Outil de gestion sur la protection des clients

Types courants de fraude que vous devez connaître et façons de vous protéger

Livre 2 de 3

Table des matières

Message de Keith Gordon

Vice-président à la direction et chef de la sécurité,
Banque Canadienne Impériale de Commerce
(Banque CIBC)

La technologie occupe une grande place dans nos vies; nous nous en servons autant pour vérifier les soldes de nos comptes bancaires en ligne que pour regarder des films en continu. Les progrès technologiques nous font profiter d'avantages extraordinaires au quotidien et façonnent le monde dans lequel nous vivons. À la Banque CIBC, nous adoptons continuellement de nouvelles technologies et caractéristiques de sécurité qui vous aident à réaliser vos ambitions en protégeant votre argent et vos renseignements.

La technologie évolue, et les tactiques des fraudeurs aussi. Selon le Centre antifraude du Canada et la Federal Trade Commission, les pertes financières liées aux fraudes des Nord-Américains ont totalisé un peu plus de 6 milliards de dollars l'an dernier. Depuis le début de la pandémie, le volume d'opérations en ligne à l'échelle mondiale est monté en flèche. Ces opérations se sont révélées pratiques pour les consommateurs et essentielles pour les entreprises, mais ont créé un contexte propice à la fraude. Les fraudeurs tentent constamment de trouver des façons de soutirer de l'argent à leurs victimes et d'obtenir leurs renseignements personnels et bancaires. À la Banque CIBC, nous travaillons jour et nuit pour arrêter les fraudeurs et assurer la sécurité de nos clients.

La cybersécurité est l'affaire de tous. À l'heure actuelle, les menaces à la cybersécurité représentent l'un des plus grands risques qui pèsent sur les institutions financières. Nous devons assurer une vigilance et une amélioration constantes pour garder une longueur d'avance. Par conséquent, la Banque CIBC considère la sécurité de l'information et la cybersécurité comme une compétence de base. La protection de nos systèmes et de nos renseignements est l'un de nos objectifs stratégiques et fait partie intégrante de notre culture d'entreprise. Nous travaillons constamment à l'amélioration de la sécurité des opérations bancaires de nos clients – mais la première ligne de défense, c'est vous!

En améliorant vos connaissances sur la fraude, vous diminuez vos chances d'en être victime. Pour vous protéger, il est essentiel de savoir comment la prévenir, la repérer et la contrer. Comme elle prend de nombreuses formes, il est important de comprendre les différentes tactiques que les fraudeurs utilisent pour duper les gens. Servez-vous de cet outil de gestion comme guide. Il vous aidera à identifier les types d'arnaques les plus courants et vous fournira des conseils pour vous protéger et repérer les signes de fraude au moment opportun.

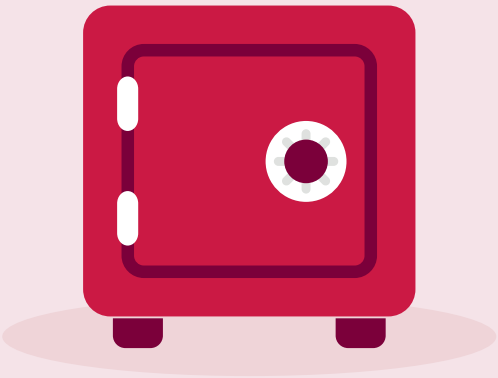
Travaillons ensemble et assurons la sécurité de tous.

Keith Gordon

Renseignements généraux sur les fraudes

Avec les avancées constantes dans les domaines de la technologie, des médias sociaux et du commerce électronique, les renseignements personnels et bancaires risquent d'être volés tous les jours. Les fraudeurs continuent de créer de nouveaux stratagèmes en évolution visant à exploiter et à obtenir illégalement les renseignements personnels de leurs victimes dans le but de faire des gains financiers.

La Banque CIBC s'est engagée à assurer votre sécurité et celle de vos renseignements bancaires et à vous renseigner sur les risques auxquels vous pourriez être exposé.



Piratage psychologique

Recours à la psychologie pour manipuler l'instinct humain et susciter une réaction aux demandes urgentes et à la peur afin d'amener les victimes à divulguer des renseignements confidentiels qui pourraient être utilisés pour commettre une fraude financière.

Fondement de nombreuses escroqueries

Les fraudeurs utilisent des tactiques de **piratage psychologique** pour obtenir des renseignements confidentiels sur des victimes et en tirer profit. Ces tactiques prennent souvent la forme de courriels, d'appels et de messages textes suspects qui peuvent sembler provenir de membres de la famille, d'amis, d'organismes gouvernementaux et d'institutions financières. Une fois que les fraudeurs ont obtenu les renseignements confidentiels, ils les utiliseront pour commettre une fraude financière et épuiser les fonds de la victime.

