

Des mesures concrètes pour se protéger :

1 > Sécurisez vos accès

Utilisez des mots de passe robustes et uniques, comprenant des symboles, des chiffres et des lettres majuscules.

2 > Protégez vos données

Ne divulguez jamais vos renseignements personnels, mots de passe ou NIP par téléphone, texto ou courriel.

3 > Méfiez-vous des offres trop belles pour être vraies

Restez vigilant face aux offres trop belles pour être vraies et vérifiez si l'entreprise est dûment autorisée.

4 > Soyez aux aguets quand on vous demande d'agir vite

Demandez-vous s'il y a vraiment urgence d'agir.

5 > Vérifiez l'identité

Si un organisme (comme votre banque ou le gouvernement) vous contacte de façon inattendue, ne fournissez aucune information. Raccrochez et rappelez l'institution en utilisant son numéro de téléphone officiel.

Si vous croyez être victime de fraude, communiquez immédiatement avec :

- > Votre institution financière
- > Le Centre antifraude du Canada au 1 888 495-8501
- > Les bureaux de crédit (TransUnion ou Équifax)

*Si vous avez été victime d'une fraude confirmée et que vous désirez porter plainte, communiquez avec votre service de police local.



RÉGIE INTERMUNICIPALE DE POLICE
RICHELIEU-SAINT-LAURENT

333, rue Hertel, Beloeil (Québec) J3G 3N3
1578, chemin du Fer-à-Cheval, Sainte-Julie (Québec) J3E 0A2

Téléphone sans frais : 1 888 678-7000



> Tous unis contre la fraude

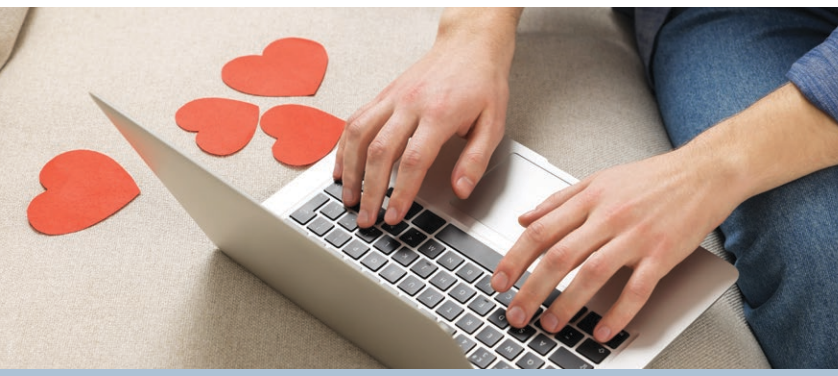
Plus on s'informe, mieux on se protège.



La meilleure façon de se protéger contre la fraude est d'être bien informée. Voici les 3 arnaques les plus communes :

La fraude amoureuse

Vous faites la connaissance d'une personne en ligne et une relation se développe au fil du temps. Après plusieurs échanges, cette personne vous demande de l'argent pour régler une urgence ou surmonter un problème personnel. En réalité, il peut s'agir d'un fraudeur qui utilise une fausse identité dans le but de vous soutirer de l'argent.



Le saviez-vous ?

- Les fraudeurs prennent le temps d'établir une relation de confiance avant de faire une première demande d'argent.
- Pour éviter les soupçons, les premiers montants demandés seront petits.

Quoi faire ?

- Vérifiez si le profil de votre interlocuteur semble récent ou contient peu de publications, d'amis ou d'interactions.
- Soyez sur vos gardes si la personne trouve des raisons pour éviter les appels vidéo ou les rencontres en personne.
- Obtenez un regard extérieur en informant une personne de confiance.



La fraude du faux représentant

Une personne vous appelle en disant travailler pour une banque, la police ou un organisme du gouvernement. Elle affirme que vous êtes victime de fraude et demande vos informations bancaires, ou bien elle mentionne que vous avez des contraventions impayées et vous invite à les rembourser en vous faisant un virement monétaire à vous-même. En lui faisant parvenir la confirmation du virement pour «vérifier» que tout fonctionne bien, elle pourra détourner et récupérer votre argent.

Le saviez-vous ?

- Une organisation légitime ne vous appellera jamais pour recueillir des informations confidentielles ou pour vous demander de transmettre de l'argent.

Quoi faire ?

- Ne partagez pas vos informations personnelles et bancaires ;
- Ne divulguez jamais vos mots de passe, NIP ou autres informations confidentielles ;
- Ne remettez pas vos cartes de débit ou de crédit à qui que ce soit ;
- Ne vous fiez pas au numéro et au nom de l'afficheur. Notez plutôt le nom de la personne qui appelle, raccrochez, puis composez le numéro officiel de l'organisation (ex. il figure au dos de vos cartes).

La fraude grands-parents

Une personne vous appelle en disant être un médecin, un policier ou un avocat. Elle prétend qu'un membre de votre famille (petit-enfant, nièce, cousin) est en situation d'urgence. Elle vous demande de rembourser rapidement les frais liés à l'événement : accident, caution, soins, etc. Elle insiste pour que vous n'en parliez à personne et offre que quelqu'un passe à votre domicile pour récupérer l'argent.

Le saviez-vous ?

- Les appels inattendus impliquant une demande urgente et/ou secrète devraient toujours être considérés comme étant suspects.
- L'intelligence artificielle (IA) peut imiter la voix d'un proche de façon très convaincante.

Quoi faire ?

- Établissez un « code secret » avec vos proches afin de confirmer leur identité au besoin.
- Si vous avez un doute, raccrochez. Appelez un membre de votre famille pour vérifier les faits ou communiquez directement avec l'organisme qui prétend vous avoir appelé.

