SOYEZ VIGILANTS, SOYEZ PROTÉGÉS !

Protégeons nos aînés contre la fraude et les cyberattaques au Québec

TABLE DE CONCERTATION
DES AÎNÉS DE PORTNEUF

Lexique

Hameçonnage (Phishing)
Messages électroniques ou SMS trompeurs pour voler vos informations.

Ransomwares
Logiciels malveillants bloquant l’accès à vos données contre paiement.

Maliciels
Programmes nuisibles infectant vos appareils pour voler des informations ou perturber leur fonctionnement.

Piratage de compte
Accès non autorisé à vos comptes en ligne (banque, courriel, réseaux sociaux).

Introduction

Les aînés du Québec sont des cibles privilégiées pour les fraudeurs et les cybercriminels. Les signalements de fraudes envers les personnes de 60 ans et plus au Centre antifraude du Canada représentaient environ 17 000 cas en 2022, totalisant plus de 137 millions de dollars en pertes à l'échelle canadienne.

Au Québec seulement, les cas déclarés de fraude ont augmenté de près de 15 % en deux ans. Avec des stratagèmes sophistiqués comme les faux représentants et les arnaques affectant directement les aînés. L'objectif de ce guide est de connaître les principaux stratagèmes utilisés par les fraudeurs, afin de mieux les reconnaître et de vous protéger.

TABLEAU 2 : Palmarès des 5 arnaques ayant causé les plus grandes pertes financières auprès des aînés québécois (60 ans et plus) en 2024.

	Nb Signalements	Nb Victimes	Pertes financières
1. Investissements	255	237	10 788 720$
2. Fraude amoureuse	111	90	4 161 947$
3. Service	249	158	1 042 681$
4. Offre d'argent de l'étranger	28	9	844 952$
5. Extorsion	211	22	815 250$

**En 2024, les pertes financières auprès des aînés du Québec totalisent 20M$,** comparativement à 17M$ en 2023 (+17,7%).

Source : Centre anti-fraude du Canada (Courtoisie : SQ)

01

LA FRAUDE TÉLÉPHONIQUE

“ Un monsieur de la Caisse m’a appelé hier pour me dire qu’ils avaient détecté une transaction suspecte sur mon compte. Ils voulaient valider mon numéro de compte et mon NIP mais pas question que je dise ça!! “

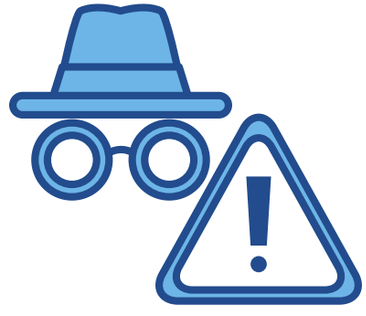
Mme Gendron

Définition

Appels prétendant provenir d’un membre de la famille, de banques, gouvernements ou institutions pour obtenir des informations personnelles ou financières.

Signes de fraude par **téléphone**

- **Demandes d’informations personnelles ou financières sensibles ;**
- **Menaces ou pressions pour agir rapidement ;**
- **Promesses de gains ou de récompenses irréalistes ;**
- **Demandes de paiement par des méthodes non traditionnelles (virements, cartes-cadeaux) ;**
- **Numéros de téléphone non reconnus ou masqués.**



Voici quelques exemples:

- **Fraude d'identité :** les fraudeurs se font passer pour des représentants d'institutions financières, de gouvernements ou d'entreprise pour obtenir des informations personnelles ou financières.
- **Arnaque au petit-fils/petite-fille :** les escrocs prétendent être un membre de la famille en difficulté financière et demandent de l'argent.
- **Arnaque au technicien informatique :** les fraudeurs affirment être des techniciens d'une entreprise de technologie pour accéder à distance à un ordinateur ou pour réparer un problème inexistant.
- **Arnaque aux impôts :** les escrocs prétendent être des agents des impôts et menaces de poursuites judiciaires ou de saisie de biens si la victime ne paie pas immédiatement une dette fiscale.
- **Arnaque aux investissements :** les fraudeurs promettent des investissements à haut rendement avec peu ou pas de risque, souvent dans des projets inexistants ou illégaux.