Voici trois principales caractéristiques des techniques de piratage psychologique :

Utilisation de la peur comme facteur de motivation en envoyant des courriels ou des messages textes menaçants ou en vous appelant pour vous inciter à divulguer des renseignements ou à effectuer des opérations.

Demandes urgentes et imprévues de renseignements personnels ou professionnels au moyen de communications écrites comme des courriels ou des messages textes.

Offres, prix ou concours qui semblent trop beaux pour être vrais et qui prétendent souvent offrir une récompense en échange de renseignements de connexion ou d'autres renseignements personnels ou professionnels.

Savoir reconnaître les signes :

Signaux d'alerte pouvant indiquer que vous avez affaire à un fraudeur

Une demande de paiement par câble ou de paiement au moyen de méthodes qui ne sont pas traçables

Les fraudeurs demandent généralement à leurs victimes d'envoyer des fonds par Virement *Interac*[MD], d'acheter des cartes-cadeaux prépayées ou de transférer des cryptomonnaies, car ces modes de paiement sont impossibles à retracer et souvent irréversibles une fois les fonds envoyés. Méfiez-vous des demandes de virement de fonds par voie électronique.

Un courriel, un message texte ou un appel téléphonique suspect et non sollicité

Méfiez-vous des appels, des courriels ou des messages textes de personnes ou d'entités qui prétendent que vous devez de l'impôt, que vos comptes ont été suspendus ou compromis, que votre colis n'a pas été livré, que votre carte de crédit a été débitée sans autorisation, ou encore, qui vous proposent un emploi très bien rémunéré pour peu d'efforts. Ces communications suscitent intentionnellement un sentiment d'urgence et vous incitent à suivre un lien suspect qui peut télécharger des logiciels malveillants sur vos appareils, ou à fournir des renseignements confidentiels, concernant par exemple votre numéro d'assurance sociale, votre permis de conduire ou vos comptes bancaires. Attardez-vous aux fautes d'orthographe et de grammaire, ainsi qu'aux adresses courriel et Web, et vérifiez s'il y a des erreurs ou des différences subtiles.

Une offre qui semble trop belle pour être vraie

Les promotions, les occasions de placement ou les ventes qui semblent trop belles pour être vraies le sont fort probablement. Le fraudeur veut que vous répondiez rapidement à une offre ou à une occasion « unique » qui n'existe pas, ce qui vous incite à effectuer une opération ou à fournir des renseignements sans tenir compte de la légitimité de la demande.

Un acheteur qui veut payer un montant trop élevé

Lorsque vous vendez des articles en ligne, méfiez-vous des acheteurs qui paient un montant supérieur à ce qu'ils vous doivent, puis vous demandent de retourner la différence, ou encore, de couvrir les frais de transport en promettant de vous rembourser après la livraison du produit. Un fraudeur peut vous envoyer un chèque contrefait d'un montant supérieur à celui affiché et vous demander de déposer le chèque, puis de lui envoyer immédiatement les fonds excédentaires par virement. Une fois les fonds envoyés, le fraudeur mettra fin à toute communication avant que le chèque « rebondisse », de sorte que vous serez responsable des fonds déposés et n'obtiendrez pas les fonds qui vous ont été transférés.

Pratiques exemplaires en ligne :

Protégez votre argent et vos renseignements en suivant les pratiques exemplaires ci-dessous

- Ne communiquez jamais vos codes de vérification à usage unique.
- Configurez la fonction Dépôt automatique de Virement *Interac* pour que les fonds qui vous sont envoyés soient automatiquement déposés dans votre compte bancaire.
- Ne suivez jamais un lien dans un courriel pour visiter un site Web; entrez plutôt l'adresse dans votre navigateur.
- Conservez vos mots de passe en sécurité hors ligne ou dans un gestionnaire de mots de passe reconnu.
- Ne sélectionnez pas les messages contextuels vous indiquant que votre ordinateur est à risque et n'y répondez pas.
- Vérifiez régulièrement vos relevés bancaires mensuels pour repérer des débits non autorisés.

Comment la Banque CIBC vous protège contre le vol d'identité et la fraude

La Banque CIBC et d'autres entités légitimes ne communiqueront jamais avec vous directement pour vous demander vos renseignements personnels ou bancaires; ne les communiquez pas aux personnes disant faire partie d'entreprises légitimes.

Inscrivez-vous à Mes alertes de la Banque CIBC dans les services bancaires mobiles ou en ligne pour surveiller les activités suspectes dans vos comptes bancaires.

