# Le Petit livre noir des escroqueries

Publié pour la première fois par le Bureau de la concurrence Canada 2012 Reproduit avec la permission de la Commission australienne de la concurrence et de la consommation
Illustrations de Pat Campbell

Cette publication est disponible en ligne à l'adresse suivante: www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/03074.html.

Pour obtenir une copie de cette publication ou pour la recevoir sous un autre format (braille, gros caractères, etc.), veuillez remplir le formulaire de demande de publication ou contacter: Centre d'information - Bureau de la concurrence 50, rue Victoria, Gatineau, QC K1A 0C9 Tél.: 819-997-4282 Sans frais: 1-800-348-5358 ATS (pour malentendants): 1-800-642-3844 Télécopieur: 819- 997-0324 Site Web: www.bureaudelaconcurrence.gc.ca


Chat. No. Iu54-42 / 2017E-PDF
ISBN 978-0-660-07567-9

**VOTRE GUIDE DE PROTECTION CONTRE LA FRAUDE**

AVANT-PROPOS
MESSAGE DU MINISTRE

La confiance des consommateurs dans le marché est de la plus haute importance pour le gouvernement. Les consommateurs informés et conscients sont des acteurs importants dans une économie d'innovation.
C’est pourquoi nous encourageons tous les Canadiens à se prendre en main en lisant Le Petit Livre noir des escroqueries et en prenant note de ses conseils sur la façon d’arrêter les fraudeurs. Cette brochure décrit la plupart des types d’escroqueries les plus courantes et répertorie les informations de contact des agences de lutte contre la fraude présentes dans le pays.

**Aidez-moi.**
Je crois en un Canada qui est un pays d’innovateurs, un pays conscient et
MESSAGE DU COMMISSAIRE:

La fraude est un crime qui menace tous les Canadiens, peu importe leur niveau de scolarité, leur âge ou leur revenu. Les fraudeurs recourent à diverses méthodes sournoises pour escroquer des victimes sans méfiance, par exemple en imitant des marques bien connues en ligne et en utilisant des allégations trompeuses pour séduire les consommateurs par le biais du télémarketing, du courrier électronique ou des médias sociaux.

Le Bureau de la concurrence s'emploie à protéger tous les Canadiens en s'attaquant aux professionnels du marketing trompeurs et en veillant à ce que les consommateurs disposent des informations nécessaires pour prendre des décisions d'achat éclairées.

Notre petit livre d'arnaques vise à vous sensibiliser aux nombreux types de fraudes ciblant les Canadiens. Il fournit des conseils sur la façon de protéger
déchargés par le coût élevé de la fraude dans les économies traditionnelles et numériques.

Les méthodes utilisées par les fraudeurs sont de plus en plus sophistiquées, mais les consommateurs le sont également. Vous pouvez faire une différence non seulement dans votre propre vie, mais également dans celle des personnes qui vous sont chères en reconnaissant, en rejetant et en signalant les fraudes. Cette brochure dans ses éditions imprimée, en ligne et vidéo est un pas important dans cette direction.

L'hon. Navdeep Bains, ministre de l'Innovation, des Sciences et du Développement économique vous-même et démystifiez les mythes courants qui pourraient permettre aux fraudeurs de gagner votre confiance.

Depuis que nous avons lancé la brochure en mars 2012, celle-ci est restée l’une de nos publications les plus populaires. Nous avons distribué plus de 100 000 exemplaires imprimés à des Canadiens et notre version en ligne a été visitée ou téléchargée à partir du site Web du Bureau de la concurrence plus de 250 000 fois.

Je suis très reconnaissant à la Commission australienne de la concurrence et des consommateurs, qui a initialement mis au point Le petit livre de fraude noir et nous a autorisé à produire cette édition à l'intention des Canadiens.
John Pecman Commissaire de la concurrence

**CONTENU**

Introduction 1
Loteries, tirages au sort et concours 2
Schémas pyramidaux 4
Demandes de transfert d'argent 6
Escroqueries sur Internet 8
Les escroqueries par téléphone mobile 10
Escroqueries médicales et de santé 12
Escroqueries d'urgence 14
Rencontres et escroqueries romantiques 16
Escroqueries charitables 18
Escroqueries d'emploi et d'emploi 20
Escroqueries de petite entreprise 22
Escroqueries de service 24
Conseils pratiques pour vous protéger 26
Les escroqueries et vous: que faire si vous êtes arnaqué! 28
Obtenir de l'aide et signaler une arnaque 29

**La vérité**

**INTRODUCTION**

Chaque année, les Canadiens perdent des millions de dollars à cause des activités des escrocs qui nous bombardent d'escroqueries en ligne, par courrier, par porte-à-porte et par téléphone. Nous avons le plaisir de vous présenter la première édition canadienne de The Little Black Book of Scams. Nous espérons que ce livre vous permettra de prendre conscience du vaste éventail d’escroqueries qui ciblent les Canadiens et de partager avec vous certaines mesures simples que vous pouvez prendre pour vous protéger.

Les arnaqueurs ne discriminent pas Les arnaqueurs ciblent des personnes de tous les âges, de tous âges et de tous niveaux de revenus. Les fausses loteries, les fraudes sur Internet, les systèmes d’enrichissement rapide et les remèdes miracles constituent quelques-uns des moyens privilégiés de séparer les imprudents de leur argent. De nouvelles variétés de ces escroqueries apparaissent tout le temps.

Le Bureau de la concurrence a constaté les effets dévastateurs des escroqueries sur les personnes et leurs familles. L'un des meilleurs moyens de

Combattre ce type de fraude consiste à prendre des mesures pour éviter de se faire prendre. PROTÉGEZ-VOUS Si vous souhaitez rester au courant des escroqueries, renseignez-vous sur la manière de reconnaître les différents types d'escroqueries et de protéger vos informations personnelles en visitant les sites Web des organismes d'application de la loi, du Centre canadien de lutte antifraude (www.antifraudcentre.ca) ou d'autres organisations réputées.

# LOTERIES, CONCOURS ET CONCOURS

Beaucoup de Canadiens sont attirés par l'excitation d'une victoire surprise et se voient envoyer des sommes énormes pour réclamer de faux prix.

CE QUI À RECHERCHER Vous ne pouvez pas gagner d'argent ou un prix dans une loterie à moins que vous ne l'ayez entré vous-même ou que quelqu'un d'autre ne l'ait inscrit en votre nom. Vous ne pouvez pas être choisi comme gagnant aléatoire si vous n'avez pas de participation.

De nombreuses arnaques de loterie tentent de vous amener à fournir vos coordonnées bancaires et personnelles pour réclamer votre prix. Vous ne devriez pas avoir à payer de frais ni d'impôt pour réclamer un prix légitime.

Ne vous fiez pas à l'idée que l'offre est légale ou approuvée par le gouvernement - de nombreux escrocs vous le diront. Au lieu de recevoir un grand prix ou une fortune, vous perdrez chaque centime que vous envoyez à un escroc. Et si vous avez fourni d'autres informations personnelles, votre identité pourrait également être utilisée de manière abusive.

Une fausse arnaque de prix vous dira que vous avez gagné un prix ou un concours. Vous pouvez recevoir un appel téléphonique, un courrier électronique, un message texte ou un écran contextuel sur votre ordinateur. Réclamer votre prix implique souvent des coûts, et même si vous recevez un prix, il se peut que ce ne soit pas ce qui vous avait été promis.