Conseils de protection

- **Vérifiez l'identité et prenez-la en note ;**
- **Ne donnez pas d'informations personnelles ;**
- **Si vous soupçonnez une fraude, RACCROCHEZ ;**
- **S'inscrire au registre fédéral contre le télémarketing.**

02

LA FRAUDE PAR COURRIEL

“ Aïe, figure-toi donc que je vais être riche demain! Un roi d’Afrique a besoin de moi pour faire un paiement de dernière minute et il va me donner 10 000$ pour l’avoir aidé demain. “

M. Paquet

Définition

Ce sont des messages électroniques trompeurs pour obtenir diverses informations ou pour inciter les victimes à effectuer des actions nuisibles.

Signes de fraude par **courriels**

- **Demandes d’informations personnelles ou financières sensibles ;**
- **Urgence ou menace pour inciter à agir rapidement ;**
- **Erreurs de grammaire ou d’orthographe ;**
- **Adresses de courriel suspectes ou non officielles ;**
- **Liens ou pièces jointes inattendus ou suspects ;**
- **Promesses de gains ou de récompenses irréalistes.**

Voici quelques exemples:

- **Hameçonnage (Phishing) :** messages prétendant provenir d'institutions financières, de gouvernements ou d'entreprises légitimes, demandant des informations confidentielles (mots de passe, numéros de carte de crédit).

- **Hameçonnage spéculatif (Spear Phishing) :** messages ciblés contre des individus ou organisations spécifiques, utilisant des informations personnelles pour paraître plus crédibles.

- **Arnaque au prince/noble :** messages prétendant qu'un individu riche ou un noble a besoin d'aide pour transférer de l'argent, souvent en échange d'une part de la somme.

- **Arnaque aux factures :** courriels avec des factures ou des paiements prétendument dus à des entreprises légitimes, mais en réalité destinés à voler des informations ou de l'argent.

- **Maliciels (Ransomwares, etc.) :** pièces jointes ou liens infectés par des logiciels malveillants, bloquant l'accès à des données ou exigeant un paiement pour la récupération.

Conseils de protection

- **Vérifiez l'adresse de courriel de l'expéditeur ;**
- **Ne cliquez pas sur des liens suspects ;**
- **Si vous soupçonnez une fraude, NE RÉPONDEZ PAS ;**
- **Utilisez des logiciels anti-virus ;**
- **En cas de doute, contactez la Sûreté du Québec.**

03 LA FRAUDE EN LIGNE

“ Aïe, t’aurais-tu reçu une demande d’ami de ma part? Pourtant, on est amis depuis plusieurs années. J’crois ben que je me suis fait “hacker” mon compte. Comment je fais pour avertir tout le monde! “

M. Gariépy

Définition

La fraude en ligne, également appelée cybercriminalité, désigne les actes malveillants commis sur Internet pour voler des informations personnelles, financières ou pour commettre des escroqueries.

Les conséquences de la fraude en ligne peuvent être graves, incluant des pertes financières, des dommages à la réputation, des problèmes juridiques et un impact émotionnel considérable pour les victimes, comme le stress, l’anxiété et la perte de confiance.

Comment se protéger contre ce type de fraude

- **Utiliser des mots de passe robustes et uniques pour chaque compte ;**
- **Activer l'authentification à deux facteurs pour une sécurité renforcée ;**
- **Être prudent avec les courriels et liens suspects ;**
- **Limiter les informations personnelles partagées sur les réseaux sociaux ;**
- **Utiliser des logiciels de protection et les maintenir à jour ;**
- **Vérifier régulièrement les comptes et activités en ligne.**

Des ressources offrent des conseils et des outils pour prévenir et gérer la fraude en ligne. En restant vigilant et informé, vous pouvez réduire significativement les risques de devenir une victime de fraude en ligne.

