

Outil de gestion sur la protection des clients

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



Livre 3 de 3

Table des matières

Message de Keith Gordon, vice-président à la direction et chef de la sécurité, Banque CIBC	page 2	Fraude par interception d'opération de Virement <i>Interac</i> ^{MD}	pages 8 et 9
Renseignements généraux sur les fraudes	page 3	Fraudes liées aux achats des Fêtes	pages 10 et 11
Savoir reconnaître les signes de fraude et pratiques exemplaires en ligne	page 4	Fraudes liées aux vacances et à la location	pages 12 et 13
Comment la Banque CIBC vous protège contre le vol d'identité et la fraude	page 5	Arnaques liées à une loterie ou à un prix	pages 14 et 15
Vol d'identité	pages 6 et 7	Coordonnées des personnes-ressources et ressources supplémentaires	page 16

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.

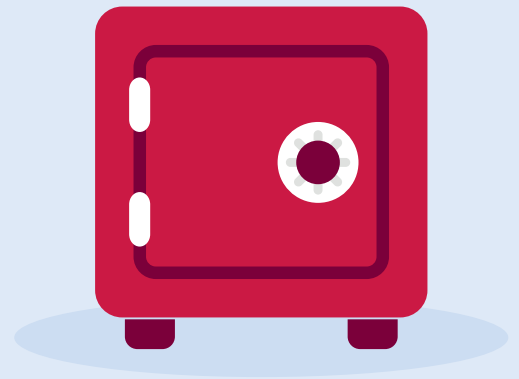
A handwritten signature in black ink that reads "Keith Gordon". The signature is fluid and cursive.

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.

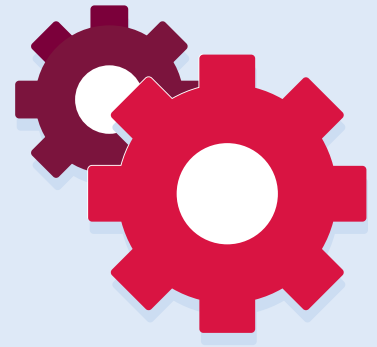
Vol d'identité

Fonctionnement

Le vol d'identité est l'acte de voler l'identité ou les renseignements personnels d'une personne. Le fraudeur tente généralement de voler les renseignements personnels ou bancaires de sa victime par les trois moyens suivants :

- 1) **Détournement de carte SIM**
- 2) **Hameçonnage**
- 3) **Logiciel malveillant**

Une fois qu'il a volé l'identité de sa victime, le fraudeur l'utilise à des fins illégales et pour effectuer des opérations financières. C'est ce qu'on appelle la fraude d'identité.



De quoi s'agit-il?	Signaux d'alerte à surveiller
<p>Détournement de carte SIM</p> <p>Après avoir volé les renseignements personnels de sa victime au moyen d'un logiciel malveillant ou de tactiques d'hameçonnage, le fraudeur se fait passer pour elle auprès de son fournisseur de téléphone cellulaire dans le but de transférer le numéro de téléphone mobile de la victime sur sa propre carte SIM.</p>	<ul style="list-style-type: none">✗ Perte soudaine de connexion au service de votre fournisseur de téléphonie cellulaire✗ Un message texte de votre fournisseur de services indiquant qu'une demande a été faite pour transférer votre numéro à une autre carte SIM
<p>Hameçonnage par courriel, par téléphone ou par texto</p> <p>Communication non sollicitée de la part d'un fraudeur qui se fait passer pour un organisme gouvernemental ou une autre institution et qui demande un paiement ou des renseignements personnels par courriel, par téléphone ou par texto.</p>	<ul style="list-style-type: none">✗ Demande d'argent ou de renseignements personnels ou bancaires✗ Adresses courriel mal orthographiées ou comportant une combinaison inhabituelle de caractères et messages mal écrits✗ Demandes urgentes accompagnées de menaces
<p>Logiciel malveillant</p> <p>Logiciel conçu pour obtenir un accès non autorisé et à distance aux fichiers d'un appareil et désactiver l'accès de l'utilisateur à ces fichiers ou surveiller les frappes sur le clavier de l'utilisateur. Les enregistreurs de frappe, les rançongiciels, les publiciels et les logiciels espions sont des exemples de logiciels malveillants.</p>	<ul style="list-style-type: none">✗ Fenêtre contextuelle indiquant que votre ordinateur est à risque et vous demandant d'installer un antivirus en suivant un lien cliquable✗ Vos fichiers ont été verrouillés et vous devez payer une rançon pour y avoir accès✗ Vous ne pouvez pas ouvrir une session dans les comptes que vous utilisez fréquemment (services bancaires, courriels, médias sociaux, etc.)

