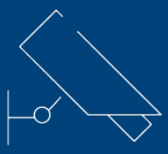
Sécurité numérique et escroqueries

Votre guide pour repérer les escroqueries, protéger vos comptes et être en sécurité

Table des matières



Garder une longueur d'avance

Que ce soit pour magasiner, effectuer des opérations bancaires ou garder le contact, nous menons une vie plus connectée que jamais. Toutefois, le côté pratique d'une telle connectivité comporte également des risques. Les escrocs trouvent constamment de nouvelles façons de manipuler les gens afin qu'ils divulguent leurs renseignements personnels ou qu'ils leur envoient de l'argent.

La bonne nouvelle, c'est que vous n'avez pas à être un expert en technologie pour vous protéger. Ce guide offre des conseils pratiques pour vous aider à vous protéger en ligne, notamment des listes de vérification faciles à suivre et une liste de ressources qui vous seront utiles au cas où vous, ou quelqu'un que vous connaissez, auriez besoin de signaler une escroquerie.

Connaître les fondements de la cybersécurité : votre liste de vérification pour vous protéger

Votre première ligne de défense consiste à adopter de bonnes habitudes en matière de cybersécurité. Voici quelques mesures simples à prendre pour protéger vos renseignements personnels, sécuriser vos appareils et réduire le risque d'être victime d'escroqueries en ligne.

☐ **Installez des logiciels antivirus et antilogiciels malveillants et assurez-vous qu'ils soient toujours à jour**

Ces outils permettent de détecter les programmes malveillants qui pourraient voler vos renseignements ou endommager votre appareil.

☐ **Mettez à niveau vos appareils et vos applications dès que des correctifs sont disponibles**

Les mises à niveau viennent souvent corriger les failles de sécurité connues que les escrocs peuvent exploiter.

☐ **Utilisez un mot de passe ou une phrase d'identification sûr et unique pour tous vos justificatifs d'ouverture de session**

Si l'un de vos mots de passe est volé ou compromis, le fait d'utiliser différents mots de passe uniques empêche les escrocs d'accéder à tous vos justificatifs d'ouverture de session.

☐ **Activez l'authentification à double facteur ou multifacteur**

L'authentification à double facteur ou multifacteur ajoute une étape supplémentaire pour toute personne qui tente de se connecter à votre compte, ce qui rend l'accès beaucoup plus difficile pour les escrocs, même avec votre mot de passe. La configuration d'un appareil de confiance peut aider à prouver que c'est bien vous lors des vérifications de sécurité. Elle peut également simplifier l'expérience d'ouverture de session et faciliter les vérifications de sécurité lorsque des limites plus élevées sont utilisées.

☐ **Effectuez régulièrement des copies de sauvegarde de vos fichiers (idéalement dans l'infonuagique et hors ligne)**

De cette façon, si votre appareil est piraté ou verrouillé par un rançongiciel, vous pourrez récupérer vos renseignements importants.

☐ **Évitez de télécharger des applications, logiciels ou fichiers provenant de sources inconnues**

Certains téléchargements cachent des virus ou des logiciels espions conçus pour voler vos données personnelles.

☐ **Ne publiez pas trop de renseignements dans les médias sociaux. Limitez le contenu de vos publications et le nombre de personnes qui peuvent les consulter**

Les escrocs utilisent des renseignements personnels comme votre date d'anniversaire ou le nom de votre animal de compagnie pour deviner vos mots de passe ou vous tromper.

☐ **Rendez vos profils sur les réseaux sociaux privés et vérifiez régulièrement vos contacts**

Vous empêcherez ainsi les inconnus (et les escrocs) de voir vos renseignements personnels ou de les utiliser à mauvais escient.

☐ **Utilisez des connexions sécurisées et évitez les réseaux Wi-Fi publics pour faire vos opérations financières**

Les réseaux Wi-Fi publics peuvent être dangereux, ce qui facilite l'interception de vos données par des escrocs.