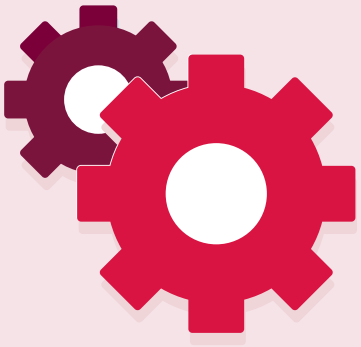
Inscrivez-vous à la caractéristique de sécurité de vérification vocale de la Banque CIBC pour effectuer vos opérations bancaires plus rapidement et en toute sécurité, et vous protéger contre la fraude. *Vous devez avoir 13 ans ou plus pour vous inscrire. Au Québec, vous devez avoir 14 ans ou plus.*

Si vous effectuez une opération à risque élevé, **inscrivez-vous aux notifications de la Banque CIBC** dans Services bancaires mobiles pour recevoir un code de vérification à usage unique.

Abonnements piégés

Fonctionnement

Dans ce type de fraude, le fraudeur ou l'entreprise dépeint ses produits en ligne comme étant des produits miracles. La publicité vante des avantages convaincants et peut même mentionner l'appui de vedettes. La victime se voit offrir un essai gratuit d'une durée limitée, sans condition, et n'a que de faibles frais d'expédition et de manutention à payer.



Selon des dispositions cachées dans les petits caractères ou les modalités, le consommateur qui fournit sa carte de crédit et effectue sa commande accepte de payer un abonnement mensuel coûteux pour des produits. Dans certains cas, il paie automatiquement pour des produits complémentaires qu'il n'a même jamais commandés. La victime se retrouve coincée avec d'importants paiements périodiques qu'elle aura souvent beaucoup de mal à se faire rembourser.

Produits qui font souvent l'objet d'abonnements piégés	Suppléments alimentaires	Produits amaigrissants	Pilules de renforcement musculaire	Produits anti-âge pour le visage
Signaux d'alerte à surveiller				
Le produit est annoncé comme un essai gratuit et le client ne paie que les frais d'expédition et de manutention.	✕	✕	✕	✕
Le site Web ou la publicité utilise, par exemple, un compte à rebours pour inciter le client à agir rapidement.	✕	✕	✕	✕
Les modalités, les politiques de retour et les coordonnées sont difficiles à trouver ou à comprendre.	✕	✕	✕	✕
L'entreprise a peu ou pas d'évaluations en ligne, ses communications et son site Web comportent des erreurs de grammaire ou elle a fait l'objet de plaintes.	✕	✕	✕	✕

Protégez-vous contre les abonnements piégés

1. Repérez tout signal d'alerte

Vérifiez si des éléments de l'offre d'abonnement semblent douteux.
Posez-vous les questions suivantes :

- Qu'est-ce qu'on m'offre exactement, et à quel prix?
- L'offre est-elle claire et facile à comprendre?
- La publicité vante-t-elle les avantages du produit sur la santé ou autre de façon exagérée?
- Que dit une recherche rapide sur Google sur l'entreprise ou le produit?

2. Creusez plus loin

Lisez attentivement les modalités de l'offre avant de l'accepter. Recherchez des avis indépendants sur le produit et l'entreprise sur Google avec des mots clés comme « fraude » ou « arnaque ».
S'il y a peu ou pas d'avis sur le produit ou si vous trouvez plusieurs plaintes contre l'entreprise, ne répondez pas à l'offre.

3. Prenez votre temps. N'agissez pas trop vite.

Ne passez jamais de commande et ne souscrivez jamais un abonnement parce que vous vous sentez obligé. Les fraudeurs utilisent plusieurs méthodes pour vous inciter à agir rapidement. Par exemple, ils affichent un compte à rebours sur le site du produit ou utilisent des phrases comme « L'OFFRE SE TERMINE BIENTÔT ».
Acceptez l'offre seulement lorsque vous avez confirmé sa légitimité, lu les modalités et bien compris ce qui vous est proposé.

4. Faites preuve de prudence

Méfiez-vous toujours des sites Web qui font la promotion des avantages d'un produit sur la santé ou autre, sans s'appuyer sur la science. Vérifiez l'exactitude des affirmations en consultant, par exemple, des articles de revues médicales publiés par des chercheurs réputés. Si vous avez encore des doutes, consultez votre fournisseur de soins de santé. Ne vous laissez pas influencer par les témoignages de vedettes, car ils sont difficiles à vérifier et ne peuvent avoir de véritable valeur quant à l'efficacité d'un produit.

Si vous décidez de faire l'essai d'un produit, vérifiez attentivement vos relevés bancaires mensuels et de carte de crédit pour repérer les frais supplémentaires ou les frais d'abonnement non désirés.

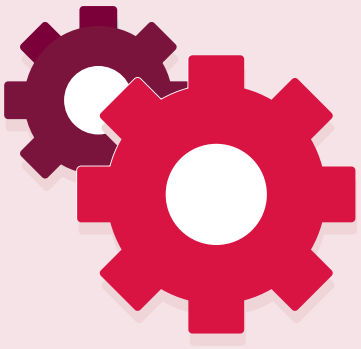
5. Demandez l'opinion d'une personne de confiance

En cas de doute, parlez à quelqu'un. Demandez à un proche en qui vous avez confiance de vous donner son avis. Si vous n'êtes toujours pas convaincu ou si vous avez des doutes, ne souscrivez pas l'abonnement et ignorez toutes les communications.

