éducaloi

Savoir c'est pouvoir

ÉVITER LA FRAUDE EN LIGNE

Un guide pour les personnes aînées

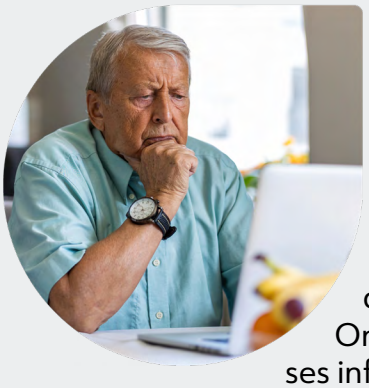
Éducaloi est un organisme sans but lucratif qui a pour mission de vulgariser le droit et développer les compétences juridiques de la population du Québec.

Précisions importantes :

Le droit change! L'information juridique contenue dans ce guide est valide en date du 1er mars 2024. L'information contenue dans ce guide s'applique uniquement au Québec et n'est pas un avis juridique. Ce guide peut être reproduit et utilisé à des fins non commerciales. Il doit être utilisé dans son format original, sans modifications. Il demeure la propriété d'Éducaloi.

Table des matières

Protégez vos données bancaires et personnelles



Histoire inspirée de faits réels

L'histoire d'André

André reçoit un courriel d'une compagnie de livraison concernant l'arrivée d'un colis qu'il a commandé récemment. On lui demande de confirmer ses informations personnelles pour lui acheminer le colis.

Après avoir cliqué sur le lien fourni, André insère son adresse et son numéro de téléphone sur le formulaire qui apparaît à l'écran. Il indique aussi les informations relatives à sa carte de crédit.

André espère alors que son colis arrivera rapidement.

Quelques jours plus tard, il vérifie son relevé de carte de crédit. Plusieurs transactions dont il n'a aucune connaissance ont été effectuées avec sa carte. Trois articles de luxe ont été commandés pour un montant de 4 700 $.

AUTRES PRÉTEXTES POUR VOUS CONTACTER

Les fraudeuses et fraudeurs peuvent également se faire passer pour :

- votre compagnie de téléphonie ou d'abonnement internet,
- un site de commerce en ligne,
- votre banque ou votre caisse,
- une agence gouvernementale, comme l'Agence du revenu du Canada.

La stratégie des escrocs

Une stratégie fréquemment utilisée par les fraudeuses et fraudeurs est de vous envoyer un courriel en **se faisant passer pour une compagnie bien connue**.

Le prétexte peut être, par exemple :

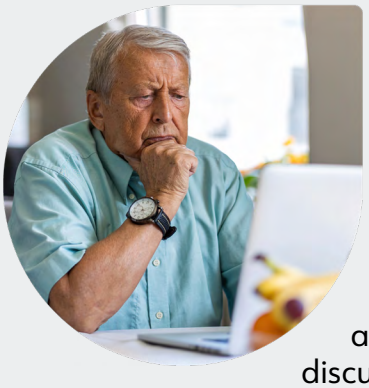
- de confirmer une commande,
- d'éviter que votre compte soit suspendu ou qu'il passe automatiquement à un abonnement premium,
- de vous rembourser des frais facturés par erreur.

Lorsque vous cliquez sur le lien qu'on vous envoie, vous arrivez sur **un site qui ressemble en tous points au site légitime.**

On vous demande de **réintroduire les renseignements de votre carte de crédit ou vos identifiants bancaires.**

Une fois ces renseignements obtenus, les fraudeuses et fraudeurs les utilisent pour effectuer des paiements ou faire de gros achats.

Protégez vos données bancaires et personnelles



Et le vol d'identité ?

Après sa mésaventure avec sa carte de crédit, André s'est beaucoup renseigné sur internet, auprès de sa banque et en discutant avec son entourage. Même si la fraude qu'il a subie lui a fait perdre un gros montant, il se rend compte qu'il a peut-être évité le pire.