☐ **Inscrivez-vous au Dépôt automatique pour les télévirements afin de réduire les risques de fraude**

Le Dépôt automatique envoie l'argent directement à votre compte, ce qui permet d'éviter qu'il soit intercepté.

☐ **Utilisez des questions d'identification difficiles à deviner**

Des réponses comme « Quel est le nom de votre chien ? » peuvent souvent être trouvées en ligne. Choisissez donc des questions dont vous êtes le seul à connaître la réponse.

Repérer les escroqueries courantes

Les escroqueries se présentent sous diverses formes, et elles sont de plus en plus difficiles à repérer. Il peut être utile de connaître les signaux d'alerte pour ne pas tomber dans le piège d'un faux message, appel téléphonique ou site Web, aussi convaincant soit-il.

Escroqueries par piratage psychologique

Les escrocs essaient souvent d'exploiter votre penchant naturel à agir rapidement ou à aider les autres ; c'est là l'essence même d'une escroquerie par piratage psychologique. Dans ce type d'escroqueries, les escrocs tentent d'amener les gens à divulguer des renseignements confidentiels, comme des mots de passe ou des renseignements bancaires, en se faisant passer pour une personne de confiance. Ces escroqueries peuvent inclure des demandes urgentes de la part d'un « ami », d'un « patron » ou du « soutien clientèle » qui semblent légitimes.

Si vous recevez un message urgent vous demandant d'effectuer une tâche inhabituelle ou d'envoyer de l'argent, prenez toujours un moment pour vérifier les faits et ne vous sentez jamais obligé de répondre sur-le-champ.

Escroqueries sur les médias sociaux

Les escrocs utilisent des plateformes de médias sociaux et des applications de messagerie pour communiquer directement avec les victimes, en leur offrant souvent de faux cadeaux, des remboursements d'impôt ou des subventions à l'entreprise. Méfiez-vous des messages directs de personnes que vous ne connaissez pas et évitez de cliquer sur des liens ou de divulguer des renseignements personnels.

De plus, si vous recevez d'une personne que vous connaissez un message privé qui semble anormal ou qui ne correspond pas à son caractère, ne répondez pas : il pourrait s'agir d'un escroc utilisant un compte compromis. Essayez de joindre la personne par un autre moyen de communication, comme un appel téléphonique ou un texto à un numéro de confiance, pour confirmer la légitimité du message.

Escroqueries en ligne (faux sites Web, fausses applis et fausses nouvelles)

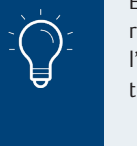
Les fraudeurs sont passés maîtres dans l'art de créer de faux sites Web de magasinage, de fausses applis et de faux sites de nouvelles qui sont très semblables aux vrais. Ces sites peuvent vous demander votre numéro de carte de crédit ou des renseignements personnels sans vous livrer un produit, ou ils peuvent diffuser de fausses nouvelles sur les médias sociaux pour vous inciter à cliquer sur des liens ou à faire des placements frauduleux.

Comment savoir s'il s'agit d'un faux site? Soyez à l'affût des erreurs de conception, des liens brisés, des politiques vagues ou de l'absence de coordonnées. Sur les applis, vérifiez le nom de l'éditeur, lisez les avis des utilisateurs et évitez les applis qui demandent trop d'autorisations. En ce qui concerne les sites de nouvelles, surveillez les titres sensationnels, les URL anormales et les histoires qui ne figurent que sur des sources douteuses ou dans les médias sociaux.

Escroqueries par téléphone (hameçonnage vocal et hameçonnage par texto)

Lors d'une escroquerie par téléphone, le fraudeur peut se faire passer pour le représentant d'une banque ou d'un organisme gouvernemental, voire un officier chargé de l'application des lois. Dans bien des cas, il dira que vous devez de l'argent ou que votre compte est à risque et insistera pour que vous divulguiez des renseignements personnels ou financiers.

