L'Union culturelle des Franco-Ontariennes

Bulletin spécial

Mon argent, j'y ai droit!

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.

Qui donc est assez imprudent pour tomber dans ce genre de pièges? «C'est une question qui revient souvent, constate Philippe Viel, responsable des communications à l'Union des consommateurs. Et la réponse est simple: tout le monde. Il n'existe pas un profil type de victime. La fraude touche tous les Canadiens, quels que soient leur milieu social, leur profession, leur âge ou leur origine.»

C'est la force des fraudeurs de savoir s'adapter vite et bien à chaque victime potentielle, poursuit Philippe Viel. Les mécanismes frauduleux sont très évolués et évolutifs grâce, en particulier, aux technologies informatiques. Six des dix principales arnaques ont lieu en ligne par le biais des réseaux sociaux, des courriels d'hameçonnage ou de faux sites Internet.

Pour les associations de consommateurs, la réglementation existe, mais elle peine à s'ajuster à l'évolution des pratiques frauduleuses. Alexandre Plourde, avocat à Option consommateurs, rappelle que 5 % seulement des pertes réelles sont recensées par le Centre antifraude du Canada, «car un grand nombre de personnes décident de ne pas signaler les fraudes dont elles ont été victimes».

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 vos renseignements personnels et apprenez à reconnaître les diverses formes de fraude :

- ## Loteries, tirages au sort et concours

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

  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.

  Vos renseignements personnels pourraient également être utilisés à mauvais escient.

  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.

Numéros 1-900

Des numéros de téléphone 1-900 sont souvent utilisés pour des services comme des lignes téléphoniques de rencontres, des bulletins météo, des concours et des horoscopes. Les numéros 1-900 peuvent donner l'impression d'être des numéros sans frais; mais, en réalité, de tels appels sont facturés à des taux très élevés. Il existe d'autres numéros du même genre, notamment les 1-976 et 1-809.

Les véritables numéros sans frais, ceux par lesquels vous pouvez effectuer des appels gratuitement, utilisent les codes régionaux 1-800, 1-888 et 1-887.

• Ventes pyramidales

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

• Demandes de transfert d'argent

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.
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 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. 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.

- ## Fraudes sur Internet

De nombreuses fraudes sur Internet sont commises à l'insu de la victime.
Les fraudeurs ont recours à Internet pour escroquer leurs victimes, notamment grâce aux pourriels. 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.

Hameçonnage ou vol d'identité

Il y a vol d'identité quand quelqu'un utilise vos renseignements personnels — comme votre numéro de compte de banque ou de carte de crédit — sans votre permission. Dans certains cas, des voleurs d'identité utilisent votre nom pour commettre des crimes graves.
Les courriels reçus peuvent paraître légitimes, mais les fraudeurs peuvent aisément copier le logo ou même la totalité du site Web d'une organisation officielle. 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.

- ## Fraudes par téléphone
    - ### Escroqueries par télémarketing

Certains escrocs se présentent comme des télévendeurs et prétendent vous offrir des produits ou des services à des conditions avantageuses. Ils vous demandent des renseignements sur votre compte de banque ou sur votre carte de crédit pour se faire payer.

Ils peuvent ensuite utiliser vos renseignements pour retirer tout l'argent de votre compte de banque et débiter votre carte de crédit jusqu'à sa limite. Ils pourraient vous envoyer un article de piètre qualité qui ne correspond pas à la description qu'ils ont fournie, ou ils pourraient ne rien vous envoyer du tout.

Pour échapper à la plupart des appels de télémarketing à l'avenir, inscrivez-vous à la Liste nationale de numéros de télécommunication exclus. Pour vous inscrire, visitez **www.lnnte-dncl.gc.ca** ou **1-866-580-3625**.

- ### 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.

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. 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. 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.

Textez « STOP » pour faire cesser l'envoi de messages non désirés et mettre fin à un abonnement.

- ## Fraudes médicales ou liées à la santé

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 fraudeurs promettent une perte de poids considérable sans effort, ou presque. 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.