Il savait qu'il faut toujours éviter de transmettre son numéro d'assurance sociale (NAS) sur des sites Web qui n'en n'ont pas légitimement besoin. Par contre, il ignorait qu'il en est de même pour sa date de naissance ou son numéro de permis de conduire.

En en parlant autour de lui, il a appris qu'une amie d'enfance s'était fait voler son identité de cette manière.

En recoupant sa date de naissance avec d'autres données personnelles, des malfrats avaient réussi à se faire ouvrir un compte chez Hydro-Québec, puis se faire délivrer un permis de conduire et une carte d'assurance-maladie à son nom.

Avec ces pièces d'identité, ils étaient finalement parvenus à emprunter une grosse somme d'argent auprès d'une banque en hypothéquant son condo.

La stratégie des escrocs

Les fraudeuses et fraudeurs cherchent à **obtenir de nombreux renseignements personnels.** Pas uniquement des numéros de cartes de crédit ou des identifiants bancaires.

Avec suffisamment de renseignements personnels, certains escrocs **réussissent à obtenir des pièces d'identité au nom de leurs victimes** et à se faire passer pour elles.

Les fraudeuses et fraudeurs peuvent alors **effectuer des opérations importantes**, comme vendre la maison de leur victime, emprunter de grosses sommes d'argent en leur nom ou toucher des prestations sociales ou de retraite à leur place. C'est ce qu'on appelle le vol d'identité.

Comment éviter de vivre l'histoire d'André?

Examinez bien les **courriels qui vous invitent à mettre à jour les informations de votre compte ou de votre abonnement** et traitez-les adéquatement :

- **Comparez l'adresse courriel dont provient le message et l'adresse du site internet légitime de la compagnie** que vous reconnaissez.

  Y a-t-il une petite différence qui peut révéler une fraude?

  Par exemple : info@nomdelacompagnie.s.com au lieu de info@nomdelacompagnie.com ?

- **Évitez de cliquer sur un lien dans un tel courriel.**

  Les compagnies légitimes ne vous demandent généralement pas de cliquer sur un lien dans un courriel pour encoder des informations personnelles.

- Si vous pensez devoir mettre vos données personnelles à jour ou modifier un de vos comptes, **rendez-vous sur le site de la compagnie directement via votre navigateur**, sans passer par le lien fourni dans le courriel.

- Si vous recevez un message frauduleux, **supprimez-le tout simplement**, sans y donner suite.

LE SAVIEZ-VOUS?

Chaque jour sur la planète, plus de six milliards de courriels cherchent à soutirer des données bancaires ou personnelles à leurs destinataires.

Protégez vos données bancaires et personnelles

Et aussi…

- **Inscrivez votre numéro de carte de crédit** pour payer **uniquement sur les sites de compagnies bien établies**.

  Vérifiez que vous êtes sur une **connexion sécurisée** lorsque vous inscrivez votre numéro de carte ou des données personnelles :

  Un cadenas verrouillé devrait apparaître au début de la barre d'adresse du navigateur, **ainsi qu'un 's' après le 'http'**.

- **Refusez de donner vos numéros de pièces d'identité,** comme votre numéro d'assurance sociale (NAS), votre numéro de permis de conduire ou votre numéro de carte d'assurance maladie sur des sites qui n'ont pas besoin de les obtenir.

- **Évitez de donner votre date de naissance ou votre adresse** lorsque vous estimez que cela n'est pas nécessaire.

- **Vérifiez** régulièrement **vos relevés bancaires** et détectez les opérations inhabituelles.

- **Utilisez un mot de passe différent** pour chacun de vos comptes en ligne.

- **Vérifiez votre dossier de crédit chaque année,** via les sites internet d'Equifax ou Transunion. Activez une alerte de sécurité ou le gel de votre dossier si vous avez des soupçons.

Que faire immédiatement…?

Si vous avez fourni votre numéro de carte de crédit après avoir cliqué sur un lien reçu dans un courriel?