Certaines escroqueries sont transmises par texto et demandent de cliquer sur un lien suspect (hameçonnage par texto) et d'autres, par téléphone (hameçonnage vocal).



En cas de doute sur l'interlocuteur, raccrochez ou ignorez le message et rappelez l'organisation en composant un numéro de téléphone en lequel vous avez confiance.

Escroqueries par courriel (hameçonnage)

Dans un courriel hameçon, les escrocs prétendent être des représentants de marques ou d'entreprises réputées (p. ex., service d'expédition, gouvernement, banque) et utilisent des tactiques pour vous inciter à divulguer vos renseignements personnels ou à cliquer sur des liens malveillants. Les courriels d'hameçonnage semblent souvent provenir d'une entreprise ou d'une organisation légitime et utilisent une tactique de peur pour vous inciter à cliquer sur un lien ou à entrer des renseignements personnels (« Votre compte est bloqué ! »).

Même les courriels d'apparence professionnelle peuvent être faux. Peu importe qui semble en être l'expéditeur, ne cliquez pas sur les liens suspects et ne fournissez jamais vos mots de passe ou les renseignements sur votre compte par courriel. Vous n'êtes pas certain si un courriel est légitime ? Communiquez directement avec l'entreprise à l'aide d'un numéro ou d'un site Web vérifiés.

Escroqueries amoureuses

Les escroqueries amoureuses commencent généralement sur les sites de rencontre ou les médias sociaux. L'escroc établit une relation, souvent au fil des semaines ou des mois, et gagne la confiance de ses victimes. De nombreux messages seront échangés, de forts sentiments seront exprimés et de nombreux compliments seront faits. Ces escroqueries sont extrêmement efficaces et jouent sur les émotions des victimes, les laissant ainsi vulnérables à l'escroquerie. Éventuellement, l'escroc vous demandera de l'argent, en invoquant souvent une urgence, comme la nécessité de régler des frais de voyage, voire une occasion de placement avantageuse.

Méfiez-vous des indicateurs d'alerte, tels que les excuses pour ne pas vous rencontrer en personne, les demandes de poursuivre la conversation en dehors de la plateforme, les demandes urgentes de soutien financier ou les occasions de placement trop belles pour être vraies, impliquant souvent la cryptomonnaie.

Escroqueries par usurpation d'identité bancaire

Ces escroqueries commencent souvent par un appel, un texto ou un courriel prétendant provenir de votre banque. L'escroc peut prétendre que votre compte a été compromis et, pour vérifier l'activité, il vous demande votre mot de passe, votre NIP, voire le code d'accès à usage unique envoyé à votre téléphone.

Ces interactions peuvent sembler tout à fait légitimes et tromper même les personnes les plus cybervigilantes. Sachez toutefois qu'aucune banque ne vous demandera de fournir ces renseignements. Ne communiquez jamais aucun code ou mot de passe à qui que ce soit. En cas de doute, raccrochez et appelez directement la banque en utilisant le numéro figurant sur votre carte ou sur le site Web officiel.

Souvent, ces escrocs demandent aux victimes d'ouvrir une session dans Banque en direct et d'envoyer un télévirement à un bénéficiaire nouvellement ajouté sous leur propre nom. Les escrocs vont prétendre que ce virement est nécessaire pour protéger les fonds dans le compte pendant que l'enquête est en cours.

Souvenez-vous que RBC ne vous demandera jamais d'effectuer une opération financière en son nom, surtout pour résoudre une situation de fraude ou d'escroquerie.

Escroqueries s'appuyant sur l'IA

L'intelligence artificielle (IA) a rendu les escroqueries plus difficiles à détecter. Les criminels utilisent l'IA pour accroître la fréquence, la portée et l'apparence de leurs escroqueries, ce qui leur permet de faire ce qui suit :

- Rédiger des messages d'hameçonnage impeccables.
- Cloner des voix pour les escroqueries par téléphone.
- Créer de faux emplois ou des appels vidéo avec hypertrucages.
- Créer de faux sites Web convaincants.

