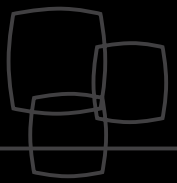
Bureau de la concurrence Canada
Competition Bureau Canada



L'édition canadienne

LE PETIT LIVRE NOIR DE LA **FRAUDE**

VOTRE GUIDE DE PROTECTION CONTRE LA FRAUDE

Canada

Publié pour la première fois par le Bureau de la concurrence Canada en 2012
Reproduit avec l'autorisation de l'Australian Competition and Consumer Commission

Illustrations de Pat Campbell
Photographie de Melanie Aitken par Couvrette (Ottawa)

Pour de plus amples renseignements sur le Bureau de la concurrence ou pour obtenir un exemplaire de cette publication, s'adresser au :
Centre des renseignements, Bureau de la concurrence
50, rue Victoria, Gatineau (Québec) K1A 0C9
Téléphone : 819-997-4282
Sans frais : 1-800-348-5358
ATS (pour les malentendants) : 1-800-642-3844
Télécopieur : 819-997-0324
Site Web : www.bureaudelaconcurrence.gc.ca

On peut obtenir cette publication sur supports accessibles, sur demande. Communiquer avec la :
Section des services du multimédia, Direction générale des communications et du marketing
Industrie Canada
Bureau 441F, tour Est
235, rue Queen, Ottawa (Ontario) K1A 0H5
Téléphone : 613-947-5177
Télécopieur : 613-954-6436
Courriel : production.multimedia@ic.gc.ca

Cette publication est offerte par voie électronique sur le Web au : www.bureaudelaconcurrence.gc.ca.

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

N° de catalogue Iu54-42/2012
ISBN 978-1-100-54163-1
60987
2012-03-01
Also available in English under the title *The Little Black Book of Scams*.

L'édition canadienne

LE PETIT LIVRE NOIR DE LA **FRAUDE**

VOTRE GUIDE DE PROTECTION CONTRE LA FRAUDE

AVANT-PROPOS

MINISTRE DE L'INDUSTRIE

La fraude est un crime qui touche les personnes, les entreprises et l'ensemble de l'économie. Les criminels délestent chaque année les Canadiens de millions de dollars au moyen de publicités fausses ou trompeuses, de loteries frauduleuses, de systèmes de vente pyramidale ainsi que de nombreuses autres techniques illégales.

Le gouvernement du Canada, par l'entremise du Bureau de la concurrence et d'autres organismes, veille à l'application rigoureuse des lois canadiennes pour lutter contre la fraude. Vous aussi, vous pouvez apporter votre contribution.

L'édition canadienne du livret intitulé *The Little Black Book of Scams* se veut une ressource utile expliquant comment éviter de se faire prendre dans des escroqueries et comment les signaler aux autorités compétentes.

Je vous invite à prendre le temps de lire ce livret et de faire part des leçons que vous en tirerez à votre famille et à vos amis, alors que nous nous efforçons tous de mettre un terme à la fraude au Canada.

Christian Paradis
Ministre de l'Industrie

COMMISSAIRE DE LA CONCURRENCE

En vertu des dispositions de la *Loi sur la concurrence* et d'autres lois, le Bureau de la concurrence poursuit les entreprises et les personnes qui adoptent des pratiques commerciales trompeuses, notamment la publicité mensongère, la fraude par Internet, le télémarketing trompeur ou les concours trompeurs.

De plus, le Bureau veille à ce que les consommateurs disposent de l'information nécessaire pour prendre des décisions d'achat éclairées.

Nous avons produit l'édition canadienne du livret intitulé *The Little Black Book of Scams* pour vous sensibiliser davantage aux nombreux types de fraude qui prennent pour cible la population canadienne et vous informer de quelques mesures de protection faciles à prendre.

Grâce à des conseils utiles, des questions à se poser et aux coordonnées de personnes-ressources dans de nombreux organismes qui s'efforcent de faire échec à la fraude, ce livret vous donne les moyens de lutter contre la fraude et vous aide à consommer activement en toute sécurité.

À l'origine, *Le Petit Livre noir de la fraude* a été élaboré par l'Australian Competition and Consumer Commission. Je tiens à remercier la Commission d'avoir autorisé la reproduction et l'adaptation de ce livret à l'intention des Canadiens.

Melanie Aitken
Commissaire de la concurrence

TABLE DES MATIÈRES

MYTHES À DÉTRUIRE

Voici quelques mythes répandus à détruire pour éviter d'être victime d'une fraude.

- Toutes les compagnies, entreprises et organisations sont légitimes parce qu'elles détiennent un permis du gouvernement et sont surveillées par ce dernier. Ce n'est pas toujours vrai. Même s'il existe des règles à suivre pour lancer et exploiter une entreprise au Canada, il est facile pour un fraudeur de prétendre détenir les autorisations nécessaires, alors que ce n'est pas le cas. Certaines entreprises en règle peuvent tout de même essayer de vous frauder en agissant de façon malhonnête.

- Tous les sites Internet sont légitimes. Ce n'est pas toujours vrai. Il est relativement facile et peu coûteux de créer un site Web. Les fraudeurs sont capables de reproduire sans difficulté un site Web légitime afin de vous duper.

- Il est possible de faire fortune rapidement, mais seules quelques personnes savent comment s'y prendre. Ce n'est pas toujours vrai. Posez-vous la question suivante : si quelqu'un connaissait le secret de la richesse instantanée, pourquoi voudrait-il le partager avec les autres?

- Les fraudeurs ne s'intéressent qu'à de grosses sommes d'argent. Ce n'est pas toujours vrai. Parfois, les fraudeurs visent de nombreuses personnes et essaient de leur soutirer de petites sommes.

- Seul l'argent intéresse les fraudeurs. Ce n'est pas toujours vrai. Certaines fraudes visent vos renseignements personnels.

RÈGLES D'OR

N'oubliez pas ces règles d'or pour faire obstacle aux fraudeurs.

- Si on vous fait une offre pour laquelle vous devez verser de l'argent ou fournir des renseignements personnels, ou encore vous engager à titre personnel, demandez toujours des conseils objectifs.

- Il n'y a pas de stratagème garanti pour s'enrichir rapidement — parfois, seuls les fraudeurs s'en tirent gagnants.

- N'acceptez jamais une offre et ne concluez jamais un marché sur-le-champ. Si vous pensez avoir saisi une belle occasion, prenez le temps de demander des conseils objectifs avant d'agir et insistez pour que l'on vous accorde ce délai de réflexion.

- Ne donnez jamais d'argent ou vos renseignements personnels, et ne signez rien avant d'avoir fait vos devoirs et vérifié les antécédents de la compagnie à laquelle vous avez affaire.

- Ne vous fiez pas aux témoignages élogieux : trouvez des preuves concrètes du succès d'une entreprise.

- Si un site Web vous intéresse, accédez-y directement plutôt que de cliquer sur les liens fournis dans un courriel.

- N'envoyez jamais d'argent ou de détails sur votre carte de crédit ou vos comptes bancaires à une personne que vous ne connaissez pas et en qui vous n'avez pas confiance.

- Si vous constatez une fraude ou si vous avez été victime d'une fraude, demandez de l'aide. Communiquez avec le Centre antifraude du Canada, le Bureau de la concurrence ou votre service de police local. Vous trouverez les coordonnées de ces organismes à la page 29.

Les fraudeurs sont des manipulateurs qui ne manquent pas d'imagination. Ils savent quoi dire pour obtenir ce qu'ils veulent.