Protégez-vous contre le vol d'identité



1. Repérez tout signal d'alerte



Ce n'est pas toujours facile de reconnaître un vol d'identité. Souvent, la victime découvre la fraude seulement après qu'elle a été commise. **Repérez rapidement les signes** pour que des mesures soient prises dès que possible :

- Messages ou appels suspects ou inattendus vous demandant d'effectuer une opération financière ou de fournir des renseignements personnels.
- Messages affirmant que vous avez gagné un prix pour un concours auquel vous n'avez jamais participé ou messages à propos d'offres qui semblent trop belles pour être vraies.
- Message ou appel qui utilisent un ton menaçant ou alarmiste ou qui suscitent un sentiment d'urgence dans le but de vous faire agir rapidement.
- Demandes d'envoi de fonds au moyen de paiements par câble, de cartes-cadeaux, de cartes prépayées ou de bitcoins ou autres cryptomonnaies.

2. Creusez plus loin



Examinez attentivement les éléments du message qui vous font douter, comme le ton et la grammaire, la ligne d'objet et l'adresse courriel de l'expéditeur. S'il y a plusieurs erreurs grammaticales et que l'adresse courriel est une combinaison inhabituelle de lettres et de caractères, le message pourrait être frauduleux.

De plus, méfiez-vous des messages qui prétendent provenir d'un organisme gouvernemental ou de votre institution financière et qui vous invitent à suivre un lien pour confirmer des renseignements personnels ou sur une opération.

Si vous recevez un tel message, ignorez-le ou appelez votre institution financière pour vérifier sa légitimité.

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



Les fraudeurs sont exigeants et veulent que vous agissiez rapidement. Gardez la maîtrise de toute situation en ralentissant; réfléchissez attentivement à ce qu'on vous demande et déterminez si cela vous paraît logique. Menez une enquête sur les demandes de renseignements personnels et vérifiez leur légitimité avant de les communiquer.

4. Faites preuve de prudence



La meilleure défense contre le vol d'identité consiste à surveiller votre présence en ligne et à faire attention à ce que vous partagez. Plus les fraudeurs en savent sur vous, plus ils peuvent vous piéger. Créez toujours des mots de passe uniques et difficiles à deviner pour chacun de vos comptes en ligne. Installez un logiciel à jour sur votre ordinateur pour détecter et supprimer les programmes malveillants. Ne répondez pas aux courriels ou aux messages textes non sollicités qui vous demandent de suivre un lien ou de fournir des renseignements personnels.

La Banque CIBC veille à votre sécurité et à celle de vos renseignements bancaires. Pour en savoir plus sur la façon de vous protéger contre le vol d'identité, visitez le site www.cibc.com/fraude et consultez notre guide de référence sur la protection contre le vol d'identité.

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

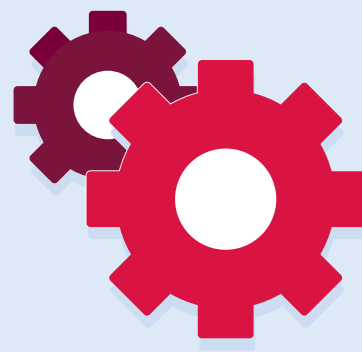


En cas de doute, parlez à quelqu'un. Demandez à un proche en qui vous avez confiance de vous donner son avis sur la légitimité des messages, des appels ou de toute autre forme de communication non sollicitée. Si vous avez encore des doutes, refusez toute demande à fournir des renseignements personnels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

Fraude par interception d'opération de Virement *Interac*

Fonctionnement

Dans ce type de fraude, le fraudeur intercepte une opération de Virement *Interac* envoyée d'un compte bancaire à un autre en accédant à l'adresse courriel ou aux messages textes du destinataire et en répondant correctement à la question de sécurité. La victime reçoit un courriel confirmant la réussite du virement, mais les fonds ont été détournés vers un compte bancaire contrôlé par le fraudeur.