Bien que l'IA rende les escroqueries plus difficiles à détecter, la meilleure façon de s'en protéger est d'être prudent face aux communications inhabituelles, en particulier celles qui vous demandent d'agir rapidement ou d'envoyer de l'argent.

Escroqueries liées aux placements et escroqueries à la cryptomonnaie

Les escroqueries liées aux placements et les escroqueries à la cryptomonnaie ciblent souvent des personnes par des moyens sollicités ou non. Les escrocs vous invitent à profiter d'occasions d'investir (souvent liées aux cryptomonnaies) en promettant des taux de rendement élevés dans un court laps de temps, avec peu ou pas de risque.

Les escrocs créent de faux sites Web ainsi que des publicités, et peuvent aussi se faire passer pour des sociétés de confiance ou des personnes connues. Ils utilisent parfois l'hypertrucage pour se faire passer pour quelqu'un d'autre. Ils jouent aussi sur le long terme, faisant de la sollicitation sur des plateformes de médias sociaux, des applications de messagerie et même des sites de rencontre, en prenant souvent le temps d'établir la confiance. Ils peuvent envoyer des « captures d'écran » ou des « graphiques des tendances » en direct illustrant l'évolution du placement. Méfiez-vous des indicateurs d'alerte tels que des instructions d'envoi de télévirements à des sociétés de cryptomonnaie, ou de télévirements ou de dépôts dans des GAB Bitcoin, où les fonds sont ensuite obtenus par l'escroc.

Assurez-vous d'avoir un accès direct à votre compte de placement et de pouvoir vérifier le rendement de façon indépendante. Faites toujours des recherches approfondies avant d'investir, et n'oubliez pas que si l'occasion est trop belle pour être vraie, c'est probablement une escroquerie.

Savoir quoi faire si vous êtes victime d'une fraude ou d'une escroquerie

Avez-vous déjà été victime de fraude ? Si c'est le cas, sachez que vous n'êtes pas seul. Beaucoup hésitent à signaler une arnaque par honte, mais les fraudeurs sont aujourd'hui si sophistiqués qu'ils peuvent piéger même les plus prudents. Signaler une arnaque permet non seulement de vous protéger, mais aussi d'empêcher qu'elle ne touche d'autres personnes.

Voici les mesures à prendre si vous pensez avoir été victime d'une fraude.

1. Avisez votre banque

Si vous êtes victime de fraude, votre banque peut vous aider à limiter les dommages et protéger vos comptes. Communiquez avec votre banque sans tarder pour que toutes les cartes ou tous les comptes touchés puissent être bloqués, surveillés et remplacés rapidement. La banque dispose d'experts en prévention de la fraude prêts à vous guider et à assurer la sécurité de vos informations.

Clients de RBC

Si vous êtes un client de RBC et que vous avez été victime de fraude, communiquez sans délai avec votre succursale, votre bureau local, ou appelez-nous. N'hésitez pas à nous appeler si vous avez des questions ou des commentaires d'ordre général concernant la protection des renseignements personnels et la sécurité.

- 1 800 769-2511 (services bancaires par téléphone)
- 1 800 769-2555 (services bancaires mobiles et en ligne)
- 1 800 769-2512 (cartes de crédit)
- 1 800 769-2535 (Centre de soutien clientèle, Services bancaires en ligne RBC Express)
- *RBC Bank (Georgia), N.A. : 1 800 769-2553
- ATS/Téléimprimeur : 1 800 661-1275

Si vous habitez aux États-Unis, veuillez également aviser les autorités locales et la FTC (Federal Trade Commission) en composant le 1 877 438-4338.

2. Avisez les agences d'évaluation du crédit

Si un fraudeur a accédé à vos renseignements personnels, prévenez immédiatement les agences de crédit. Elles peuvent ajouter une alerte de fraude à votre dossier afin de limiter l'ouverture de comptes non autorisés. Il est également judicieux de consulter votre rapport de solvabilité pour détecter toute opération suspecte.