INTRODUCTION

Chaque année, des Canadiens sont victimes de fraudes, qu'elles soient en ligne, par la poste, en personne ou au téléphone, et ils y perdent des millions de dollars.

Nous avons le plaisir de vous présenter la première édition canadienne du *Petit Livre noir de la fraude*. Cet ouvrage a pour but de vous sensibiliser au vaste éventail de fraudes qui visent les Canadiens et de décrire les mesures que vous pouvez prendre pour vous protéger.

LES FRAUDEURS NE FONT PAS DE DISCRIMINATION

Les fraudeurs se moquent bien de vos origines, de votre âge ou de votre revenu. Les fausses loteries, les fraudes sur Internet, les offres de s'enrichir rapidement et les cures miracles sont quelques-unes des combines favorites des fraudeurs pour alléger votre portefeuille. De nouvelles formes de fraude apparaissent tous les jours.

Le Bureau de la concurrence peut témoigner des effets dévastateurs de la fraude sur les Canadiens et leur famille. Pour combattre la fraude, il faut commencer par ne pas tomber dans le panneau.

PROTÉGEZ-VOUS

Pour rester à l'affût, apprenez à reconnaître les diverses formes de fraude et protégez vos renseignements personnels en visitant les sites Web des organismes d'application de la loi, du Centre antifraude du Canada (www.centreantifraude.ca) ou d'autres organisations reconnues.

LOTERIES, TIRAGES AU SORT ET CONCOURS

De nombreux Canadiens engloutissent des sommes importantes pour réclamer des prix qui n'existent pas.

SOYEZ À L'AFFÛT

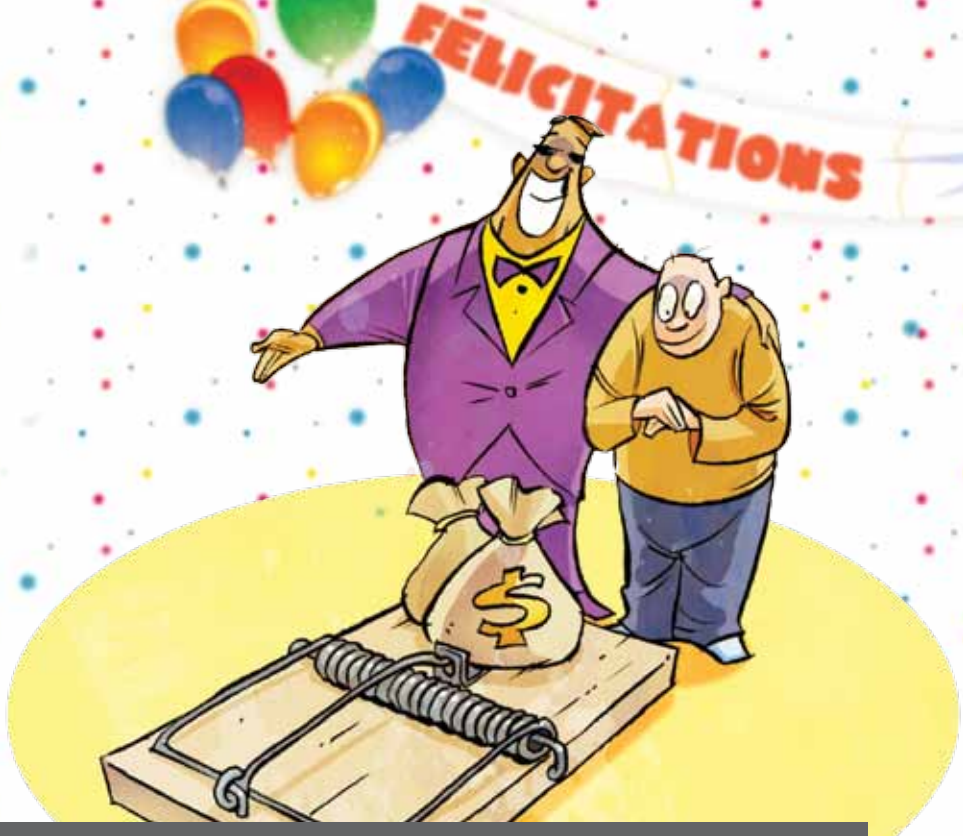
Pour remporter un **prix ou une somme d'argent dans le cadre d'une loterie**, vous devez vous y inscrire, ou quelqu'un doit l'avoir fait en votre nom. Si ce n'est pas le cas, vous ne pouvez pas avoir été choisi au hasard.

On vous demandera parfois de fournir vos données bancaires et personnelles pour réclamer votre prix. Vous ne devriez jamais avoir à payer quoi que ce soit pour réclamer un prix légitime.

Ne vous laissez pas séduire par des fraudeurs qui affirment que leur offre est légale ou approuvée par le gouvernement. Chaque dollar envoyé à un fraudeur est un dollar perdu. Vos renseignements personnels pourraient également être utilisés à mauvais escient.

Dans ce type d'arnaque, on vous annoncera au téléphone, par courriel, par message texte ou à l'écran de votre ordinateur que vous avez remporté un prix ou un concours. Vous devez souvent payer pour réclamer votre prix et, quand vous en recevez un, ce dernier ne correspond pas toujours à ce que l'on vous avait promis.

Ces fraudeurs s'enrichissent en vous demandant de composer leur numéro tarifé ou d'envoyer des textos pour réclamer votre prix. Ces appels peuvent être très coûteux. Attention! Ils vous garderont longtemps au bout du fil ou vous demanderont de composer différents numéros tarifés.



!	PROTÉGEZ-VOUS
RAPPELEZ-VOUS	Vous n'avez rien à payer pour réclamer un prix dans le cadre d'une loterie légitime.
SOYEZ PRUDENT	N'envoyez jamais d'argent à quelqu'un que vous ne connaissez pas et en qui vous n'avez pas confiance.
RÉFLÉCHISSEZ	Ne donnez pas de détails bancaires à une personne que vous ne connaissez pas et en qui vous n'avez pas confiance.
INFORMEZ-VOUS	Étudiez attentivement toutes les conditions d'une offre. Il y a souvent des frais cachés. Le coût des appels ou des textos pourrait vous réserver toute une surprise.
POSEZ-VOUS DES QUESTIONS	Ai-je participé à un concours? Vous ne pouvez pas gagner un prix dans le cadre d'un concours auquel vous n'êtes pas inscrit.

VENTES PYRAMIDALES

Les ventes pyramidales vous promettent des rendements alléchants à faible coût. Elles sont illégales, très risquées et pourraient vous coûter cher.

SOYEZ À L'AFFÛT

Dans un **système de vente pyramidale** type, on invite des investisseurs crédules à payer des frais d'adhésion élevés afin de réaliser d'importants bénéfices. Pour récupérer votre investissement, vous n'avez qu'une seule option : convaincre d'autres investisseurs. Les gens sont souvent recrutés par des amis ou des parents. Mais rien ne garantit que vous pourrez récupérer votre investissement initial.

Même si ces arnaques sont bien déguisées, elles visent à recruter des investisseurs plutôt qu'à vendre des produits ou à fournir des services légitimes. Ces pyramides finissent toujours par s'effondrer et vous risquez de tout perdre. Au Canada, promouvoir un tel système de vente pyramidale, et même y participer, constitue un acte criminel.

Les **chaînes de Ponzi** sont inspirées des systèmes de vente pyramidale. Elles visent à attirer des investisseurs de bonne foi en leur offrant un taux de rendement à court terme anormalement supérieur à celui d'autres investissements ou inhabituellement stable. Le fraudeur établit un lien direct avec tous les investisseurs et réussit à convaincre la plupart des participants de réinvestir leur argent. Ainsi, l'apport constant de nouveaux joueurs n'est pas aussi important que dans un système de vente pyramidale.