Les escrocs gagnent leur vie en vous faisant payer des frais ou des taxes, en appelant leurs numéros de téléphone à tarif préférentiel ou en envoyant des messages texte avec prime pour réclamer votre prix. Ces appels à tarif majoré peuvent être très coûteux et les escrocs essaieront de vous garder en ligne pendant une longue période ou vous demanderont d'appeler un autre numéro à tarif majoré.

**MISE EN GARDE**

**PENSE**

## ENQUÊTER

## DEMANDE TOI

Les loteries légitimes ne vous obligent pas à payer des frais ou une taxe pour collecter les gains.

N'envoyez jamais d'argent à des personnes que vous ne connaissez pas et en lesquelles vous ne faites pas confiance.

Ne communiquez pas de coordonnées bancaires à des personnes que vous ne connaissez pas et en lesquelles vous n’avez pas confiance.

Examinez très attentivement toutes les conditions d’une offre - les demandes d’offre gratuites ou très bon marché ont souvent des coûts cachés. Les appels vers des numéros de téléphone surtaxés ou des messages texte surtaxés peuvent coûter très cher.

Ai-je participé à ce concours? Vous ne pouvez pas gagner d’argent ou un prix dans un concours à moins que vous n’ayez vous-même inscrit ou que quelqu'un d’autre ne l’ait inscrit pour vous.

4

#### SCHÉMAS DE PYRAMIDE

Les systèmes pyramidaux promettent un retour financier important pour un coût relativement faible. Les systèmes pyramidaux sont illégaux et très risqués - et peuvent vous coûter très cher.

CE QUI À RECHERCHER Dans un système pyramidal typique, les investisseurs non avertis sont encouragés à payer des frais d’abonnement élevés pour participer à des activités lucratives. La seule façon pour vous de récupérer de l’argent est de convaincre d’autres personnes de s’y joindre et de se séparer de leur argent. Les membres de la famille ou des amis sont souvent persuadés de rejoindre le groupe. Mais rien ne garantit que vous récupérerez votre investissement initial.

Bien que les systèmes pyramidaux soient souvent habilement déguisés, ils gagnent de l'argent en recrutant du personnel plutôt qu'en vendant un produit légitime ou en fournissant un service. Les régimes pyramidaux s'effondrent inévitablement et vous perdrez votre argent. Au Canada, promouvoir un système pyramidal ou même y participer est un crime.

Les systèmes de Ponzi sont des opérations d’investissement frauduleuses qui fonctionnent de la même manière que les systèmes pyramidaux. Le système de Ponzi attire généralement les investisseurs nouveaux et aisés en offrant des rendements supérieurs à ceux des autres investissements, sous la forme de rendements à court terme anormalement élevés ou inhabituellement cohérents. Habituellement, l'internaute interagit directement avec tous les investisseurs, persuadant souvent la plupart des participants existants de réinvestir leur argent, minimisant ainsi la nécessité de recruter de nouveaux participants, comme le ferait un système pyramidal.

Soyez prudent, mais ne vous découragez pas de rechercher avec soin des opportunités commerciales basées sur des commissions. Il existe de nombreuses opportunités légitimes de marketing multiniveau où vous pouvez légalement gagner de l'argent en vendant des produits ou des services authentiques.

Protégez!

VOUS SOUVENEZ-VOUS

Des combinaisons de pyramides et de Ponzi peuvent vous être envoyées par des membres de la famille et des personnes en qui vous avez confiance - ils peuvent ne pas savoir qu'ils peuvent être illégaux ou impliqués dans une arnaque.

MISE EN GARDE

Ne vous engagez à rien lors de réunions ou de séminaires sous pression.

PENSE

Ne prenez aucune décision sans faire vos devoirs - recherchez l'offre en cours et demandez conseil à un indépendant avant de prendre une décision.

ENQUÊTER

Faites des recherches sur toutes les opportunités d'affaires qui vous intéressent.

Si je ne vends pas un produit ou un service authentique, la participation à cette activité est-elle légale?

6

**DEMANDES DE TRANSFERT D'ARGENT**

Les escroqueries par transfert d'argent sont à la hausse. Faites très attention lorsque quelqu'un vous propose de l'argent pour aider à transférer leurs fonds. Une fois que vous envoyez de l'argent à quelqu'un, il peut être très difficile, voire impossible, de le récupérer.

CE QU'IL FAUT REGARDER L'escroquerie nigériane (aussi appelée fraude 419) est à la hausse depuis le début des années 1990 au Canada. Bien que bon nombre de ces types d'escroqueries soient originaires du Nigéria, des arnaques similaires ont été lancées dans le monde entier (en particulier dans d'autres régions de l'Afrique de l'Ouest et en Asie). Ces escroqueries sont de plus en plus qualifiées de «fraude sur les frais d'avance».

Dans l'arnaque nigériane classique, vous recevez un courrier électronique ou une lettre d'un arnaqueur vous demandant de transférer une grosse somme d'argent à l'étranger. Une part de l'argent vous est ensuite proposée si vous acceptez de fournir vos coordonnées bancaires afin de faciliter le transfert. Ils vous demanderont ensuite de payer toutes sortes d'impôts et de taxes avant de pouvoir recevoir votre «récompense». Vous ne recevrez jamais rien de cet argent et perdrez les frais que vous avez payés.

Ensuite, il y a le courrier électronique frauduleux qui prétend provenir d'un avocat ou d'un représentant de la banque informant qu'un de vos proches, disparu depuis longtemps, est décédé et vous a légué un énorme héritage. Les fraudeurs peuvent raconter des histoires si authentiques que vous pourriez être amené à fournir des documents personnels et des détails de compte bancaire afin que vous puissiez confirmer leur identité et réclamer votre héritage. L '«héritage» est probablement inexistant et, en plus de perdre tout l'argent que vous pourriez avoir versé à l'escroc en frais et taxes, vous pourriez également risquer de vous faire voler votre identité.

Si vous ou votre entreprise vendez des produits ou des services en ligne ou par le biais de petites annonces dans les journaux, vous pouvez être la cible d'une escroquerie de paiement excédentaire. En réponse à votre annonce, vous pourriez recevoir un généreux.

## PROTÈGE TOI!

Si quelqu'un vous a demandé de lui transférer de l'argent, il s'agit probablement d'une arnaque. N'envoyez jamais d'argent, ni ne donnez les détails de cartes de crédit ou de comptes en ligne à des personnes que vous ne connaissez pas et en lesquelles vous ne faites pas confiance. N'acceptez pas de chèque ou de mandat pour le paiement de biens supérieurs à ce que vous avez convenu. Renvoyez-le et demandez à l'acheteur de vous envoyer le paiement correspondant au montant convenu avant de livrer les biens ou les services.
Est-ce vraiment sûr de transférer de l'argent pour quelqu'un que je ne connais pas?

**RAPPELLES TOI**
**MISE EN GARDE**
**PENSE**
**DEMANDE TOI**

Consultez les informations sur le site Web du Centre canadien de lutte antifraude pour savoir comment vous protéger contre les escroqueries par virement de fonds.

