Que faire en cas d'escroquerie ou de fraude financière ?
Guide de référence

Gestion de patrimoine

Une aide pour se relever en cas de fraude ou d'escroquerie

Voici une liste de vérification qui vous aidera à signaler les cas de fraude et d'escroquerie, ainsi qu'à prendre des mesures de protection pour l'avenir. Utilisez la section des notes à la fin du présent guide pour consigner vos mesures, vos entretiens et les prochaines étapes.

Conseils généraux à l'attention des victimes de fraude et d'escroquerie

- ☐ Avisez votre conseiller en placement, RBC Dominion valeurs mobilières, votre gestionnaire de portefeuille, RBC PH&N SCP et toutes les institutions financières qui ont traité les opérations liées à cette fraude ou à cette escroquerie.
  - – Signalez immédiatement toute activité non autorisée ou frauduleuse.
  - – Demandez si vous êtes en mesure de présenter une demande de règlement ou si les fonds peuvent être récupérés ou recouvrés.
  - – Envisagez sérieusement d'ajouter une personne-ressource de confiance au dossier pour votre conseiller en placement ou votre gestionnaire de portefeuille à titre de protection supplémentaire lorsque vous n'êtes pas joignable.
- ☐ Cessez immédiatement tout contact avec les escrocs ou les fraudeurs : ceux-ci auront une explication à tout et vous harcelleront de plus belle. Une fois l'argent obtenu d'une victime, ils reviennent souvent à la charge (nouvelle excuse, urgence ou demande).
- ☐ Communiquez avec votre service de police local pour déposer un rapport de police.
- ☐ Signalez la fraude ou l'escroquerie au Centre antifraude du Canada (CAFC). Voir la section sur le signalement aux autorités à la page 4.
- ☐ Si vos renseignements personnels ou vos appareils ont été piratés ou compromis, suivez la liste de vérification pour vous aider à vous relever après une usurpation d'identité ou une compromission à la page 3.

Cas de fraude par téléphone

- ☐ Bloquez les numéros à partir desquels les fraudeurs appellent et ne répondez pas aux appels de numéros inconnus.
- ☐ Signalez le problème à votre opérateur téléphonique, et demandez-lui de signaler le numéro de téléphone, et de vous aider à repérer et à filtrer les autres numéros de fraude potentiels.
- ☐ Si les appels se poursuivent, songez à changer de numéro de téléphone.

Cas de fraude par courriel ou par Internet

- ☐ Bloquez l'adresse de courriel du fraudeur.
- ☐ Rendez vos profils publics privés ou supprimez tout renseignement personnel.
- ☐ Signalez les cas d'escroquerie, de fraude et de harcèlement à l'entreprise propriétaire du site Web ou au fournisseur de services de courriel.

Restez vigilant

Un fraudeur cible souvent les mêmes personnes. Les escrocs se font souvent passer pour des organismes gouvernementaux, des services frauduleux ou des avocats et affirment qu'ils peuvent récupérer votre argent ou vous demandent de déposer des fonds supplémentaires dans des comptes sûrs. Si vous vous trouvez dans cette situation, demandez une réunion en personne à votre poste de police local ou à l'institution financière désignée avant de donner des renseignements ou de l'argent.

Aide pour vous relever après une usurpation d'identité et signalement aux autorités

Il est essentiel de signaler les cas de fraude, d'escroquerie et d'usurpation d'identité pour aider les enquêteurs à établir des dossiers sur les fraudeurs et les escrocs afin de les arrêter.

Si vous croyez avoir été victime d'une tentative d'usurpation ou d'une usurpation d'identité, suivez la liste de vérification ci-dessous pour vous aider à vous relever. Utilisez également la section des notes à la fin de cette boîte à outils pour consigner vos entretiens et les prochaines étapes.

- ☐ Avisez votre conseiller en placement, RBC Dominion valeurs mobilières ou votre gestionnaire de portefeuille, RBC PH&N SCP au sujet de tout renseignement personnel compromis et examinez votre activité du compte.
  - – Signalez les tentatives d'hameçonnage* à phishing@rbc.com.
  - – Signalez toute activité suspecte ou non autorisée et annulez toute carte de débit ou de crédit compromise, ou tout numéro de compte de chèques ou de chéquier compromis.
  - – Assurez-vous d'indiquer une personne-ressource de confiance au dossier pour votre conseiller en placement ou votre gestionnaire de portefeuille à titre de protection supplémentaire lorsque vous n'êtes pas joignable.
- ☐ Modifiez vos mots de passe en ligne et informez toutes vos institutions financières que vos renseignements personnels ont été compromis.
  - – Suivez la procédure appropriée de mise à jour des mots de passe : Pourquoi il est important d'utiliser des mots de passe plus robustes – Et comment les créer.

Continuez à surveiller les activités non autorisées

Examinez vos comptes, vos rapports de solvabilité et vos historiques bancaires, et signalez rapidement toute activité suspecte ou non autorisée.