- ## Fraude du « besoin d'argent urgent »

Ces fraudeurs visent les grands-parents et profitent de leur émotivité pour les voler.
Dans le scénario type, 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 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.
Dans certains cas, les fraudeurs prétendent être un ancien voisin ou un ami de la famille…
Les fraudeurs comptent sur le fait que vous agirez rapidement pour aider un être cher. Avant d'aider quelqu'un, assurez-vous d'avoir bien vérifié son identité et posez des questions auxquelles seule une personne de votre famille peut répondre.

- ## 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 ». 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 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.

Assurez-vous de ne fréquenter que des sites légitimes et reconnus.

- ## 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. 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.
  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.

- ## 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.
  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.
  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 (systèmes de vente pyramidale).

- ## 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.
  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.
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 payé 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.
Vous pouvez prévenir ces fraudes en appliquant des procédures efficaces liées à la vérification, au paiement et à la gestion des comptes et factures.

- ## Fraudes liées à une offre de services

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.
- 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.
- 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.
Seul votre fournisseur de service peut vous offrir un meilleur prix pour ses propres services.
- Attention aux contrats d'énergie. Les compagnies locales de services publics (hydro, gaz), les municipalités, les organismes gouvernementaux et les organismes de réglementation n'envoient pas de vendeurs à domicile.

Mise en garde: Si vous allez sur le site internet de l'entreprise et que vous transmettez de l'information telle que votre nom, votre adresse, votre numéro de facture, vous pourriez vous engager en vertu d'un contrat virtuel.

UN CONTRAT EST UN DOCUMENT LÉGAL. PENSEZ-Y !

• Pratiques déloyales

Les vendeurs ne sont pas autorisés à user de « pratiques déloyales » pour vous convaincre d'acheter leur produit ou leur service. Les assertions fausses, trompeuses ou mensongères sont au nombre des pratiques déloyales. À titre d'exemple, les vendeurs ne doivent pas, selon le cas :

- faire valoir que le produit est de meilleure qualité qu'il n'est réellement,
- dire que le produit est seulement offert pour une période limitée si ce n'est pas vrai,
- dire que vous avez besoin d'un certain produit alors que, en réalité, vous n'en avez pas besoin,
- faire valoir que vous obtenez un prix ou un avantage particulier alors que, en réalité, ce que vous offre le vendeur peut s'obtenir ailleurs.

Les pratiques déloyales comprennent également les tactiques suivantes :

- exploiter, chez vous, toute difficulté linguistique ou incapacité physique, mentale ou affective,
- vous facturer un montant beaucoup plus élevé que le prix raisonnable du produit ou du service concerné,
- exercer des pressions sur vous afin de vous faire acheter un produit ou des services que, à la connaissance du vendeur, vous n'avez pas les moyens de payer.

Si le vendeur a recouru à une pratique déloyale, quelle qu'elle soit, vous pouvez résilier la convention en tout temps **dans l'année qui suit la date à laquelle vous l'avez conclue si** votre convention est régie par la Loi sur la protection du consommateur. Vous pourriez obtenir le remboursement d'une partie ou de la totalité de l'argent que vous avez payé.

Quelques conseils :

PROTÉGEZ VOTRE IDENTITÉ

• Donnez vos renseignements personnels seulement lorsque c'est nécessaire, et que vous ayez confiance.

• Détruisez vos renseignements personnels en les découpant, en les déchiquetant ou en les brûlant.

• 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 payez 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.

• Évitez de transférer un remboursement ou un paiement excédentaire à quelqu'un que vous ne connaissez pas.

• Prenez en note toutes vos actions et gardez précieusement tous les documents concernant vos finances.

L'APPROCHE EN PERSONNE

• Si quelqu'un se présente à votre porte, exigez des pièces d'identité

• Avant de payer quoi que ce soit, prenez le temps de vous informer sur l'entreprise et sur son offre.

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. Ne donnez pas vos renseignements personnels et vos détails bancaires.

• Inscrivez-vous à la Liste nationale de numéros de télécommunication exclus. **www.lnnte-dncl.gc.ca** ou **1-866-580-3625**.

