donnez jamais de renseignements financiers sur un site de rencontre.
- Fiez-vous à votre instinct. Posez des questions et lisez attentivement les conditions d'utilisation du site avant de vous inscrire.
- Sachez quels services sont gratuits, lesquels ne le sont pas et ce qu'il faut faire pour annuler son inscription.
- Assurez-vous de n'utiliser que des sites de rencontre légitimes et fiables. Lisez toujours l'adresse attentivement; les fraudeurs imitent souvent les adresses de vrais sites.
- Souvenez-vous qu'il est très peu probable qu'une personne déclare son amour éternel après seulement quelques lettres, courriels, appels ou photos.

Si vous soupçonnez une fraude, signalez-la immédiatement.

Allez aux pages 34 et 36 pour obtenir plus de renseignements.

FRAUDES VISANT LES ENTREPRISES

Restez au courant des stratagèmes visant les entreprises!

Les entreprises de toutes tailles peuvent être la cible de fraudes bien organisées, alors assurez-vous de les reconnaître.

Une de ces arnaques concerne les annuaires d'entreprises. Un fraudeur envoie à votre entreprise une proposition pour un annuaire en ligne ou pour une inscription ou une publicité dans un magazine, un journal ou un annuaire d'entreprises. Vous recevez un appel pour confirmer l'adresse et d'autres détails. Puis, le service de la comptabilité reçoit une facture, qu'il paye sans savoir que votre entreprise n'a jamais commandé ou approuvé le service.

Une autre arnaque courante touche les produits de santé et de sécurité. Une personne prétendant travailler pour le gouvernement provincial vous appelle en disant que vous devez remplacer votre trousse de premiers soins ou mettre à jour la formation en santé et sécurité de l'entreprise. Dans chaque cas, on pourrait vous dire d'agir rapidement.

Une autre fraude possible a trait au matériel de bureau reçu sans commande, pour lequel on vous demande de payer.

Souvent, les fraudeurs vous harcèlent pour que vous payiez ce qu'ils disent que vous leur devez. Ils vous font même croire qu'ils vous dénonceront à une agence de recouvrement.

Pour vous protéger :

- Informez tous vos employés et collègues de travail de la possibilité d'appels non sollicités.
- Créez une liste des entreprises avec lesquelles vous faites affaire.
- Limitez le nombre d'employés qui peuvent approuver les achats ou payer les factures.
- Établissez des procédures claires pour la vérification, le paiement et la gestion des comptes et des factures.
- Communiquez avec les autorités provinciales pour connaître vos obligations légales.
- Vérifiez les factures attentivement avant d'effectuer un paiement. Les fraudeurs utilisent des noms ou des logos semblables à ceux d'entreprises connues pour rendre leurs factures réalistes.

Si vous soupçonnez une fraude, signalez-la immédiatement.

Allez aux pages 34 et 36 pour obtenir plus de renseignements.

HAMEÇONNAGE

Soyez aux aguets. Les messages sont faciles à créer de toutes pièces!

Puisque nous passons plus de temps en ligne, les fraudeurs inventent d'autres arnaques dans le cyberespace.

L'hameçonnage, c'est recevoir un courriel non sollicité d'une organisation qui se prétend légitime (institution financière, entreprise, organisme gouvernemental). Le fraudeur vous demande de fournir ou de confirmer, par courriel ou en cliquant sur un hyperlien, des renseignements personnels ou financiers – numéro de carte de crédit, mots de passe et numéro d'assurance sociale.

C'est le même principe pour l'hameçonnage par texto.

Ces messages reprennent souvent le ton et le logo d'un organisme de confiance et demandent en général que vous agissiez. Peu importe la forme, le but est d'obtenir vos renseignements personnels.

Pour vous protéger :

- Sachez qu'un organisme fiable ne demande jamais d'information personnelle par courriel ou texto.
- Ignorez les courriels et textos de personnes inconnues.
- Supprimez les messages suspects; ils peuvent contenir des virus.
- Ne répondez pas aux pourriels, même pour annuler votre abonnement; n'ouvrez pas les pièces jointes et ne cliquez pas sur les liens.
- Pour voir l'adresse d'un hyperlien sans cliquer, glissez votre souris sur le lien. Vérifiez soigneusement s'il est exact.
- Mettez à jour l'antivirus de tous vos appareils.
- N'utilisez jamais le numéro de téléphone ou l'adresse courriel fournis dans un message suspect; utilisez les renseignements sur les sites Web officiels.