Soyez prudent, mais n'écartez pas nécessairement toutes les possibilités d'affaires basées sur des commissions. Il existe de nombreuses méthodes de commercialisation à paliers multiples qui vous permettent de gagner un revenu honnête en vendant des produits ou des services légitimes.

!	PROTÉGEZ-VOUS
RAPPELEZ-VOUS	Ce sont souvent les parents et amis qui vous entraînent vers la vente pyramidale ou une chaîne de Ponzi. Ils ignorent parfois que ces stratagèmes sont illégaux ou qu'eux-mêmes sont impliqués dans une fraude.
SOYEZ PRUDENT	Ne prenez aucun engagement dans un contexte de vente sous pression.
RÉFLÉCHISSEZ	Ne prenez jamais de décision sans faire une recherche sur l'offre en question et sans demander des conseils objectifs.
INFORMEZ-VOUS	Faites des recherches sur toutes les occasions d'affaires qui vous intéressent.
POSEZ-VOUS DES QUESTIONS	Si je ne vends pas un véritable produit ou service, est-ce que ma participation à cette activité est légale?

DEMANDES DE TRANSFERT D'ARGENT

Les fraudes liées aux transferts d'argent sont en hausse. Soyez prudent lorsqu'on vous offre de l'argent pour transférer des fonds. Si vous envoyez de l'argent, vous risquez de ne jamais le revoir.

SOYEZ À L'AFFÛT

La fraude du **Nigéria** (également appelée fraude 419) est en hausse depuis le début des années 1990 au Canada. Même si la plupart des fraudes de ce type sont d'origine nigériane, plusieurs régions du monde (plus particulièrement d'autres régions d'Afrique de l'Ouest et des régions d'Asie) ont suivi cet exemple. On parle de plus en plus de « **fraude sur les paiements d'avance** ».

Dans un cas de fraude du Nigéria classique, vous recevez une lettre ou un courriel vous demandant votre aide pour transférer une forte somme à l'étranger. On vous offre une part de cette somme si vous acceptez de fournir vos données bancaires pour faciliter le transfert. On vous demande ensuite de payer toutes sortes de frais avant de recevoir votre « récompense ». Évidemment, vous ne toucherez jamais votre part et ne récupérerez jamais les frais payés.

Vous pouvez également recevoir un courriel d'un avocat ou d'un représentant d'une banque qui vous informe qu'un de vos parents éloignés est décédé et vous a **légué** beaucoup d'argent. Le scénario des fraudeurs est parfois si convaincant que vous acceptez de produire vos documents personnels et détails bancaires afin de confirmer votre identité et réclamer votre héritage. Cet « héritage » est souvent fictif et vous risquez de perdre toutes les sommes versées au fraudeur, mais vous pourriez également être victime d'un vol d'identité.

Si votre entreprise ou vous-même vendez des produits ou des services en ligne ou dans les petites annonces, vous pourriez être visé par la fraude du **paiement excédentaire**. En réponse à votre annonce, vous recevez une offre généreuse d'un acheteur et vous l'acceptez. Ce dernier vous envoie

ensuite un chèque ou un mandat, mais la somme est supérieure au prix convenu. L'acheteur vous expliquera qu'il s'agit d'une erreur ou inventera une excuse, par exemple que l'excédent visait à couvrir les frais d'expédition. Si on vous demande de rembourser la différence en effectuant un virement, méfiez-vous! Le fraudeur espère que vous transférerez les fonds avant de vous rendre compte que le chèque est un faux. Vous perdez ainsi la somme transférée et l'article expédié.

!	PROTÉGEZ-VOUS
RAPPELEZ-VOUS	Si quelqu'un vous demande de lui transférer des fonds, il s'agit probablement d'une fraude.
SOYEZ PRUDENT	N'envoyez jamais d'argent, de données bancaires ou de données relatives à votre carte de crédit à une personne que vous ne connaissez pas et en qui vous n'avez pas confiance.
RÉFLÉCHISSEZ	N'acceptez pas de chèques ou de mandats dont la somme est supérieure au prix convenu. Retournez le document à l'acheteur et demandez-lui de vous retourner le paiement exact avant de livrer les articles ou de fournir les services.
INFORMEZ-VOUS	Consultez le site Web du Centre antifraude du Canada pour vous protéger contre ce type de fraudes.
POSEZ-VOUS DES QUESTIONS	Est-il vraiment sécuritaire de transférer de l'argent à quelqu'un que je ne connais pas?

FRAUDES SUR INTERNET

De nombreuses fraudes sur Internet sont commises à l'insu de la victime. Vous pouvez éviter ces fraudes en prenant quelques précautions de base.

SOYEZ À L'AFFÛT

Les fraudeurs ont recours à Internet pour escroquer leurs victimes, notamment grâce aux **pourriels**. Même s'ils n'obtiennent que quelques réponses aux millions de courriels envoyés, le jeu en vaut tout de même la chandelle. Évitez de répondre à ces courriels, ne serait-ce que pour vous « désabonner », car cela indique aux fraudeurs que votre adresse est valide.

Considérez comme un pourriel tout message reçu d'un expéditeur que vous ne connaissez pas, qui ne s'adresse pas à vous directement, et qui vous promet un avantage quelconque.

Les **logiciels malveillants**, également appelés maliciels, logiciels espions, enregistreurs de frappe, chevaux de Troie, constituent une menace pour votre sécurité. Les fraudeurs tentent d'installer ces logiciels sur votre ordinateur afin d'accéder à vos fichiers et à d'autres renseignements personnels.

Pour y parvenir, les fraudeurs ont de nombreux tours dans leur sac. Ils vous feront cliquer sur un lien contenu dans un pourriel ou vous attireront vers un faux site Web conçu pour infecter l'ordinateur des internautes imprudents.

L'**hameçonnage** consiste à vous duper afin que vous transmettiez vos renseignements personnels et bancaires aux fraudeurs. Les courriels reçus peuvent paraître légitimes, mais des organisations officielles, comme les institutions bancaires ou gouvernementales, ne vous demanderont jamais d'envoyer vos renseignements personnels dans un courriel.

Les fraudeurs peuvent aisément copier le logo ou même la totalité du site Web d'une organisation officielle. Ne présumez pas que le courriel est légitime. Si on vous demande de vous rendre dans un site pour « mettre à jour » ou « valider » vos renseignements, soyez sur vos gardes.

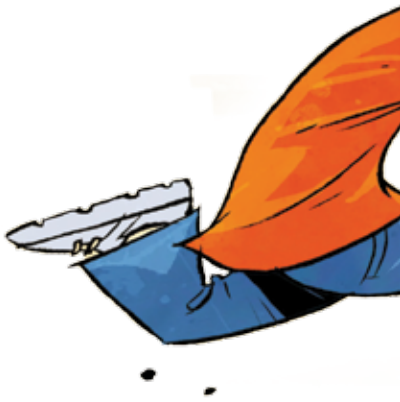
Supprimez ces courriels d'hameçonnage. Ils peuvent contenir des virus. N'ouvrez jamais les pièces jointes et ne cliquez pas sur les liens.

Les **enchères** et le **magasinage en ligne** vous permettent parfois de réaliser de bonnes affaires, mais ils attirent également les fraudeurs.