Les deux principales agences d'évaluation du crédit sont Equifax et TransUnion. Il est préférable de contacter les deux, car elles travaillent indépendamment.

Canada :

TransUnion
1 877 525-3823
transunion.ca

Equifax
1 877 323-2598
equifax.ca

États-Unis :

TransUnion
1 800 888-4213
transunion.com

Equifax
1 800 685-1111
equifax.com

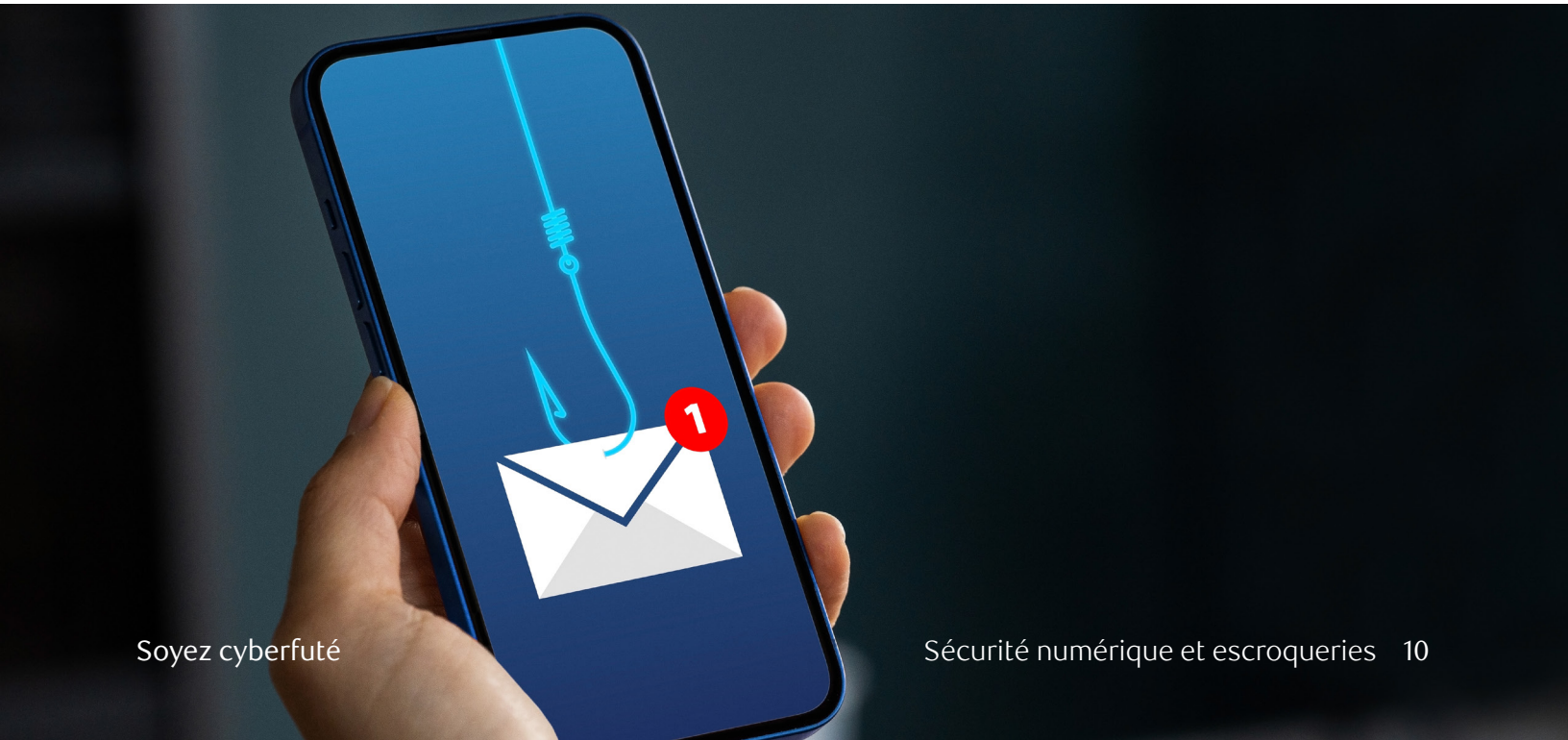
Experian
1 888 397-3742
experian.com

International (îles Britanniques) :

