

# RAPPORT D'ACTIVITÉ

## Trimestre 2 – 2024



# FRAUDE-ALERTE.CA

# FAITS SAILLANTS

**1 164 SIGNALEMENTS**

**148 129 VISITES**

**4 501\$ PERDU EN  
MOYENNE**

## Signalements

- Total signalements reçus : 1 221
- Signalements analysés : 1 164
  - Exclusions :
    - Signalements provenant de l'étranger (notamment de France)
    - Signalements non pertinents ou incohérents

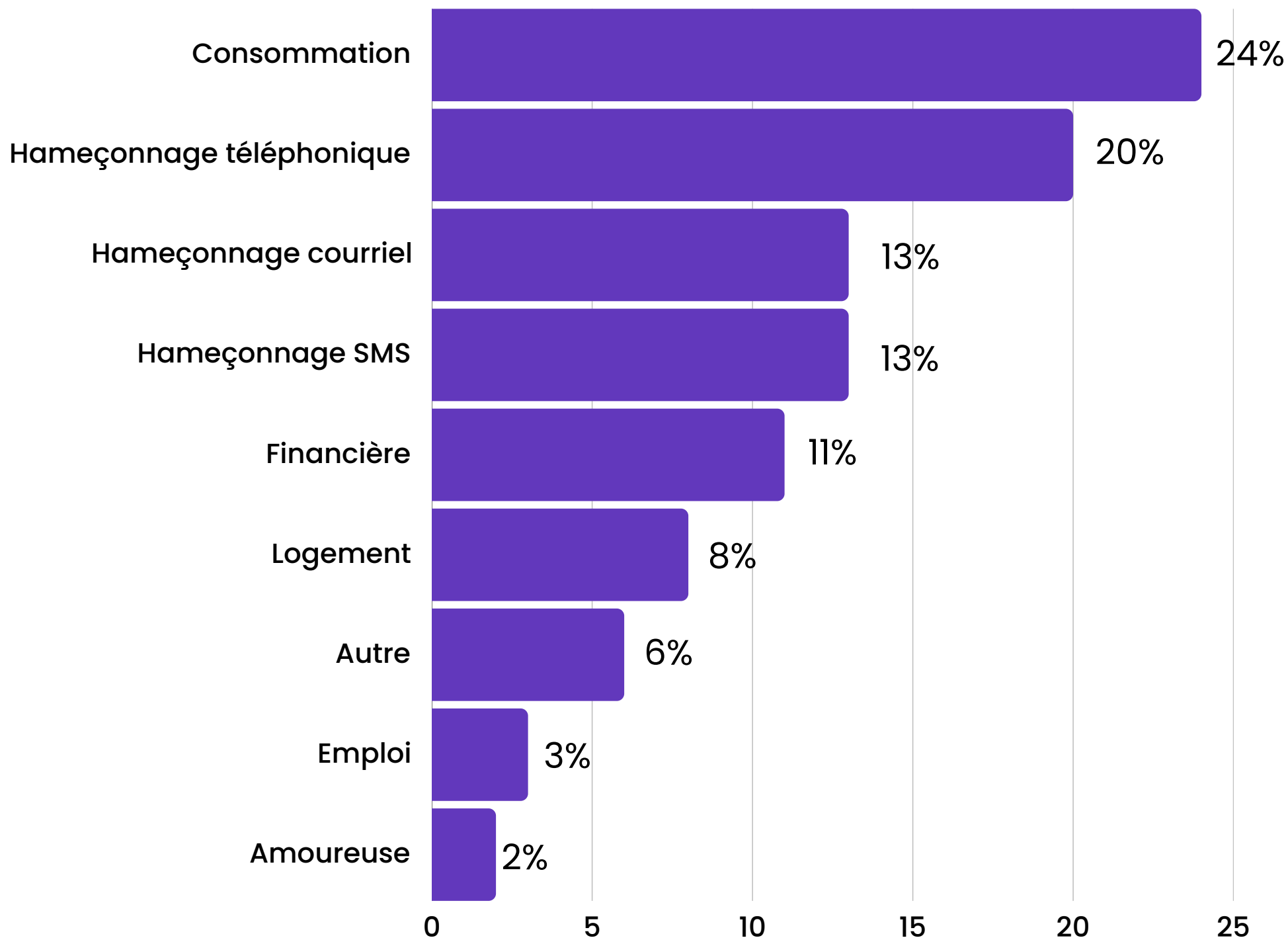
## Montant perdu

- Perte médiane : 350 \$
- Perte moyenne : 4 501\$
  - *Note* : Seuls 138 signalements mentionnaient le montant perdu
- Perte maximale : 200 000 \$ (fraude à l'investissement/crypto)
- Perte minimale : 2,74 \$ (site web frauduleux)

## Observations

- Les montants des pertes sont difficiles à évaluer avec précision en raison du faible nombre de signalements mentionnant les montants.