Ces derniers peuvent vous attirer hors du site d'enchères en ligne. Ils vous informent alors que le gagnant d'une enchère s'est retiré et que l'article pour lequel vous avez fait une offre vous revient. Une fois que vous avez payé, le fraudeur s'évanouit dans la nature et le site d'enchères ne pourra pas vous aider.

!	PROTÉGEZ-VOUS
RAPPELEZ-VOUS	Si vous faites des achats ou si vous participez à des enchères en ligne, informez-vous au sujet des politiques de remboursement et de règlement des différends. Vérifiez également le montant de la facture. Vous pouvez recourir à un service d'entiercement, comme PayPal, qui retient votre paiement et ne le verse au vendeur que lorsque vous avez reçu le bien acheté. Des frais minimes seront exigés. Une banque ou une institution financière légitime ne vous demandera jamais de cliquer sur un lien dans un courriel ou de transmettre vos données bancaires par courriel ou sur un site Web.
SOYEZ PRUDENT	N'achetez jamais d'un enchérisseur mal coté sur les sites d'enchères, et veillez à toujours faire vos achats sur des sites véritables. Ne donnez jamais vos données personnelles, bancaires ou relatives à votre carte de crédit, sauf si vous êtes convaincu de la légitimité du site.
RÉFLÉCHISSEZ	Ne répondez pas aux pourriels, même pour vous désabonner, ne cliquez jamais sur les liens et ne composez pas les numéros de téléphone qu'ils contiennent. Installez un logiciel de protection ou demandez les conseils d'un spécialiste.
INFORMEZ-VOUS	Si on vous offre un produit qui vous intéresse réellement dans un courriel ou un message flash, assurez-vous de comprendre toutes les conditions d'achat et les coûts avant de faire un achat et de transmettre vos données.
POSEZ-VOUS DES QUESTIONS	En ouvrant un courriel suspect, est-ce que je menace la sécurité de mon ordinateur? Est-ce que les coordonnées fournies sont exactes? Téléphonez à votre banque ou institution financière pour vous en assurer.

FRAUDES PAR TÉLÉPHONE CELLULAIRE



Les fraudes par téléphone cellulaire sont difficiles à reconnaître. Méfiez-vous des personnes qui vous parlent comme si elles vous connaissaient et évitez de recomposer un numéro inconnu. La facture pourrait être salée.

SOYEZ À L'AFFÛT

Les fraudes de **sonnerie** consistent à vous attirer avec une offre de sonnerie gratuite ou à faible coût. Cependant, en acceptant l'offre, vous vous abonnez à un service qui continue de vous envoyer des sonneries et qui n'hésite pas à vous les facturer. Il y a de nombreuses entreprises légitimes qui vendent des sonneries, mais les fraudeurs vous cacheront les coûts véritables de leur offre.

Soit les fraudeurs omettent de vous dire que cette première offre cache un abonnement à un service de sonneries, soit ces détails sont noyés dans une mer de petits caractères. Aussi, les fraudeurs ne vous faciliteront pas la tâche pour mettre fin au service : vous devez prendre des mesures actives pour vous sortir de ce mauvais pas.

Dans les fraudes liées aux **appels manqués**, les fraudeurs composent votre numéro, mais ne vous laissent pas le temps de répondre à l'appel. Vous ne reconnaîtrez pas le numéro apparaissant sur votre appareil. Si vous recomposez le numéro et qu'il s'agit d'une fraude, des frais s'appliqueront à votre insu.

Les fraudes par **texto** fonctionnent selon le même principe. Les fraudeurs vous envoient un texto à partir d'un numéro que vous ne reconnaissez pas. Cependant, le message semble provenir d'un ami, par exemple : « Salut! C'est Paul. Je suis revenu. Est-ce qu'on peut se voir? » Si vous répondez par curiosité, des frais pourraient s'appliquer pour chaque texto (parfois jusqu'à 4 $ pour chaque message envoyé ou reçu).

Les fraudes de **concours** ou de **jeu-questionnaire par texto** se présentent sous la forme d'un texto ou d'une publicité vous invitant à participer à un concours pour gagner un prix. Vous n'avez qu'à répondre correctement à quelques questions. Les fraudeurs vous facturent alors des frais très élevés pour chaque message envoyé et reçu. Généralement, les premières questions sont très faciles. On vous encourage ainsi à continuer de jouer. Cependant, les dernières questions auxquelles vous devez répondre pour réclamer votre prix sont très difficiles, et il est même parfois impossible de trouver la bonne réponse.

!	PROTÉGEZ-VOUS
RAPPELEZ-VOUS	Textez « STOP » pour faire cesser l'envoi de messages non désirés et mettre fin à un abonnement.
SOYEZ PRUDENT	Ne répondez jamais à des textos qui vous offrent des sonneries gratuites et ne recomposez jamais des numéros que vous ne reconnaissez pas.
RÉFLÉCHISSEZ	Ne composez pas de numéros 1-900, et n'envoyez pas de textos à ces numéros, sauf si vous connaissez les coûts et les conditions liées à l'envoi de codes abrégés.
INFORMEZ-VOUS	Lisez attentivement toutes les conditions d'une offre. Les produits offerts gratuitement ou à faible coût vous réservent souvent une surprise.
POSEZ-VOUS DES QUESTIONS	J'envisage de prendre un abonnement, mais est-ce que je saurais comment le résilier?

FRAUDES MÉDICALES OU LIÉES À LA SANTÉ

Les fraudeurs profitent de la souffrance humaine. Ils offrent des solutions « miracles » ou promettent de simplifier des traitements complexes.

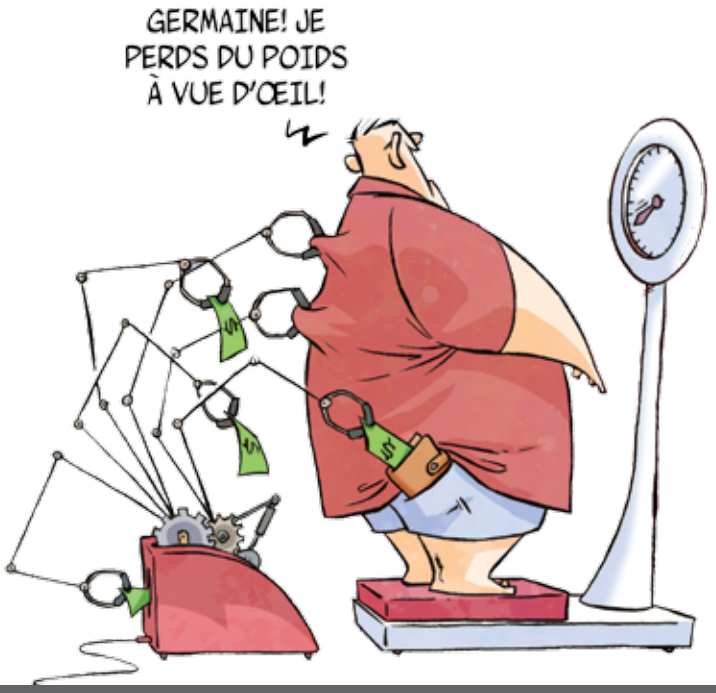
SOYEZ À L'AFFÛT

Les fraudes des **remèdes miracles** proposent un vaste éventail de produits et services qui semblent légitimes et qui promettent un traitement rapide et efficace pour de graves problèmes de santé. Ces traitements sont prétendument utiles pour toutes sortes de maladies, comme peuvent en témoigner certaines personnes qui doivent leur « guérison » à ces produits ou services.