ENQUÊTER offre d'un acheteur potentiel et l'accepter. Vous recevez le paiement par chèque ou mandat, mais le montant que vous recevez est supérieur au prix convenu. L'acheteur peut vous dire que le trop-perçu est tout simplement une erreur ou inventer une excuse, telle que de l'argent supplémentaire pour couvrir les frais de livraison. Si vous êtes invité à rembourser le montant excédentaire par virement de fonds, méfiez-vous. L'escroc espère que vous transfèrerez le remboursement avant de découvrir que son chèque ou son mandat était contrefait. Vous perdrez l'argent transféré ainsi que l'objet si vous l'avez déjà envoyé.

8

**SCAMS INTERNET**
De nombreuses escroqueries sur Internet ont lieu sans que la victime s'en aperçoive. Vous pouvez réduire considérablement les risques d'être arnaqué sur Internet si vous suivez quelques précautions simples.

CE QU'IL FAUT POUR RECHERCHER Les fraudeurs peuvent utiliser Internet pour promouvoir la fraude par le biais de messages non sollicités ou indésirables, appelés spam. Même s'ils ne reçoivent qu'une poignée de réponses parmi les millions de courriels qu'ils envoient, cela en vaut toujours la peine. Méfiez-vous des réponses, même simplement pour vous «désabonner», car cela donnerait à un fraudeur la confirmation qu'il avait atteint une véritable adresse e-mail.

Tout courrier électronique que vous recevez et qui provient d'un expéditeur que vous ne connaissez pas, qui ne vous est pas spécifiquement destiné et qui vous promet un avantage est susceptible d'être du spam.

Les logiciels malveillants (également appelés logiciels malveillants, logiciels espions, logiciels enregistreurs de frappe, chevaux de Troie ou chevaux de Troie) constituent une menace pour la sécurité en ligne. Les fraudeurs essaient d'installer ce logiciel sur votre ordinateur.
ordinateur afin qu'ils puissent accéder aux fichiers stockés sur votre ordinateur et à d'autres données personnelles et mots de passe.
Les escrocs utilisent un large éventail d'astuces pour installer leurs logiciels sur votre ordinateur. Ils vous inciteront peut-être à cliquer sur un lien ou un message contextuel dans un courrier indésirable, ou à vous faire visiter un faux site Web créé uniquement pour infecter les ordinateurs des utilisateurs.

L'escroquerie par hameçonnage consiste à vous inciter à donner vos données personnelles et bancaires à des fraudeurs. Les courriels que vous recevez peuvent sembler légitimes, mais en réalité, les organisations authentiques telles qu'une banque ou une autorité gouvernementale ne s'attendront jamais à ce que vous envoyiez vos informations personnelles par e-mail ou en ligne.

Les fraudeurs en ligne peuvent facilement copier le logo ou même
ventes aux enchères et achats sur Internet peuvent couvrir l'ensemble du site Web d'une véritable organisation.
être très amusant et peut aussi vous aider à trouver. Ne supposez donc pas que le courrier électronique que vous recevez est
bonnes affaires. Malheureusement, ils sont également légitimes. Si le message vous demande de visiter un attirer les fraudeurs. site Web pour "mettre à jour", "valider" ou "confirmer" les informations de votre compte, soyez sceptique.

Les fraudeurs essaieront souvent de vous faire traiter en dehors des sites d'enchères en ligne. Ils peuvent supprimer les emails de phishing. Ils peuvent porter
Réclamez le gagnant d'une vente aux enchères comme étant un virus pouvant infecter votre ordinateur. Ne pas enchérir sur a sorti et offrir l'élément ouvrir toutes les pièces jointes ou suivre les liens à toi. Une fois que vous avez payé, vous ne serez jamais phishing.
avoir de leurs nouvelles et le site de vente aux enchères ne pourra pas vous aider.

**PROTÈGE TOI!**

Si vous choisissez de magasiner en ligne ou de participer à des enchères en ligne, assurez-vous de connaître les règles de remboursement et les processus de traitement des litiges et veillez à ce que vous ne soyez pas surchargé. En outre, vous souhaiterez peut-être utiliser un service de dépôt fiduciaire, tel que PayPal. Ce service retiendra votre paiement et ne le remettra au vendeur qu'une fois que vous aurez confirmé avoir reçu le prix que vous avez payé. Il y a généralement un petit supplément pour ce service. Une banque ou une institution financière légitime ne vous demandera jamais de cliquer sur un lien dans un courrier électronique ou d'envoyer les détails de votre compte via un courrier électronique ou un site Web.

N'achetez jamais auprès d'enchérisseurs mal classés sur des sites d'enchères et faites de votre mieux pour vous assurer que vous effectuez uniquement des achats sur des sites de vente authentiques. Ne fournissez jamais vos informations personnelles, de carte de crédit ou de compte, sauf si vous êtes certain que le site est authentique.

Ne répondez pas aux e-mails de spam, même pour vous désabonner, et ne cliquez sur aucun lien ni n'appelez un numéro de téléphone indiqué dans un e-mail de spam. Assurez-vous de disposer du logiciel de protection actuel ou consultez un spécialiste en informatique.
En ouvrant cet e-mail suspect, vais-je risquer la sécurité de mon ordinateur? Les coordonnées fournies dans l'e-mail sont-elles correctes? Téléphonez à votre banque ou à votre institution financière pour savoir si le courrier électronique que vous avez reçu est authentique.

**RAPPELLES TOI**
**MISE EN GARDE**
**PENSE**
**DEMANDE TOI**

Si un e-mail ou une fenêtre contextuelle vous propose un produit ou un service qui vous intéresse réellement et que cela semble raisonnable, assurez-vous de bien comprendre tous les termes, conditions et coûts avant d'acheter ou de fournir vos coordonnées.
ENQUÊTER

**Dix SCAMS DE TÉLÉPHONE MOBILE**
Les escroqueries par téléphone portable peuvent être difficiles à reconnaître. Méfiez-vous des personnes qui parlent comme si elles vous connaissaient ou de rappeler un appel manqué d'un numéro inconnu - il peut y avoir des frais cachés.

CE QUI À RECHERCHER Les escroqueries de sonneries peuvent vous attirer avec une offre de sonnerie gratuite ou peu coûteuse. Ce que vous ne réalisez peut-être pas, c'est qu'en acceptant cette offre, vous vous abonnez peut-être à un service qui vous enverra des sonneries et vous facturera un tarif majoré. Il existe de nombreuses entreprises légitimes vendant des sonneries, mais il y a aussi les escrocs qui essaieront de cacher le coût réel de l'offre.

Les fraudeurs ne vous disent pas que votre demande pour la première sonnerie est en réalité un abonnement à un service de sonnerie, ou ils peuvent être masqués en petits caractères liés à l'offre. Ils rendent également difficile pour vous d'arrêter le service. Vous devez activement «désactiver» le service pour arrêter les sonneries et les frais associés.

Les arnaques aux appels manqués commencent par des arnaqueurs appelant votre téléphone et raccrochant si rapidement que vous ne pouvez pas répondre à l'appel à temps. Votre téléphone enregistre un appel manqué et vous ne reconnaîtrez probablement pas le numéro.

Vous pourriez être tenté d'appeler le numéro pour savoir qui vous a appelé. S'il s'agit d'une arnaque, vous devrez payer le tarif majoré pour l'appel sans le savoir.