Arnaques liées aux enquêtes

Fonctionnement

Dans ce type de fraude, la victime reçoit l'appel d'un fraudeur qui connaît son nom et prétend travailler pour son institution financière, un organisme d'application de la loi ou un commerçant. Le principal objectif est de persuader la victime d'envoyer des fonds par Virement *Interac*, d'effectuer des retraits en espèces, d'acheter des cartes-cadeaux ou de divulguer ses renseignements personnels et bancaires.



Prévention de la fraude liée aux codes de vérification à usage unique

Des fraudeurs pourraient vous contacter et prétendre faire partie de l'équipe Fraude de la Banque CIBC. Ils pourraient vous dire que votre compte a été compromis en raison d'une activité suspecte. Les fraudeurs pourraient vous demander de leur donner un code de vérification à usage unique de six chiffres afin de protéger votre compte. Si une telle situation se produit, terminez l'appel immédiatement et composez le numéro indiqué au verso de votre carte.

Variantes de la fraude de l'enquêteur bancaire

Le fraudeur prétend travailler pour une institution financière qui enquête sur des cas de fraude. Il demande à la victime de virer des fonds de son compte pour contribuer à l'enquête, ce qui servira de preuve pour attraper le fraudeur.	✕
Le fraudeur dépose des fonds dans le compte de la victime au moyen de chèques frauduleux ou des propres produits de prêt de la victime et prétend les avoir envoyés par erreur. Il demande ensuite à la victime de lui virer les fonds ou d'acheter des cartes-cadeaux.	✕
Le fraudeur prétend travailler pour un émetteur de carte de crédit connu et affirme que des frais non autorisés ont été portés au compte de la victime. Il demande ensuite à la victime de fournir les renseignements de sa carte de crédit.	✕

Signaux d'alerte à surveiller

La victime se fait dire de ne pas communiquer l'information au centre bancaire.	✕
Demande de renseignements personnels ou bancaires ou de codes de vérification à usage unique.	✕
Demande de virement de fonds, de retrait en espèces ou d'achat de cartes-cadeaux pour participer à une enquête.	✕
Offre de compensation financière pour participer au travail de l'enquêteur chargé de l'application de la loi.	✕
Demande de téléchargement de logiciel sur l'ordinateur de la victime.	✕

Protégez-vous contre les arnaques liées aux enquêtes

1. Repérez tout signal d'alerte

Les institutions financières et les organismes d'application de la loi ne vous demanderont jamais d'effectuer une opération financière dans le cadre d'une enquête sur une fraude. Si on vous demande de le faire, **posez-vous les questions suivantes :**

- Pourquoi me demande-t-on de retirer ou d'envoyer des fonds pour contribuer à une enquête? Pourquoi a-t-on besoin de mes renseignements personnels?
- Pourquoi mon institution financière m'offre-t-elle une compensation pour ma collaboration à une enquête interne? Pourquoi me demande-t-on de mentir aux employés du centre bancaire?
- Le courriel ou le message texte semble-t-il suspect? Dois-je suivre un lien pour télécharger un logiciel?

2. Creusez plus loin

Examinez attentivement le contenu du courriel ou du message texte. Vous semble-t-il suspect? Si vous recevez un appel, est-ce qu'on utilise la peur, un sentiment d'urgence ou une offre qui semble trop belle pour être vraie pour vous inciter à effectuer des opérations financières ou à révéler vos renseignements personnels et bancaires?

3. Prenez votre temps. N'agissez pas trop vite.

Réfléchissez attentivement à ce qu'on vous demande et déterminez si cela vous paraît logique. Souvent, les fraudeurs vont tenter de vous faire répondre à leur demande en changeant fréquemment de sujet, en vous mettant de la pression ou en vous faisant peur. Ne tombez pas dans le piège. Contrôlez la situation en prenant le temps de réfléchir aux renseignements qui vous sont présentés.

4. Faites preuve de prudence

- Si vous subissez des pressions pour effectuer des opérations ou retirer de l'argent et qu'on vous demande de ne pas divulguer ces activités à votre famille, à vos amis et à votre institution financière, il s'agit probablement d'une fraude.
- Méfiez-vous des courriels ou des messages textes qui prétendent provenir d'une institution financière, d'un organisme d'application de la loi ou d'un fournisseur de carte de crédit. Examinez attentivement les adresses courriel et les éléments du site Web qui semblent suspects.
- Refusez de fournir des renseignements confidentiels, d'effectuer des retraits ou des virements de fonds ou de télécharger des logiciels sur votre ordinateur.