04

L'ESCROQUERIE FINANCIÈRE

" J'ai reçu un drôle de courriel hier. Revenu Québec m'a écrit pour me dire qu'un remboursement est en attente, mais que je dois confirmer mes informations bancaires. J'ai rien fait, je ne connais pas ça. Je serais mieux d'appeler la police pour voir si c'est vrai cette affaire-là.! "

Mme Carrier

Définition

L'escroquerie financière désigne le fait de tromper une personne physique ou morale pour obtenir, de manière frauduleuse, des fonds, des valeurs, un bien, un service ou un acte engageant une obligation ou une décharge.

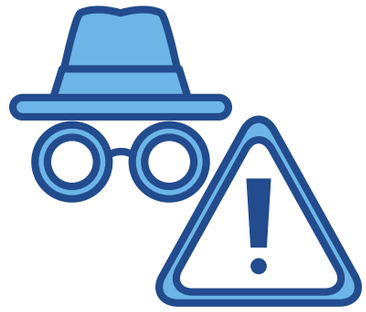
Matériel : tromperie par faux nom, fausse qualité, abus de qualité vraie ou manœuvres frauduleuses, aboutissant à une remise de fonds, valeurs, biens, services ou actes juridiques.

Morale : intention coupable de tromper et d'obtenir un avantage indu.

Légal : infraction prévue et réprimée par le Code pénal.

Que faire en cas d'escroquerie financière

- **Bloquez les transactions bancaires suspectes ;**
- **Portez plainte ;**
- **Déclenchez une procédure civile pour obtenir des dommages et intérêts.**



05

VOL D'IDENTITÉ

" Il faut que je me dépêche! Mon fils est dans le trouble en Ouganda et je dois lui envoyer 2000 piastres pour qu'il puisse sortir de prison. C'est dont ben bizarre, il n'a jamais rien fait de mal mon gars! "

M. Massé

Définition

Le vol d'identité au Québec désigne le fait de voler ou de détourner l'identité d'une personne, vivante ou décédée, pour obtenir un avantage, un bien ou causer un désavantage à un individu.

Cibles des fraudeurs

- **Accès à des comptes personnels :** comptes bancaires, courriels, réseaux sociaux ;
- **Ouverture de comptes :** bancaires, de crédit, téléphoniques ;
- **Demandes de prêts et cartes de crédit :** sous l'identité volée ;
- **Achat de biens et services :** en utilisant l'identité d'autrui;
- **Obtention de prestations gouvernementales :** ou de documents officiels (passeport, etc.) ;
- **Dissimulation d'activités criminelles :** en utilisant l'identité d'une tierce personne.

05

VOL D'IDENTITÉ

Comment se protéger contre ce type de fraude

- **Soyez prudent avec les communications :** méfiez-vous des courriels, messages, appels ou courriers suspects demandant des données personnelles ou financières.
- **Vérifiez vos comptes et rapports :** surveillez vos relevés bancaires, de carte de crédit et vos rapports de solvabilité.
- **Protégez vos documents :** déchiquetez les documents personnels ou financiers avant de les jeter.
- **Gérez votre courrier :** videz régulièrement votre boîte aux lettres et signalez votre déménagement aux institutions pertinentes.
- **En cas de soupçon :** contactez rapidement Revenu Québec, votre institution financière ou les autorités compétentes (comme le centre antifraude du Canada).

06

FRAUDE AMOUREUSE

“ Je ne pensais jamais qu’à mon âge, je retomberais en amour. Et il est beau, c’est pas possible. Je lui ai envoyé de l’argent pour se payer un billet d’avion. Il s’en vient la semaine prochaine, je n’en peux plus d’attendre. “

Mme Gingras

Définition

C’est une fraude où l’arnaqueur crée une relation affective avec la victime pour ensuite lui soutirer de l’argent, des cadeaux, ou des informations personnelles.

Les fraudeurs utilisent souvent des faux profils ou volés, des histoires très émouvantes pour susciter la compassion, des déclarations d’amour rapides pour créer un lien intense ou des urgences financières inventées.