# TYPE DE FRAUDE



Au deuxième trimestre 2024, la **fraude à la consommation** s'est imposée comme la fraude la plus fréquemment signalée sur la plateforme Fraude-alerte. Cette hausse est principalement attribuable à la multiplication des sites de vente exploitant le *dropshipping* et la recrudescence d'annonces frauduleuses sur Marketplace .

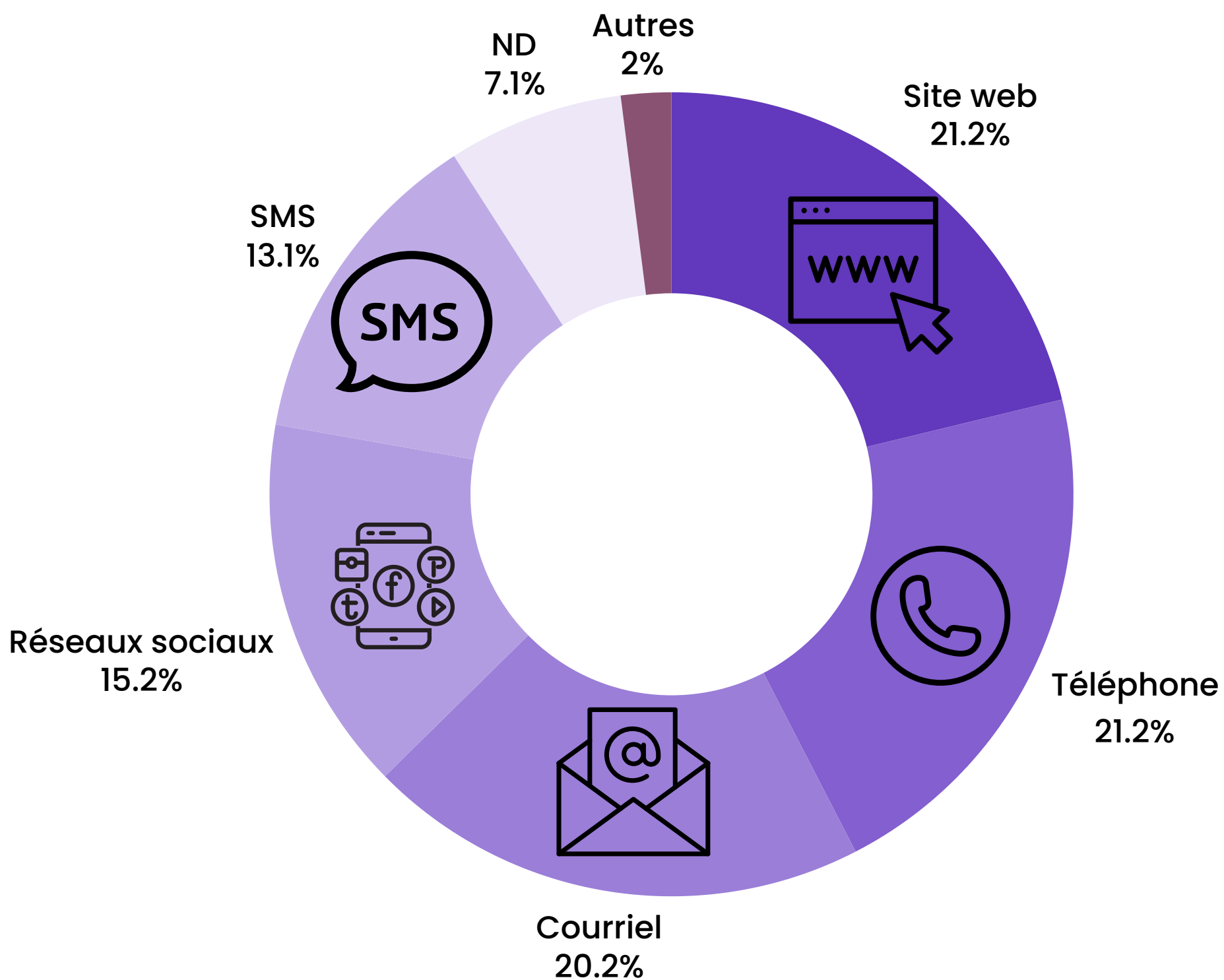
L'**hameçonnage téléphonique** est en deuxième place des fraudes les plus signalées en raison d'une vaste campagne d'hameçonnage usurpant l'identité d'Amazon et prétextant une fraude liée à des achats sur la plateforme ou bien lié à des appels silencieux. L'**hameçonnage par courriel et celui par SMS** ont été beaucoup moins signalés au deuxième trimestre 2024. Dans le cas de l'hameçonnage par SMS, cette baisse peut être attribuable à la diminution des vastes campagnes d'hameçonnage telles que celles de l'A 25 ou de la Ville de Montréal au début de l'année.