- ☐ Pour signaler une communication frauduleuse ou une usurpation d'identité dans le cadre d'une escroquerie, veuillez communiquer avec le service de lutte antifraude de la Gendarmerie royale du Canada par courriel à l'adresse info@phonebusters.com ou par téléphone au 1 888 495-8501.
- ☐ **Centre antifraude du Canada (CAFC) :** Aide les autorités chargées de l'application des lois en conservant un répertoire central de renseignements pour faciliter leurs enquêtes.
  - – Appelez le 1 888 495-8501 ou signalez une escroquerie ou une fraude en ligne à l'adresse https://antifraudcentre-centreantifraude.ca/scams-fraudes/victim-victime-fra.htm.
- ☐ Obtenez un relevé de l'historique de votre compte bancaire et vérifiez s'il comporte une activité bancaire non autorisée.
- ☐ Communiquez avec les agences d'évaluation du crédit pour placer un avis d'alerte à la fraude ou pour bloquer l'accès à votre rapport de solvabilité :
  - – **Equifax :** 1 877 323-2598 ou https://www.consumer.equifax.ca/fr/personnel/contactez-nous
  - – **TransUnion :** 1 877 525-3823 ou https://www.transunion.ca/fr/assistance/fraude-et-vol-didentite
- ☐ Si des appareils ont été piratés ou compromis, envisagez de les faire inspecter par un service de cybersécurité professionnel pour y déceler tout logiciel espion ou maliciel.
  - – Assurez-vous que le logiciel de sécurité et les navigateurs Internet de votre appareil sont à jour.

***Hameçonnage :** méthode de cyberattaque par laquelle les agresseurs se présentent comme des personnes physiques, organisations ou entités légitimes pour tromper les gens et les amener à révéler des renseignements sensibles, p. ex., les mots de passe, les numéros de carte de crédit ou les renseignements personnels. Les victimes pensent souvent qu'elles interagissent avec une source de confiance, alors qu'en réalité, elles fournissent des renseignements à des auteurs de menace.

Autres ressources

- ☐ Centre antifraude du Canada : https://antifraudcentre-centreantifraude.ca/index-fra.htm
- ☐ Agence du revenu du Canada : https://www.canada.ca/fr/agence-revenu/services/formulaires-publications/publications/rc284/protegez-vous-contre-identite.html
- ☐ Commissariat à la protection de la vie privée du Canada – vol d'identité et fraude : https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/identites/vol-d-identite/
- ☐ Centre canadien de ressources pour les victimes de crimes :
  - Abus des aînés (en anglais seulement) : https://crcvc.ca/wp-content/uploads/2021/09/Elder-Abuse_-DISCLAIMER_-Revised-April-2022_-FINAL-1.pdf
  - Cyberharcèlement (en anglais seulement) : https://crcvc.ca/wp-content/uploads/2021/09/Cyberstalking-_DISCLAIMER_Revised-Aug-2022_FINAL.pdf
- ☐ Gouvernement du Canada – Bureau de la concurrence Canada – Le petit Livre noir de la fraude : https://ised-isde.canada.ca/site/bureau-concurrence-canada/fr/petit-livre-noir-fraude-2e-edition
- ☐ Ressources RBC :

Ressources mises à jour sur les escroqueries et les fraudes :

- Restez à l'affût des dernières cyberfraudes : https://www.rbc.com/cyberfute/alertes/index.html
- Soyez cyberfuté : https://www.rbc.com/cyberfute/index.html
- Protection des renseignements personnels et Sécurité Canada – Protégez-vous : https://www.rbc.com/rensperssecurite/ca/protegez-vous.html

Mesures de protection :

- Mes finances d'abord – Comprendre la cybersécurité : https://www.rbcroyalbank.com/fr-ca/mes-finances-dabord/academie-financiere/cybersecurite/comprendre-la-cybersecurite/
- Prévention des fraudes – Escroqueries courantes et comment s'en prémunir : https://www.rbcroyalbank.com/fr-ca/mes-finances-dabord/entreprises/conseils-daffaires-appropries/secteur-commercial/surmonter-les-pressions-commerciales-internationales-grace-a-la-resilience-canadienne/prevention-des-fraudes-escroqueries-courantes-et-comment-sen-premunir/
- La chambre forte – Plan de match de la cybersécurité : https://www.rbc.com/cyberfute/_assets-custom/pdf/cyber-playbook.pdf
- Cinq façons de reconnaître une escroquerie amoureuse : https://www.rbcroyalbank.com/fr-ca/mes-finances-dabord/academie-financiere/cybersecurite/comprendre-la-cybersecurite/cinq-facons-de-reconnaitre-une-escroquerie-amoureuse/

Vos notes

Prenez des notes et faites le suivi de vos progrès sur cette page. Pour votre sécurité, n'inscrivez pas les noms d'utilisateur, les mots de passe, les numéros d'identification personnels ou les numéros de compte.

- ☐ Signalez toute activité suspecte, toute opération non autorisée ou tout transfert de fonds douteux à des fins présumées d'escroquerie ou de compromission de vos renseignements personnels.
- ☐ Si vous avez été victime d'une escroquerie ou d'une fraude, demandez à l'institution financière ou à l'organisme en question si les fonds peuvent être récupérés ou recouvrés.
- ☐ Demandez à chaque organisme ou personne-ressource si des mesures supplémentaires sont recommandées pour vous aider à protéger vos renseignements et vos actifs à l'avenir.

Entreprise contactée ou organisme contacté	Personnes-ressources (numéro de téléphone et courriel)	Nom de la personne-ressource	Numéro de demande, de dossier ou de suivi	Moment de la prise de contact (date et heure)

Signalez toute demande suspecte !

Nous renforçons votre sécurité financière

www.rbcgestiondepatrimoine.com

RBC Gestion de patrimoine