• Ne répondrez pas à des textos provenant de numéros que vous ne reconnaissez pas ou ne recomposez pas un numéro inconnu. Méfiez-vous des numéros qui commencent par 1-900. Ils sont payants!

OFFRES PAR COURRIEL

• Ne répondez jamais à un pourriel. Les réponses permettent aux fraudeurs de vérifier votre adresse. Supprimez-les sans les ouvrir et désactivez le « volet d'affichage ».

• Les banques et institutions financières légitimes ne vous demanderont jamais vos données bancaires dans un courriel, ou de cliquer sur un lien pour accéder à votre compte. De plus, elles utilisent toujours une adresse sécurisée. (HTTPS)

• Ne composez jamais un numéro de téléphone qui provient d'un pourriel et ne faites pas confiance aux coordonnées qu'il contient.

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

SUR L'INTERNET

• Installez un logiciel, à jour, qui protège votre ordinateur des virus et d'autres programmes indésirables.

• Méfiez-vous des sites qui vous proposent un téléchargement gratuit. Ces contenus pourraient contenir des maliciels.

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

• 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 et soyez attentif lorsque vous utilisez un logiciel qui remplit automatiquement les formulaires en ligne.

• Évitez d'utiliser des ordinateurs publics afin de faire des achats ou des transactions bancaires. Après son utilisation, effacez l'historique et la mémoire cachée de l'ordinateur.

• 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.

• Changer régulièrement vos mots de passe.

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

Que faire si je suis victime d'une escroquerie ?

- Rapporter l'escroquerie à la police.

- Communiquer avec les institutions financières, les émetteurs de cartes de crédit ou les sociétés qui sont visées.

- Communiquer avec Equifax : www.equifax.ca 1-800-465-7166 et

TransUnion : 1-877-713-3393 www.transunion.ca.

- Rapporter l'escroquerie aux organismes gouvernementaux concernés :

www.antifraudcentre-centreantifraude.ca 1-888-495-8501

www.bureaudelaconcurrence.gc.ca. 1-800-348-5358

www.ontario.ca/fr/page/ministere-des-services-gouvernementaux-et-des-services-aux-consommateurs, 1 844 286-8404

Procureur général : www.attorneygeneral.jus.gov.on.ca 1 800 518 7901

Pour obtenir plus d'assistance :

- Cliniques juridiques communautaires : Pour trouver la clinique juridique qui sert votre localité, visitez le site web d'Aide juridique Ontario (AJO) à **www.legalaid.on.ca** ou 1-800-668-8258.

- Barreau à **www.lsuc.on.ca** 1 800 668-7380

- **www.justicenet.ca** 1-866-919-3219

-Si vous ne parlez pas anglais

Il existe de nombreuses situations où vous avez droit à la prestation de services gouvernementaux et à la tenue d'une instance judiciaire ou quasi judiciaire en français. Ainsi, vous pouvez avoir droit à ce qu'une audience à laquelle vous êtes partie soit tenue devant un décideur qui parle français. Si vous avez un problème

juridique, vous pouvez demander à un avocat ou à un intervenant d'une clinique juridique communautaire de vous expliquer les droits linguistiques liés au fait de parler français.

L'information juridique du présent document est à caractère général et est destinée aux personnes de l'Ontario, au Canada. Ces renseignements ne doivent pas servir de conseils juridiques face à des problèmes juridiques particuliers.

Sources :

CLEO
Protégez-vous.ca
www.bureaudelaconcurrence.gc.ca
Clinique juridique populaire de Prescott et Russell Inc.
Lila Refaie, avocate
Alexandre Plourde, avocat à Option consommateurs
Philippe Viel, responsable des communications à l'Union des consommateurs

Pour en savoir plus, inscrivez-vous par courriel (ucfo@on.aibn.com) aux webinaires gratuits, offerts au début 2017.

L'Union culturelle des Franco-Ontariennes 1936-2016

450, rue Rideau, bureau 302
Ottawa, ON K1N 5Z4
613 741 1334
ucfo@on.aibn.com
www.unionculturelle.ca