Protégez-vous contre le vol d'identité

Votre guide de protection contre le vol d'identité : comment le repérer, comment vous protéger et comment réagir si cela vous arrive

Reconnaître le vol d'identité et les fraudes

Effectuez vos opérations bancaires en toute confiance, où que vous soyez. Nous veillons à votre sécurité et à celle de vos renseignements bancaires. Découvrez comment préserver la sécurité de vos renseignements et comment vous protéger contre le vol d'identité et les fraudes.

Qu'est-ce que le vol d'identité?

Le vol d'identité est l'utilisation délibérée et illégale de l'identité d'une personne et de ses renseignements personnels pour obtenir des gains financiers.

Comment les criminels s'y prennent-ils pour voler mon identité?

- Ils vous appellent en se faisant passer pour des représentants d'institutions financières, d'organismes gouvernementaux ou d'entreprises légitimes et vous demandent vos renseignements personnels et bancaires.
- Ils vous envoient des courriels qui semblent provenir d'une entreprise légitime et qui vous demandent des renseignements personnels ou bancaires.
- Ils vous envoient des messages texte vous invitant à suivre un lien et à fournir des renseignements personnels ou bancaires.
- Ils instrumentalisent les risques liés aux téléphones intelligents et aux ordinateurs (maliciels).

Qu'est-ce qu'une fraude?

Une fraude est un stratagème utilisé par des personnes pour obtenir illégalement de l'argent ou des renseignements, souvent en piégeant la victime pour y arriver.

Savoir reconnaître les signes de fraude

- ! Offres inhabituelles qui proposent un prix et qui semblent trop belles pour être vraies
- ! Messages ou appels suspects et inattendus vous demandant d'effectuer une opération financière
- ! Réception d'un paiement en avance pour un emploi auquel vous avez récemment postulé
- ! Demandes d'envoi de paiements au moyen de paiements par câble, de cartes-cadeaux, de cartes prépayées, de bitcoins et d'autres cryptomonnaies

Types de fraudes courants

Hameçonnage, hameçonnage par message texte et hameçonnage vocal

Description : Une tentative des fraudeurs visant à vous inciter à divulguer des renseignements personnels ou bancaires au moyen de communications non sollicitées par courriel (hameçonnage), par message texte (hameçonnage par message texte) ou par téléphone ou messagerie vocale (hameçonnage vocal)

Exemple : Un courriel ou un message texte qui vous mentionne que vous avez gagné un concours ou un prix et qui vous invite à sélectionner le lien joint au message; un appel d'une personne prétendant travailler pour un organisme gouvernemental ou une institution financière qui vous demande un paiement immédiat ou des renseignements personnels et qui vous dit qu'il y aura de graves conséquences si vous ne répondez pas à la demande

Indices : Demandes urgentes d'envoi de fonds à un tiers, messages et adresses de courriel mal orthographiés, demandes de renseignements personnels, liens suspects avec une combinaison inhabituelle de lettres et de chiffres

Fraude liée au détournement et au transfert du module d'identification de l'abonné

Description : Une forme de vol d'identité selon laquelle un fraudeur peut obtenir une copie de votre carte SIM et recevoir tous vos appels et messages textes (détournement de carte SIM) ou obtenir vos renseignements personnels pour transférer votre numéro de téléphone d'un fournisseur de services à un autre (transfert de numéro)

Exemple : Un fraudeur qui communique avec votre fournisseur de services sans fil et le convainc d'échanger la carte SIM liée à votre numéro de téléphone pour une carte SIM en sa possession à l'aide de vos données personnelles

Indices : Changements de mot de passe ou ouvertures de session non autorisés dans vos comptes de banque, de courriel et de médias sociaux, avis de votre fournisseur de téléphone cellulaire indiquant que votre carte SIM ou votre numéro a été activé sur un autre appareil

Fraude à l'aide d'un maliciel

Description : Tout recours à un logiciel malveillant secrètement installé sur un ordinateur et conçu pour causer des perturbations ou des dommages ou pour accéder à un système informatique sans autorisation

Exemple : Un logiciel malveillant installé sur votre ordinateur qui menace de publier vos données personnelles ou de restreindre indéfiniment l'accès à celles-ci, à moins qu'une rançon soit payée (rançongiciel)

Indices : Demandes d'installation de logiciels, de divulgation d'information personnelle ou invitations à suivre des liens

Protégez-vous contre le vol d'identité

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.

Suivez les mesures ci-dessous pour protéger vos renseignements personnels et bancaires.

Comment puis-je me protéger?

