

lautorite.qc.ca



Soyez à votre affaire pour
ne pas perdre vos affaires!

Prévenez la fraude financière



**AUTORITÉ
DES MARCHÉS
FINANCIERS**



QUI SOMMES-NOUS ?

L'Autorité des marchés financiers (l'Autorité) est l'organisme mandaté par le gouvernement du Québec pour encadrer le secteur financier québécois et prêter assistance aux consommateurs de produits et services financiers. Elle se distingue par un encadrement intégré, notamment des domaines de l'assurance, des valeurs mobilières, des instruments dérivés, du courtage hypothécaire, des institutions de dépôts – à l'exception des banques – et de la distribution de produits et services financiers.

AVIS

L'AMF, sa direction et son personnel ne sont pas responsables des conséquences d'erreurs qui pourraient avoir été commises dans la rédaction du présent document. L'AMF vous propose ce guide à titre d'information. Elle n'offre aucun conseil sur l'achat de produits ou l'utilisation de services financiers particuliers. Les textes publiés n'ont aucune valeur légale.

L'information contenue dans ce document est à jour en date d'avril 2022.

Le présent document est disponible sur le site Web de l'AMF.

Dépôt légal – Bibliothèque et Archives nationales du Québec, 2019

978-2-550-85163-9 (version imprimée)

978-2-550-85164-6 (version électronique)

Au Québec, **1 personne sur 11** croit avoir été approchée par quelqu'un qui offrait un placement possiblement frauduleux¹. Sauriez-vous déceler les signes d'une fraude ?

Voici un guide qui vous propose en première partie 5 étapes pour vous aider à éviter la fraude financière. En seconde partie, il présente les principaux types de fraudes employés par les fraudeurs pour tenter de voler votre argent. Mieux vaut les connaître pour diminuer les risques de vous laisser tenter par une offre frauduleuse et vous éviter peut-être bien des ennuis.

Table des matières

Étape 1	4
Étape 2	5
Étape 3	7
Étape 4	8
Étape 5	9
1. L'hameçonnage	10
2. La fraude à la Ponzi	13
3. Les ventes pyramidales d'investissement	14
4. Les plateformes de négociation en ligne frauduleuses	15
5. La fraude utilisant des cryptoactifs ou des ICO	17
6. Les paradis fiscaux	18
7. La promotion de vente de titres (<i>pump and dump</i>)	19
8. Les fausses rumeurs pessimistes	19
9. Le rachat d'actions	20
10. La fraude REER ou les stratégies d'emprunt sur les REER	21
11. Le télémarketing frauduleux.....	23
12. Les groupes d'affinité	24
13. Un proche en détresse	24
14. La fraude sur l'assurance.....	25

¹ Source : Autorités canadiennes en valeurs mobilières (ACVM).
Sondage Indice ACVM des investisseurs 2017.

Étape 1

Avant d'investir, vérifiez si la personne ou l'entreprise qui vous offre un placement est autorisée à le faire. Faites également ces vérifications si une personne ou une entreprise vous offre de l'assurance.

Pour vérifier, communiquez avec le Centre d'information de l'AMF, au 1 877 525-0337.

Vous pouvez aussi consulter le [Registre des entreprises et des individus autorisés à exercer](http://lautorite.qc.ca), à lautorite.qc.ca.

Si la personne ou l'entreprise qui vous offre un placement n'est pas autorisée à le faire, communiquez avec l'AMF pour la dénoncer.

Ne vous laissez pas convaincre par une simple carte professionnelle ou un diplôme affiché sur un mur.

LE SAVIEZ-VOUS?

1/25

Proportion des répondants au sondage Indice ACVM des investisseurs 2017 qui ont indiqué avoir déjà été victimes d'une fraude financière.

Étape 2

Avant d'investir, exigez que l'on vous remette de l'information qui explique le placement offert. Assurez-vous de lire et de bien comprendre cette information.

Les documents reçus devraient notamment indiquer :

- › Le type de placement (action, obligation, etc.)
- › Les risques à investir
- › La possibilité ou non d'avoir accès à votre argent au besoin et, si c'est possible, à quelles conditions
- › Les frais associés au placement

Un fraudeur pourrait vous transmettre de faux documents d'information sur un placement. Vérifiez que les documents fournis se trouvent sur le site de SEDAR, à sedar.com. Ce site renferme les données exigées par les membres des Autorités canadiennes en valeurs mobilières (ACVM), dont l'AMF fait partie. Si vous n'obtenez pas de l'information écrite et fiable, mieux vaut ne pas investir.

Assurez-vous que les relevés de compte et de transactions que vous recevez sur vos placements ne proviennent pas seulement de votre représentant, mais aussi de l'institution où votre argent est investi. Cette institution devrait également être inscrite au [Registre des entreprises et des individus autorisés à exercer](#) de l'AMF.



Étape 2 (suite)

Si vous désirez vous procurer (souscrire) une assurance, vous ne recevrez possiblement pas le contrat avant la souscription. Exigez néanmoins de vous faire expliquer les points importants du contrat (la police), notamment les garanties offertes, le coût de l'assurance et les exclusions.

Dès réception de votre contrat d'assurance, lisez-le pour vous assurer qu'il est conforme à ce qui vous a été vendu et pour prendre connaissance de toutes les modalités. Si vous n'êtes pas satisfait, faites-en immédiatement part à l'assureur. Plusieurs assureurs offrent la possibilité d'annuler la police sans frais dans les 10 jours suivant la réception du contrat.

Ne déposez jamais vos documents confidentiels – comme un relevé de placement ou de carte de crédit, ou une déclaration de revenus – dans votre bac de récupération. Un fraudeur pourrait utiliser l'information qu'on y trouve. Déchiquez ces documents.