Si vous soupçonnez une fraude, signalez-la immédiatement.

Allez aux pages 34 et 36 pour obtenir plus de renseignements.

FRAUDES CIBLANT LES CONTRIBUABLES

Vous recevez un appel ou un courriel d'un percepteur d'impôt. Est-il authentique?

Un texte ou un courriel de l'Agence du revenu du Canada (ARC) vous parvient, prétendant que vous avez droit à un remboursement. Il suffit de fournir vos informations bancaires. Faites attention! Cette situation, trop belle pour être vraie, est un exemple parfait d'arnaque.

Cette arnaque peut aussi prendre la forme d'un appel. On vous dit que vous devez de l'argent à l'ARC et que, si vous ne payez pas immédiatement, vous serez dénoncé à la police.

Bref, si vous recevez un appel, une lettre, un courriel ou un texte disant que vous devez de l'argent à l'ARC, vérifiez votre information en ligne à « Mon dossier » ou composez le 1-800-959-8281.

Pour vous protéger :

En aucun cas l'ARC :

- n'utilisera un langage agressif ou menaçant;
- ne menacera d'appeler ou d'envoyer la police;
- ne demandera de payer par carte de crédit prépayée ou carte-cadeau (par exemple, iTunes ou Home Depot);
- ne percevra ou n'enverra des paiements par transfert électronique Interac;
- n'utilisera les textos pour communiquer avec vous.

Les courriels de l'ARC :

- ne demandent jamais d'information financière;
- ne donnent jamais d'information financière.

L'ARC accepte les méthodes de paiement suivantes :

- opérations bancaires en ligne;
- cartes de débit;
- prélèvements automatiques.

Si vous soupçonnez une fraude, signalez-la immédiatement.

Allez aux pages 34 et 36 pour obtenir plus de renseignements.

FRAUDES LIÉES AU PORTE-À-PORTE

Toc, toc, toc! Qui est là? Un fraudeur!

Même si nous vivons à l'ère numérique, des fraudeurs utilisant de bonnes vieilles méthodes peuvent se présenter à la porte – une menace pour vous et les entreprises. Ces vendeurs frappent à votre porte et insistent pour vous convaincre d'acheter un produit ou un service dont vous ne voulez pas ou dont vous n'avez pas besoin.

Ces discours agressifs servent souvent à soutirer de l'argent pour des dons de bienfaisance, des occasions d'investissement ou des services ménagers ou d'entretien de divers appareils (chauffe-eau, fournaise, conditionneur d'air).

Dans la plupart des cas, vous ne recevrez jamais le produit ou le service promis; dans d'autres, il est de mauvaise qualité ou ne correspond pas à ce qui avait été promis.

Pour vous protéger :

- Ne prenez pas de décision hâtive; faites vos recherches sur le vendeur et le produit.
- Demandez à voir une pièce d'identité avec photo et notez le nom de la personne et de l'entreprise ou de l'organisme qu'elle représente.
- Demandez comment les dons sont distribués par l'organisme et obtenez ces renseignements par écrit.
- Ne donnez jamais de renseignements personnels ni de copie de factures ou de relevés bancaires.
- Ne laissez entrer que les personnes en qui vous avez confiance.
- Ne signez rien et lisez toujours les petits caractères.
- Connaissez vos droits. Communiquez avec votre organisme de protection des consommateurs local, car la plupart des provinces et des territoires possèdent leurs propres lois et lignes directrices.

Si vous soupçonnez une fraude, signalez-la immédiatement.

Allez aux pages 34 et 36 pour obtenir plus de renseignements.

FRAUDES DE LA SITUATION D'URGENCE

Grands-parents gâteau, n'agissez pas trop vite!

La fraude de la situation d'urgence cible des grands-parents attentionnés, en profitant de leurs émotions pour voler leur argent.

Généralement, la fraude se déroule comme suit : les grands-parents reçoivent un appel d'une personne prétendant être un de leurs petits-enfants. Cette personne affirme être en difficulté (avoir un accident d'auto, être en prison, ne pas pouvoir revenir au pays) et avoir besoin d'argent immédiatement.

Elle vous posera des questions pour vous faire révéler des renseignements personnels et vous fera jurer de ne rien dire pour éviter que la famille ne l'apprenne, sous prétexte d'être embarrassée par la situation.

Dans certaines versions, deux personnes seront au téléphone : l'une prétendant être le petit-fils ou la petite-fille et l'autre, un policier ou avocat.