Les escroqueries par message texte fonctionnent de la même manière, mais via un service de messages courts (SMS). Les fraudeurs vous envoient un message texte à partir d'un numéro que vous ne connaissez peut-être pas, mais il semble que ce soit celui d'un ami, par exemple: «Bonjour, c'est John. Je suis revenu! Quand êtes-vous libre de vous rattraper? »Si vous répondez par curiosité, des SMS peuvent vous être facturés au tarif majoré (parfois jusqu'à 4 USD pour chaque message envoyé et / ou reçu).

**PROTÈGE TOI!**

**RAPPELLES TOI**
**MISE EN GARDE**
**PENSE**
**DEMANDE TOI**

Texte «STOP» pour mettre fin aux messages texte non désirés ou aux abonnements non désirés.

Ne répondez jamais aux messages texte en vous offrant des sonneries gratuites ou des appels en absence de numéros que vous ne reconnaissez pas.

N'appelez et n'envoyez pas de numéros de téléphone commençant par 1-900, à moins que vous ne connaissiez le coût, et lisez attentivement les conditions d'utilisation du code court.

Lisez très attentivement toutes les conditions d'une offre. Les services offrant des produits gratuits ou très bon marché ont souvent des coûts cachés.

Est-ce que je sais comment arrêter tout service d'abonnement auquel je veux m'inscrire?

Un concours SMS ou une arnaque par SMS liée à un questionnaire arrive généralement sous forme de message texte ou dans une publicité et vous encourage à participer à un jeu-questionnaire pour obtenir un grand prix. Tout ce que vous avez à faire est de répondre correctement à un certain nombre de questions. Les escrocs gagnent de l'argent en facturant des taux extrêmement élevés pour les messages que vous envoyez et pour tout autre message qu'ils vous envoient. Avec les arnaques, la première série de questions sera très facile. Ceci est destiné à vous encourager à continuer à jouer. Cependant, les dernières questions auxquelles vous devez répondre pour réclamer votre «prix» pourraient être très difficiles voire impossibles à répondre correctement.

12

**SANTÉ ET SCAMS MÉDICAUX**

Les escroqueries médicales sont la proie de la souffrance humaine. Ils offrent des solutions là où il n'existe pas ou promettent de simplifier les traitements complexes pour la santé.

Les escroqueries de cure miracle offrent une gamme de produits et services qui peuvent sembler être des médecines alternatives légitimes, promettant généralement des remèdes rapides et efficaces pour des conditions médicales graves. Les traitements prétendent être efficaces contre un très grand nombre d'affections et sont souvent promus à l'aide de témoignages de personnes qui ont utilisé le produit ou le service et qui ont été «guéries».
Les escroqueries de perte de poids promettent une perte de poids spectaculaire avec peu ou pas d'effort. Ce type d'escroquerie peut impliquer un régime alimentaire inhabituel ou restrictif, des exercices révolutionnaires ou des dispositifs anti-graisse, ou encore des produits révolutionnaires tels que pilules, timbres ou crèmes. Les produits sont promus avec l'utilisation de fausses allégations telles que «perdre 10 kilos en
10 jours »ou« perdre du poids pendant que vous dormez »et nécessitent souvent des paiements anticipés importants ou la conclusion d'un contrat à long terme pour participer au programme.

Les fausses pharmacies en ligne utilisent Internet et des spams pour proposer des médicaments et des médicaments à des prix très bas prix et / ou sans ordonnance d'un médecin. Si vous utilisez un tel service et que vous recevez effectivement les produits en réponse à votre commande, rien ne garantit qu'ils sont réellement.

Il existe des pharmacies en ligne légitimes. Ces entreprises auront leurs coordonnées complètes sur leur site Web et devront également obtenir une ordonnance valide avant d'envoyer tout médicament qui en nécessite un.

**RAPPELLES TOI**
**MISE EN GARDE**
**PENSE**
**ENQUÊTER**
**DEMANDE TOI**

Il n'existe pas de pilule magique, de remède miracle ni d'option sûre en cas de maladie grave ou de perte de poids rapide.

Ne jamais s'engager à rien sous pression.

Ne vous fiez pas à une allégation non corroborée concernant des médicaments, des suppléments ou d'autres traitements. Consultez votre professionnel de la santé.

Recherchez des articles médicaux et de recherche publiés pour vérifier l'exactitude des déclarations des promoteurs.

S'il s'agissait vraiment d'un remède miracle, mon professionnel de la santé ne m'en aurait-il pas parlé?

**SCAMS D'URGENCE**
Les escroqueries d'urgence visent les grands-parents et jouent sur leurs émotions pour leur voler leur argent.

CE QUI À RECHERCHER Dans le scénario typique d'une arnaque d'urgence, un grand-parent reçoit un appel téléphonique d'un fraudeur prétendant être l'un de ses petits-enfants. Les appelants continuent en disant qu'ils ont des problèmes et qu'ils ont besoin d'argent immédiatement. Ils affirment avoir été victimes d'un accident de voiture, avoir du mal à revenir d'un pays étranger ou avoir besoin d'une caution.

Vous pouvez recevoir un appel de deux personnes, l'une prétendant être votre petit-enfant et l'autre prétendant être un agent de police ou un avocat. Votre "petit-enfant" vous pose des questions pendant l'appel, vous amenant à fournir des informations personnelles.

Les appelants disent qu'ils ne veulent pas que les autres membres de la famille découvrent ce qui s'est passé. Il vous sera demandé de transférer de l'argent via une société de transfert d'argent. Souvent, les victimes ne vérifient pas l'histoire avant l'envoi de l'argent.

Dans certains cas, les fraudeurs prétendent être votre ancien voisin ou un ami de la famille, mais l'escroquerie d'urgence concerne principalement les grands-parents.

**MISE EN GARDE**
**PENSE**
**ENQUÊTER**
**DEMANDE TOI**

Les escrocs comptent sur le fait que vous voudrez agir rapidement pour aider vos proches en cas d'urgence.

N'envoyez jamais d'argent à des personnes que vous ne connaissez pas et en qui vous n'avez pas confiance. Vérifiez l'identité de la personne avant de prendre des mesures pour aider.

Ne communiquez aucune information personnelle à l'appelant.

Posez à la personne des questions auxquelles seul votre proche serait capable de répondre.

Appelez les parents ou les amis de l’enfant pour vérifier l’histoire.

L’histoire de l’appelant a-t-elle un sens?

16

**DATING ET ROMANCE SCAMS**
En dépit des nombreux sites Web de rencontres légitimes en activité au Canada, il existe également de nombreuses escroqueries dans les domaines des rencontres et des romances. Les escroqueries amoureuses et amoureuses tentent de réduire vos défenses en faisant appel à votre côté romantique et compatissant.

CE QUI À RECHERCHER Certaines escroqueries de datation et de romance fonctionnent en mettant en place un site de rencontre où vous payez pour chaque email ou message que vous envoyez et recevez. L'escroc va essayer de vous accrocher en continuant de vous envoyer des courriels à la sonorité vague, pleins de discussions sur l'amour ou le désir. L'escroc peut également envoyer des courriels contenant des détails de son pays ou de sa ville d'origine qui ne vous parlent pas beaucoup du tout. Il s’agit de tentatives pour vous empêcher d’écrire et de payer de l’argent pour utiliser le site Web de rencontres frauduleuses.

