



1 LA FRAUDE AMOUREUSE

En ligne, le **fraudeur** tisse un **lien de confiance** avec une **victime** et lui dévoile de prétendus **sentiments amoureux**. Une fois la **relation établie**, il donne différents **prétextes** (urgence, frais médicaux ou achats de billets d'avion, etc.) pour lui **soutirer de l'argent**.

L'**arnaqueur** ne **rencontre jamais la victime** en personne, car il trouve toujours une **excuse** (travail à l'étranger, urgence, problème familial, etc.).



Nos meilleurs conseils :

- **N'envoyez aucun** montant d'**argent** ni **aucune photo** ou **vidéo intime** de vous;
- **Parlez de la relation** avec votre entourage.

2 LA FRAUDE DU FAUX REPRÉSENTANT

Sous prétexte de **transactions suspectes** ou de **fraudes** sur sa **carte bancaire**, le **fraudeur** **demande** à la victime d'effectuer une opération sur son compte bancaire ou de **mettre** ses **cartes** et ses **mots de passe dans une enveloppe** que l'on viendra chercher à son domicile.



Notre meilleur conseil : RACCROCHEZ!

Ce simple geste vous permettra :

- d'**éviter** de ressentir de la **pression** et du **stress**;
- d' un **proche** ou une **personne de confiance**;
- de faire une **vérification** auprès de votre **institution bancaire** et auprès de votre **service de police local**.

3 LA FRAUDE GRANDS-PARENTS

Le **fraudeur** se fait passer pour un **membre de la famille** (ou de l'entourage) en situation de **détresse** ou d'**urgence** et ayant besoin d'**aide financière urgente**.



Notre meilleur conseil : RACCROCHEZ!

Ce simple geste vous permettra :

- d'**éviter** de ressentir de la **pression** et du **stress**;
- d' un **proche** ou une **personne de confiance**;
- de faire une **vérification** auprès de votre **institution bancaire** et auprès de votre **service de police local**.



4

LA FRAUDE DU PRÉSIDENT

Le **fraudeur** cible le **responsable de la comptabilité** ou des **finances** d'une entreprise.

Il **personnifie le président** de la compagnie et **leurre cet employé** (sous divers prétextes), l'amenant ainsi à effectuer un **transfert de fonds**.



Nos meilleurs conseils :

- **Vérifiez toujours l'identité** de la personne qui vous écrit ou vous appelle.
- **Sensibilisez le personnel** à ce stratagème, aux **procédures de transactions** (ou de virements), ainsi qu'à toutes autres **mesures de sécurité** mises en place.

5

LA FRAUDE À L'INVESTISSEMENT

Fausse promesse d'investissement alléchant. Comme variante, les **fraudeurs** peuvent **amener** des victimes à **recruter d'autres « investisseurs »** (en échange d'une commission).

Lorsqu'il est impossible pour les victimes de récupérer leur argent, celles-ci réalisent la fraude.



Nos meilleurs conseils :

- **Vérifiez toujours si la personne** qui vous **offre un placement** est **autorisée** à le **faire**;
- Communiquez avec l'Autorité des marchés financiers (AMF)** ou consultez le registre disponible sur son site Web : lautorite.qc.ca;
- **Méfiez-vous des offres de profits extraordinaires** ou mirobolants et **des offres non sollicitées** (en personne, par téléphone, par courriel, par Internet, etc.).
 - **Vérifiez la légitimité** de votre **interlocuteur** et la **source** de cette information.

6

HAMEÇONNAGE

Envoi massif de messages frauduleux (par courriel, par texto ou par rappel).

Usurpant l'identité d'une organisation, ces messages ont pour **but d'induire** les destinataires **en erreur** et de les **inciter à transmettre** leurs **informations personnelles** ou **bancaires**.



Nos meilleurs conseils :

SUPPRIMEZ LE MESSAGE OU RACCROCHEZ.

Vérifiez sur le site officiel sécurisé (adresse débutant par "https" avec un cadenas fermé)

Ne jamais :

- **Rappeler** au numéro indiqué sur le message;
- **Confirmer** ou **donner d'informations** personnelles;
- **Cliquer sur l'hyperlien** du message;
- **Inscrire le numéro** de téléphone **dans un moteur de recherche**.