Étape 3

Assurez-vous que le placement offert n'est pas trop beau pour être vrai.

Dans presque tous les cas, plus le rendement que vous espérez d'un placement est élevé, plus vous devez être prêt à supporter un risque important. C'est une règle de base en matière de placement.

Si on vous offre un rendement supérieur à ce qui est offert sur le marché, et ce, sans le moindre risque, vous pouvez douter du sérieux de l'offre.

Si on vous dit que le placement est garanti, demandez-vous :

- ▶ Qui garantit le placement? Si c'est un individu qui le garantit, c'est douteux. Normalement, un placement peut être garanti par une institution financière ou, dans le cas d'un dépôt, par le [Régime de protection des dépôts](#) de l'AMF ou de la Société d'assurance-dépôts du Canada.
- ▶ Qu'est-ce qui est garanti? Le rendement, la somme investie, ou les deux?
- ▶ Y a-t-il des frais pour profiter de cette garantie?
- ▶ Quelles sont les conditions pour profiter de la garantie? Faut-il conserver le placement pendant cinq ans, dix ans, vingt ans?

De la même manière, si on vous offre une assurance trop belle pour être vraie, méfiez-vous!

Si on vous promet un rendement élevé à faible risque, questionnez-vous sur le placement offert et la personne qui vous le présente! Aucun placement n'offre des rendements élevés sans risque. Si c'était le cas, tout le monde investirait dans ce placement. De plus, ne vous laissez pas avoir sous prétexte que les quantités sont limitées ou qu'il s'agit d'une occasion pour quelques privilégiés.

Étape 4

Méfiez-vous des belles paroles souvent utilisées par les fraudeurs :

- » « J'ai une source fiable, la valeur de ce placement fera un bond vertigineux. C'est garanti. »
- » « J'y ai moi-même investi tout mon argent et celui de mes parents. »
- » « Si vous êtes insatisfait, je vous rembourse. »

Ces énoncés visent à vous démontrer que le placement ne présente aucun risque et qu'il convient à tout le monde. Dans les faits, cela ne vous donne aucune garantie.

- » « Vous faites partie d'un club sélect. Vous êtes un des rares privilégiés à pouvoir profiter de cette offre exceptionnelle. »
- » « Très peu de gens le savent, mais l'entreprise est sur le point d'être achetée et sa valeur va doubler. »
- » « La société va être cotée en bourse bientôt. »
- » « Le gouvernement va leur accorder un brevet. »

Ces énoncés tentent de vous faire croire que le fraudeur dispose d'une information privilégiée qui s'avère fautive en fait.

Attention au délit d'initié!

Un délit d'initié est un acte illégal qui consiste à acheter ou à vendre des titres en utilisant une information qui n'est pas accessible au public. La communication d'information privilégiée peut également être considérée comme un délit d'initié. Une information privilégiée est une information qui, si elle était publique, pourrait influencer le prix d'une action à la bourse.

- » « Vous devez absolument investir aujourd'hui : demain, ce sera trop tard. »
- » « Il y a une brèche dans la loi. Nous pouvons ainsi éviter de payer de l'impôt. Gardez le secret... N'en parlez même pas à votre famille. La loi pourrait être modifiée. »

Le fraudeur ne veut pas vous laisser le temps de réfléchir ou de consulter des proches ou un organisme comme l'AMF.

- » « L'AMF a approuvé le placement. »

Sachez que l'AMF n'approuve pas de placements. Elle autorise plutôt des individus et des entreprises à offrir des placements ou de l'assurance.

Étape 5

Ne vous laissez pas convaincre par des comportements douteux. Par exemple, la personne qui vous offre un placement :

- ▶ Trouve trop souvent des points semblables entre votre situation et la sienne.
- ▶ Vante ses compétences et ses succès de façon démesurée.
- ▶ Vous culpabilise si vous ne prenez pas les placements qu'elle vous offre, ou si vous mettez en doute ses affirmations.
- ▶ Refuse de dire pour quelle firme elle travaille ou tente de changer de sujet après vous avoir donné très peu d'information.
- ▶ Communique avec vous de façon répétitive.
- ▶ Fait pression sur vous pour que vous investissiez dans le placement proposé.
- ▶ Vous demande d'investir en faisant un chèque à son nom ou en lui remettant de l'argent comptant.
- ▶ Ne vous pose pas de questions pour connaître votre [profil d'investisseur](#).

ATTENTION!

Bien que les points précédents ne cachent pas à coup sûr une tentative de fraude, une fraude peut découler de ces situations. Redoublez de prudence si vous en êtes témoin!

LES APPARENCES SONT PARFOIS TROMPEUSES!

Méfiez-vous des personnes qui vous offrent d'investir tout en étalant leur prétendue richesse ou en prétendant connaître d'influents personnes. Avant tout, faites les vérifications appropriées sur cette personne et l'entreprise qu'elle représente auprès de l'AMF.