Même sur un site de rencontre légitime, un escroc peut vous contacter, par exemple quelqu'un qui prétend avoir un membre de la famille très malade ou qui est au plus profond du désespoir (ces escrocs prétendent souvent être russes ou Europe de l’Est). Après qu'ils vous aient envoyé quelques messages, et peut-être même une photo glamour, il vous sera demandé (directement ou plus subtilement) de leur envoyer de l'argent pour améliorer leur situation. Certains escrocs s’organisent même pour vous rencontrer, dans l’espoir que vous leur offrez des cadeaux ou de l’argent - puis ils disparaissent.

Dans d'autres cas, les escrocs essaieront de vous lier d'amitié, peut-être même de vous envoyer des fleurs ou d'autres petits cadeaux. Après avoir noué une relation, l’escroc vous informera d’une importante somme d’argent dont il a besoin pour transférer de son pays ou qu’il souhaite partager avec vous. Ils vous demanderont ensuite vos coordonnées bancaires ou votre argent pour des frais administratifs ou une taxe qui, selon eux, devrait être payée pour libérer cet argent.

**RAPPELLES TOI**
**MISE EN GARDE**
**PENSE**
**ENQUÊTER**
**DEMANDE TOI**

Vérifiez les adresses de sites Web avec soin. Les fraudeurs installent souvent de faux sites Web avec des adresses très similaires aux sites de rencontres légitimes.

N'envoyez jamais d'argent, ni ne donnez les détails de cartes de crédit ou de comptes en ligne à des personnes que vous ne connaissez pas et en lesquelles vous ne faites pas confiance.

Ne communiquez aucune information personnelle dans un courrier électronique ou lorsque vous discutez en ligne.

Assurez-vous que vous utilisez uniquement des sites de rencontres légitimes et réputés.

Est-ce que quelqu'un que je n'ai jamais rencontré aurait vraiment déclaré son amour pour moi après seulement quelques lettres ou courriels?

18

**Arnaques de charité**
Les escroqueries caritatives tirent parti de la générosité et de la gentillesse de personnes en demandant des dons à une fausse œuvre de bienfaisance ou en imitant une véritable œuvre de bienfaisance.

CE QU'IL FAUT RECHERCHER Les escroqueries impliquant des arnaqueurs impliquent des arnaqueurs qui collectent de l'argent en prétendant être un véritable organisme de bienfaisance. Les escrocs peuvent vous approcher de différentes façons: dans la rue, chez vous, par téléphone ou sur Internet. Les courriels et les boîtes de collecte peuvent même porter les logos des véritables œuvres de bienfaisance.

Souvent, l’escroc exploitera une catastrophe naturelle ou une famine qui a fait l’actualité.

D'autres escrocs jouent sur vos émotions en prétendant être des organismes de bienfaisance qui aident les enfants malades.

Les fraudeurs peuvent essayer de faire pression sur vous pour faire un don et refuser de fournir des détails sur l'organisme de bienfaisance, tels que leur adresse ou leurs coordonnées. Dans d'autres cas, ils peuvent simplement fournir de fausses informations.

Non seulement ces escroqueries coûtent de l'argent aux gens; ils détournent également des dons indispensables d’organismes de bienfaisance légitimes et de leurs causes. Tous les organismes de bienfaisance enregistrés au Canada sont supervisés par l'Agence du revenu du Canada et répertoriés dans sa base de données. Vous pouvez également contacter votre

bureau d'éthique commerciale local pour savoir s'il possède des informations sur les organisations qui vous intéressent. Si l'organisme de bienfaisance est authentique et que vous souhaitez faire un don, obtenez ses coordonnées dans l'annuaire téléphonique ou sur un site Web de confiance.

Si vous ne voulez pas donner d'argent ou si vous êtes satisfait du montant que vous avez déjà fait à des œuvres de bienfaisance, ignorez tout simplement l'e-mail ou la lettre, raccrochez le téléphone ou dites non à la personne à votre porte. Vous n'êtes pas obligé de donner de l'argent du tout.

**RAPPELLES TOI**
**MISE EN GARDE**
**PENSE**
**DEMANDE TOI**

Si vous avez le moindre doute sur la personne qui demande de l'argent, ne lui communiquez pas d'espèces, de carte de crédit ou de compte bancaire.

Ne communiquez jamais par téléphone les informations personnelles de votre compte, de votre carte de crédit ou de votre compte en ligne, à moins que vous ayez passé l'appel et que le numéro de téléphone provienne d'une source fiable.

En cas de doute, adressez-vous directement à une organisation humanitaire pour faire un don ou offrir votre soutien.

Consultez la base de données de l'Agence du revenu du Canada pour vérifier que l'organisme de bienfaisance qui vous a contacté est authentique.

Comment et à qui voudrais-je apporter une contribution?

20

**SCAMS EMPLOI ET EMPLOI**
Les escroqueries en matière d'emploi et d'emploi ciblent les personnes à la recherche d'un emploi. Ils promettent souvent beaucoup de revenus, parfois même le garantissent, avec peu ou pas d'effort.

CE QU'IL FAUT RECHERCHER Les escroqueries liées au travail «à domicile» sont souvent encouragées par le biais de spams ou d'annonces publicitaires en ligne ou dans les journaux. La plupart de ces annonces ne sont pas de véritables offres d'emploi. Nombre d'entre eux sont des fronts d'activités illégales de blanchiment d'argent ou de systèmes pyramidaux.

Vous pouvez recevoir un courrier électronique proposant un emploi sur lequel vous utilisez votre compte bancaire pour recevoir et transférer des paiements pour une entreprise étrangère. Ou alors, on pourrait vous proposer un emploi en tant qu '«acheteur secret» engagé pour tester les services d'une entreprise d'encaissement de chèques ou de transfert d'argent.

Certaines «offres d'emploi» vous promettent de percevoir une commission en pourcentage pour chaque paiement que vous transmettez. Parfois, les fraudeurs cherchent juste après les détails de votre compte bancaire pour pouvoir accéder à votre compte. Ils pourraient aussi vous envoyer un faux chèque ainsi que des instructions pour que vous puissiez encaisser le chèque et virer une partie de la somme via un service de virement de fonds.

Une arnaque d'emploi ou de revenu garantie prétend vous garantir un emploi ou un certain niveau de revenu. Les escrocs vous contactent généralement par courrier électronique indésirable et les offres impliquent souvent le paiement de frais initiaux pour un «plan d'entreprise», certains matériels de démarrage ou logiciels.

Il existe toute une gamme d'escroqueries présentées comme des opportunités commerciales. Vous pouvez être amené à effectuer un paiement initial (pour quelque chose qui ne fonctionne pas ou ne correspond pas à vos attentes) ou à recruter d'autres personnes dans le système (reportez-vous à la section Systèmes pyramidaux à la page 4).

**RAPPELLES TOI**
**MISE EN GARDE**
**PENSE**
**ENQUÊTER**
**DEMANDE TOI**

Il n'y a pas de raccourci vers la richesse - les fraudeurs sont les seules personnes qui gagnent de l'argent.

N'envoyez jamais les détails de votre compte bancaire ou de votre carte de crédit à une personne que vous ne connaissez pas et en qui vous avez confiance. Si vous encaissez le chèque et que celui-ci est contrefait, votre banque pourrait être tenue pour responsable de la perte monétaire totale.

Ne prenez aucune décision sans rechercher soigneusement l’offre. Demander un avis indépendant avant de prendre une décision.

Méfiez-vous des produits ou des systèmes prétendant garantir un revenu et des offres d'emploi nécessitant le paiement de frais initiaux ou l'envoi d'argent par le biais d'un service de transfert d'argent. Assurez-vous que toute opportunité commerciale de franchise est légitime.