Experian
+44 844 481-8000
Appel depuis l'étranger (hors Royaume-Uni)

0844 481-8000
Appel local (au Royaume-Uni)
experian.co.uk

Equifax
equifax.co.uk
(tous les contacts se font en ligne, sauf si vous êtes membre du service Equifax)



3. Prenez des mesures pour atténuer toute autre incidence

L'argent et les renseignements personnels partagés en ligne sont souvent difficiles à récupérer. Agir vite est donc essentiel. Voici les principales mesures à prendre pour réduire les risques et vous protéger, ainsi que protéger les autres, contre d'éventuelles fraudes.

- ☐ **Vérifiez votre appareil au moyen d'une analyse antivirus** : Si vous avez cliqué sur un lien ou une pièce jointe, il est possible que l'escroc ait tenté d'installer un logiciel malveillant sur votre appareil. Il est donc recommandé de lancer une analyse antivirus pour le vérifier.

- ☐ **Changez vos mots de passe** : Si vous utilisez le même mot de passe pour plusieurs comptes, vous devriez en créer de nouveaux immédiatement. Il s'agit d'une excellente occasion de créer des mots de passe plus sûrs.

- ☐ **Protégez vos informations de crédit** : Si un fraudeur a vos renseignements personnels, il pourrait notamment les exploiter pour usurper votre identité. Il serait donc avisé de faire ajouter une alerte à la fraude dans votre dossier de crédit. Cela avertira les créanciers et autres agences d'évaluation du crédit que vous pourriez être victime d'usurpation d'identité ou de fraude. Ces alertes peuvent empêcher toute autre personne d'ouvrir un compte à l'aide de vos renseignements personnels.

- ☐ **Bloquez ou annulez votre carte de crédit** : Si vous avez fourni par inadvertance vos renseignements de carte de crédit ou de débit à un escroc, vous pouvez immédiatement bloquer votre carte et appeler la banque pour l'annuler. Cela empêchera les fraudeurs d'utiliser votre carte pour effectuer des achats non autorisés.

4. Surveillez vos relevés

Passez en revue vos relevés de compte, de cartes de crédit et d'autres comptes pour vous assurer de la légitimité de toutes les opérations. La vérification de vos relevés est recommandée en tout temps, mais elle est essentielle en cas de fraude.

5. Faites preuve de vigilance

Les victimes d'escroquerie et de fraude peuvent être ciblées à répétition, surtout après qu'elles ont perdu de l'argent. Les escrocs se font souvent passer pour des organismes gouvernementaux, des services de prévention de la fraude ou des avocats, et prétendent qu'ils peuvent récupérer votre argent (en vous demandant d'envoyer de l'argent supplémentaire pour ce faire). Ne répondez pas à un message dont vous ne pouvez pas vérifier l'authenticité. Contactez l'organisme en passant plutôt par des voies de communication officielles pour confirmer le tout.

Il n’est pas nécessairement compliqué de naviguer en ligne en toute sécurité. En adoptant certaines bonnes habitudes et en faisant preuve d’une bonne dose de prudence, vous pouvez vous protéger contre les escroqueries et menaces numériques les plus courantes. Transmettez ce que vous avez appris à vos amis et à votre famille, car plus nous sommes informés, plus il devient difficile pour les escrocs de parvenir à leurs fins.

Remarques

Liste de verification

- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐

Pour en savoir plus sur la cybersécurité, consultez le site rbc.com/cyberfute

Créé en : octobre 2025
Dernière mise à jour : decembre 2025