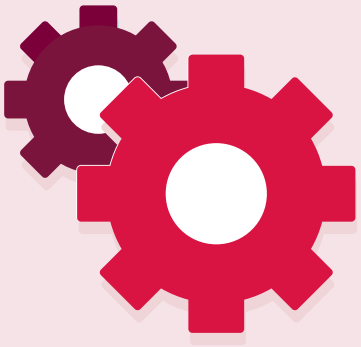
5. Demandez l'opinion d'une personne de confiance

En cas de doute, parlez à quelqu'un. Demandez à un proche en qui vous avez confiance de vous donner son avis sur la cohérence des communications ou des offres que vous avez reçues. Si vous n'êtes toujours pas convaincu ou si vous avez des doutes, refusez la demande ou communiquez avec votre institution financière ou votre fournisseur de carte de crédit pour obtenir une confirmation.

Fraudes liées à l'impôt ou à l'ARC

Fonctionnement

Dans ce type d'arnaque, la victime reçoit des communications frauduleuses de personnes qui prétendent faire partie de l'Agence du revenu du Canada (ARC). Le fraudeur informe sa victime qu'elle doit donner ses renseignements personnels pour recevoir un remboursement d'impôt, ou rembourser de l'impôt impayé immédiatement sous peine de conséquences extrêmes. Souvent, le fraudeur demande un envoi de fonds par Virement *Interac*, cartes-cadeaux prépayées ou cryptomonnaies, comme le bitcoin.



Le fraudeur envoie des communications prétendument de l'ARC par différentes méthodes, notamment par **téléphone, message texte, courriel ou courrier**. En persuadant sa victime qu'elle a une dette ou qu'elle doit récupérer son remboursement d'impôt, le fraudeur peut obtenir ses renseignements personnels comme son NAS ou son numéro de carte de crédit, et les utiliser pour obtenir des gains financiers.

Qui est touché?

La fraude liée à l'ARC peut toucher n'importe qui, mais les personnes les plus souvent ciblées sont les aînés, les nouveaux arrivants au Canada et les propriétaires de PME ou les travailleurs autonomes.

Signaux d'alerte à surveiller	Aînés	Nouveaux arrivants au Canada	Propriétaires de PME
La personne qui communique avec vous ne peut pas prouver qu'elle travaille pour l'ARC, en donnant, par exemple, son nom et son lieu de travail.	✕	✕	✕
On vous demande des renseignements que vous n'incluriez pas dans votre déclaration de revenus (p. ex., numéro de carte de crédit).	✕	✕	✕
On vous demande de payer avec des cartes prépayées, de la cryptomonnaie ou une autre méthode non conventionnelle, et on vous presse d'agir rapidement.	✕	✕	✕
On vous offre de faire une demande de prestations du gouvernement du Canada en votre nom et on vous demande vos renseignements personnels.	✕	✕	✕

Protégez-vous contre la fraude liée à l'ARC

1. Repérez tout signal d'alerte

Avant de donner de l'argent ou des renseignements personnels à quelqu'un qui prétend travailler pour l'ARC, **posez-vous les questions suivantes :**

- Est-ce qu'on menace de m'arrêter ou est-ce qu'on me pousse à rembourser immédiatement de l'impôt impayé au moyen d'un mode de paiement inhabituel?
- La personne qui communique avec moi peut-elle fournir son nom, son numéro de téléphone et son lieu de travail pour confirmer qu'elle travaille comme représentant de l'ARC?
- Me demande-t-on des renseignements que je n'inclurais pas dans ma déclaration de revenus, ou qui n'ont aucun lien avec ma déclaration, comme mon numéro de passeport ou de permis de conduire?
- Est-ce qu'on m'envoie un courriel me demandant mes renseignements personnels ou bancaires, ou me demandant de suivre un lien pour entrer ces renseignements?

2. Creusez plus loin

Il est important d'enquêter sur la situation et de confirmer si la communication de l'ARC est légitime avant de fournir des renseignements personnels.

Déterminez si vous devriez recevoir un appel de l'ARC. Par exemple, demandez à l'appelant d'expliquer le but de son appel tout en vérifiant si vous avez reçu une lettre indiquant que votre déclaration de revenus est en cours d'examen. Si vous êtes inscrit aux avis par courriel, vérifiez si vous avez récemment reçu un message en ouvrant une session dans Mon dossier de l'ARC.

3. Prenez votre temps. N'agissez pas trop vite.

Réfléchissez attentivement à ce qu'on vous demande et déterminez si cela vous paraît logique. Rappelez-vous qu'en aucun cas l'ARC ne demandera de paiement immédiat par téléphone, n'utilisera un langage agressif, ne vous menacera d'arrestation et ne vous laissera de message vocal menaçant. De plus, l'ARC ne vous enverra jamais de courriel vous demandant des renseignements personnels ou contenant un lien vers un formulaire en ligne que vous devez remplir et fournir des renseignements personnels ou bancaires. Si vous recevez ce type de message, il s'agit probablement d'une fraude.