Ai-je reçu tous les détails par écrit avant de payer ou de signer quelque chose?

**SCAMS DES PETITES ENTREPRISES**
Les escroqueries qui ciblent les petites entreprises peuvent prendre différentes formes, des factures de publicité aux répertoires non commandés en passant par des offres de fournitures de bureau douteuses.

CE QUI À RECHERCHER Les exploitants de petites entreprises et les particuliers qui possèdent leur propre site Internet continuent d'être confus et pris au piège par des lettres non sollicitées les avertissant que leur nom de domaine Internet va expirer et doit être renouvelé, ou leur offrant un nouveau nom de domaine similaire à leur nom actuel. un.

Si vous avez enregistré un nom de domaine, veillez à vérifier attentivement les avis de renouvellement de nom de domaine ou les factures que vous recevez. Bien que l'avis puisse être authentique, il peut également provenir d'une autre entreprise qui tente de vous inscrire ou d'un fraudeur.
• Vérifiez que l'avis de renouvellement correspond exactement à votre nom de domaine actuel. Recherchez les petites différences, par exemple «.com» au lieu de «.ca» ou les lettres manquantes dans l'adresse URL.
• Vérifiez que l'avis de renouvellement provient de la société auprès de laquelle vous avez initialement enregistré votre nom de domaine.
• Vérifiez dans vos enregistrements la date d'expiration réelle de votre nom de domaine existant.

Une liste de répertoires ou une arnaque de publicité non autorisée tente de facturer une entreprise pour une liste ou une publicité dans un magazine, une revue ou un répertoire d'entreprises, ou pour une liste de répertoires en ligne.

L'escroquerie pourrait provenir d'une proposition d'abonnement déguisée en mise à jour d'une fiche existante dans un répertoire professionnel. Vous pourriez également être amené à croire que vous répondez à une offre pour une inscription gratuite alors qu'il s'agit en réalité d'une commande pour une inscription nécessitant un paiement ultérieur.

Une autre approche commune utilisée par escroquerie de fournitures de bureau implique que vous recevez des escrocs est d'appeler une entreprise demandant à et étant facturé pour des biens que vous confirmez les détails d'une annonce n'a pas commandé. Ces escroqueries impliquent souvent qu'ils prétendent avoir déjà été réservés. Le biens ou services que vous commandez régulièrement - arnaqueur pourrait citer une entrée authentique par exemple, du papier, des fournitures d'impression ou de la publicité pour votre entreprise fournitures d'entretien ou de publicité. dans une publication ou un répertoire différent pour vous convaincre que vous avez vraiment utilisé le Vous pourriez recevoir un appel téléphonique du

produit d’un fraudeur, prétendant faussement être votre «fournisseur habituel», en vous disant que l'offre est une offre «spéciale» ou méfiez-vous des bons de commande.

La publicité
«Disponible pour un temps limité», ou faire semblant d'opportunités dans les annuaires d'entreprises. Celles-ci
pour confirmer uniquement votre adresse ou votre commande existante. les formulaires de commande peuvent ressembler à leur origine
Si vous acceptez d'acheter l'une des fournitures proposées auprès d'un fournisseur de répertoires bien connu
pour vous, ils seront souvent trop cher et de la publicité, quand ils ne le font pas.
mauvaise qualité.

**PROTÈGE TOI!**
Assurez-vous que les personnes qui traitent les factures ou répondent aux appels téléphoniques sont au courant de ces escroqueries. Ils seront le plus souvent le point de contact des fraudeurs. Vérifiez toujours que les biens ou les services ont été commandés et livrés avant de payer une facture.

Ne donnez jamais ou ne mettez à jour aucune information sur votre entreprise à moins de savoir à quoi elle servira.

Ne consentez pas à une proposition commerciale par téléphone - demandez toujours une offre par écrit. Limitez le nombre de personnes de votre entreprise ayant accès aux fonds et disposant du pouvoir d'approuver les achats.

Si un appelant affirme que j'ai commandé ou autorisé quelque chose et que je ne pense pas que cela sonne juste, ne devrais-je pas demander de preuve?

**RAPPELLES TOI**
**MISE EN GARDE**
**PENSE**
**DEMANDE TOI**

Des procédures de gestion efficaces peuvent contribuer dans une large mesure à empêcher ces escroqueries de réussir. Disposer de procédures clairement définies pour la vérification, le paiement et la gestion des comptes et des factures constitue un moyen de défense efficace contre ces types d’escroqueries.

**ENQUÊTER**

24

**SCAMS DE SERVICE**

De nombreux Canadiens sont ciblés par des personnes qui prétendent offrir des tarifs réduits ou des offres pour divers services.

CE QU'IL FAUT POUR RECHERCHER Ces escroqueries impliquent généralement des individus qui proposent des services de télécommunications, Internet, des finances, des services médicaux et des services énergétiques. Cette catégorie d'escroqueries peut également inclure des offres telles que l'extension de garantie, l'assurance et la vente à domicile.

Les deux types d'escroqueries les plus signalées à l'intention des Canadiens sont les logiciels antivirus et les réductions de taux d'intérêt par carte de crédit.
Les fraudeurs impliqués dans l'escroquerie antivirus promettent de réparer votre ordinateur via Internet. Cela peut impliquer l'installation d'un logiciel ou l'autorisation d'accéder à distance à votre ordinateur. Le paiement du logiciel ou de la réparation s'effectue généralement par carte de crédit.

Télécharger un logiciel à partir d'une source inconnue ou permettre à quelqu'un d'accéder à distance à votre ordinateur est risqué. Les fraudeurs peuvent utiliser des logiciels malveillants pour capturer vos informations personnelles, telles que noms d'utilisateur et mots de passe, informations de compte bancaire, informations d'identité, etc.

Tout le monde aime avoir un accord et les arnaqueurs le savent. Les personnes à l'origine des arnaques liées à la réduction du taux d'intérêt des cartes de crédit usurpent souvent l'identité d'institutions financières et prétendent négocier avec des sociétés émettrices de cartes de crédit pour abaisser vos taux d'intérêt. Ils garantissent qu'ils peuvent vous faire économiser des milliers de dollars en intérêts. L'appelant vous dira que les taux d'intérêt plus bas ne sont valables que pour un temps limité et que vous devez agir maintenant.

**PROTÈGE TOI!**

**RAPPELLES TOI**
**MISE EN GARDE**
**PENSE**
**DEMANDE TOI**

Seul votre fournisseur de services peut vous proposer un meilleur taux ou un meilleur prix pour leurs services.

Méfiez-vous des appels non sollicités de personnes offrant beaucoup «pour un temps limité».

Ne communiquez pas votre numéro de carte de crédit par téléphone à moins d'avoir passé l'appel et si le numéro provenait d'une source fiable.

Si un appelant prétend représenter votre banque, appelez-la pour savoir si l'offre que vous avez reçue est authentique.

En offrant cette information, est-ce que je me mets en danger?