Dans d'autres cas, le fraudeur prétend être un ancien voisin ou un ami de la famille.

Pour vous protéger :

- Prenez le temps de confirmer l'histoire. Les fraudeurs comptent sur votre désir d'aider rapidement vos proches en situation d'urgence.
- Appelez les parents ou les amis pour savoir où votre petit-fils ou petite-fille se trouve.
- Posez des questions au téléphone auxquelles seuls vos proches peuvent répondre et confirmez leur identité avant de les aider.
- N'envoyez jamais d'argent à une personne que vous ne connaissez pas ou en qui vous n'avez pas confiance.
- Ne donnez aucun renseignement personnel à la personne qui appelle.

Si vous soupçonnez une fraude, signalez-la immédiatement.

Allez aux pages 34 et 36 pour obtenir plus de renseignements.

FRAUDES LIÉES À L'ACHAT DE MARCHANDISES

Les vendeurs en ligne ne sont pas tous fiables!

Le magasinage en ligne est le passe-temps préféré de nombreux consommateurs. Cependant, plusieurs aubaines en ligne sont trop belles pour être vraies. Elles vont des sacs à main de marque bon marché aux articles électroniques à prix très réduit, et bien plus.

Les fraudeurs peuvent créer des comptes sur des sites d'enchères légitimes, comme eBay, ou de marché en ligne, comme Kijiji ou Craigslist. Ils vont alors annoncer des produits à un prix dérisoire pour vous inciter à les acheter.

Au bout du compte, si vous recevez le produit, il pourrait être de mauvaise qualité ou une contrefaçon médiocre.

Dans certains cas, les fraudeurs vous demandent de cliquer sur un lien commandité qui vous dirige vers un site Web qui semble authentique. Si vous achetez quelque chose, vous n'aurez ni la protection ni le service offerts par un site Web légitime.

Si un site ou une offre sautent aux yeux, il y a sûrement quelque chose qui cloche.

Pour vous protéger :

- Achetez auprès d'entreprises ou de personnes avec qui vous avez déjà fait affaire ou que vous connaissez de réputation.
- N'acceptez rien en dehors du site d'enchères.
- Méfiez-vous des vendeurs à l'étranger ou qui ont peu de rétroaction, voire aucune.
- Utilisez une carte de crédit pour vos achats en ligne; de nombreuses cartes offrent une protection et peuvent vous rembourser.
- Méfiez-vous des sites Web qui contiennent des erreurs d'orthographe ou de grammaire.
- Lisez attentivement les politiques de retour et de remboursement, y compris les petits caractères.
- Demandez au fournisseur de confirmer le service, les délais de livraison et le coût total.

Si vous soupçonnez une fraude, signalez-la immédiatement.

Allez aux pages 34 et 36 pour obtenir plus de renseignements.

FRAUDES LIÉES À LA VENTE DE MARCHANDISES

Les fraudeurs peuvent se faire passer pour des acheteurs.

Si vous vendez des articles en ligne, à des fins personnelles ou professionnelles, faites attention à qui vous les vendez. Sinon, vous pourriez vous faire prendre par des filous qui cherchent à voler votre marchandise, votre argent ou les deux.

Dans certains cas, le fraudeur accepte d'acheter l'article sans le voir. Vous recevez une notification PayPal ou par courriel comme quoi le paiement est en attente.

Le hic, c'est que vous ne pouvez recevoir le paiement qu'après avoir fourni un numéro de suivi pour l'article en question. Quand vous donnez le numéro, l'article est déjà envoyé et vous vous rendrez compte que l'avis de paiement était faux.

Dans d'autres cas, le paiement pourrait se faire au moyen d'un faux transfert d'argent, d'un chèque frauduleux ou d'une carte de crédit volée.

Le fraudeur pourrait aussi envoyer un message expliquant qu'un problème avec votre compte PayPal ou votre compte bancaire empêche le paiement. Vous devez payer des frais pour ouvrir un compte d'affaires afin de terminer la transaction. Le filou offrira de les payer si vous le remboursez au moyen d'un service de transfert ou de virement. Si vous acceptez, les « frais » ne profiteront qu'au fraudeur.

Pour vous protéger :

- Effectuez toujours un échange dans un endroit public, sécuritaire et connu.
- Méfiez-vous des courriels génériques remplis de fautes.
- Méfiez-vous des acheteurs à l'étranger qui veulent acheter des produits ou des articles sans les voir.
- Vérifiez les adresses courriel; les fraudeurs utilisent souvent des adresses qui semblent légitimes, à une ou deux lettres près.
- N'envoyez jamais de l'argent pour en recevoir.