Signes d’alerte à surveiller

- **Déclarations d’amour très rapides ;**
- **Refus de faire des appels vidéo ;**
- **Photos trop parfaites ou floues ;**
- **Demandes d’argent, même « temporaires » ;**
- **Incohérences dans les histoires ;**
- **Pression émotionnelle ou culpabilisation.**

06

FRAUDE AMOUREUSE

Scénario-type au Québec

- **Premier contact :** sur un site de rencontre, Facebook, Instagram, TikTok ou même par SMS.
- **Création d'un lien émotionnel :** l'arnaqueur se montre attentionné, disponible, flatteur.
- **Isolement :** il encourage la victime à garder la relation secrète ou à s'éloigner de ses proches.
- **La demande d'argent :** elle arrive après un lien émotionnel fort (Ex : visa, problème de famille, investissement bloqué).
- **Escalade :** une fois un transfert fait, les demandes continuent.

Comment se protéger contre ce type de fraude

- Cesser tout contact immédiatement ;
- Ne jamais envoyer d'argent ;
- Ne pas partager d'informations personnelles ;
- Signaler le profil frauduleux à la compagnie ;
- Contacter rapidement la Sûreté du Québec ;
- Parler à quelqu'un de confiance pour briser l'isolement.

07 ANNEXE

Informations supplémentaires de la Sûreté du Québec, poste de Pont-Rouge

- **FAUX CONSEILLER D'UNE INSTITUTION FINANCIÈRE :** Utilise différentes plateformes (ex. médias sociaux, notices nécrologiques) pour récolter des informations personnelles sur les victimes (ex. recherche des prénoms associés aux générations précédentes dans le bottin Canada 411). Personnifie un conseiller d'une institution financière (en complicité ou non avec un faux avocat) auprès d'une victime. Prétexte que ses cartes ont été clonées, qu'elle a été victime d'un vol d'identité, que des transactions suspicieuses ont été détectées, etc. Demande à la victime d'insérer ses cartes et ses mots de passe (NIP) dans une enveloppe qui sera récupérée par un complice.

  Variantes observées : Convainc une victime d'effectuer un « virement Interac à elle-même » afin de protéger ses fonds. Fournit la question et le mot de passe au préalable à la victime. L'opération du virement génère un courriel d'instructions (incluant un hyperlien) permettant de procéder au dépôt des fonds dans le compte bancaire d'une institution de son choix. Obtient de la part de la victime le lien URL associé au virement. Accède au lien et encaisse les fonds avant la victime. OU Fournit à la victime le numéro d'un nouveau compte ouvert « à son nom » et lui demande d'effectuer un virement entre « comptes ».

07 ANNEXE

- **FAUX PETIT-FILS (FRAUDE GRANDS-PARENTS) :**
  Personnifie le petit-enfant (ou un avocat) d'une victime. Prétexte une situation de détresse (ex. arrestation, accident d'auto, hospitalisation) et exige une somme d'argent dans l'immédiat (ex. caution exigée pour remise en liberté) tout en avisant la victime de « surtout n'en parler à personne! ».

Variantes observées : Convainc une victime d'effectuer un « virement Interac à elle-même » afin de protéger ses fonds. Fournit la question et le mot de passe au préalable à la victime. L'opération du virement génère un courriel d'instructions (incluant un hyperlien) permettant de procéder au dépôt des fonds dans le compte bancaire d'une institution de son choix. Obtient de la part de la victime le lien URL associé au virement. Accède au lien et encaisse les fonds avant la victime. OU Fournit à la victime le numéro d'un nouveau compte ouvert « à son nom » et lui demande d'effectuer un virement entre « comptes ».

OPÉRATION MOT-CODE : Discutez avec vos proches d'un mot ou phrase-code que vous seuls pouvez connaître. Assurez-vous d'en discuter verbalement seulement.

20M$: pertes financières chez les personnes âgées au Québec (2024)

07 ANNEXE

ARNAQUE DU FAUX CONSEILLER FINANCIER : Votre institution financière vous informe d'activités frauduleuses sur votre compte? Votre carte de crédit a été clonée? Vous devez fournir vos renseignements personnels et bancaires au téléphone? Méfiez-vous, refusez. Les fraudeurs peuvent commencer leur appel en vous demandant de confirmer votre identité à l'aide des renseignements déjà en leur disposition. Leur but? Vous mettre en confiance! On invoque une nouvelle procédure pour vous demander d'insérer vos cartes de paiement et vos mots de passe dans une enveloppe afin qu'un employé ou un coursier vienne les récupérer à votre domicile? On vous demande d'effectuer une opération sur votre compte bancaire? Refusez, raccrochez, c'est de la fraude.