Les fraudes liées à la **perte de poids** promettent une perte de poids considérable sans effort, ou presque. Elles reposent sur une diète inhabituelle ou très limitée, des exercices révolutionnaires ou des appareils qui brûlent les gras, ou encore des produits comme des pilules, des timbres ou des crèmes. On fait de fausses promesses, par exemple « perdez 10 kilos en 10 jours » ou « maigrissez en dormant ». En contrepartie, vous devrez verser une avance substantielle ou vous inscrire à un programme à long terme.

Les **fausses pharmacies en ligne** font appel à Internet et aux pourriels pour vendre des médicaments à faible coût ou sans ordonnance d'un médecin. Si vous avez recours à ce genre de pharmacie et que vous recevez les produits commandés, rien ne garantit qu'ils sont authentiques.

Il existe des pharmacies légitimes en ligne. Elles affichent leurs coordonnées complètes sur leur site et exigent une ordonnance valide avant de vous expédier vos médicaments.



!	PROTÉGEZ-VOUS
RAPPELEZ-VOUS	Il n'y a pas de pilules ou de cures miracles pour des problèmes de santé graves ou une perte de poids rapide.
SOYEZ PRUDENT	Ne prenez aucun engagement dans un contexte de vente sous pression.
RÉFLÉCHISSEZ	Méfiez-vous des prétentions non prouvées relatives à des médicaments, des suppléments ou d'autres traitements. Consultez un professionnel de la santé.
INFORMEZ-VOUS	Vérifiez si les affirmations des promoteurs sont véridiques en consultant des publications médicales.
POSEZ-VOUS DES QUESTIONS	S'il s'agit réellement d'un remède miracle, pourquoi mon médecin ne m'en a-t-il pas parlé?

FRAUDE DU « BESOIN D'ARGENT URGENT »

Ces fraudeurs visent les grands-parents et profitent de leur émotivité pour les voler.

SOYEZ À L'AFFÛT

Dans le scénario type de la fraude du « **besoin d'argent urgent** », un grand-parent reçoit un appel d'un fraudeur qui se fait passer pour un de ses petits-enfants. Il affirme être en difficulté et avoir besoin d'argent immédiatement. En général, il est question d'un accident, des difficultés éprouvées pour revenir au pays et d'un besoin d'argent urgent pour payer sa caution.

Vous pourriez recevoir l'appel de deux personnes, l'une prétendant être votre petite-fille ou votre petit-fils, et l'autre se disant policier ou avocat. Votre « petit-fils » vous pose des questions lors de l'appel pour vous amener à divulguer spontanément des renseignements personnels.

Les fraudeurs insistent pour que les autres membres de la famille ne soient pas au courant de leur situation. Ils vous demanderont de leur transférer des fonds. Souvent, les victimes ne se rendent compte de leur méprise qu'après avoir envoyé l'argent.

Dans certains cas, les fraudeurs prétendent être un ancien voisin ou un ami de la famille, mais en général, ce type de fraude s'adresse directement aux grands-parents.

!	PROTÉGEZ-VOUS
RAPPELEZ-VOUS	Les fraudeurs comptent sur le fait que vous agirez rapidement pour aider un être cher.
SOYEZ PRUDENT	N'envoyez jamais d'argent à quelqu'un que vous ne connaissez pas et en qui vous n'avez pas confiance. Avant d'aider quelqu'un, assurez-vous d'avoir bien vérifié son identité.
RÉFLÉCHISSEZ	Ne donnez pas de renseignements personnels à votre interlocuteur.
INFORMEZ-VOUS	Posez des questions auxquelles seule une personne de votre famille peut répondre. Téléphonez aux parents ou amis de l'enfant pour vérifier son histoire.
POSEZ-VOUS DES QUESTIONS	Est-ce que l'histoire qu'on me raconte est crédible?

FRAUDES RELATIVES AUX SERVICES DE RENCONTRE

Malgré le grand nombre de sites de rencontre légitimes au Canada, il existe de nombreuses fraudes relatives à ces services, dites « romantiques ». Elles vous poussent à baisser votre garde en faisant appel à votre compassion et à votre désir de rencontrer l'âme sœur.

SOYEZ À L'AFFÛT

Dans certaines de ces arnaques dites « **romantiques** », les fraudeurs créent un site Web où vous devez payer pour chaque courriel ou message reçu et envoyé. Ils maintiennent votre intérêt en vous envoyant des messages vagues où il est question d'amour et de désir. Ils peuvent également vous envoyer des courriels où ils décrivent leur pays ou leur ville d'origine, descriptions qui sont évidemment invérifiables. Ainsi, vous restez « accroché » et vous continuez de payer pour utiliser le site Web du fraudeur.

Même sur un site légitime, vous pouvez être approché par un fraudeur. Il s'agit parfois de personnes qui prétendent avoir un parent très malade ou être désespérées (ces fraudeurs affirment souvent être originaires de Russie ou d'Europe de l'Est). Après vous avoir envoyé quelques messages, et parfois même une photo très convaincante, ils vous demandent (subtilement ou plus directement) de leur envoyer de l'argent. Certains fraudeurs essaieront même de vous rencontrer, dans l'espoir que vous leur donniez de l'argent ou des cadeaux. Ensuite, ils disparaissent dans la nature.

Dans d'autres cas, les fraudeurs vous envoient des fleurs ou de petits cadeaux afin de se rapprocher de vous et de devenir votre ami. Ensuite, ils vous parlent d'une forte somme d'argent qu'ils doivent transférer hors de leur pays ou qu'ils souhaitent partager avec vous. Ils vous demandent vos données bancaires ou de l'argent pour payer les frais administratifs requis pour libérer cette somme.

!	PROTÉGEZ-VOUS
RAPPELEZ-VOUS	Vérifiez attentivement les adresses Internet. Les fraudeurs créent souvent de faux sites dont l'adresse est similaire à celle de véritables sites de rencontre.
SOYEZ PRUDENT	N'envoyez jamais d'argent, de données bancaires ou relatives à votre carte de crédit à une personne que vous ne connaissez pas et en qui vous n'avez pas confiance.
RÉFLÉCHISSEZ	Ne donnez jamais vos renseignements personnels dans un courriel ou lorsque vous clavardez.
INFORMEZ-VOUS	Assurez-vous de ne fréquenter que des sites légitimes et reconnus.
POSEZ-VOUS DES QUESTIONS	Pourquoi une personne que je n'ai jamais rencontrée me déclarerait-elle son amour après seulement quelques lettres ou courriels?

FRAUDES RELATIVES AUX ORGANISMES DE BIENFAISANCE

Ces fraudeurs profitent de la générosité et de la bonté des gens en leur demandant de faire un don à un faux organisme de bienfaisance ou en prétendant représenter un véritable organisme.

SOYEZ À L'AFFÛT

Les fraudeurs impliqués dans les fraudes relatives aux **organismes de bienfaisance** recueillent des fonds en prétendant représenter un véritable organisme de bienfaisance. Ils peuvent vous approcher sur la rue, à la maison, au téléphone ou sur Internet. Les courriels et boîtes de collecte portent même parfois le logo d'organismes légitimes.

Souvent, les fraudeurs profitent d'une catastrophe naturelle récente ou d'une famine rapportée aux nouvelles. D'autres prétendent venir en aide à des enfants malades.

Ils peuvent exercer des pressions pour vous obliger à faire un don et refuser de vous fournir des détails sur l'organisme qu'ils représentent, comme l'adresse et les coordonnées, ou encore vous donner de faux renseignements.