- ✓ **À FAIRE :** Créer des mots de passe difficiles et uniques pour chacun de vos comptes (p. ex., compte de courriel, compte bancaire, compte de médias sociaux)
- ✓ **À FAIRE :** Configurer la section « **Mes alertes** » dans CIBC en direct ou dans Services bancaires mobiles CIBC pour être informé de toute opération non autorisée
- ✓ **À FAIRE :** Installer un logiciel antivirus à jour sur votre ordinateur pour détecter et supprimer les logiciels malveillants
- ✓ **À FAIRE :** S'inscrire à la fonction Dépôt automatique de Virement *Interac*[MD] pour que les fonds soient automatiquement déposés dans votre compte
- ✓ **À FAIRE :** Communiquer avec votre fournisseur de services mobiles pour en savoir plus sur la protection des ports afin d'éviter que votre carte SIM et votre appareil mobile soient compromis

- ✗ **À NE PAS FAIRE :** Donner vos mots de passe personnels ou vos codes de vérification à usage unique à quiconque
- ✗ **À NE PAS FAIRE :** Répondre aux courriels ou aux messages texte non sollicités et sélectionner les liens intégrés dans les messages
- ✗ **À NE PAS FAIRE :** Utiliser vos renseignements personnels ou bancaires pour créer des mots de passe uniques ou des réponses aux questions de sécurité d'un virement électronique (p. ex., NAS, date de naissance, adresse domiciliaire, numéros de carte)
- ✗ **À NE PAS FAIRE :** Transmettre vos renseignements personnels ou bancaires dans n'importe quelle fenêtre contextuelle en ligne
- ✗ **À NE PAS FAIRE :** Réutiliser la même réponse à une question de sécurité pour plusieurs destinataires de virements électroniques, ou transmettre cette réponse par l'intermédiaire des médias sociaux ou par courriel
- ✗ **À NE PAS FAIRE :** Enregistrer vos renseignements de connexion sur l'un ou l'autre de vos appareils électroniques

Que puis-je faire si je suis victime?

Suivez immédiatement les étapes ci-dessous pour éviter d'avoir d'autres pertes et d'être à nouveau victime :

1. **Passez en revue tous vos produits** (p. ex., comptes de chèques et d'épargne, cartes de crédit) pour repérer toute activité non autorisée.
2. **Remplacez rapidement les comptes compromis** en passant à un centre bancaire CIBC ou en appelant au numéro indiqué au verso de votre carte.
3. **Confirmez l'exactitude de vos renseignements personnels** (p. ex., adresse, adresse de courriel, numéros de téléphone) en passant à n'importe quel centre bancaire CIBC (deux pièces d'identité délivrées par le gouvernement sont requises) ou en appelant Services bancaires téléphoniques.
4. **Réinitialisez ou établissez votre mot de passe vocal** auprès de Services bancaires téléphoniques pour vos nouvelles cartes de crédit, et faites la même chose pour le NIP à trois chiffres de votre carte de débit en appelant au numéro indiqué au verso de votre carte.

Autres mesures

5. **Communiquez avec les agences d'évaluation du crédit** pour demander l'ajout d'une alerte à la fraude à votre dossier. Cette alerte avisera les entreprises de ne pas offrir de crédit à quiconque fera une demande en votre nom sans procéder à une vérification.
6. **Installez un logiciel antivirus réputé** sur votre ordinateur et effectuez régulièrement des balayages pour éliminer les virus.
7. **Changez vos mots de passe,** y compris celui de vos services bancaires en ligne et de votre adresse de courriel, à partir d'un appareil **non infecté** par un logiciel malveillant.
8. **Vérifiez vos paramètres de transfert de courriel et de messages vocaux** pour vous assurer qu'il n'y a pas de règle qui n'a pas été établie par vous.
9. **Communiquez immédiatement avec votre fournisseur de services mobiles** si vous ne pouvez pas faire d'appels ou envoyer de messages textes, ou si vous avez été avisé que votre numéro de téléphone a été activé sur un autre appareil.

Ne laissez pas les cybercriminels s'en tirer à bon compte

D'autres questions?

Pour en savoir plus sur la façon de vous protéger, visitez le site www.cibc.com/fraude

Si vous croyez avoir remarqué une activité suspecte dans l'un de vos comptes, passez immédiatement au centre bancaire CIBC le plus près ou communiquez avec nous à l'un des numéros suivants :

Opérations bancaires courantes CIBC	1 888 872-2422	**Pro-Investisseurs CIBC et SII**	1 800 567-3343
Services de cartes de crédit CIBC	1 800 465-4653	**CIBC Wood Gundy**	1 800 563-3193