VOICI 14 TYPES DE FRAUDES FINANCIÈRES PARMIS LES PLUS COURANTS ET QUELQUES TRUCS POUR S'EN PROTÉGER

1. L'hameçonnage

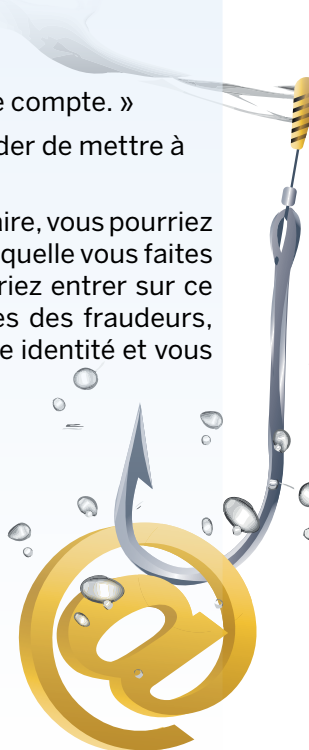
L'hameçonnage est une technique frauduleuse qui consiste à faire croire à la victime qu'elle s'adresse à une entité de confiance, par exemple une institution financière ou un gouvernement, dans l'objectif de lui soutirer des renseignements personnels et de l'argent.

Exemple : vous recevez un courriel ou un texto non sollicité d'une société avec laquelle vous faites affaire. On vous demande de mettre à jour immédiatement vos renseignements personnels.

Rappelez-vous que les fraudeurs ne manquent jamais d'imagination pour mettre la main sur votre argent et peuvent invoquer plusieurs raisons pour le faire. Par exemple :

- » « La société a été victime d'une fraude. »
- » « On a repéré des opérations anormales dans votre compte. »
- » « Une nouvelle loi oblige l'institution à vous demander de mettre à jour vos renseignements. »

Si vous cliquez sur le lien fourni pour remplir le formulaire, vous pourriez voir une copie conforme du site de l'institution avec laquelle vous faites affaire. En réalité, toute l'information que vous pourriez entrer sur ce FAUX site irait directement dans la base de données des fraudeurs, qui pourraient ensuite vider votre compte, voler votre identité et vous causer bien des ennuis pour plusieurs années.



Pour éviter cette fraude :

- ▶ Si vous croyez devoir répondre à un tel message demandant des renseignements personnels, utilisez les coordonnées que vous possédez déjà. Surtout, n'utilisez pas les coordonnées fournies dans le courriel ou le texto non sollicité, ne cliquez pas sur les liens et n'ouvrez aucune pièce jointe. Ne cliquez JAMAIS sur un lien reçu dans un courriel ou un texto non sollicité qui vous demande de l'information bancaire ou personnelle avant d'avoir fait les vérifications nécessaires.
- ▶ Ne soyez pas intimidé par un courriel ou un texto qui vous met en garde contre des conséquences désastreuses qui pourraient survenir si vous ne suivez pas les consignes qui y sont indiquées.
- ▶ Si vous n'étiez pas déjà informé sur l'envoi d'un tel message, communiquez avec l'institution ou l'organisme visé pour lui signaler ce qui vous arrive, à l'aide du vrai numéro de téléphone trouvé sur son site, et non celui indiqué dans le courriel ou le texto.
- ▶ Tapez vous-même l'adresse complète du site que vous désirez consulter.



L'hameçonnage vise également les entreprises

L'hameçonnage est un véritable fléau à l'échelle de la planète. Les victimes peuvent aussi bien être des personnes que des entreprises.

Dans ce dernier cas, les fraudeurs peuvent réussir à se faire passer pour le président de l'entreprise visée, envoyer un courriel à leur victime, qui est réellement à l'emploi de l'entreprise, et tenter de la convaincre d'effectuer certaines actions. Par exemple, ils peuvent demander de transférer des fonds d'un compte à un autre compte.

Afin de donner plus de crédibilité à leur courriel, qui semble provenir de l'adresse courriel du président, les fraudeurs peuvent mentionner que certains points doivent être respectés afin de suivre la réglementation de l'AMF, par exemple.

Les fraudeurs peuvent même indiquer que le destinataire du courriel a été choisi parce qu'il est digne de confiance. On lui demande alors de transmettre des données bancaires ou de faire un virement bancaire vers une personne externe et de demeurer discret pour respecter la procédure de l'AMF ou de tout autre organisme de réglementation.

Pour éviter d'être victime de l'hameçonnage et d'un possible vol d'identité, ne répondez jamais à ce type de courriel et n'hésitez pas à dénoncer rapidement la situation en communiquant avec le Centre d'information de l'AMF. Vérifiez toujours la légitimité de la demande en appelant vous-même à l'institution concernée.



2. La fraude à la Ponzi

La fraude à la Ponzi consiste à prendre des sommes appartenant à un investisseur pour payer de faux rendements à d'autres investisseurs ou simplement pour rembourser les investisseurs qui veulent récupérer leur argent. Les fraudeurs peuvent ainsi donner une fausse impression que l'argent investi rapporte de bons rendements et qu'il n'y a aucun problème pour récupérer l'argent investi.

Le plus souvent, une fraude à la Ponzi est découverte une fois que le fraudeur a disparu ou qu'il ne peut plus répondre aux demandes de retrait des placements. Il est alors trop tard puisqu'il n'y a plus d'argent dans les comptes. La fraude à la Ponzi peut être combinée à plusieurs autres types de fraude.

Exemple

Vous investissez 1 000 \$ dans un placement offert par Luc, un fraudeur. Après seulement une semaine, vous recevez un chèque de 100 \$ de la part de Luc, qui vous explique que c'est le revenu généré par votre investissement de 1 000 \$.

Malheureusement, dans les faits, aucun rendement n'a été réalisé sur vos 1 000 \$. En fait, Luc a utilisé une partie de votre investissement pour vous payer 100 \$ de faux « bénéfices ». En agissant de la sorte, il espère que vous investirez davantage dans le placement ou que vous convaincrez d'autres personnes d'y investir. Aussi, Luc dépense lui-même une bonne partie des sommes que vous lui avez versées.