Points de compromission pouvant mener à l'interception d'une opération de Virement *Interac*

La réponse à la question de sécurité est facile à deviner.	✗
Les coordonnées du destinataire sont désuètes ou inexactes.	✗
La réponse à la question de sécurité a été envoyée par le même mode de communication que celui utilisé pour envoyer l'opération de Virement <i>Interac</i> .	✗

Signes de fraude par Virement *Interac*

Le destinataire prévu ne reçoit pas le virement presque immédiatement.	✗
Le destinataire prévu reçoit un courriel qui confirme le virement, mais ne peut pas percevoir les fonds.	✗

Protégez-vous contre la fraude par Virement *Interac*



À faire (si vous êtes l'expéditeur) :

- Créez une question de sécurité unique et difficile à deviner, à laquelle seuls vous et votre destinataire connaissez la réponse.
- Si nécessaire, utilisez un mode de communication sûr, par exemple le téléphone, pour communiquer au destinataire la réponse à votre question de sécurité.



À faire (si vous êtes le destinataire) :

- Inscrivez-vous à la fonction Dépôt automatique de Virement *Interac* pour que votre argent soit déposé automatiquement, sans que le destinataire doive répondre à une question de sécurité.
- Créez des mots de passe uniques et difficiles à deviner pour protéger vos comptes, y compris vos comptes de courriel et de médias sociaux.



À ne pas faire (si vous êtes l'expéditeur) :

- Inclure la réponse avec la question de sécurité.
- Divulguer la réponse à votre question de sécurité par courriel, par message texte ou sur les médias sociaux.
- Réutiliser la même question de sécurité et la même réponse.



À ne pas faire (si vous êtes le destinataire) :

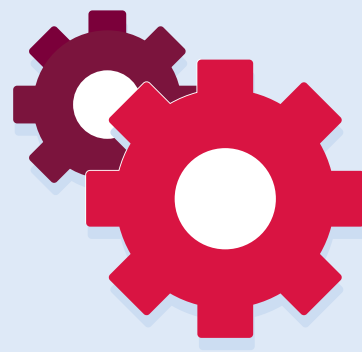
- Créer des mots de passe faibles que tout le monde peut facilement deviner.
- Communiquer vos mots de passe et utiliser les mêmes mots de passe pour tous vos comptes.
- Suggérer à plusieurs expéditeurs d'utiliser la même question de sécurité et la même réponse.

Fraudes liées aux achats des Fêtes

Fonctionnement

Le fraudeur profite de l'augmentation des dépenses de consommation de la période des Fêtes pour se faire passer pour une entreprise légitime, exploiter la générosité des consommateurs ou inciter sa victime à divulguer des renseignements personnels ou bancaires ou à envoyer des fonds.

Les fraudes liées aux achats des Fêtes les plus courantes sont expliquées ci-dessous.



Fonctionnement des arnaques

Faux avis d'expédition

- **Méthode 1 :** Le fraudeur envoie un courriel qui ressemble à s'y méprendre à un avis d'expédition d'une entreprise légitime. Ce courriel contient un lien qui, lorsque sélectionné, télécharge un programme malveillant ou demande des renseignements personnels ou bancaires.
- **Méthode 2 :** Le fraudeur laisse un avis de livraison manquée à la porte de la victime sur lequel est indiqué un numéro de téléphone que la victime doit composer. Lorsque la victime appelle, le fraudeur tente d'obtenir ses renseignements personnels ou bancaires.