Les **fraudes financières** restent en tête des pertes les plus lourdes et l'augmentation des signalements s'explique en partie de la résurgence des services frauduleux d'offres de prêts. La **fraude à l'emploi**, impliquant de fausses offres souvent liées à des fraudes au logement, ou nécessitant l'achat de cartes cadeaux ou d'investissements pour effectuer des tâches rémunérées, reste également préoccupante.

La **fraude au logement**, que ce soit à travers les courriels réclamant des loyers impayés et les fausses annonces de logement sur Marketplace ont été moins signalées ce trimestre.

La catégorie "**Autre**", qui regroupe des cas de fraude à l'immigration, des services frauduleux (escortes, informatiques), ainsi que des usurpations d'identité et des piratages sur les réseaux sociaux, a connu une légère hausse des signalements, en particulier pour ces deux derniers types de fraude. Enfin, plusieurs cas de **fraude amoureuse** ont été signalés.

# CANAL DE COMMUNICATION



À l'instar des types de fraudes, les **sites web** ont été le canal privilégié des fraudeurs, puisque mobilisés dans les cas de fraude à la consommation. Le **téléphone** reste un canal exploité par les fraudeurs, que ce soit pour des appels silencieux ou usurpant l'identité d'Amazon prétextant des cas de fraude sur le compte de l'appelant. Les fraudeurs continuent également de recourir au **courriel**, particulièrement dans les cas de fraude au logement prétextant des loyers impayés et de faux concours prétendument organisés par de grandes enseignes.

Les **réseaux sociaux**, et plus spécifiquement Facebook, ont joué un rôle central dans plusieurs types de fraudes. Cette plateforme reste populaire auprès des fraudeurs dans les cas de fraude à l'investissement, fraude à la consommation, et fraude au logement.

Enfin, tout comme les types de fraudes, le **SMS** a été moins mobilisé par les fraudeurs au deuxième trimestre de cette année.