**ENQUÊTER**

Vous pouvez recevoir un appel automatisé vous invitant à «appuyer sur 1» et à fournir des informations personnelles, telles que votre date de naissance et votre numéro de carte de crédit. Vous serez également invité à payer des frais pour le service. Les fraudeurs utiliseront ces informations pour effectuer des achats avec votre carte de crédit ou pour accéder à des avances de fonds.
26

**CONSEILS PRATIQUES POUR SE PROTÉGER**

Protégez votre identité

• N'indiquez vos informations personnelles que dans les cas où cela est absolument nécessaire et lorsque vous faites confiance à la personne avec qui vous parlez ou avec qui vous traitez.
• Détruisez les informations personnelles: ne les jetez pas. Vous devriez couper ou déchiqueter les vieux billets, relevés ou cartes, par exemple les cartes de crédit et les cartes de guichet automatique.
• Traitez vos données personnelles comme vous traiteriez de l'argent: ne les laissez pas traîner pour que les autres les prennent.

**LES QUESTIONS D'ARGENT**

• N'envoyez jamais d'argent à des personnes que vous ne connaissez pas et en lesquelles vous ne faites pas confiance.
• N'envoyez pas d'argent et ne payez aucun frais pour réclamer un prix ou un gain à la loterie.
• Les «emplois» vous demandant simplement d'utiliser votre propre compte bancaire pour transférer de l'argent pour quelqu'un pourraient constituer un front pour les activités de blanchiment d'argent. Le blanchiment d'argent est une infraction criminelle grave.
• Évitez de transférer ou de transférer des remboursements ou des trop-payés à une personne que vous ne connaissez pas.

**L'APPROCHE FACE À FACE**

• Si quelqu'un se présente à votre porte, demandez à voir une pièce d'identité. Vous n'êtes pas obligé de les laisser entrer, et ils doivent partir si vous leur demandez de le faire.
• Avant de décider de payer de l'argent, si vous êtes intéressé par ce qu'un vendeur à domicile peut offrir, prenez le temps de vous renseigner sur son entreprise et son offre.
• Contactez le Bureau de la concurrence, les bureaux de la consommation provinciaux et territoriaux ou le Bureau d'éthique commerciale de votre province ou de votre territoire si vous

n'êtes pas sûr d'un vendeur qui se présente à votre porte. Voir pages 29 et 30 pour les coordonnées.

**AFFAIRES TÉLÉPHONIQUE**

• Si vous recevez un appel de quelqu'un que vous ne connaissez pas, demandez toujours le nom de la personne à qui vous parlez et son représentant. Vérifiez ces informations en appelant vous-même la société.
• Ne communiquez pas par téléphone les détails de votre compte personnel, de votre carte de crédit ou de votre compte en ligne, à moins que vous ayez passé l'appel et que le numéro de téléphone provienne d'une source fiable.
• Il est préférable de ne pas répondre aux messages texte ou aux appels manqués provenant de numéros que vous ne reconnaissez pas. Méfiez-vous particulièrement des numéros de téléphone commençant par 1-900. Ceux-ci peuvent être facturés à un taux plus élevé que les autres numéros et peuvent être très coûteux.

**OFFRES DE COURRIEL**

• Ne répondez jamais à un courrier indésirable, même pour vous désabonner - cela sert souvent à «vérifier» votre adresse aux fraudeurs. La meilleure solution consiste à supprimer tous les courriels suspects sans les ouvrir.
• Désactivez le «volet de visualisation» car le simple affichage du courrier électronique peut envoyer un avis de vérification à l'expéditeur indiquant que votre adresse de courrier électronique est valide.
• Les banques et les institutions financières légitimes ne vous demanderont jamais les détails de votre compte dans un courrier électronique ou vous demanderont de cliquer sur un lien dans un courrier électronique pour accéder à votre compte.
• N'appelez jamais un numéro de téléphone ou ne faites pas confiance aux autres coordonnées que vous voyez dans un courrier indésirable.

**AFFAIRES INTERNET**

• Installez un logiciel qui protège votre ordinateur contre les virus et les programmes indésirables et assurez-vous qu'il est à jour. En cas de doute, demandez l'aide d'un professionnel de l'informatique.
• Si vous souhaitez accéder à un site Web, utilisez un lien en favori avec ce site ou saisissez vous-même l'adresse du site dans le navigateur. Ne suivez jamais un lien dans un email.
• Vérifiez soigneusement les adresses des sites Web. Les fraudeurs installent souvent de faux sites Web avec des adresses très similaires à celles des utilisateurs légitimes.  sites Internet.
• Méfiez-vous des sites Web offrant des téléchargements «gratuits» (tels que de la musique, du contenu pour adultes, des jeux et des films). Le téléchargement de ces produits peut installer des programmes nuisibles sur votre ordinateur à votre insu.
• Évitez de cliquer sur les annonces contextuelles, car cela pourrait entraîner l’installation de programmes nuisibles sur votre ordinateur.
• N'entrez jamais vos informations personnelles, de carte de crédit ou de compte en ligne sur un site Web dont vous ne savez pas s'il est authentique.

• N'envoyez jamais vos coordonnées personnelles, de carte de crédit ou de banque en ligne par courrier électronique.
• Évitez d'utiliser des ordinateurs publics (bibliothèques ou cybercafés) pour vos transactions bancaires ou vos achats en ligne.
• Lorsque vous utilisez des ordinateurs publics, effacez l'historique et le cache de l'ordinateur lorsque vous avez terminé votre session.
• Soyez prudent lorsque vous utilisez un logiciel sur votre ordinateur qui complète automatiquement les formulaires en ligne. Cela peut permettre aux fraudeurs d'Internet d'accéder facilement aux informations personnelles et à celles de votre carte de crédit.
• Choisissez des mots de passe difficiles à deviner, par exemple des mots de passe comportant des lettres et des chiffres. Vous devez également changer régulièrement les mots de passe.
• Lors de tout achat en ligne, imprimez des copies de toutes les transactions et payez uniquement via un site sécurisé. Si vous utilisez un site de vente aux enchères sur Internet, notez les numéros d'identification impliqués et lisez d'abord tous les conseils de sécurité du site.

28

**LES SCAMS ET VOUS: QUE FAIRE SI VOUS OBTENEZ SCAMMED!**
Les autorités canadiennes pourraient ne pas toujours être en mesure de prendre des mesures contre les escroqueries, même s'il semble qu'un fraudeur aurait enfreint la loi.

RÉDUCTION DES DOMMAGES Bien qu'il soit difficile de récupérer l'argent que vous avez perdu à cause d'une arnaque, vous pouvez prendre certaines mesures pour réduire les dégâts et éviter de devenir la cible d'une escroquerie de suivi. Plus vous agissez rapidement, plus vous réduisez vos pertes.

Signaler une arnaque. En signalant l'escroquerie aux autorités, elles pourront peut-être avertir d'autres personnes de l'escroquerie et minimiser les risques de propagation de l'escroquerie. Vous devez également avertir vos amis et votre famille de toute escroquerie que vous rencontrerez. Les détails sur la manière de signaler une arnaque se trouvent aux pages 29 et 30 de cette publication.

SI VOUS AVEZ ÉTÉ CONÇU DE SIGNER UN CONTRAT OU D'ACHETER UN PRODUIT OU UN SERVICE, contactez votre bureau de la consommation provincial ou territorial et envisagez de demander à un conseiller indépendant d'examiner vos options: il peut y avoir un délai de réflexion ou vous pouvez être en mesure de négocier un remboursement. .

SI VOUS PENSEZ QUELQU'UN A ACCÈS ACCÉDÉ À VOTRE COMPTE EN LIGNE, À UN COMPTE BANCAIRE TÉLÉPHONIQUE OU À UNE CARTE DE CRÉDIT Appelez immédiatement votre institution financière pour qu'elle suspende votre compte et limite le montant que vous perdez.