Ces fraudeurs vous volent, mais ils privent également des causes et des organismes légitimes de vos précieux dons. Tous les organismes de bienfaisance inscrits au Canada sont régis par l'Agence du revenu du Canada et enregistrés dans une base de données. Vous pouvez également communiquer avec votre bureau d'éthique commerciale local pour obtenir de l'information sur les organismes qui vous intéressent. Si l'organisme est légitime et que vous souhaitez faire un don, obtenez ses coordonnées dans le répertoire téléphonique ou sur un site Web digne de confiance.

Si vous ne voulez pas faire de don, ou si vous êtes satisfait des dons que vous avez déjà versés aux organismes de bienfaisance de votre choix, ignorez tout simplement les lettres et courriels, raccrochez ou dites non aux démarcheurs. Vous n'êtes pas obligé de donner.

!	PROTÉGEZ-VOUS
RAPPELEZ-VOUS	Si vous avez des doutes sur ceux qui vous demandent de l'argent, ne leur donnez rien : ni argent, ni données bancaires ou relatives à votre carte de crédit.
SOYEZ PRUDENT	Ne donnez jamais de renseignements personnels, de données bancaires ou relatives à votre carte de crédit au téléphone, sauf si c'est vous qui avez communiqué avec l'organisme et seulement si le numéro provient d'une source sûre.
RÉFLÉCHISSEZ	En cas de doute, communiquez directement avec l'organisme pour faire un don ou offrir votre soutien.
INFORMEZ-VOUS	Consultez la base de données de l'Agence du revenu du Canada pour vous assurer du caractère légitime de l'organisme qui vous a approché.
POSEZ-VOUS DES QUESTIONS	Comment et à qui souhaiterais-je faire une contribution?

FRAUDES LIÉES À L'EMPLOI

Les fraudes liées à l'emploi visent les personnes qui se cherchent du travail. Les fraudeurs promettent, et parfois même garantissent, un revenu alléchant sans effort.

SOYEZ À L'AFFÛT

Les fraudes du **travail à domicile** sont souvent annoncées dans des pourriels ou des publicités en ligne ou dans les journaux. Dans la majorité des cas, il ne s'agit pas de vraies offres d'emploi, mais plutôt de stratagèmes visant à blanchir des fonds ou à vous attirer dans une chaîne pyramidale.

Vous pourriez recevoir un courriel dans lequel on vous offre un emploi et vous demande de fournir votre numéro de compte pour transférer et recevoir des fonds d'une entreprise étrangère. On peut aussi vous engager pour tester les services d'une entreprise de transfert d'argent ou d'encaissement de chèques. Pour chaque paiement transféré, les fraudeurs vous promettent une commission. La plupart du temps, ils ne s'intéressent qu'à vos détails bancaires. Ils peuvent également vous envoyer un faux chèque et vous demander de le déposer et d'en transférer une partie vers un service de transfert de fonds.

Dans une fraude d'**emploi** ou de **revenu garanti**, les fraudeurs vous garantissent un emploi ou un certain revenu. Ils communiquent avec vous par pourriel et promettent de vous verser un certain montant pour établir un « plan d'affaires » et acquérir de l'équipement informatique.

D'autres fraudes prennent l'allure d'**occasions d'affaires**. On vous demandera de faire un premier versement (pour payer un article qui ne fonctionne pas ou différent de ce à quoi vous vous attendiez) ou de recruter d'autres participants (voir les systèmes de vente pyramidale à la page 4).

!	PROTÉGEZ-VOUS
RAPPELEZ-VOUS	Il n'y a pas de raccourci vers la richesse — les seuls à s'enrichir sont les fraudeurs.
SOYEZ PRUDENT	N'envoyez jamais vos coordonnées bancaires à quelqu'un que vous ne connaissez pas et en qui vous n'avez pas confiance. Si vous encaissez un faux chèque, la banque pourrait vous en tenir pour responsable.
RÉFLÉCHISSEZ	Ne prenez pas de décision sans étudier l'offre attentivement. Obtenez des conseils objectifs avant d'agir.
INFORMEZ-VOUS	Méfiez-vous des stratagèmes qui vous promettent un revenu garanti ou des offres d'emploi pour lesquelles vous devez payer des frais ou transférer des fonds. Assurez-vous que les offres concernant les franchises sont légitimes.
POSEZ-VOUS DES QUESTIONS	Est-ce que je dispose de tous les détails par écrit avant de payer ou de signer quoi que ce soit?

FRAUDES VISANT LES PETITES ENTREPRISES

Les fraudes qui visent les petites entreprises se présentent sous des formes diverses : factures pour de la publicité, répertoires qui n'ont jamais été commandés ou encore offres de fournitures douteuses.

SOYEZ À L'AFFÛT

Les exploitants de **petites entreprises** et les personnes qui possèdent un site Internet reçoivent parfois des lettres les avertissant que leur nom de domaine est presque expiré et doit être renouvelé, ou leur offrant un nouveau nom de domaine similaire au leur. Ces offres peuvent porter à confusion.

Si vous avez enregistré un nom de domaine, vérifiez attentivement vos factures ou avis de renouvellement. Même si l'avis est véritable, il peut également provenir d'une autre compagnie qui veut vous avoir comme client, ou encore d'un fraudeur.

- Assurez-vous que l'avis de renouvellement correspond exactement à votre nom de domaine. Soyez à l'affût des petites différences : p. ex. « .com » au lieu de « .ca » ou encore des lettres manquantes dans l'adresse URL.
- Assurez-vous que l'avis de renouvellement provient de l'entreprise auprès de laquelle vous avez enregistré votre nom de domaine.
- Vérifiez la véritable date d'expiration de votre nom de domaine.

Dans le cadre de la fraude des **répertoires** ou de la **publicité non autorisée**, les fraudeurs facturent une entreprise pour figurer dans un répertoire ou pour de la publicité.

La proposition d'inscription est souvent déguisée en mise à jour d'un abonnement existant. Les fraudeurs peuvent également vous duper en vous faisant croire que vous répondez à une offre d'inscription gratuite, alors qu'en fait, un paiement vous sera facturé plus tard.

Les fraudeurs peuvent également appeler des entreprises pour leur demander de confirmer les détails d'une publicité déjà réservée. Pour être plus convaincants, ils mentionnent une véritable publicité ou une véritable inscription dans un répertoire déjà payée par votre entreprise.

Méfiez-vous des **bons de commande** qui vous offrent de la publicité dans des répertoires d'entreprises. Ces bons sont souvent similaires à ceux de véritables vendeurs de publicité, mais ce sont des faux.

Dans la fraude des **fournitures de bureau**, vous recevez des marchandises que vous n'avez pas commandées, ainsi qu'une facture. Il s'agit généralement de biens et de services que vous avez l'habitude de commander : papier, cartouches d'encre, produits d'entretien ou publicité.

Une personne qui prétend faussement être votre « fournisseur habituel » vous téléphonera pour vous faire profiter d'une « offre spéciale » ou « pour une durée limitée », ou encore pour confirmer votre adresse ou votre commande. Les produits généralement offerts sont de mauvaise qualité et plus chers.

!	PROTÉGEZ-VOUS
RAPPELEZ-VOUS	Veillez à ce que les employés qui traitent les factures ou répondent aux appels soient informés de ces fraudes. C'est à eux que s'adresseront les fraudeurs. Assurez-vous que les biens ou services ont été commandés et livrés avant de payer une facture.
SOYEZ PRUDENT	Ne donnez jamais de renseignements sur votre entreprise, sauf si vous savez à quoi servira cette information.
RÉFLÉCHISSEZ	N'acceptez jamais une proposition d'affaires au téléphone — demandez une version de l'offre par écrit. Limitez le nombre d'employés ayant accès aux fonds de l'entreprise ou le pouvoir d'approuver des achats.
INFORMEZ-VOUS	Vous pouvez prévenir ces fraudes en appliquant des procédures efficaces liées à la vérification, au paiement et à la gestion des comptes et factures.
POSEZ-VOUS DES QUESTIONS	Si quelqu'un affirme que j'ai commandé un article ou autorisé un achat et que j'ai des doutes, ne devrais-je pas demander des preuves?