- **Contactez votre compagnie de carte de crédit** pour faire **bloquer** votre carte et en commander une nouvelle.
- S'il y a eu des dépenses non autorisées depuis l'incident, **vérifiez** avec votre compagnie de carte de crédit **si vous avez le droit de récupérer le montant** fraudé. Dans certains cas, les compagnies de carte de crédit absorbent les pertes en cas de fraude.

Si vous avez donné vos identifiants bancaires sur un site qui vous paraît finalement suspect?

- **Changez votre mot de passe et contactez immédiatement votre banque** pour lui exposer la situation.

Si vous avez des soupçons quant à un **vol d'identité**?

- **Appelez votre compagnie de carte** de crédit pour **faire changer** votre ou vos cartes.
- **Contactez votre banque** afin de changer vos identifiants et vérifier que votre adresse et numéro de téléphone n'ont pas été modifiés dans leur système.
- **Contactez Equifax ou Transunion** pour activer une alerte de sécurité ou le gel de sécurité sur votre dossier de crédit.
- Vos soupçons sont sérieux? **Contactez la police** ainsi que les **organismes publics** et tous **vos autres fournisseurs** pour vérifier les données à votre dossier.

Consultez également la
dernière section de ce guide sur les autres actions utiles
en cas de fraude.

Protégez-vous des arnaques sentimentales

Histoire inspirée de faits réels

L'histoire de Suzanne

Veuve depuis plusieurs années, Suzanne s'est inscrite sur un site de rencontre il y a quelques mois.

Au fil des semaines, elle a créé une relation particulière avec un homme de son âge, veuf lui-aussi.

Suzanne échange avec cet homme tant sur sa vie de tous les jours que sur toute une série de sujets qui l'intéressent. Peu à peu, elle élabore même des projets avec lui.

Un jour, le correspondant de Suzanne vit une situation difficile et lui demande de lui envoyer de l'argent.

Confiante dans la relation, Suzanne souhaite l'aider et lui envoie le montant dont il a besoin. Au fil des mois, elle envoie plusieurs sommes significatives à son nouvel amoureux en difficulté.

Mais un jour, l'homme met abruptement fin à la conversation lorsque Suzanne lui explique ne plus être capable de lui envoyer de nouveaux montants. Il ne répond plus à ses messages et semble s'être volatilisé avec l'argent déjà envoyé…

AUTRES PRÉTEXTES POUR VOUS CONTACTER

Pour parvenir à leurs fins, les fraudeuses et fraudeurs **manipulent vos sentiments**. Mais les fraudeuses et fraudeurs ont plus d'un tour dans leur sac… Pour vous mettre en confiance, ils peuvent **aussi se faire passer pour un de vos proches.**

La fraude du «petit-fils»

La fraude du «petit-fils» vise les grands-parents. Un escroc pourrait par exemple écrire un message à Suzanne sur les réseaux sociaux, en se faisant passer pour un de ses petits-enfants dans une situation difficile.

Dans son message, le faux petit-enfant explique avoir été arrêté par la police et avoir besoin d'argent pour se sortir de ce mauvais pas. Ou s'être fait voler son portefeuille lors d'un voyage à l'étranger.

Si Suzanne répond et envoie de l'argent pour aider, elle vient de succomber au stratagème du fraudeur.

Comment éviter de vivre l'histoire de Suzanne?

L'arnaque amoureuse est extrêmement répandue. Elle touche tous les genres, tous les âges, et toutes les catégories sociales. Y compris celles et ceux qui pensaient ne jamais se faire prendre.

Reconnaitre l'arnaque amoureuse

C'est louche si la personne avec qui vous correspondez sur un site de rencontre :

- trouve toujours une excuse pour **ne pas faire de rencontre vidéo ou en personne**.
- **propose rapidement de continuer la conversation ailleurs** que sur le site de rencontre, sur Whatsapp ou Messenger par exemple. C'est une stratégie classique des fraudeuses et fraudeurs, car les sites de rencontre suppriment régulièrement les faux profils de leur plateforme.
- vous **demande de l'argent**.