3. Les ventes **pyramidales** d'investissement

Les ventes pyramidales d'investissement sont des systèmes de vente de produits (par exemple des placements) pour lesquels les profits proviennent principalement du recrutement de nouveaux membres. Le produit vendu est un prétexte pour recruter des membres.

Les personnes qui utilisent cette technique ne diront pas qu'il s'agit d'une vente pyramidale.

Il existe plusieurs variantes à cette fraude.

Exemple

On vous offre d'investir dans un placement très prometteur qui devrait rapporter un rendement important. Vous devez conserver le placement un certain temps, par exemple six mois. En plus de faire un excellent rendement sur le placement, vous pouvez faire plus d'argent en recrutant des investisseurs qui profiteront à leur tour de ce placement « exceptionnel ». Par exemple, on vous demande de recruter deux personnes. Pour chaque investisseur recruté, vous obtenez une commission, généralement un pourcentage des sommes investies par vos recrues. Pour chaque investisseur que ces dernières recrutent à leur tour, vous empochez une commission supplémentaire.

LA FRAUDE

En réalité, il n'y a pas de placement miraculeux. Les fraudeurs utilisent votre propre argent pour vous payer vos revenus de placements et vos commissions de recrutement (fraude à la Ponzi). Lorsque les fraudeurs sentent que la fraude sera bientôt découverte, ils disparaissent avec votre argent.

Prenez garde lorsqu'on vous promet de l'argent pour recruter de nouveaux investisseurs, partenaires ou collaborateurs, peu importe la façon dont ils sont nommés par les fraudeurs.

ATTENTION!

Les personnes qui organisent des ventes pyramidales de même que celles qui y participent sont passibles de poursuites judiciaires.

4. Les plateformes de négociation en ligne frauduleuses (faux sites de courtage en ligne)

Vous désirez investir en ligne et vous trouvez un site de négociation prometteur. Ou encore, des fraudeurs vous contactent pour vous inciter à investir sur une plateforme de négociation où vous réaliserez, selon eux, des gains très importants sans trop de risques. Ils vous offrent même d'investir simplement 100 \$. Vous investissez. Le lendemain, votre investissement de 100 \$ vaut 150 \$. Les fraudeurs vous rappellent pour vous demander si vous désirez investir davantage.

Soyez vigilant!

- Certains promoteurs de ce type de plateformes frauduleuses vont même jusqu'à utiliser faussement le nom de personnes inscrites à l'AMF et à vous référer à notre [Registre des entreprises et des individus autorisés à exercer](#) pour que vous fassiez une vérification.
- Ils offrent souvent des produits financiers réels (ex. : devises, dérivés sur cryptomonnaie, actions de compagnies comme Amazon, Google, Apple). L'offre s'adapte aux tendances et porte généralement sur le produit qui suscite le plus d'intérêt dans les médias. En réalité, votre argent ira dans leurs poches et vous ne recevrez pas les produits financiers.
- Ils publient des témoignages positifs sur des sites d'avis (ex. : communautés d'utilisateurs, blogs) et sur les médias sociaux.
- Dans certains cas, ils vous offriront des formations gratuites qui vous vanteront grandement les avantages d'investir sur leur site de négociation en ligne.
- Dans d'autres cas, vous pourrez vous pratiquer à tenter de gagner des sommes en utilisant la plateforme de négociation fournie. Lors de ces tests, il peut arriver que la plateforme soit truquée pour que vous gagniez souvent. Cela vous incitera à investir davantage, mais la réalité pourrait être fort différente lorsque vous investirez avec votre véritable argent.
- Méfiez-vous des promesses trop belles pour être vraies. Par exemple :
 - « Devenez un pro du FOREX en quelques jours! »
 - « Vous ne pouvez pas perdre. »
 - « Investissez sans risque! »
 - « Enrichissez-vous sans efforts en restant à la maison! »
 - « Utilisez notre logiciel infaillible pour faire de l'argent! »

Pour éviter ce type de fraude

- › Validez l'inscription du courtier auprès de l'AMF. Pour ce faire, rappelez la personne au numéro de téléphone qui se trouve dans le registre de l'AMF et non au numéro qu'elle vous donne.
- › Si on vous demande d'investir en utilisant une carte de crédit, posez-vous des questions. Vous ne devriez jamais le faire!

Pour plus d'information sur ce type de fraude, consultez le site de l'AMF.

Prenez garde à la fraude sur le marché des devises - FOREX

À la base, il n'y a rien d'illégal à investir sur le marché des devises. Méfiez-vous toutefois des faux sites transactionnels et assurez-vous que l'investissement correspond à votre profil d'investisseur! Les fraudeurs ont l'habitude de suivre les tendances et les nouveaux produits pour les mettre au cœur de leurs approches frauduleuses, qui demeurent sensiblement les mêmes : opérer sans en avoir l'autorisation et chercher à voler votre argent et vos renseignements personnels.



5. La fraude utilisant des cryptoactifs ou des ICO

L'investissement dans des cryptoactifs présente de nombreux risques. Même s'il n'est pas illégal en soi, il est sujet à de nombreux types de fraude. Voici quelques fraudes classiques :