Si vous soupçonnez une fraude, signalez-la immédiatement.

Allez aux pages 34 et 36 pour obtenir plus de renseignements.

SIGNAUX D'ALARME : LES CHOSES À SURVEILLER

Apprenez à reconnaître les signes indiquant qu'il y a anguille sous roche.

Virement électronique. De nombreuses fraudes utilisent une demande de virement électronique au moyen d'un service de transfert d'argent (MoneyGram ou Western Union) ou de cryptomonnaie (Bitcoins). N'oubliez pas que ce genre de transfert équivaut à un envoi d'argent comptant. Une fois que le montant a été retiré, il est presque impossible de revoir son argent.

Trop payé. Lorsque vous vendez quelque chose, surtout en ligne, faites attention à la façon dont vous êtes payé. Un fraudeur peut vous envoyer un chèque de caisse, personnel ou d'affaires contrefait, indiquant un montant supérieur à ce qu'il vous doit. Il vous demande de déposer le chèque et de transférer l'argent en trop immédiatement. Lorsque votre banque réalise que le chèque est faux, votre argent a déjà été retiré.

Erreurs d'orthographe. Méfiez-vous des courriels, messages ou sites Web qui contiennent des mots courants mal orthographiés, des erreurs de grammaire qui rendent la lecture difficile, ou des expressions mal utilisées. Les courriels et les adresses Web devraient aussi être lus attentivement pour repérer des erreurs ou des différences subtiles.

Demande de renseignements personnels. Les fraudeurs peuvent demander aux victimes éventuelles de fournir davantage de renseignements personnels ou financiers pour finaliser la transaction ou pour discuter. Méfiez-vous si une personne vous demande des copies de votre passeport, permis de conduire et numéro d'assurance sociale, ou votre date de naissance, surtout si vous ne connaissez pas cette personne.

Appels non sollicités. Vous pourriez recevoir un appel d'une personne prétendant qu'il y a un virus dans votre ordinateur, que vous devez des impôts, ou que des activités frauduleuses se produisent dans votre compte de banque. Sachez qu'un organisme légitime ne vous appellera pas directement. Raccrochez et appelez vous-même l'organisme en utilisant le numéro obtenu d'une source sûre, par exemple l'annuaire téléphonique, le site Web ou des factures et des relevés de compte.

Demandes d'amitié non sollicitées sur les médias sociaux. Avant d'accepter les demandes d'amitié d'une personne que vous ne connaissez pas, examinez son profil ou demandez à vos amis s'ils la connaissent. Son profil est-il plutôt vide ou montre-t-il des publications génériques? A-t-elle l'air de proposer plus qu'une amitié? Ce sont des signaux d'alarme d'une fraude. Supprimez la demande et empêchez la personne de vous en envoyer d'autres.

Offres extraordinaires par courrier. Vous recevez une carte de jeu par courrier qui garantit que vous avez déjà remporté ou remporterez un prix. Ce prix peut aller d'une voiture à un voyage. Si vous n'avez pas participé à un concours, jetez la carte. C'est fort probablement une fraude!

C'est trop beau pour être vrai. Tout le monde aime les bonnes affaires. Toutefois, les offres renversantes, les rabais faramineux et les taux inimaginables indiquent tous que les offres ne sont pas ce qu'elles semblent. Des prix incroyablement bas sont souvent synonymes de produits de mauvaise qualité ou contrefaits. Des offres gratuites demandent souvent que vous fournissiez vos renseignements de carte de crédit pour la livraison. Ces simples techniques profitent énormément aux fraudeurs.

SIGNALER UNE FRAUDE

À qui signaler une fraude dépend de l'endroit où vous habitez et du type de fraude en jeu.

Que vous vous soyez fait piéger ou ayez été ciblé par un fraudeur, vous devriez toujours le signaler. Les autorités canadiennes ne sont pas toujours à même de prendre des mesures contre les fraudes, mais vous pouvez aider. En signalant une fraude, vous permettez aux autorités d'avertir la population et les médias, ce qui réduit la probabilité que cette fraude cible d'autres personnes. Vous devriez aussi avertir vos amis et votre famille des fraudes dont vous êtes témoin.