LE SAVIEZ-VOUS?

En 2021, les signalements d'arnaque amoureuse totalisaient plus de *60 millions* de dollars au Canada.

Reconnaitre la fraude du « petit-fils »

- Si un ou une de vos proches vous contacte pour un besoin d'argent urgent sans pouvoir vous parler au téléphone, **ne répondez pas au message que vous avez reçu**.
- **Recontactez votre proche** par téléphone ou via une autre adresse courriel ou un autre profil que vous avez l'habitude d'utiliser pour cette personne sur les réseaux sociaux, afin de vérifier qu'il s'agit bien d'elle.
- **Posez-lui des questions personnelles**, auxquelles votre proche seulement peut avoir les réponses.
- S'il n'est pas possible de recontacter votre proche, **appelez d'autres membres de son entourage** pour confirmer l'histoire qui vous est présentée.

Protégez-vous des arnaques sentimentales

Et aussi…

- Configurez les paramètres de vos comptes de **réseaux sociaux** : vos publications devraient être **visibles uniquement par les personnes que vous connaissez**.

  Dans le cas contraire, les fraudeuses et fraudeurs peuvent accéder aux photos et aux informations que vous publiez sur vous et votre famille. Ces escrocs les utilisent ensuite pour se rapprocher de vous ou se faire passer pour une ou un de vos proches.

Consultez également la
dernière section de ce guide sur les autres actions utiles
en cas de fraude.

Protégez vos investissements

Histoire inspirée de faits réels

L'histoire d'Amir

Depuis quelques temps, Amir s'intéresse aux possibilités d'investir ses économies. Il est membre d'un groupe Facebook d'entraide en investissement. Un matin, il reçoit un message d'une conseillère en investissement membre de ce même groupe Facebook. Cette conseillère lui vante quelques investissements qu'elle considère très prometteurs.

Amir accepte que la conseillère lui envoie le lien vers le site via lequel elle propose d'investir. Cela ne l'engage à rien.

Après avoir comparé les frais de transaction avec ceux demandés par sa banque, Amir opte pour ce site qu'il découvre.

Il investit d'abord un petit montant, pour tester. Mais après 3 semaines, les rendements sont exceptionnels. Il décide alors d'y investir la majorité de ses économies.

Deux mois plus tard, c'est la catastrophe : Amir a beau chercher, le site n'existe plus. La conseillère qui l'avait contacté s'est elle aussi volatilisée. Avec toutes ses économies…

AUTRES FORMES DE FRAUDE À L'INVESTISSEMENT

La fraude à l'investissement peut prendre d'autres formes. Certains fraudeurs ou fraudeuses peuvent vous inviter à transférer vos économies à l'étranger ou à réinvestir l'argent de vos REER. D'autres profitent de l'absence de réglementation en matière de cryptomonnaies (voir les pages suivantes).

Protégez vos investissements

Transférer ses économies à l'étranger

On pourrait vous proposer d'investir dans des pays où les impôts sur vos gains en investissements sont pratiquement nuls.

Attention à cet argument! Vous pouvez bien sûr investir à l'extérieur du pays. Mais **vous devez déclarer au Canada vos revenus d'investissement gagnés à l'étranger** et payer l'impôt canadien sur ces revenus.'

Si une conseillère ou un conseiller n'a pas de scrupule à vous proposer de contourner les lois pour vous éviter de payer de l'impôt, peut-être cette personne n'en aura aucun à disparaître avec votre argent!

LE SAVIEZ-VOUS?

Les personnes et les sites situés à l'étranger qui offrent des services d'investissement à des québécoises et des québécois doivent **aussi être inscrits à l'Autorité des marchés financiers** au Québec (AMF).

Si vous transférez vos économies à l'étranger, votre argent ainsi que votre fraudeuse ou fraudeur peuvent plus facilement devenir intraçables. Vous leur facilitez ainsi la tâche.