Faux organismes de bienfaisance

- Le fraudeur envoie un courriel ou un message sur les médias sociaux pour attirer sa victime vers le site Web d'un faux organisme de bienfaisance et la manipule sur le plan émotionnel pour l'inciter à faire un don.
- Le faux organisme demande de faire un don en utilisant une méthode qui n'est pas traçable (p. ex., paiement par câble, cartes-cadeaux prépayées et cryptomonnaie).

Fausse cartes-cadeaux

- Le fraudeur envoie des courriels d'hameçonnage et se sert de publicités qui s'affichent dans une fenêtre contextuelle pour offrir des cartes-cadeaux gratuites.
- En sélectionnant le lien du courriel ou la publicité, la victime peut télécharger un logiciel malveillant à son insu ou être amenée à donner ses renseignements personnels ou bancaires.

Offres ou occasions qui semblent trop belles pour être vraies

Offres ou occasions qui semblent trop belles pour être vraies	✗
Demande de renseignements personnels ou bancaires	✗
Courriel ou autre type de communication qui contient des erreurs de grammaire	✗
Demande de paiement par des méthodes impossibles à retracer	✗

Protégez-vous contre la fraude liée aux achats des Fêtes



1. Repérez tout signal d'alerte

Que vous attendiez des colis ou que vous soyez d'humeur généreuse, il est important de distinguer le vrai du faux.

Posez-vous les questions suivantes :

- Pourquoi me demande-t-on de suivre un lien dans le courriel de l'entreprise de livraison? Pourquoi ont-ils besoin de mes renseignements personnels?
- Le site Web de cet organisme de bienfaisance semble-t-il légitime? Y a-t-il des commentaires sur l'organisme de bienfaisance en ligne?
- Est-ce que je reçois des communications non sollicitées pour des offres auxquelles je n'ai pas souscrit?



2. Creusez plus loin

Examinez attentivement le contenu du courriel, de la publication sur les médias sociaux ou du message texte. Vous semble-t-il suspect? Portez une attention particulière à la grammaire, à l'adresse courriel de l'expéditeur et à la présence globale du compte de média social, et vérifiez si ce dernier a été créé récemment. Si vous avez reçu un avis de livraison manquée, vérifiez l'état de la commande que vous attendez en utilisant le lien de suivi fourni par l'entreprise où vous avez fait l'achat.



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 vous avez reçu des communications affirmant que vous avez gagné des cartes-cadeaux lors d'une remise de prix ou d'un concours auquel vous n'avez pas participé, il s'agit probablement d'une fraude.
- Méfiez-vous des courriels ou des sites Web qui prétendent être d'une entreprise de livraison de bonne réputation (p. ex., UPS, Postes Canada, DHL). Examinez les adresses courriel et les éléments du site Web qui semblent suspects.
- Si ça semble trop beau pour être vrai, c'est sans doute le cas! De nombreux prêteurs frauduleux attirent les victimes en leur offrant des « occasions à ne pas manquer », en échange de leurs renseignements personnels ou de leur argent. Si vous croyez que l'offre est suspecte, il est préférable de la refuser, tout simplement.



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

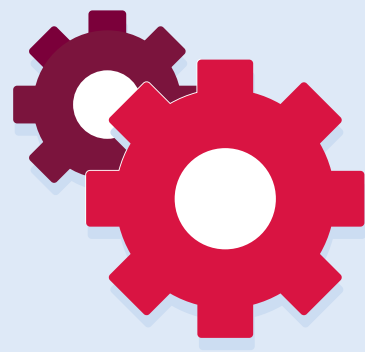
En cas de doute, parlez à quelqu'un. Demandez à un proche en qui vous avez confiance de vous donner son avis sur la communication ou les offres. Demandez à la personne si elle connaît le nom ou la réputation de l'organisme de bienfaisance auquel vous souhaitez faire un don. Si vous n'êtes toujours pas convaincu ou si vous avez des doutes, ne faites pas de don et ignorez toutes les communications.

Fraudes liées aux vacances et à la location

Fonctionnement

Dans ce type de fraude, le fraudeur annonce la location d'un chalet, d'un appartement ou d'une maison sur un marché en ligne où les hôtes et les propriétés ne sont pas vérifiés. Il se sert des photos et des descriptions d'une annonce réelle et modifie les coordonnées, ou crée une annonce en utilisant des images provenant de recherches dans Google.