4. Faites preuve de prudence

Si vous recevez un appel d'une personne qui prétend être un représentant de l'ARC :

1. Dites-lui que vous voulez d'abord vérifier son identité.
2. Prenez en note son nom, son numéro de téléphone et son lieu de travail.
3. Vérifiez les renseignements en communiquant avec l'ARC au numéro indiqué sur le site Web.
4. Demandez à l'employé de vous donner la raison de son appel.

Si vous recevez un courriel qui semble provenir de l'ARC :

- Vérifiez l'adresse et déterminez si elle semble suspecte.
- Ignorez les courriels qui vous demandent des renseignements personnels directement ou via un lien que vous devez suivre.

Pour en savoir plus, visitez le site Web de l'ARC :
À quoi vous attendre lorsque l'Agence du revenu du Canada communique avec vous

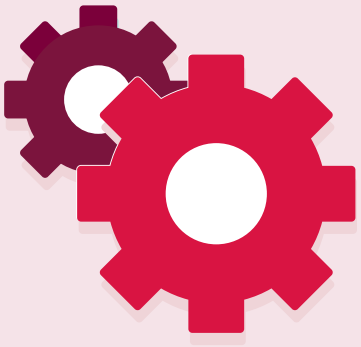
5. Demandez l'opinion d'une personne de confiance

En cas de doute, parlez à quelqu'un. Demandez à un proche en qui vous avez confiance de vous donner son avis sur la légitimité des messages, des appels ou de toute autre forme de communication non sollicitée. Si vous avez encore des doutes, refusez toute demande à fournir des renseignements personnels et communiquez avec l'ARC au numéro indiqué sur le site Web.

Arnaques de soutien technique

Fonctionnement

Dans ce type de fraude, le fraudeur prétend travailler pour une entreprise informatique bien connue et communique avec sa victime par téléphone, par courriel ou au moyen de fenêtres contextuelles. En utilisant un langage technique, le fraudeur convainc sa victime que son ordinateur est à risque et qu'elle doit fournir des renseignements personnels ou d'authentification, ou encore, qu'elle doit télécharger une application pour lui permettre d'accéder à son ordinateur à distance et de régler le problème.



Aujourd'hui, la technologie permet aux fraudeurs de falsifier l'identification de l'appelant afin qu'il corresponde à celui d'une entreprise légitime et de créer de faux sites Web d'entreprises réelles qui semblent légitimes.

Tactiques fréquemment utilisées par les fraudeurs dans les arnaques de soutien technique

Inscrire la victime à un programme d'entretien informatique qui n'existe pas ou qui n'a aucune valeur en échange de frais.	✕
Demander des renseignements de carte de crédit pour facturer à la victime des services frauduleux ou sans valeur.	✕
Diriger la victime vers de faux sites Web qui lui demandent d'entrer ses renseignements personnels ou bancaires.	✕
Installer des maliciels déguisés en programmes légitimes qui permettent d'accéder à distance à l'ordinateur de la victime et à ses données sensibles.	✕

Signaux d'alerte à surveiller

Message contextuel indiquant que votre ordinateur est à risque et vous invitant à installer un logiciel ou à suivre un lien.	✕
Offre de compensation financière pour participer au travail de l'enquêteur chargé de l'application de la loi.	✕
Appel ou courriel non sollicité d'une personne qui vend des logiciels ou des services de réparation et qui vous demande des renseignements ou de télécharger une application.	✕
Appel concernant du soutien technique alors que vous n'en attendez pas et n'avez pris aucun rendez-vous.	✕

Protégez-vous contre la fraude liée au soutien technique

1. Repérez tout signal d'alerte

Les sociétés technologiques légitimes ne communiqueront pas avec vous par téléphone, par courriel ou par message texte pour vous dire que votre ordinateur est à risque. Leurs messages contextuels de sécurité ne vous demanderont pas non plus de suivre un lien externe. Avant de répondre aux communications de soutien technique, **posez-vous les questions suivantes :**

- Un technicien communique-t-il avec moi pour me vendre un logiciel ou des services que je dois payer au moyen d'une carte-cadeau ou d'un paiement par câble?
- Le message contextuel me demande-t-il de télécharger un programme pour supprimer des virus ou de suivre un lien?
- Le courriel ou le message texte semble-t-il suspect? Dois-je suivre un lien pour télécharger un logiciel?