La fraude aux REER

Les fraudeuses et fraudeurs ciblent **régulièrement les personnes aînées** qui ont des sommes économisées dans leur Régime enregistré d'épargne retraite (REER) ou dans leur Fonds enregistré de revenus de retraite (FERR).

Ces escrocs vous attirent en proposant de sortir vos économies de votre REER ou de votre FERR en **promettant un rendement plus important** que celui accumulé actuellement.

Une technique frauduleuse consiste à **vous assurer que le retrait de votre REER/ FERR sera exempté d'impôt**. La raison avancée est que le nouvel investissement est lui-même soustrait à l'impôt.

Dans les faits, la fraudeuse ou le fraudeur **disparaît avec votre argent**. Vous pourriez en plus recevoir une demande de l'Agence du revenu du Canada et de Revenu Québec de **payer de l'impôt sur le retrait** que vous avez effectué.

Comment éviter de vivre l'histoire d'Amir?

Ne traitez qu'avec des sites Web ou personnes spécialistes en investissement inscrites auprès de l'Autorité des marchés financiers du Québec (AMF).

Seuls les personnes et les sites Web inscrits sont **encadrés**. Le risque de fraude diminue alors fortement.

De plus, un **fonds peut vous indemniser** en cas de fraude, à certaines conditions et pour un montant maximal. Toutefois, ce fonds n'intervient que si vous avez fait affaire avec une personne ou un site inscrit auprès de l'AMF.

LE SAVIEZ-VOUS?

L'**Autorité des marchés financiers** est un organisme gouvernemental qui encadre le secteur financier au Québec. Un de ses rôles est de protéger les particuliers.

Vérifier l'inscription à l'AMF est simple : visitez www.lautorite.qc.ca/grand-public/registres ou appelez au 1 877 525-0337.

Et aussi...

- **Méfiez-vous** des **placements avec promesse de rendements exceptionnels et garantis**. De tels placement **n'existent pas**.

  Une offre trop belle pour être vraie est généralement frauduleuse.
- **N'accédez pas à un site d'investissement via un courriel** qu'on vous envoie.

  Les fraudeuses et fraudeurs créent des répliques parfaites de sites internet légitimes, mais avec des adresses internet très légèrement différentes.
- **Aucune question** ne vous est posée **sur vos objectifs d'investissements et votre situation financière?** C'est suspect.

  La loi oblige les conseillères et conseillers en investissement à vous poser ces questions avant de vous recommander des placements.
- **Laissez-vous toujours un temps de réflexion et de vérification**.

  Méfiez-vous des courriels vous proposant des opportunités d'investissement accessibles seulement pour un temps limité. Une des techniques privilégiées des fraudeuses et fraudeurs est de vous forcer à agir dans l'urgence.

Protégez vos investissements

Et les cryptomonnaies ?

Vous avez peut-être ces personnes dans votre entourage : elles se vantent d'avoir fait des profits records en un temps limité en investissant dans les cryptomonnaies.

Quoi savoir…

Si vous souhaitez investir dans les cryptomonnaies?

- **L'anonymat** des investissements en cryptomonnaie **facilite la tâche des fraudeuses et fraudeurs**.
- Ne croyez pas celles et ceux qui vous disent que les cryptomonnaies sont des placements au rendement exceptionnel et garanti. Il y a **toujours un risque que le marché baisse, ou s'effondre**.
- Les **formations et séminaires sur les cryptomonnaies** sont une manière privilégiée par laquelle les fraudeuses et fraudeurs rentrent en contact avec vous, afin de vous donner confiance.
- Méfiez-vous des **offres pour transférer vos cryptomonnaies d'une plateforme à une autre**. Il peut s'agir d'une technique de fraude pour vous subtiliser vos investissements en cryptomonnaies.

Quoi faire…

Si vous décidez d'investir?

