



Depuis la pandémie, nous entendons plus souvent parler de fraudes qu'avant. On ne le dira jamais assez à quel point il est important de rester vigilants en tout temps. En effet, les fraudeurs n'agissent pas seulement sur le web ou juste en temps de pandémie. Les arnaques prennent différentes formes et les fraudeurs utilisent tous les moyens mis à leur disposition pour tromper les gens : téléphone, petites annonces, le réseau immobilier, etc. Certains vont même jusqu'à aller vous visiter directement à votre domicile !



## Fraude aux employés très serviables

Un fraudeur vous téléphone en se faisant passer pour un employé d'une Caisse populaire Desjardins ou de la Banque Nationale du Canada et vous mentionne que vous venez d'être victime de fraude. Le nom de l'institution bancaire peut même apparaître sur l'afficheur, pour lui donner plus de crédibilité. Ce dernier vous signale que pour des raisons de sécurité, vous devez remettre d'urgence vos cartes bancaires et vos numéros d'identification personnelle (NIP) afin de sécuriser votre compte de banque. Un complice se présente et cogne peu après à la porte de votre résidence pour recueillir vos cartes et vos NIP. Sans tarder, les voleurs agissent et effectuent rapidement pour plusieurs milliers de dollars de retraits bancaires.

### Se protéger de cette fraude

Dans le cas d'une telle arnaque, il est important de se rappeler qu'aucun représentant ni employé d'une institution financière ne sollicitera un client afin de se faire remettre une carte bancaire et le NIP, peu importe les circonstances.

### **Ressource et référence pour cet article :**

Clinique de Cyber-Criminologie  
[www.clinique-cybercriminologie.ca](http://www.clinique-cybercriminologie.ca)



## Arnaque à l'investissement



Les arnaqueurs approchent leurs victimes en leur promettant des rendements supérieurs à la moyenne sur différents produits de placement : assurances, hypothèques, REER, rachat d'actions, investissement international, manipulations boursières frauduleuses, etc.

### Astuces pour la reconnaître

Demande de renseignements personnels

Offre « exclusive » et limitée dans le temps

Urgence d'investir

Pas ou peu de détails dans le contrat

Sollicitation non demandée

Site web non sécurisé qui utilise l'image d'une institution connue

### Se protéger

- Vérifier la présence de fautes d'orthographe ;
- Vérifier l'inscription du conseiller auprès de l'Autorité des marchés financiers
- Ne pas répondre aux offres spontanées et non sollicitées ;
- Ne pas transmettre d'informations personnelles ;
- Refuser les modes de paiement inhabituels (cryptomonnaie, transferts électroniques, etc.) ;
- Demander l'avis d'un conseiller financier indépendant.



## Fraude par sollicitation

Des « colporteurs » se présentent à votre domicile et insistent pour entrer faire une inspection des lieux sous divers prétextes en se faisant passer pour des représentants d'une entreprise pouvant effectuer des travaux sur les bâtiments. Rapidement, ils découvrent des problèmes qui doivent être effectués en urgence (moisissures, fissures, électricité, etc.). Ils vous proposent alors d'exécuter eux-mêmes les travaux et font une soumission qu'ils signent. À la signature du contrat, on vous demande un dépôt, mais les travaux n'auront jamais lieu.

### Se protéger de cette fraude

- La majorité des municipalités exigent un permis pour faire de la sollicitation à domicile ;
- Des règles strictes s'appliquent pour les contrats de travaux domiciliaires ;
- Ne jamais signer de contrat sans faire les vérifications préalables (validation du permis du représentant, vérification auprès de l'OPC, etc.) ;
- Ne jamais donner de dépôt avant le début des travaux. S'il s'agit d'un commerçant itinérant, vous avez 10 jours pour annuler sans pénalité.



## Arnaque Téléphonique



Par téléphone ou par texto, tous les moyens sont bons pour obtenir des victimes leurs informations et données personnelles.

Les arnaqueurs prétexteront que vous avez gagné un prix pour lequel vous devez payer les frais de livraison, par exemple. Ils se feront passer pour un représentant d'un corps de police, un représentant d'une institution financière ou gouvernementale, un informaticien de Microsoft, etc. pour vous informer de l'urgence de régler une situation problématique avec votre dossier, votre compte ou votre ordinateur, etc.

Certains autres pousseront l'audace jusqu'à téléphoner, au beau milieu de la nuit, à des victimes, souvent âgées, en se faisant passer pour le petit-fils qui a un problème, qui a eu un accident ou qui s'est fait agresser, voler ou arrêter. Demandant argent et discrétion.

Les appels silencieux ou les appels abandonnés (on laisse sonner un coup et on raccroche) peuvent être des actions préalables à la fraude.

### Astuces pour la reconnaître

Demande d'argent ou de payer des frais (livraison-douane, etc.)

Demande de renseignements personnels pour valider votre identité

Demande de télécharger un programme ou de prendre le « contrôle » de votre ordinateur pour le réparer

Urgence d'agir

On vous informe que vous avez gagné un prix ou qu'une agence gouvernementale a un chèque pour vous.