- › Certains fraudeurs opèrent par **l'émission d'un faux cryptoactif**. Ils peuvent se donner de bonnes intentions pour se démarquer et attirer des victimes (projet communautaire, humanitaire, socialement responsable, etc.). Les transactions ne s'inscrivent pas sur une chaîne de blocs publique (*blockchain*), mais uniquement sur le réseau des fraudeurs.
- › Les fraudeurs peuvent aussi procéder avec une **plateforme de négociation de cryptoactifs truquée**. Par exemple, vous achetez des cryptoactifs sur la plateforme, puis vous en voyez la valeur augmenter. En réalité, les fraudeurs ont programmé la plateforme pour que vous voyiez les sommes investies prendre de la valeur comme leurs fausses promesses l'annonçaient. Dans les faits, les sommes que vous investissez se retrouvent directement dans les poches des fraudeurs sans que vous vous en rendiez compte. Même si la plateforme peut avoir l'air très professionnelle, ce que vous voyez à l'écran ne représente aucunement la réalité.
- › Certains fraudeurs vous persuadent de faire l'acquisition de cryptoactifs sur une plateforme. Après avoir faussement construit une relation de confiance, ils pourront prétendre vous aider à hausser vos rendements en **transférant vos cryptoactifs sur une autre plateforme**. En fait, la deuxième plateforme est frauduleuse et affiche de faux résultats. Vos cryptoactifs ont été volés et vous ne pourrez pas les récupérer.
- › Certains fraudeurs pourraient aussi **utiliser les fonds recueillis lors d'une ICO à d'autres fins** que celles précisées dans la présentation du projet.
- › Certains fraudeurs peuvent proposer de vous aider à **récupérer les sommes perdues** en cas de fraude impliquant des cryptoactifs. Ils facturent des **frais payables à l'avance**, mais ne vous fournissent aucun service. Ils demandent aussi parfois de partager des informations personnelles, qu'ils utilisent ensuite pour vous frauder sans vous aider à récupérer les sommes perdues.

Pour éviter ce type de fraude

- › Soyez sur vos gardes si l'entreprise qui gère la plateforme n'a pas d'adresse civique au Canada ou si la personne qui vous contacte et avec qui vous souhaiteriez transiger est à l'extérieur du pays.
- › Comprenez bien le produit offert avant d'y investir. Faites des recherches auprès de plusieurs sources et n'hésitez pas à contacter l'[Autorité des marchés financiers](#).
- › Méfiez-vous des offres trop belles pour être vraies. De gros rendements sans risque, ça n'existe pas.
- › Refusez de transférer vos cryptoactifs d'une plateforme à une autre qui n'est pas inscrite à l'Autorité.
- › Ne confiez jamais vos mots de passe ou le contrôle de votre ordinateur à quiconque, particulièrement à un inconnu qui prétend vouloir vous aider à investir.
- › Évitez les offres d'investissement faites sur les réseaux sociaux ou provenant d'un inconnu que vous n'avez pas sollicité.

6. Les paradis fiscaux

De manière simplifiée, un paradis fiscal est un endroit dans le monde où l'impôt est très faible ou même nul. Pour vous attirer, les fraudeurs vous offrent d'y investir. Ils peuvent vous dire que c'est légal, mais que vous ne devez pas partager cette information, car les lois pourraient être modifiées pour fermer la brèche du système.

Investir à l'étranger n'est pas illégal. C'est toutefois illégal de ne pas déclarer les revenus et les gains sur ces placements. Si une personne est prête à vous aider à contourner les lois pour que vous payiez moins d'impôt, elle pourrait ne ressentir aucune culpabilité à se sauver avec votre argent!

Dans les faits, les fraudeurs n'ont pas choisi le paradis fiscal au hasard. Ils ont investi les sommes dans un pays pour lequel il est pratiquement impossible pour les organismes qui appliquent les lois de retracer les sommes.



7. La **promotion** de vente de titres (*pump and dump*)

Vous lisez des nouvelles qui vous laissent croire que la valeur d'un titre (le plus souvent une action) augmentera de façon importante. Vous recevez l'information sur des forums de discussion, sur les médias sociaux et par la voie de communiqués de presse. Vous achetez le titre comme plusieurs autres investisseurs, ce qui en fait augmenter le prix. Il ne vous reste plus qu'à attendre que la valeur du titre augmente encore plus, comme prévu. Erreur! Voilà que la valeur du titre tombe soudainement à presque rien. Vous avez tout perdu. Que s'est-il passé?

Puisque le titre est peu liquide (la demande pour le titre est relativement faible), un seul acheteur peut faire augmenter significativement le prix. L'inverse est aussi vrai : un seul vendeur peut faire diminuer rapidement la valeur du titre. Les fraudeurs possèdent une grande quantité du titre que vous avez acheté. Ils l'ont obtenu à un prix très faible et vous le vendent à un prix plus élevé en raison de l'engouement qu'ils ont frauduleusement suscité. Vous payez donc beaucoup trop cher pour un titre qui ne vaut rien. L'entreprise dans laquelle vous avez investi ne possède pas d'actif. Vous vous retrouvez donc avec un placement sans valeur.

Pour éviter cette fraude, demandez-vous ce que les gens gagnent à vous donner des tuyaux sur des placements.

8. Les **fausses rumeurs** pessimistes

C'est l'inverse de la fraude précédente. Ici, les fraudeurs font circuler de l'information qui vous laisse croire que la valeur d'un titre peu liquide risque de baisser beaucoup et qu'il faut le vendre. Vous vendez le titre, comme beaucoup d'autres personnes qui ont vu l'information, ce qui fait chuter rapidement le cours du titre. Les fraudeurs en profitent alors pour l'acheter à un prix peu élevé.

9. Le rachat d'actions

Vous avez subi des pertes importantes sur vos placements : prenez garde aux fraudeurs!

Certains fraudeurs profitent du fait que vous avez subi des pertes sur vos placements pour vous faire une offre difficile à refuser : on vous offre de racheter vos placements à un prix plus élevé que leur valeur réelle. Par exemple, vous aviez payé 2 \$ pour chaque action. Ces actions ne valent plus que 0,06 \$ aujourd'hui. On vous offre de vous les racheter pour 1 \$ l'action. On vous explique que certaines personnes ont intérêt à vous acheter vos actions plus cher que leur valeur, car elles obtiennent alors des pertes en capital qui leur feront épargner beaucoup d'impôt.