- **N'investissez** que via un **site inscrit auprès de l'Autorité des marchés financiers** du Québec (AMF). Seuls ceux-là sont **encadrés**. Le risque de fraude diminue alors fortement.

  Vérifier l'inscription est simple : visitez www.lautorite.qc.ca/grand-public/registres ou appelez au 1 877 525-0337

Procédures en justice en cas de fraude

La fraude est un crime, quelle que soit sa forme. Des poursuites en justice sont donc possibles si vous êtes victime de fraude.

Porter plainte à la police

Si vous portez plainte et que les services de police estiment avoir suffisamment de pistes à investiguer, ils ouvriront une enquête. Par la suite, si la police parvient à identifier les coupables de la fraude, il pourra y avoir une **poursuite au criminel**.

La **difficulté** est que les fraudeuses et fraudeurs agissent sous de faux-noms, et souvent depuis l'étranger. Il est donc difficile **de les retrouver**.

Si la procédure aboutit, les fraudeuses ou fraudeurs pourront être condamnés à une **peine de prison**.

Dans le cadre d'une telle plainte, il n'est **pas nécessaire d'être représenté par une avocate ou un a vocat**.

Procès au civil

Poursuivre vous-même la personne responsable de la fraude est possible. On parle alors de **procès au civil**.

Toutefois, il s'avère la plupart du temps **très difficile d'identifier** correctement votre fraudeuse ou votre fraudeur.

Si vous arrivez malgré tout à retrouver cette personne, vous pouvez demander qu'elle soit **condamnée à vous indemniser** pour les pertes et désagréments subis.

Vous aurez vraisemblablement **besoin d'une avocate ou d'un avocat** pour mener cette poursuite.

Avec la difficulté des poursuites en matière de fraude,
votre meilleure arme reste la prudence.

Autres actions utiles si vous avez été victime de fraude

Outre les mesures d'urgence à prendre en cas de fuite de données personnelles ou bancaires (pages 7-9), certaines actions peuvent être aidantes si vous avez été victime de fraude :

Signaler la fraude au Centre anti-fraude du Canada

Les signalements permettent aux autorités de mieux comprendre les stratégies des fraudeuses et fraudeurs et **aident à prévenir les futures fraudes**. En signalant votre histoire, vous évitez à d'autres de subir les mêmes désagréments que vous.

www.antifraudcentre-centreantifraude.ca ou 1-888-495-8501.

Contacter un Centre d'aide aux victimes d'actes criminels

En cas de fraude, les Centres d'aide aux victimes d'actes criminels (CAVAC) peuvent vous **orienter vers les ressources les plus appropriées** pour votre cas. Tant sur le plan légal et financier que sur le plan psychologique.

Les CAVAC peuvent aussi vous offrir un **service d'accompagnement**.

www.cavac.qc.ca ou 1-866-532-2822.

Signaler la fraude à l'Autorité des marchés financiers

Si vous avez été victime d'une fraude en matière d'investissement, signalez-la auprès de l' l'Autorité des marchés financiers (AMF) et vérifiez si vous avez accès au **fonds d'indemnisation des services financiers**.

www.lautorite.qc.ca ou 1-877-525-0337.

Pour bénéficier de l'intervention du fonds, il faudra entre autres que vous ayez investi via une personne ou un site inscrit auprès de l'AMF.

Visitez le site Web aineavise.ca/fraude pour plus de ressources afin de vous protéger.

La mission et les activités d'Éducaloi vous tiennent à cœur?

Faites un don!

Donnez | Éducaloi | Savoir, c'est pouvoir

Dons par chèque. Libellez votre chèque au nom de **«Éducaloi»**.
C.P.55032, CSP Notre-Dame 11, rue Notre-Dame Ouest Montréal (Québec) H2Y 4A7
educaloi.qc.ca

Questions droit?

educaloi.qc.ca

Facebook @Éducaloi

Instagram @educaloi / @educaloi_en

Twitter @educaloi

LinkedIn @Éducaloi