FRAUDES LIÉES À UNE OFFRE DE SERVICES

De nombreux Canadiens sont la cible de fraudeurs qui leur offrent des rabais pour différents services.

SOYEZ À L'AFFÛT

Les fraudeurs vous offrent généralement des services dans les domaines des télécommunications, d'Internet, des finances, des soins de santé et de l'électricité. Il peut également s'agir de garanties prolongées, d'assurances et de ventes par démarchage.

Dans cette catégorie, les deux fraudes les plus souvent signalées sont celles qui concernent les **logiciels antivirus** et la **réduction du taux d'intérêt sur carte de crédit**.

Les fraudeurs spécialistes des antivirus promettent de réparer votre ordinateur par Internet, ce qui suppose l'installation d'un logiciel ou la permission d'accéder à votre ordinateur à distance. Vous devez effectuer le paiement par carte de crédit.

Télécharger un logiciel d'une source inconnue ou autoriser une personne à accéder à votre ordinateur à distance comporte des risques. Les fraudeurs utilisent un maliciel pour saisir différents renseignements personnels, dont vos noms d'usager et mots de passe, vos données bancaires, etc.

Tout le monde aime faire une bonne affaire, et les fraudeurs le savent. Dans le cas des fraudes de réduction de taux d'intérêt, les fraudeurs se font passer pour des représentants d'une banque et affirment négocier avec les sociétés de crédit pour réduire votre taux d'intérêt. Ils vous promettent de fabuleuses économies. Ils ajoutent que cette offre n'est valide que pour une durée limitée et qu'il vous faut agir rapidement.

Vous pourriez recevoir un appel automatisé au cours duquel on vous demandera d'appuyer sur « 1 » et de fournir vos renseignements personnels, comme votre date de naissance et votre numéro de carte de crédit. On vous demandera de payer le service d'avance. Les fraudeurs se servent de cette information pour effectuer des achats ou obtenir des avances de fonds avec votre carte.

!	PROTÉGEZ-VOUS
RAPPELEZ-VOUS	Seul votre fournisseur de service peut vous offrir un meilleur prix pour ses propres services.
SOYEZ PRUDENT	Méfiez-vous des appels de personnes dont les offres ne sont « que pour une durée limitée ».
RÉFLÉCHISSEZ	Ne donnez pas votre numéro de carte de crédit au téléphone, sauf si c'est vous qui avez téléphoné et seulement si le numéro provient d'une source sûre.
INFORMEZ-VOUS	Si quelqu'un prétend représenter votre banque, téléphonez à votre banque pour vous assurer que l'offre est légitime.
POSEZ-VOUS DES QUESTIONS	En fournissant cette information, est-ce que je prends un risque pour ma sécurité?

QUELQUES CONSEILS PRATIQUES pour vous protéger

PROTÉGEZ VOTRE IDENTITÉ

- Ne donnez vos renseignements personnels que lorsque cela est absolument nécessaire, et seulement lorsque vous avez confiance en la personne à qui vous vous adressez.
- Détruisez vos renseignements personnels : ne faites pas que les jeter à la poubelle. Vous pouvez découper ou déchiqueter vos anciennes factures ou relevés de cartes de crédit ou bancaires.
- Traitez vos renseignements personnels comme vous traitez votre argent : gardez-les à l'abri des regards indiscrets.

QUESTIONS D'ARGENT

- N'envoyez jamais d'argent à quelqu'un que vous ne connaissez pas et en qui vous n'avez pas confiance.
- Vous ne devez jamais envoyer d'argent ou payer des frais pour réclamer un prix ou un gain de loterie.
- Un « emploi » dans le cadre duquel on vous demande d'utiliser votre compte bancaire pour transférer des fonds peut se révéler un stratagème pour blanchir de l'argent. Le blanchiment d'argent est un crime grave.
- Évitez de transférer un remboursement ou un paiement excédentaire à quelqu'un que vous ne connaissez pas.

L'APPROCHE EN PERSONNE

- Si quelqu'un se présente à votre porte, exigez des pièces d'identité. Vous n'avez pas à laisser entrer qui que ce soit dans votre domicile et cette personne doit partir si vous le lui demandez.
- Avant de payer quoi que ce soit, si le produit que vend un démarcheur vous intéresse, prenez le temps de vous informer sur l'entreprise qu'il représente et sur son offre.
- Communiquez avec le Bureau de la concurrence, votre bureau d'information aux consommateurs local ou provincial ou avec le bureau d'éthique commerciale de votre province ou territoire si vous avez des questions au sujet d'un démarcheur qui se présente à votre porte. Vous trouverez leurs coordonnées aux pages 29 et 30.

AU TÉLÉPHONE

- Si vous recevez un appel d'une personne que vous ne connaissez pas, demandez toujours le nom de cette personne et de l'entreprise qu'elle représente. Vérifiez cette information en appelant vous-même l'entreprise.
- Ne donnez pas vos renseignements personnels et vos détails bancaires au téléphone, sauf si c'est vous qui téléphonez et que le numéro provient d'une source sûre.
- Il est plus prudent de ne pas répondre à des textos provenant de numéros que vous ne reconnaissez pas ou de ne pas recomposer un numéro inconnu. Méfiez-vous plus particulièrement des numéros de téléphone qui commencent par 1-900. Vous pourriez devoir payer des frais supérieurs à ceux en vigueur et la facture risque d'être salée.

OFFRES PAR COURRIEL

- Ne répondez jamais à un pourriel, même pour vous désabonner. Souvent, ces réponses permettent aux fraudeurs de « vérifier » votre adresse. La meilleure façon de procéder consiste à supprimer les courriels douteux sans les ouvrir.
- Désactivez le « volet d'affichage », puisque le seul fait de consulter le courriel peut transmettre à l'expéditeur un message attestant de la validité de votre adresse de courriel.
- Les banques et institutions financières légitimes ne vous demanderont jamais vos données bancaires dans un courriel, ou encore de cliquer sur un lien pour accéder à votre compte.
- Ne composez jamais un numéro de téléphone qui provient d'un pourriel et ne faites pas confiance aux coordonnées qu'il contient.

SUR INTERNET

- Installez un logiciel qui protège votre ordinateur des virus et d'autres programmes indésirables, et assurez-vous qu'il est à jour. Si vous avez des questions, consultez un professionnel.

- Si vous souhaitez accéder à un site Web, utilisez un signet qui vous dirigera vers le site ou inscrivez l'adresse du site dans la fenêtre du navigateur. Ne suivez jamais un lien fourni dans un courriel.

- Vérifiez attentivement les adresses de sites Web. Les fraudeurs créent souvent de faux sites Web dont l'adresse est similaire à celle de véritables sites.

- Méfiez-vous des sites qui vous proposent un téléchargement gratuit (musique, contenu réservé aux adultes, jeux et films). En téléchargeant ces contenus, vous pourriez également installer des maliciels à votre insu.

- Évitez de cliquer sur les publicités qui apparaissent à votre écran. Vous pourriez installer des logiciels malveillants sur votre ordinateur.

- N'entrez jamais vos renseignements personnels, vos données bancaires ou relatives à votre carte de crédit sur un site Web dont vous doutez de la légitimité.