Les sociétés émettrices de cartes de crédit peuvent également être en mesure de procéder à une «facturation» (transaction inversée) si elles estiment que votre carte de crédit a été facturée de manière frauduleuse.

N'utilisez pas les coordonnées figurant dans des courriels ou sur des sites Web pour lesquels vous avez des doutes, elles seront probablement
faux et vous conduire à un escroc. Vous pouvez trouver des informations de contact légitimes dans le répertoire, un relevé de compte ou au verso de votre carte de guichet automatique.

SI L'ARNAQUE RELIE À VOTRE SANTÉ Arrêtez de prendre des médicaments ou des substances dont vous n'êtes pas sûr. Consultez un médecin ou un autre professionnel de la santé qualifié dès que vous le pourrez. Assurez-vous de leur parler du traitement vendu par l'escroc (emportez toutes les substances, y compris leur emballage). Dites-leur également si vous avez arrêté un traitement que vous preniez avant l'escroquerie.

SI VOUS AVEZ ENVOYÉ DE L'ARGENT À QUELQU'UN QUI VOUS A PENSEZ PEUT ÊTRE UN SCAMMER Si vous avez envoyé les détails de votre carte de crédit, suivez les instructions dans la section ci-contre.

Si vous avez envoyé de l'argent par transfert électronique de fonds (par Internet), contactez immédiatement votre institution financière. S'ils n'ont pas déjà traité le transfert, ils peuvent peut-être l'annuler.

Si vous avez envoyé un chèque, contactez immédiatement votre institution financière. Si l'escroc n'a pas déjà encaissé votre chèque, il pourra peut-être l'annuler.

Si vous avez envoyé de l'argent par l'intermédiaire d'un service filaire (tel que Western Union ou Money Gram), contactez-le immédiatement. Si vous êtes très rapide, ils pourront peut-être arrêter le transfert.

SI VOUS AVEZ ÉTÉ FRAPPÉ PAR UN VENDEUR DE PORTE À PORTE Vous pouvez être protégé par des lois qui vous accordent une période de réflexion, au cours de laquelle vous pouvez annuler un contrat ou un contrat que vous avez signé. Contactez le service à la consommation de votre province ou de votre territoire pour obtenir des conseils sur les lois relatives à la vente à domicile.

Si vous avez été victime d'une arnaque à l'aide de votre ordinateur Si vous utilisiez votre ordinateur lorsque vous vous êtes fait arnaquer, il est possible qu'un virus ou un autre logiciel malveillant se trouve toujours sur votre ordinateur. Exécutez une vérification complète du système à l'aide d'un logiciel de sécurité fiable.

Si aucun logiciel de sécurité (antivirus et pare-feu, par exemple) n'est installé sur votre ordinateur, un professionnel de l'informatique peut vous aider à choisir ce dont vous avez besoin.

Les fraudeurs peuvent également avoir eu accès à vos mots de passe en ligne. Modifiez-les à l'aide d'un ordinateur sécurisé.

SI L'ARNAQUE IMPLIQUE VOTRE TÉLÉPHONE MOBILE, appelez votre opérateur téléphonique et informez-le de ce qui s'est passé.

Obtenir de l'aide et signaler une arnaque
La meilleure agence à contacter dépend de votre lieu de résidence et du type d'escroquerie en cause.

Si vous pensez avoir repéré une arnaque ou si vous avez été ciblé par une arnaque, vous pouvez contacter un certain nombre d'agences gouvernementales et d'application de la loi au Canada pour obtenir des conseils ou rédiger un rapport. Cela peut vous aider et empêcher d'autres arnaqueurs de vous arnaquer.

Centre canadien de lutte antifraude www.antifraudcentre.ca 1-888-495-8501
Centre d'information du Bureau de la concurrence www.bureaudelaconcurrence.gc.ca
1-800-348-5358

Escroqueries locales Contacter votre bureau local de la consommation Votre bureau local de la consommation est le mieux placé pour enquêter sur les escroqueries qui semblent provenir de votre propre province ou territoire. Une liste des bureaux de la consommation provinciaux et territoriaux se trouve dans le Guide du consommateur canadien sur le site Web du Bureau de la consommation.
www.consumerhandbook.ca

SCAMS FINANCIERS ET INVESTISSEMENTS Contacter les autorités canadiennes en valeurs mobilières Les escroqueries financières impliquent des offres commerciales ou des promotions sur des produits et services financiers tels que les pensions, les fonds gérés, les conseils financiers, les assurances, les comptes de crédit ou de dépôts.

Les escroqueries en matière d'investissement impliquent l'achat d'actions, le négoce de devises étrangères, les investissements étrangers, les systèmes de Ponzi ou les principaux programmes d'investissement bancaire.

30

Vous pouvez signaler les arnaques liées aux finances et aux investissements aux autorités canadiennes en valeurs mobilières (ACVM) ou à votre autorité en valeurs mobilières locale. *www.securities-administrators.ca*

SIGNALER UNE ESCRAMME DE CARTES DE CRÉDIT ET DE BANQUES Contactez votre banque ou votre institution financière En plus de signaler ces escroqueries au Centre canadien de lutte antifraude, vous devez informer votre banque ou votre institution financière de la correspondance suspecte que vous recevez à propos de votre compte. Ils peuvent vous conseiller sur ce qu'il faut faire ensuite.

Assurez-vous que le numéro de téléphone que vous utilisez provient de l'annuaire, de votre relevé de compte ou du verso de votre carte de crédit ou de votre guichet automatique.

SIGNALER DES E-MAILS ET DES SMS DE SPAM De nombreuses escroqueries arrivent par e-mail et par SMS. Visitez www.fightspam.gc.ca pour plus d'informations sur la législation canadienne anti-pourriel.

Les e-mails frauduleux (ou «phishing») demandant des informations personnelles peuvent également être signalés à la banque, à une institution financière ou à une autre organisation concernée (veillez à utiliser un numéro de téléphone ou une adresse e-mail qui ne figuraient pas dans l'e-mail pour générer votre rapport).

RAPPORTS DE FRAUDE, DE VOL ET D'AUTRES CRIMES Contactez la police De nombreuses escroqueries pouvant enfreindre les lois sur la protection du consommateur (celles appliquées par le Bureau de la concurrence, les autres organismes gouvernementaux et les forces de l'ordre) peuvent également enfreindre les dispositions du Code criminel relatives à la fraude.

Si vous êtes victime d'une fraude (vous avez subi une perte en raison de la malhonnêteté ou de la tromperie d'une personne), vous devriez envisager de contacter votre police locale (en particulier si le montant en jeu est important).

Vous devez contacter définitivement la police si votre propriété a été volée, menacée ou agressée par un escroc.

Vous pouvez également contacter l'une des organisations suivantes:
Better Business Bureau www.bbb.org

Agence du revenu du Canada - Direction des organismes de bienfaisance www.cra-arc.gc.ca
1-800-267-2384

Votre police locale, les sociétés de cartes de crédit, les banques et les archives provinciales.

Les bureaux de crédit peuvent créer une alerte à la fraude sur votre compte, ce qui alertera les prêteurs et les créanciers des fraudes potentielles:

Equifax: 1-800-465-7166 TransUnion: 1-866-525-0262