Ci-dessous, vous trouverez des conseils pour signaler une fraude au bon endroit, selon le type de fraude :

Centre antifraude du Canada
www.centreantifraude.ca
1-888-495-8501

Bureau de la concurrence
www.bureaudelaconcurrence.gc.ca
1-800-348-5358

Fraudes locales

Communiquez avec votre bureau d'information aux consommateurs local

Votre bureau d'information aux consommateurs local est le mieux placé pour enquêter sur des fraudes qui semblent provenir de votre province ou territoire. Vous trouverez une liste des bureaux provinciaux et territoriaux dans le Guide du consommateur canadien.

www.guideduconsommateur.ca

Fraudes financières et en matière d'investissements

Communiquez avec les Autorités canadiennes en valeurs mobilières

Les fraudes financières concernent généralement des offres de vente ou des promotions sur des produits et services financiers, comme les pensions de retraite, les fonds de placement gérés, les conseils financiers, l'assurance, le crédit et les comptes de dépôt.

En matière d'investissements, les fraudes reposent sur l'achat d'actions, la vente de devises étrangères, les investissements à l'étranger, les chaînes de Ponzi ou les investissements à rendement élevé.

Vous pouvez signaler une fraude financière ou en matière d'investissements aux Autorités canadiennes en valeurs mobilières ou à votre organisme de réglementation des valeurs mobilières local.

www.autorites-valeurs-mobilieres.ca

Fraudes bancaires et relatives aux cartes de crédit

Communiquez avec votre banque ou votre institution financière

En plus de signaler ces fraudes au Centre antifraude du Canada, vous devriez alerter votre banque ou votre institution financière au sujet de toute correspondance douteuse que vous recevez au sujet de vos comptes. Ces institutions vous indiqueront les étapes à suivre.

Assurez-vous de composer le numéro de téléphone qui figure dans le répertoire téléphonique, sur votre relevé ou au dos de votre carte de guichet ou de crédit.

Fraudes par pourriels et textos

Communiquez avec le Centre de notification des pourriels

De nombreuses fraudes passent par votre courriel et vos textos. Visitez le site www.combattrelepourriel.gc.ca pour obtenir plus d'information sur la loi canadienne antipourriel et sur les façons de signaler les pourriels.

Les courriels frauduleux (ou hameçonnage) dans lesquels on vous demande des renseignements personnels doivent être signalés à la banque, à l'institution financière ou à l'organisation concernée. À nouveau, assurez-vous d'utiliser une adresse courriel ou un numéro de téléphone fournis dans une source officielle fiable, et non ceux qui se trouvent dans le courriel.

Fraude, vol ou autres crimes

Communiquez avec la police

De nombreuses fraudes qui contreviennent aux dispositions sur la protection des consommateurs (comme celles appliquées par le Bureau de la concurrence et d'autres organismes gouvernementaux et d'application de la loi) peuvent également contrevenir aux dispositions sur la fraude du *Code criminel*.

Si vous êtes victime d'une fraude parce qu'une personne malhonnête vous a soutiré de l'argent, vous devriez communiquer avec votre poste de police local (surtout si la somme est importante). Vous devez absolument communiquer avec la police si vous avez été victime d'un vol ou si un fraudeur vous a menacé ou agressé.

Vol d'identité

Communiquez avec la police

Le vol d'identité concerne généralement l'acquisition et la collecte des renseignements personnels d'une autre personne à des fins criminelles.

Si vous croyez être ou êtes réellement la cible d'un vol d'identité, ou si vous avez fourni à votre insu des renseignements personnels ou financiers, vous devriez :

- communiquer avec votre service de police local et remplir une déclaration;
- communiquer avec votre banque ou institution financière, ainsi que la société émettrice de votre carte de crédit;
- communiquer avec les deux agences nationales de crédit afin de marquer votre rapport de solvabilité d'une alerte à la fraude;
- toujours signaler le vol d'identité. Communiquez avec le Centre antifraude du Canada.

Communiquez avec des organismes supplémentaires en fonction de la situation :

- Le bureau d'éthique commerciale de votre province
- L'Agence du revenu du Canada — Ligne d'information sur les organismes de bienfaisance

  www.cra-arc.gc.ca
  1-800-267-2384
- Le bureau des documents de votre province
- Les agences de crédit peuvent marquer vos comptes d'une alerte à la fraude, ce qui avertira les prêteurs et créanciers d'une éventuelle fraude :

  Equifax Canada
  1-800-465-7166

  TransUnion Canada
  1-866-525-0262

Le petit livre noir de la fraude est accessible en ligne à www.bureaudelaconcurrence.gc.ca.

Savoir, c'est avoir le pouvoir!