Arnaque de l'Agence du revenu du Canada (ARC) : On vous informe que vous devez rembourser un montant d'argent d'impôt et que vous serez arrêté par un policier si vous ne payez pas immédiatement? Raccrochez. Aucun organisme gouvernemental ne procède ainsi ou ne formule de telle demande.

ARNAQUE DU GRAND-PARENT : Un membre de votre famille (ex. petit-fils) invoque un besoin d'argent urgent en raison d'un accident d'auto, d'une détention, d'une hospitalisation, etc.? Vous ne devez surtout en glisser mot à personne? N'envoyez pas d'argent dans l'immédiat.

07 ANNEXE

ARNAQUE DU GRAND-PARENT (SUITE) : Validez l'histoire qui vous est présentée et l'identité de la personne avec qui vous communiquez en appelant un autre membre de la famille ou des amis.
Même si vous croyez reconnaître la voix d'un proche, vous pourriez être en présence d'un fraudeur. Convenez avec les membres de votre famille d'un code secret (ex. un mot ou une expression) que vous pourrez utiliser lors d'une situation similaire. Ce code permettra de déterminer si vous êtes réellement en communication avec un membre de votre famille. Ne diffusez jamais ce code sur Internet, parlez-en directement aux membres de votre famille.

ARNAQUE DU FAUX-POLICIER : Vous devez rembourser de prétendus constats d'infraction impayés? Vous êtes menacé d'un état d'arrestation si vous refusez de fournir votre numéro de carte de crédit ou d'acheter des cryptoactifs? Refusez. Raccrochez au nez de ces fraudeurs.

POUR OBTENIR DE L'AIDE OU SIGNALER UNE FRAUDE :

Contactez la Sûreté du Québec ou votre service de police local au **9-1-1.**

Signalez l'incident au Centre antifraude du Canada, par téléphone au **1 888 495-8501** ou en visitant le **antifraudcentre-centreantifraude.ca**.

Vincent Hardy, travailleur de milieu pour aînés **418 268-3502**
Jessie Fortin, travailleuse de milieu pour aînés **418 284-2693**

08 SOURCES

- Sureté du Québec : sq.gouv.qc.ca
- Centre canadien de protection contre la cybercriminalité : cyber.gc.ca/fr/orientation/evaluation-cybermenaces-nationales-2025-2026
- Autorité des marchés financiers : lautorite.qc.ca/grand-public
- Option consommateur : option-consommateurs.org
- Industrie Canada : grc.ca/fr/police-federale/cybercriminalite
- Gouvernement du Canada, Sécurité et protection : securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/index-fr.aspx
- Equifax Canada: equifax.ca/fr/personnel/education/identite/
- TransUnion Canada: transunion.ca/fr/vol-didentite
- https://www.adpq.qc.ca/s-unir-pour-l-avenir/capsule/capsule-de-sensibilisation-aux-fraudes
- faafc.ca/ressources/videos/capsules-video-sur-la-fraude/

Sûreté du Québec
Déjouer les fraudeurs : youtube.com/watch?v=q9XlWU7kEzI
5 conseils pour prévenir la fraude téléphonique : youtube.com/watch?v=fPOvMBKZvWc
Comment faire pour déposer une plainte : sq.gouv.qc.ca/wp-content/uploads/2021/01/sq-3616.pdf
J'ai besoin d'aide pour préparer mon dossier de fraude : sq.gouv.qc.ca/services/campagnes/mpf/

Une réalisation :

TABLE DE CONCERTATION
DES AÎNÉS DE PORTNEUF

Merci au Programme Nouveaux Horizons pour les aînés du gouvernement du Canada.

Le guide a été réalisé en collaboration avec la Sûreté du Québec