Paiement exigé par carte-cadeau ou par transfert de fonds ou même par Bitcoin

L'appelant parle seulement anglais

### Se protéger

- Ne pas envoyer d'argent ou cartes-cadeaux ;
- Ne pas accepter d'argent d'une autre personne (blanchiment d'argent) ;
- Ne pas donner d'information personnelle et financière ;
- Ne pas se fier à l'afficheur (souvent trafiqué) ;
- Ne pas rappeler un numéro inconnu ;
- Ne pas cliquer sur les liens dans les textos d'inconnus ;
- Inscrire son numéro de téléphone et cellulaire sur la liste nationale de numéros exclus ;
- Raccrocher quand il n'y a pas de réponse à l'autre bout de la ligne ;
- Prétexter être occupé et demander le numéro de téléphone (effectuer une recherche sur le numéro donné).



## Arnaque Locative



L'arnaque consiste à publier une offre très alléchante sur les réseaux sociaux ou des sites populaires et demander à un locataire potentiel d'envoyer un dépôt « remboursable » pour visiter le logement ou une somme d'argent pour réserver l'appartement.

Très souvent, le propriétaire prétend être à l'extérieur du pays et ne peut pas être joint autrement que par courriel.

## Fraude à l'emploi



On demande au candidat de l'argent pour sa formation ou de donner ses renseignements personnels et financiers via un faux processus d'embauche.

### Astuces pour la reconnaître

Demande d'argent pour visiter ou réserver

Demande de renseignements personnels pour « enquête de crédit »

Propriétaire joignable seulement par courriel

Urgence d'agir (plusieurs candidats intéressés)

Peu ou pas de photos ou des photos de l'extérieur seulement.

### Se protéger

- Ne pas envoyer d'argent (illégal au Québec) ;
- Refuser de faire une transaction pour une tierce personne (blanchiment d'argent) ;
- Comparer les images de l'appartement sur internet ;
- Ne pas transmettre d'informations personnelles ;
- Parler avec les voisins pour confirmer l'identité du propriétaire ;
- Communiquer avec le constructeur pour confirmer l'identité du propriétaire dans le cas d'un nouveau projet immobilier.

### Astuces pour la reconnaître

Offre sur des sites non officiels (Facebook, Kijiji)

Processus d'embauche totalement à distance

Candidat doit rembourser un surplus sur leur chèque de paie

Le candidat doit faire de fausses formations

### Se protéger

- Quand c'est trop beau, c'est souvent tout faux ;
- Faire des recherches sur l'entreprise avant de postuler ;
- Consulter les sites reconnus de recherche d'emploi ;
- Ne pas transmettre d'informations personnelles ;
- Proposer d'aller chercher les documents sur place.





## Rester vigilant en tout temps

Dans ce deuxième volet sur la fraude, l'ACEF a voulu mettre en lumière des fraudes diverses ayant lieu sur le territoire Lanaudois.

Malgré tous les avertissements et les mises en garde, il ne faut jamais oublier que les fraudeurs font preuve d'une grande créativité afin d'accéder aux informations personnelles de leurs victimes. Commettre ces crimes c'est leur spécialité ! Dès qu'une opportunité se présente : désastre naturel, guerre, nouvelle subvention offerte par un gouvernement, période d'impôt, etc., vous pouvez être certains qu'une fraude naîtra de ces situations.

C'est pourquoi, il est important de rester sur ses gardes en tout temps et de dénoncer et de ne pas tenir pour acquis que quelqu'un d'autre a probablement déjà signalé la fraude à notre place.

## La clé, c'est de s'informer

Les meilleurs atouts des fraudeurs est l'ignorance des victimes et leur peur de la fraude. En effet, par ignorance du fonctionnement des différents outils numériques (applications, plateforme web, réseaux sociaux, etc.), ou des derniers développements dans les moyens de communication les victimes tombent plus facilement dans les filets des arnaqueurs.

Par manque d'informations, les cibles ont ainsi une plus grande prédisposition à tomber dans le piège des escrocs lorsque ceux-ci les informent, faussement, qu'ils ont été la proie d'un malfaiteur. Déguisés sous les apparences d'une organisation ou d'une institution connue, les crapules utilisent la peur de se faire frauder pour amener les victimes à leur faire confiance et leur remettre leurs données et informations personnelles sur un plateau d'argent.

En terminant, nous vous invitons à passer le test L'Autorité des marchés financiers a publié un petit jeu-questionnaire pour vous permettre d'évaluer vos connaissances en matière de prévention de la cyberfraude.

[Test de l'AMF](#)

### Dénoncer une fraude ou une activité criminelle de manière anonyme

Montréal : Info-Crime 514 393-1133

[www.infocrimemontreal.ca](http://www.infocrimemontreal.ca)

Ailleurs au Québec : Échec au crime, 1 800 711-1800

[www.echecaucrime.com](http://www.echecaucrime.com)