2. Creusez plus loin

Examinez attentivement le contenu du courriel ou du message texte. Vous semble-t-il suspect? Si vous recevez un appel, est-ce qu'on utilise la peur, un sentiment d'urgence ou une offre qui semble trop belle pour être vraie pour vous inciter à effectuer des opérations financières, à payer pour des services dont vous n'avez pas besoin ou à révéler vos renseignements personnels et bancaires?

3. Prenez votre temps. N'agissez pas trop vite.

Réfléchissez attentivement à ce qu'on vous demande et déterminez si cela vous paraît logique. Souvent, les fraudeurs vont tenter de vous faire répondre à leur demande en changeant fréquemment de sujet, en vous mettant de la pression ou en vous faisant peur. Ne tombez pas dans le piège. Contrôlez la situation en prenant le temps de réfléchir aux renseignements qui vous sont présentés.

4. Faites preuve de prudence

- Si vous recevez un appel, un courriel ou un message texte non sollicité vous informant que votre ordinateur est à risque et vous demandant de télécharger un logiciel, il s'agit probablement d'une fraude.
- **Dans une récente variante de ce type de fraude, la victime reçoit des courriels non sollicités qui prétendent que son compte** (p. ex., Netflix, iTunes, Zoom, médias sociaux) a été suspendu. Ne sélectionnez aucun lien suspect, car ce dernier peut entraîner l'installation d'un logiciel malveillant qui permet aux fraudeurs d'accéder à votre ordinateur à distance.
- Refusez de fournir des renseignements confidentiels, d'acheter des cartes-cadeaux, d'effectuer des paiements par câble ou de télécharger des logiciels que vous ne connaissez pas sur votre ordinateur.

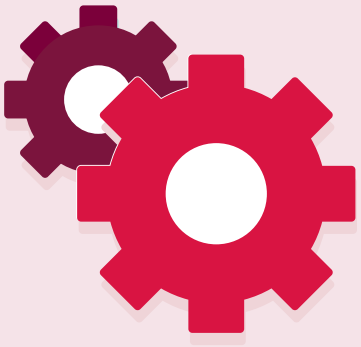
5. Demandez l'opinion d'une personne de confiance

En cas de doute, parlez à quelqu'un. Demandez à un proche en qui vous avez confiance de vous donner son avis sur la cohérence des communications ou des offres que vous avez reçues. Si vous n'êtes toujours pas convaincu ou si vous avez des doutes, refusez la demande.

Fraudes liées aux prêts

Fonctionnement

Dans ce type de fraude, le fraudeur crée une fausse publicité pour un prêt ou communique directement avec sa victime par téléphone ou par courriel. Le fraudeur se fait passer pour un prêteur légitime et propose des taux plus avantageux que ceux d'autres entreprises. Il attire sa victime en lui disant qu'un prêt a été approuvé pour elle ou qu'elle peut obtenir un prêt garanti sans vérification du crédit moyennant une avance ou des frais initiaux. Une fois que la victime a accepté la fausse offre et a payé les frais initiaux au moyen du mode de paiement privilégié par le fraudeur, elle n'entend plus jamais parler de ce dernier.



Types courants de fraudes liées aux prêts

Fraude liée aux prêts-autos	✕	Fraude liée aux prêts étudiants	✕
Fraude liée aux prêts hypothécaires	✕	Fraude liée aux prêts personnels	✕
Fraude liée aux prêts sur salaire	✕		

Signaux d'alerte à surveiller

Approbations de prêts non sollicités; on vous félicite par téléphone ou par courriel d'avoir obtenu une approbation pour un prêt que vous n'avez pas demandé.	✕
Vous ne trouvez pas d'évaluations sur le prêteur et ce dernier n'a pratiquement aucune présence en ligne.	✕
Sentiment d'urgence ou tactiques de vente agressives utilisées par le prêteur qui insiste sur le fait que l'offre de prêt se termine bientôt.	✕
Le prêteur exige un paiement ou des frais initiaux avant d'accorder le prêt, et demande un paiement par bitcoin, par carte-cadeau ou par Virement *Interac*.	✕

Protégez-vous contre les fraudes liées aux prêts

1. Repérez tout signal d'alerte

Avant de contracter un prêt, il est important de comprendre l'offre et de déterminer si elle est légitime.
Posez-vous les questions suivantes :

- Le prêteur promet-il une approbation dès le départ, sans procéder à une vérification du crédit?
- Dois-je payer des frais initiaux avant de recevoir les fonds du prêt?

REMARQUE : Il est illégal pour les prêteurs en Amérique du Nord de demander au consommateur de verser un paiement ou des frais initiaux avant la réception du prêt. Bien que de nombreux prêts comportent des frais de traitement, les prêteurs légitimes les déduisent de la somme prêtée. (Source : Bureau d'éthique commerciale)

- Y a-t-il un contrat à signer? Si oui, est-il incomplet? Comporte-t-il des cases déjà cochées?

