Protégez-vous contre la fraude durant la pandémie de COVID-19

Depuis le début de la pandémie de COVID-19, la fraude a augmenté et de nombreux Canadiens ont perdu de l'argent ou se sont fait voler leur identité. Apprenez à reconnaître les fraudes et les escroqueries, découvrez les mesures de précaution que vous pouvez prendre et sachez quoi faire si vous pensez avoir été victime d'une fraude.

Les renseignements ci-dessous ne sont qu'un aperçu des types courants d'escroqueries et de techniques frauduleuses utilisées par les fraudeurs. Les meilleurs moyens de vous protéger consistent à prendre des précautions, à demeurer vigilant et à signaler toute activité suspecte.

Techniques frauduleuses courantes et conseils pour vous protéger

Les escrocs et les fraudeurs tentent de vous soutirer de l'argent ou des renseignements personnels ou de vous inciter à accéder à des sites Web ou à des fichiers dangereux. Ils ont souvent recours à des tactiques de peur, comme vous dire que vous aurez des ennuis, que vous ferez face à des amendes ou que vous serez puni si vous ne leur obéissez pas. D'autres peuvent exiger que vous versiez une somme d'avance pour un produit ou un service qu'ils tentent de vous vendre.

Fraude par téléphone

Signaux avertisseurs courants

- Vous recevez un appel automatisé dans lequel vous entendez un message préenregistré.
- La personne qui appelle parle de manière à vous mettre de la pression ou à vous faire peur afin que vous lui donniez des renseignements ou de l'argent.
- La personne qui appelle affirme représenter le gouvernement, une agence de recouvrement ou la police, et elle prétend que vous devez de l'argent ou que vous faites l'objet d'une enquête pour un crime.
- La personne qui appelle affirme représenter votre institution financière ou un ministère et avoir besoin de vérifier vos renseignements personnels ou financiers.
- La personne qui appelle affirme représenter une entreprise de prêts ou de services financiers, un organisme de santé ou une autre entreprise de bonne réputation, et elle tente de vous convaincre de payer à l'avance pour un produit ou un service.
- La personne qui appelle prétend représenter un organisme de bienfaisance et vous demande de faire un don.
- La personne qui appelle affirme qu'un membre de votre famille ou l'"un de vos proches a des ennuis et que pour l'aider, vous devez fournir de l'argent ou des renseignements bancaires.

Protégez-vous

- Si vous pensez que l'appel est une escroquerie ou que la personne au téléphone n'est pas qui elle prétend être, **raccrochez immédiatement**.
- **Si vous recevez un appel d'une personne suspecte ou d'un spécialiste du télémarketing qui semble vouloir vous soutirer des renseignements personnels, raccrochez.** Voici des exemples de renseignements que ces personnes pourraient vous demander :
  - Votre nom
  - Votre adresse
  - Votre date de naissance
  - Votre numéro d'assurance sociale (NAS)
  - Des renseignements sur votre carte de crédit ou vos données bancaires
- **Ne donnez pas de renseignements personnels ou de détails sur votre compte bancaire par téléphone, à moins d'avoir vérifié que votre interlocuteur est légitime :**
  - Cherchez sur Internet les coordonnées de l'entreprise que votre interlocuteur affirme représenter, puis appelez l'entreprise pour confirmer que l'appel est légitime.
  - Vérifiez les appels auprès de la société qui a émis votre carte de crédit en téléphonant au numéro inscrit au verso de votre carte.
  - Vérifiez la légitimité des organismes de bienfaisance canadiens auprès de l'Agence du revenu du Canada (ARC).
  - Vérifiez la légitimité des agences de recouvrement auprès de l'organisme provincial approprié.

Protégez-vous contre la fraude durant la pandémie de COVID-19

Fraude par courriel, par message texte, par message instantané ou par la poste

Signaux avertisseurs courants

- Le message (courriel, message texte, lettre, etc.) semble provenir du gouvernement, d'une institution financière ou d'une entreprise, mais son apparence est différente des messages que vous avez déjà reçus de cet expéditeur.
- L'adresse courriel, l'adresse du site Web, le numéro de téléphone ou l'adresse postale ne correspondent pas aux coordonnées de votre institution financière ou de l'entreprise d'où le message prétend provenir.
- Le message (courriel, message texte, lettre, etc.) ne vous est pas adressé directement : par exemple, le message commence par « Cher client ».
- Le message vous invite à cliquer sur un lien ou à répondre en fournissant un paiement ou des renseignements personnels ou financiers.
- L'apparence (format, images, qualité) du courriel, du site Web ou de la lettre n'est pas la même qu'habituellement ou laisse à désirer. Le message ou le site Web contient des liens qui ne fonctionnent pas ou des fautes d'orthographe et de grammaire.