- N'envoyez jamais vos renseignements personnels, vos données bancaires ou relatives à votre carte de crédit par courriel.

- Évitez d'utiliser des ordinateurs publics (dans les bibliothèques ou dans les cafés Internet) afin de faire des achats en ligne ou des transactions bancaires.

- Lorsque vous utilisez des ordinateurs publics, effacez l'historique et la mémoire cache de l'ordinateur lorsque vous avez terminé.

- Soyez attentif lorsque vous utilisez un logiciel qui remplit automatiquement les formulaires en ligne. Il pourrait fournir aux fraudeurs un accès facile à vos renseignements personnels et données relatives à votre carte de crédit.

- Choisissez des mots de passe qui sont difficiles à deviner, qui comprennent par exemple des lettres et des chiffres. Vous devriez également les changer régulièrement.

- Lorsque vous achetez un article en ligne, imprimez des copies de toutes les transactions et ne payez que par le truchement d'un site sécurisé. Si vous fréquentez les sites d'enchères sur Internet, notez les numéros d'identification et lisez toutes les consignes de sécurité sur le site.

LA FRAUDE ET VOUS : QUE FAIRE SI VOUS EN ÊTES VICTIME

Les autorités canadiennes ne sont pas toujours en mesure d'intervenir en cas de fraude, même si les fraudeurs semblent avoir enfreint la loi.

LIMITER LES DOMMAGES

Même s'il peut être difficile de récupérer les sommes perdues dans le cadre d'une fraude, il y a des mesures à prendre pour **limiter les dommages** et se protéger d'une nouvelle fraude. Plus vous agissez rapidement, mieux vous réussirez à circonscrire vos pertes.

Signalez la fraude. En rapportant la fraude aux autorités, ces dernières pourront avertir la population et réduire le risque que la fraude ne prenne de l'ampleur. Vous devez également en informer tous vos parents et amis. Vous trouverez des renseignements sur la façon de signaler une fraude aux pages 29 et 30 de cette publication.

SI ON VOUS A DUPÉ ET QUE VOUS AVEZ SIGNÉ UN CONTRAT OU ACHETÉ UN PRODUIT OU UN SERVICE

Communiquez avec votre bureau d'information aux consommateurs provincial ou territorial et demandez des conseils objectifs pour évaluer vos options : vous bénéficiez peut-être d'une période de rétractation ou vous pourriez également négocier un remboursement.

SI VOUS CROYEZ QUE QUELQU'UN A EU ACCÈS À VOS DONNÉES BANCAIRES OU AUX DONNÉES DE VOTRE CARTE DE CRÉDIT EN LIGNE OU AU TÉLÉPHONE

Communiquez avec votre institution financière immédiatement afin que cette dernière bloque votre compte, dans le but de limiter les pertes éventuelles. Les sociétés émettrices de cartes de crédit peuvent également procéder à un « remboursement » (inverser la transaction) si elles jugent que votre carte de crédit a été utilisée frauduleusement.

N'utilisez pas les coordonnées qui figurent dans des courriels ou sur des sites Web d'apparence douteuse : elles sont probablement fausses et risquent de vous mener tout droit au fraudeur. Vous pouvez trouver les véritables coordonnées de l'institution recherchée dans le répertoire téléphonique, sur un relevé ou au dos de votre carte de guichet.

SI LA FRAUDE EST LIÉE À VOTRE SANTÉ

Cessez de prendre des pilules ou d'autres substances sur lesquelles vous avez des doutes. Consultez un médecin ou un autre professionnel de la santé dès que vous le pourrez. Décrivez-lui le traitement vendu par le fraudeur (apportez les médicaments, ainsi que leur emballage). Mentionnez également au médecin si vous avez interrompu un traitement pour prendre ce médicament.

SI VOUS AVEZ ENVOYÉ DE L'ARGENT À UNE PERSONNE QUI POURRAIT ÊTRE UN FRAUDEUR

Si vous avez envoyé les données relatives à votre carte de crédit, suivez les instructions de la section ci-contre.

Si vous avez transféré des fonds par voie électronique (sur Internet), communiquez immédiatement avec votre institution financière. Si elle n'a pas encore traité le transfert, elle pourra peut-être l'annuler.

Si vous avez envoyé un chèque, communiquez immédiatement avec votre institution financière. Si le fraudeur ne l'a pas encore encaissé, votre banque pourra peut-être l'annuler.

Si vous avez transféré de l'argent par le biais d'un service de virement (comme Western Union ou Money Gram), communiquez immédiatement avec ce service. Si vous êtes rapide, il sera peut-être possible de bloquer le transfert.

SI VOUS AVEZ ÉTÉ DUPÉ PAR UN DÉMARCHEUR

Vous êtes peut-être protégé par les lois qui garantissent aux consommateurs une période de rétractation pendant laquelle ils peuvent annuler une entente ou un contrat. Communiquez avec votre bureau d'information aux consommateurs provincial ou territorial pour obtenir des conseils à ce sujet.

SI VOUS AVEZ ÉTÉ VICTIME D'UNE FRAUDE INFORMATIQUE

Si vous utilisiez votre ordinateur au moment de la fraude, il est possible qu'un virus ou un maliciel continue d'infecter votre ordinateur. Procédez à une vérification complète de votre système à l'aide d'un antivirus fiable.

Si vous n'avez pas de logiciel de protection (comme un antivirus et un pare-feu), un professionnel en informatique peut vous aider à choisir un produit qui répond à vos besoins.

Les fraudeurs ont peut-être eu accès à vos mots de passe. Changez-les pour garantir votre sécurité.

SI LA FRAUDE A ÉTÉ COMMISE AVEC VOTRE TÉLÉPHONE CELLULAIRE

Communiquez avec votre fournisseur de services et expliquez-lui la situation.

OBTENIR DE L'AIDE ET SIGNALER UNE FRAUDE

L'endroit où vous habitez et le type de fraude commise détermineront avec qui vous devez communiquer.

Vous pouvez vous adresser à certains organismes gouvernementaux ou d'application de la loi au Canada si vous croyez que vous avez découvert une fraude ou que vous avez été dupé par un fraudeur. Ces organismes seront en mesure de vous informer ou de recevoir votre plainte. Cette démarche est non seulement utile pour vous, mais elle permet également d'éviter à d'autres innocentes victimes de se faire prendre au piège.

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

Centre des renseignements du 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* ou sur le site Web du Bureau de la consommation.

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

FRAUDE BANCAIRE ET RELATIVE À LA CARTE 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.

SIGNALER LES FRAUDES PAR POURRIELS ET TEXTOS

De nombreuses fraudes passent par votre courriel et vos textos. Visitez le www.combattrelepourriel.gc.ca pour plus d'information sur la loi canadienne antipourriel.

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 (n'utilisez pas une adresse de courriel et ne composez pas un numéro fourni dans le courriel que vous souhaitez dénoncer).

SIGNALER UNE FRAUDE, UN VOL OU D'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 du *Code criminel* sur la fraude.

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.

Vous pouvez également communiquer avec une des organisations suivantes :

Conseil canadien des bureaux d'éthique commerciale
www.ccbbb.ca

Agence du revenu du Canada — Organismes de bienfaisance
www.arc-cra.gc.ca
1-800-267-2384

Votre service de police local, les sociétés émettrices de carte de crédit, les banques et les bureaux des documents provinciaux.

Les agences d'évaluation du crédit peuvent joindre une alerte à votre dossier qui permet d'aviser les organismes prêteurs d'une fraude possible :

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