En acceptant cette offre, vous devrez toutefois payer des frais importants pour effectuer le transfert. Ces frais étant payés, les fraudeurs disparaissent avec cet argent et « oublient » de vous racheter vos actions.

10. La fraude REER ou les stratégies d'emprunt sur les REER

On vous indique que vous pouvez profiter immédiatement des sommes déposées dans votre REER*, et ce, sans payer d'impôt. Pour ce faire, on vous offre de transférer les sommes que vous y avez investies dans un placement qui vous rapportera un rendement très intéressant. On vous indique que ce placement est également admissible au REER : c'est pourquoi vous ne paierez pas d'impôt.

Les fraudeurs ont tellement confiance en ce placement qu'ils vous offrent de vous remettre en argent comptant une avance sur le rendement futur. Par exemple, si vous investissez 50 000 \$, ils pourraient vous remettre 25 000 \$ comptant. Les fraudeurs vous expliquent que vous ne risquez rien et vous disent : « De toute façon, si vous aviez sorti l'argent de votre REER, vous auriez dû en remettre la moitié pour payer l'impôt applicable. »

* Il peut également s'agir d'un compte de retraite immobilisé (CRI), d'un régime de retraite ou d'autres sommes enregistrées.



Que risquez-vous à investir dans ce placement?

- ▶ Votre argent n'a jamais été investi dans le placement en question au taux de rendement incroyable. Vous risquez d'avoir plutôt investi dans une société qui ne vaut rien ou qui appartient aux fraudeurs. Vos 50 000 \$ sont donc perdus. De plus, le placement n'est pas admissible au REER, contrairement à ce que vous avaient dit les fraudeurs.
- ▶ L'Agence du revenu du Canada pourrait ainsi vous envoyer un avis vous indiquant que vous avez retiré des sommes de votre REER et que vous n'avez pas payé l'impôt applicable. Vous pourriez devoir payer les impôts correspondants. Pour rembourser les impôts, vous risquez de perdre les 25 000 \$, si généreusement offerts par les fraudeurs (il s'agit de votre argent).

Les sommes que vous retirez de vos REER, CRI ou fonds de pension sont bel et bien imposables.

Il existe plusieurs variantes à cette fraude. Par exemple, certains fraudeurs vous diront que pour sortir votre argent de votre REER sans payer d'impôt, vous devez d'abord transférer votre REER chez un « courtier en ligne » (courtier à escompte). Pour donner de la crédibilité à leur stratagème, les fraudeurs peuvent vous laisser choisir le courtier que vous préférez. Ils vous demanderont ensuite vos mots de passe pour accéder à vos comptes en vous disant qu'ils vont les gérer pour vous. Les fraudeurs utiliseront ensuite cette information pour vider vos comptes dès qu'ils en auront l'occasion.

ATTENTION!

Certains fraudeurs demandent de signer des procurations soi-disant pour vous faire profiter d'offres qui semblent intéressantes. Dans les faits, ils utilisent ces procurations pour vider votre compte.

11. Le **télémarketing** frauduleux

Vous recevez un appel téléphonique d'un inconnu qui vous offre d'investir dans un placement exceptionnel. En effet, en plus d'offrir un rendement nettement supérieur à toute autre forme de placement, ce placement ne comporterait aucun risque.

Ne vous laissez jamais avoir par ce genre d'appel non sollicité. En fait, n'investissez tout simplement jamais au téléphone si un inconnu vous appelle pour investir. Vous risquez de mettre votre argent directement entre les mains d'un fraudeur.

Le faux message sur la boîte vocale

Vous avez un message sur votre boîte vocale.

« Sylvie, c'est Paul. J'ai perdu ton ancien numéro et Johanne m'a dit que ceci est ton nouveau numéro, j'espère que c'est le bon. Est-ce que tu te souviens du gars qui m'aide à investir? Il avait fourni un bon tuyau à mon père. Le placement en question a doublé en moins d'un mois et je me souviens que tu étais déçue de ne pas en avoir été informée. Bien, j'ai un nouveau tuyau de mon ami.

L'entreprise XYZ est sur le point de lancer un produit révolutionnaire; ce sera annoncé plus tard cette semaine. C'est le temps d'acheter des actions, la valeur augmentera considérablement sous peu. Mon ami dit qu'il faut investir tout de suite. J'en achète demain et mon père aussi. Je suis sur la route aujourd'hui, rappelle-moi sur mon cellulaire au XXX-XXXX. À bientôt! »

Vous ne connaissez pas Paul, ni Sylvie. Dans les faits, on tente de vous manipuler. Si vous rappelez au numéro laissé dans votre boîte vocale, on vous offrira d'investir dans le placement (frauduleux) et vous perdrez votre argent. Ce message a peut-être été laissé sur des milliers de boîtes vocales. Cette manœuvre se fait également par courriel, par texto et sur Internet.



12. Les groupes d'affinité

Les fraudeurs s'associent avec des gens qui partagent les mêmes croyances ou les mêmes intérêts afin de repérer de potentielles victimes. Comme pour d'autres types de fraudes, ils n'hésiteront pas à étaler, d'abord subtilement, puis avec plus d'éclat, leurs succès et leurs richesses. Ils créeront des liens et vous proposeront ensuite des placements « exceptionnels ». Il se peut même que leurs victimes fassent elles-mêmes les premiers pas pour investir et profiter de fabuleux rendements. Dans certains cas, ils vous demanderont de ne pas ébruiter l'affaire, car c'est une occasion en or qu'ils ne veulent partager qu'avec leurs amis. Dans les faits, le fraudeur est le seul à bénéficier de cette occasion en or!