Lorsque la victime répond à l'annonce et communique avec le fraudeur, celui-ci lui demande un dépôt de garantie ou un paiement initial par Virement *Interac* ou par carte-cadeau prépayée, puis cesse immédiatement toute communication. La victime se rend compte que la propriété ne se trouve pas à l'adresse indiquée ou que le véritable propriétaire n'est pas au courant de l'annonce frauduleuse.



Marchés en ligne où les fraudeurs publient fréquemment leurs annonces :	Craigslist	Kijiji	Marketplace sur Facebook
Signaux d'alerte à surveiller			
Demande de dépôt de garantie ou de paiement initial par Virement <i>Interac</i> ou par carte-cadeau prépayée, sans facture ni reçu.	×	×	×
L'annonceur vous demande votre numéro de carte de crédit ou de débit et d'autres renseignements personnels, ou vous dit qu'il ne peut pas vous rencontrer à la propriété faisant l'objet de l'annonce.	×	×	×
On vous presse d'effectuer un paiement initial dès que possible et on affirme que l'offre est la meilleure sur le marché.	×	×	×
L'annonce est affichée à un prix bien inférieur au prix courant ou semble trop belle pour être vraie.	×	×	×

Protégez-vous contre les fraudes liées aux vacances et à la location



1. Repérez tout signal d'alerte



Avant de répondre à une annonce de location, il est important de vérifier si l'offre est légitime.

Posez-vous les questions suivantes :

- La propriété existe-t-elle vraiment à l'adresse indiquée? Que révèle une recherche dans Google Maps?
- Le prix de location semble-t-il trop beau pour être vrai? Quel est le prix de propriétés comparables ou situées à proximité?
- L'annonceur se montre-t-il évasif? Refuse-t-il les demandes de rencontre en personne?
- Est-ce qu'on me presse d'aller de l'avant avec l'offre? Dois-je donner des renseignements personnels ou bancaires?

2. Creusez plus loin



Vérifiez que la propriété existe réellement à l'adresse indiquée en effectuant une recherche rapide dans Google ou en vous rendant sur place.

Recherchez l'adresse sur d'autres sites Web de location et, si vous trouvez une annonce, vérifiez si les coordonnées correspondent à celles de l'annonce qui vous intéresse. Après avoir fait vos vérifications, évaluez si vous faites toujours confiance à l'annonceur.

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 un annonceur vous demande des renseignements personnels ou bancaires (p. ex., numéro de carte de crédit ou de débit ou NAS), il pourrait s'agir d'un fraudeur.
- Méfiez-vous des annonceurs qui refusent de vous rencontrer en personne ou à la propriété décrite dans l'annonce.
- Si ça semble trop beau pour être vrai, c'est sans doute le cas! De nombreux annonceurs de propriétés locatives frauduleuses prétendent qu'ils ont la meilleure offre sur le marché et vous incitent à agir rapidement en raison de la forte demande. Si vous croyez que l'offre est suspecte, il est préférable de la refuser, tout simplement.
- Demandez toujours une trace écrite sous forme de facture ou de reçu lorsque vous payez pour une location, et réservez vos locations de vacances avec une carte de crédit ou de débit sur un site Web réputé (Airbnb, Vrbo) pour profiter des avantages en matière de protection des consommateurs.

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

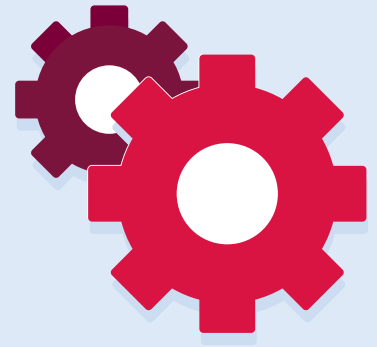


En cas de doute, parlez à quelqu'un. Demandez à un proche en qui vous avez confiance de vous donner son avis sur la légitimité des messages, des appels ou de toute autre forme de communication. Si possible, réservez des locations de vacances ou louez des propriétés où des proches ont déjà séjourné.