Protégez-vous

- **Vérifiez la légitimité de l'adresse courriel, de l'adresse du site Web, du numéro de téléphone ou de l'adresse postale sur le site Web officiel de l'entreprise ou de l'organisation concernée**.
- **Vérifiez l'adresse courriel réelle de l'expéditeur** en plaçant le curseur de votre souris sur le nom de l'expéditeur ou en vérifiant que le domaine inscrit dans l'adresse de l'expéditeur correspond à celui de l'organisation d'où le message prétend provenir.
- **N'utilisez pas le numéro de téléphone, l'adresse courriel, le site Web ou l'adresse postale qui vous sont fournis.** Si vous devez communiquer avec l'entreprise ou l'agence, utilisez les coordonnées que vous savez exactes.
- **N'envoyez pas de renseignements personnels confidentiels (comme votre NAS) par Internet.**
- **Accédez directement aux sites Web que vous voulez consulter** au lieu de cliquer sur des liens dans des courriels ou d'autres messages.
- **Installez des logiciels antipourriel, anti-espion et antivirus** sur votre ordinateur et vos appareils mobiles, et assurez-vous qu'ils sont à jour.
- **Tenez à jour vos systèmes** (p. ex., Windows sur votre ordinateur ou le système d'exploitation de votre téléphone mobile).
- **Créez des mots de passe difficiles** à deviner et changez-les régulièrement. N'utilisez pas le même mot de passe pour différents comptes importants.
- **Ne choisissez pas des questions de sécurité auxquelles il est possible de répondre en utilisant des informations publiques.**
- **Si vous payez quelque chose en ligne, assurez-vous que le site Web que vous utilisez est sécuritaire.** Vérifiez si la barre d'adresse du site Web affiche une icône de cadenas fermé ou si l'adresse du site Web commence par « https » plutôt que « http » (le « s » signifie que le site Web est sécurisé).

Protégez-vous contre la fraude durant la pandémie de COVID-19

Conseils généraux

Méfiez-vous. Les banques et les organismes gouvernementaux n'envoient pas de messages texte ou de messages instantanés vous demandant de fournir des renseignements personnels ou des détails sur votre compte. Ne fournissez pas vos renseignements personnels, ne cliquez pas sur des liens suspects et ne répondez pas aux messages (courriels, messages texte, lettres, etc.) suspects. Apprenez à reconnaître les escroqueries et sachez à quoi vous attendre lorsque l'ARC communique avec vous.

Vérifiez à qui vous parlez. Communiquez directement avec les organisations et les entreprises au moyen des coordonnées qu'elles mettent à la disposition du public.

Vérifiez régulièrement vos relevés. Vérifiez souvent vos relevés bancaires et de carte de crédit : si vous remarquez une transaction suspecte, signalez-la immédiatement à votre banque ou à la société qui a émis votre carte de crédit. Vous pouvez également faire le suivi de vos renseignements personnels au sujet de l'impôt sur le revenu et des prestations en vous inscrivant à Mon dossier sur le site Web de l'ARC.

Signalez la fraude. Si vous êtes victime de fraude, signalez l'incident à votre service de police local et conservez toute preuve de l'incident. Ces renseignements pourraient servir dans le cadre d'une enquête.

Pour signaler une activité frauduleuse ou suspecte, vous pouvez communiquer avec le Centre antifraude du Canada par l'intermédiaire de son site Web au www.centreantifraude.ca, ou par téléphone au 1-888-495-8501.

Renseignements supplémentaires sur les fraudes et les escroqueries

Pour obtenir de plus amples renseignements sur les divers types de fraude et sur les moyens de vous protéger, y compris des informations sur les escroqueries liées aux prestations gouvernementales et d'autres escroqueries commises durant la pandémie de COVID-19, consultez les ressources ci-dessous.

Escroqueries liées à la PCU et autres fraudes courantes durant la pandémie de COVID-19 – Prospérité Canada

Base de données sur les fraudes et les escroqueries – Commission des services financiers et des services aux consommateurs (Nouveau-Brunswick)

Prévention de la fraude – Association des banquiers canadiens

Identité 101 (information sur le vol d'identité) – Gouvernement du Canada

Protection contre la fraude et les escroqueries – Agence de la consommation en matière financière du Canada (ACFC)

Protégez-vous contre les fraudes – Centre antifraude du Canada

À bas l'arnaque – Protégez-vous contre la fraude – Agence du revenu du Canada (ARC)