Si la personne qui vous offre des placements est un de vos amis, soyez aussi critique que si c'était un étranger. Même s'il s'agit d'un ami, vérifiez s'il est autorisé à vendre le placement qu'il vous offre (voir page 4).

13. Un proche en détresse

Un fraudeur vous écrit sur Facebook ou un autre réseau social, ou vous téléphone. Il parvient à se faire passer pour un de vos proches et vous explique qu'il se trouve dans une situation difficile et qu'il a immédiatement besoin de votre aide financière. Par exemple, il s'est injustement fait arrêter en voyage et il a besoin d'argent pour payer une amende, sinon il sera emprisonné dans des conditions affreuses.

Soyez prudent! Certains fraudeurs arrivent à prendre l'identité d'une connaissance pour extorquer de l'argent. Si un proche semble se trouver dans une situation abracadabrante et qu'il vous demande de l'argent, posez-lui des questions auxquelles seule cette personne peut répondre, par exemple, le nom du conjoint d'une amie commune. Surtout, ne posez aucun geste sans avoir vérifié son identité et en avoir parlé avec des proches.

14. La fraude sur l'assurance

Un représentant de la société d'assurance XYZ évalue vos besoins d'assurance et vous vend une assurance à un prix très compétitif. Pour que votre assurance entre en vigueur, vous devez payer la prime en argent comptant ou faire un chèque à l'ordre du représentant, car ce dernier encaisse sa commission et transfère électroniquement la différence à l'assureur. Vous serez ainsi assuré le jour même.

Quelques mois plus tard, vous mettez de l'ordre dans vos papiers et vous vous demandez pourquoi vous n'avez pas reçu une confirmation d'assurance. Vous tentez de téléphoner au représentant, mais le numéro de téléphone qu'il vous avait donné est celui d'une pizzeria d'une ville voisine. Vous téléphonez donc à l'assureur XYZ. Vous apprenez que le représentant ne travaille pas pour cette société! En fait, il ne travaille pour aucun assureur : il travaille pour lui-même.

Vous avez remis des sommes à un fraudeur. Il vend de fausses assurances et empêche les primes versées par les clients. Il vend de l'assurance vie, automobile, habitation, et même des placements!



On n'entend pas beaucoup parler de ce type de fraude. La victime ne perd souvent que le montant de la prime, soit des sommes beaucoup moins importantes que dans le cas de certaines fraudes sur les placements. Mais qu'arriverait-il si vous subissiez un sinistre « couvert » par la fausse assurance? La perte pourrait être très importante!

Pour éviter cette fraude :

- 】 Vérifiez que la personne qui vous offre l'assurance est autorisée à vous la vendre. Pour ce faire, appelez le Centre d'information de l'AMF. Vous pouvez également consulter le [Registre des entreprises et des individus autorisés à exercer](#) sur le site de l'AMF.
- 】 Appelez l'assureur pour confirmer que votre assurance est en vigueur.
- 】 Payez votre prime au moyen d'un paiement au nom de l'entreprise inscrite à l'AMF. Il peut s'agir d'un cabinet en assurance ou d'un assureur. Ne faites jamais le chèque au nom de la personne qui vous offre l'assurance.



VOS RENSEIGNEMENTS PERSONNELS ONT ÉTÉ VOLÉS?

On a soutiré une information importante et personnelle vous concernant, par exemple un mot de passe, votre date de naissance, votre numéro de carte de crédit, le montant de votre salaire ou même votre numéro d'assurance sociale (NAS)? Malheureusement, des personnes mal intentionnées pourraient se servir de vos renseignements pour commettre une fraude. Voici quelques conseils pour limiter les ennuis.

Si vous pouvez vous inscrire gratuitement à un service de surveillance de crédit, faites-le. Ce service surveille votre dossier pour déceler des informations inhabituelles et vous recevez une alerte en cas de transaction inhabituelle.

DEMEUREZ VIGILANT!

Malgré tous ses avantages, l'inscription à un service de surveillance de votre dossier de crédit n'est pas une garantie absolue contre la fraude.

- ▶ Surveillez régulièrement vos relevés de comptes bancaires et de cartes de crédit ainsi que toute nouvelle facture reçue par la poste. Signalez immédiatement toute activité suspecte à votre institution financière.
- ▶ Consultez votre dossier de crédit auprès des principaux bureaux de crédit ([Equifax](#) et [TransUnion](#)) de façon régulière pour voir s'il contient des erreurs.
- ▶ Vous pourriez aussi placer un message d'alerte à la fraude auprès de ces mêmes bureaux de crédit (des frais peuvent être exigés). Ce message indique aux prêteurs qui consultent votre dossier qu'ils doivent porter une attention particulière aux demandes de crédit vous concernant et qu'ils doivent confirmer votre identité avant d'accepter toute demande.
- ▶ En cas de besoin, contactez votre service de police.

MÉFIEZ-VOUS DES SITUATIONS SUIVANTES

Ne vous fiez pas aveuglément à votre afficheur!

Certains fraudeurs peuvent modifier le numéro et le nom apparaissant sur votre afficheur pour vous faire croire que l'appel provient par exemple de votre institution financière ou d'un organisme public.