2. Creusez plus loin

Vérifiez la crédibilité du prêteur en vérifiant s'il est inscrit en Ontario ou s'il est accrédité auprès du Bureau d'éthique commerciale.

Recherchez des commentaires sur le prêteur et vérifiez sa présence en ligne. Examinez attentivement les modalités du prêt et demandez-vous si elles sont logiques.

3. Prenez votre temps. N'agissez pas trop vite.

Prenez le temps de bien réfléchir à ce qu'on vous demande. L'offre semble-t-elle réaliste ou trop belle pour être vraie? Souvent, les fraudeurs vont tenter de vous faire agir rapidement en changeant fréquemment de sujet, en vous mettant de la pression ou en vous faisant peur. Ne tombez pas dans le piège. Contrôlez la situation en prenant le temps de réfléchir aux renseignements qui vous sont présentés.

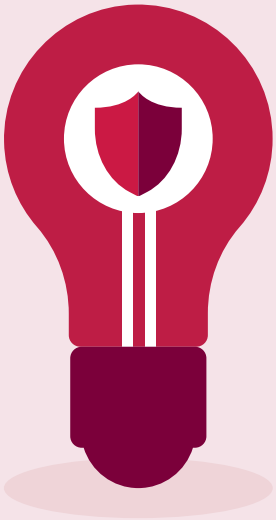
4. Faites preuve de prudence

- Si on communique avec vous au sujet d'un prêt que vous n'avez pas demandé, il s'agit probablement d'une fraude. Ignorez la communication et ne fournissez pas de renseignements personnels ou bancaires.
- Méfiez-vous des prêteurs qui garantissent l'accès aux fonds, qui approuvent le prêt sans vérification du crédit et qui demandent des frais ou des paiements initiaux avant l'obtention du prêt.
- Si ça semble trop beau pour être vrai, c'est sans doute le cas! Si vous croyez que l'offre de prêt est suspecte, il est préférable de la refuser, tout simplement.

5. Demandez l'opinion d'une personne de confiance

En cas de doute, parlez à quelqu'un. Demandez à un proche en qui vous avez confiance de vous donner son avis sur cette offre de prêt. Demandez-lui aussi s'il connaît le prêteur de nom ou de réputation. Si vous n'êtes toujours pas convaincu ou si vous n'êtes pas à l'aise avec les modalités du prêt, refusez-le et cessez toute communication avec le prêteur.

Sachez reconnaître une fraude avant qu'il ne soit trop tard



Nous tenons à vous rappeler que vous devez signaler immédiatement toute fraude ou activité non autorisée réelle ou présumée liée à vos comptes et à vos cartes de débit et de crédit, toute perte ou tout vol de vos cartes et toute compromission des renseignements ou des NIP de vos cartes. Vous devez immédiatement remplacer votre carte de débit ou de crédit et modifier vos NIP et vos mots de passe bancaires.

Pour en savoir plus sur les ressources à votre disposition ou sur la façon dont la Banque CIBC peut vous aider si vous êtes victime de fraude, consultez les renseignements ci-dessous ou visitez le site **cibc.com/fraude**.

Restez bien informé partout où vous allez

Surveillez de près vos achats, l'activité de votre carte de crédit et les opérations qui semblent inusitées grâce aux alertes CIBC sur l'application de services bancaires mobiles. En configurant des alertes personnalisées, vous êtes informé en temps réel par message texte, courriel ou téléphone si une opération semble inhabituelle. S'il s'agit d'une fraude, nous vous mettrons en contact avec un spécialiste, Prévention de la fraude.

Vous souhaitez vous inscrire ou en savoir plus? Visitez la **page sur les alertes CIBC**.

Ce que la Banque CIBC peut faire

Veuillez communiquer immédiatement avec la Banque CIBC au **1 800 872-2422** ou par courriel à l'adresse **fraude@cibc.com** si vous croyez avoir été victime d'une fraude, si vos comptes ont été compromis ou si votre identité a été volée.

Si vous recevez des courriels ou des messages textes frauduleux ou si vous souhaitez signaler des sites Web qui se font passer pour la Banque CIBC, écrivez-nous à **fraude@cibc.com** et décrivez l'incident, en incluant les courriels ou les liens frauduleux à des fins d'analyse.

Autres ressources

Pour signaler un cas de fraude, appelez le Centre antifraude du Canada au **1 888 495-8501** ou visitez le site **centreantifraude.ca**.

Pour consulter l'outil de suivi et les conseils sur la fraude du Bureau d'éthique commerciale, visitez les sites : **BBB.org/ScamTracker** ou **BBB.org/ScamTips** (en anglais seulement)

Pour obtenir d'autres conseils sur la fraude, visitez les sites suivants :

Bureau de la concurrence Canada	**bureaudelaconcurrence.gc.ca**
Gendarmerie royale du Canada	**RCMP-GRC.gc.ca/fr**