Arnaques liées à une loterie ou à un prix

Fonctionnement

Les fraudeurs utilisent les loteries et les prix pour obtenir de l'argent ou vos renseignements personnels et bancaires. La victime reçoit une lettre, un appel, un message texte ou un courriel inattendu l'informant qu'elle a gagné un prix, mais qu'elle doit payer des frais pour le réclamer. En général, la victime ne se souvient pas d'avoir participé à un concours, car il y a de fortes chances qu'elle ne l'ait pas fait. Une fois les frais payés, elle s'attend à recevoir un prix... qui n'arrive jamais.



Types de frais que le fraudeur peut invoquer pour escroquer sa victime :

✘ Frais bancaires

✘ Assurances

✘ Impôts

Signaux d'alerte à surveiller

Vous devez payer des frais pour recevoir le prix. Les véritables concours ne vous obligent pas à payer des frais. ✘

Vous ne vous souvenez pas d'avoir participé à un tirage ou à un concours. ✘

Vous devez fournir vos renseignements financiers pour réclamer le prix. ✘

On vous dit de réclamer rapidement le prix ou vous risquez de manquer votre chance. ✘

Protégez-vous contre les arnaques liées à une loterie ou à un prix



1. Repérez tout signal d'alerte

Gagner un prix, c'est emballant! Encore faut-il qu'il soit réel. Avant de réclamer le prix, **posez-vous les questions suivantes** :

- Est-ce que j'ai participé pour courir la chance de gagner ce prix? Comment ont-ils eu mes coordonnées?
- Récupérer un prix devrait être gratuit – pourquoi dois-je payer des frais?
- Si j'ai gagné ce prix, pourquoi me presse-t-on pour le récupérer?
- Pourquoi me demande-t-on de fournir mes renseignements financiers?



2. Creusez plus loin

Recueillez le plus de renseignements possible pour vérifier la légitimité du prix. Si vous avez reçu une communication écrite indiquant que vous avez gagné, vérifiez qui en est l'expéditeur, son adresse courriel et si le message contient des fautes d'orthographe ou de grammaire. Si vous recevez un appel, demandez à la personne de s'identifier et tentez d'obtenir le plus de renseignements possible. Faites des recherches en ligne sur le concours pour confirmer les renseignements qu'on vous a donnés. Si l'appelant prétend travailler pour une entreprise de renom, contactez l'entreprise directement en utilisant ses coordonnées en ligne.



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

S'il s'agit d'un véritable prix, rien ne presse. Prenez le temps de comprendre ce qu'on vous demande. Si vous ne vous souvenez pas d'avoir participé au tirage ou au concours, il s'agit probablement d'une fraude. Si vous devez payer des frais ou fournir vos renseignements financiers, c'est une fraude.



4. Faites preuve de prudence

Peu importe le type de fraude, l'intention du fraudeur est de vous voler – que ce soit votre argent, des renseignements personnels et financiers, ou les deux. Le fraudeur profitera de votre enthousiasme pour vous inciter à faire rapidement ce qu'il dit pour réclamer le prix. Ne lui permettez pas de voler votre argent et votre identité.



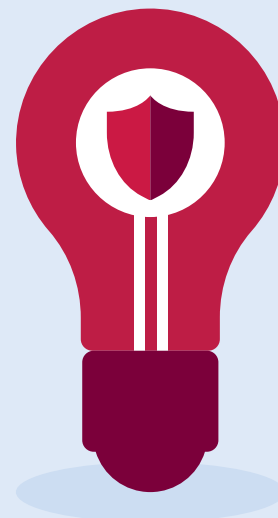
5. Demandez l'opinion d'une personne de confiance

En cas de doute, parlez à quelqu'un. Demandez à un proche en qui vous avez confiance de vous donner son avis. Si vous vous demandez toujours si la situation est légitime après avoir fait vos propres recherches et obtenu un avis, faites confiance à votre instinct et ne réclamez pas le prix.

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

Veillez 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