- ▶ Vous recevez un courriel ou un texto semblant provenir d'un organisme public ou d'une société avec laquelle vous faites affaire. On vous demande de mettre à jour immédiatement vos renseignements personnels ou de cliquer sur un lien fourni dans le courriel. Attention! Il pourrait s'agir d'une tentative d'hameçonnage (voir fraude 1).
- ▶ On vous offre de protéger votre ordinateur en y accédant à distance afin d'installer les mises à jour, antivirus et autres systèmes requis. Ne permettez jamais à des inconnus d'accéder à votre ordinateur à distance.
- ▶ Vous recevez un relevé de compte de carte de crédit par la poste qui indique des dépenses que vous n'avez pas faites. Appelez votre émetteur de carte de crédit à l'aide du vrai numéro de téléphone. N'utilisez pas le numéro figurant sur le relevé. Certains fraudeurs inventent de faux relevés en indiquant un numéro de téléphone qui leur appartient. Si vous les contactez, ils vous demandent des renseignements personnels soi-disant pour vérifier votre identité.
- ▶ On vous offre un service pour modifier votre numéro d'assurance sociale (NAS) moyennant certains frais.

REFUSEZ! Sachez que Service Canada n'attribue pas un nouveau NAS à la suite de la fuite de renseignements personnels. Aussi, ne conservez pas votre NAS sur vous : cachez le numéro dans un endroit sûr.



LE SAVIEZ-VOUS ?

La cybersurveillance

L'AMF dispose d'une équipe d'enquêteurs spécialisés en cybersurveillance. À l'aide de logiciels spécialisés, cette équipe veille à la détection des personnes et des entreprises qui offrent des produits financiers aux investisseurs québécois sans être dûment autorisées pour le faire. De plus, les enquêteurs surveillent les activités de certains sites considérés comme suspects.

Selon les cas, ces enquêteurs font de l'infiltration et amènent l'AMF à déposer des demandes d'interdiction d'opérations et de blocage.

Cette mesure vise notamment à protéger les actifs pendant l'enquête. L'AMF dépose aussi des poursuites devant les tribunaux.

N'hésitez pas à dénoncer un site suspect à l'AMF.

LES SERVICES D'ASSISTANCE DE L'AMF

Le Centre d'information – 1 877 525-0337

N'hésitez pas à communiquer avec l'AMF si vous croyez être la cible d'une tentative de fraude financière. Nos agents pourront vous informer et vous assister au besoin.

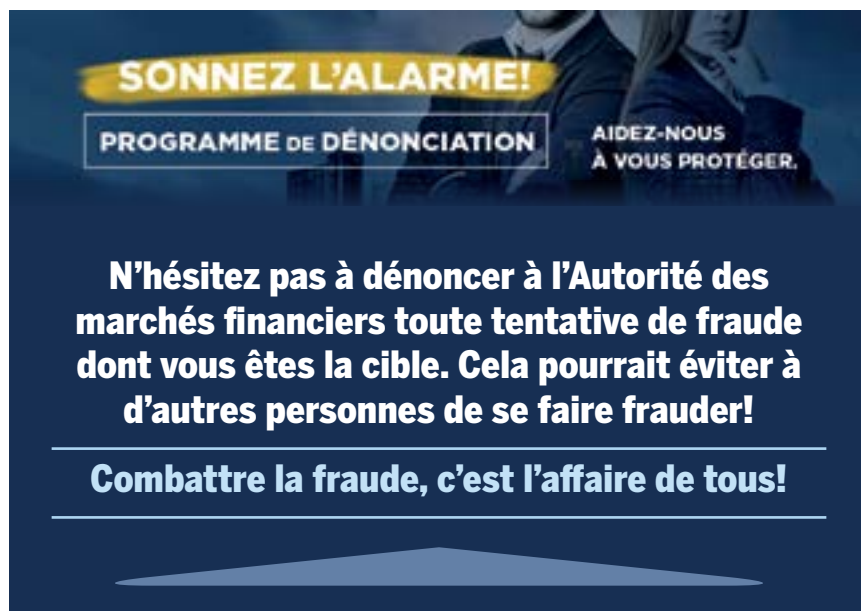
Le Fonds d'indemnisation des services financiers (FISF)

Le FISF peut indemniser, jusqu'à un maximum de 200 000 \$ par réclamation, les personnes ayant été victimes d'une fraude en faisant affaire avec un représentant en assurance, en épargne collective ou en plans de bourses d'études, un expert en sinistre, un planificateur financier ou, à compter du 1^{er} mai 2020 seulement, un courtier hypothécaire.

Certaines conditions s'appliquent. [Consultez le site de l'AMF](#) ou communiquez avec le Centre d'information pour plus de détails.

Le [Programme de dénonciation](#) – 1 866 332-0115

L'AMF a mis en place un guichet sécurisé par lequel les dénonciateurs peuvent transmettre des informations. Les dénonciations ainsi produites sont traitées de manière confidentielle par une équipe spécialisée.



SONNEZ L'ALARME!

PROGRAMME DE DÉNONCIATION

AIDEZ-NOUS
À VOUS PROTÉGER.

N'hésitez pas à dénoncer à l'Autorité des marchés financiers toute tentative de fraude dont vous êtes la cible. Cela pourrait éviter à d'autres personnes de se faire frauder!

Combattre la fraude, c'est l'affaire de tous!

Pour joindre
l'Autorité des marchés financiers

QUÉBEC

Place de la Cité, tour Cominar
2640, boulevard Laurier, bureau 400
Québec (Québec) G1V 5C1

MONTRÉAL

800, rue du Square-Victoria, 4^e étage
C.P. 246, Place Victoria
Montréal (Québec) H4Z 1G3

CENTRE D'INFORMATION

Québec: 418 525-0337
Montréal: 514 395-0337
Autres régions: 1 877 525-0337

lautorite.qc.ca