# ORGANISATION PERSONNIFIÉE



Au deuxième trimestre 2024, plus d'un quart (27 %) des signalements portaient sur des cas d'usurpation d'identité d'une organisation. En tête de liste figure **Amazon** (16 %), prise pour cible dans une vaste campagne d'hameçonnage par téléphone prétextant des achats frauduleux, loin devant **Postes Canada** (7 %) et la **Ville de Montréal** (7 %), également usurpées dans le cadre de campagne d'hameçonnage par SMS. .

Le **Mouvement Desjardins** (6 %) a également été usurpé dans plusieurs cas de fraude, que ce soit dans des cas d'hameçonnage par SMS ou d'hameçonnage téléphonique de type "fraude grands-parents". Enfin, étant donné l'approche de la saison des impôts, l'**Agence du revenu du Canada** (5 %) a également été mobilisée par les fraudeurs.

Par ailleurs, de nombreuses **institutions financières** (14 %), **entreprises technologiques** (11%), **commerces** (11 %), **agences gouvernementales** (8 %), **services de télécommunications** (6 %) et de **livraison** (4 %) ont également été usurpés par les fraudeurs, confirmant la diversité des cibles exploitées pour tromper le public.

450-805-4719

450-805-4708

514-375-2413

438-738-1424

Nyzara

Les internautes se sont rendus sur Fraude-alerte en utilisant diverses requêtes sur les moteurs de recherche. Comme au premier trimestre, dans la majorité des cas, ces requêtes avaient pour but de vérifier l'identité d'un appelant. Les internautes se sont interrogés sur divers numéros de téléphone, tels que, **450-805-4708** (9 649 requêtes), un appel téléphonique invitant à participer à un sondage, qui était déjà en tête des requêtes au premier trimestre. Le numéro de téléphone **450-5805-4719** (8 568 requêtes) et le **514-375-2413** (7 740 requêtes) associés à des appels silencieux et/ou de sondage et le **438-738-1424** (6 527 requêtes) correspondant à un appel faisant la promotion de l'ouverture d'un magasin ont également fait l'objet de recherche de la part des internautes.

"**Nyzara**", un site de vente frauduleux s'appuyant sur du *dropshipping*, a également fait l'objet d'un nombre de requêtes (5 605 requêtes) en raison d'un reportage télévisé sur les pratiques douteuses de ces sites.



# GLOSSAIRE ET RESSOURCES

- **Fraude à la consommation:** fraudes impliquant les sites de vente en ligne frauduleux usurpant l'identité d'entreprises légitimes ou basés sur le dropshipping et les sites de petites annonces (Marketplace, Kijiji, etc.)
- **Hameçonnage par SMS:** messages texte frauduleux ayant pour but de tromper les destinataires et leur voler des informations personnelles, financières ou des identifiants de connexion
- **Hameçonnage par courriel:** courriel frauduleux ayant pour but de tromper les destinataires et leur voler des informations personnelles, financières ou des identifiants de connexion
- **Hameçonnage téléphonique:** appel frauduleux ayant pour but de tromper les destinataires et leur voler des informations personnelles, financières ou des identifiants de connexion
- **Fraude financière:** fraudes impliquant celles liées à l'investissement, à l'investissement en cryptomonnaies ou les offres de prêts d'argent.

- **Fraude au logement:** fausses offres de logement à loyers ou courriel frauduleux demandant le paiement d'un loyer.
- **Fraude à l'emploi:** fausses offres d'emploi impliquant l'achat de carte-cadeaux, l'encaissement de chèques frauduleux, ou bien encore l'arnaque à la tâche.
- **Autres:** fraudes impliquant des services (escortes, soutien informatique, voyance, etc.), usurpation d'identité sur les réseaux sociaux ou piratage informatique.
- **Fraude amoureuse/interpersonnelle:** la fraude amoureuse se produit lorsqu'un individu gagne la confiance et l'affection de sa victime en prétendant entretenir une relation romantique, dans le but d'obtenir de l'argent ou des informations personnelles.

**FRAUDE-ALERTE.CA**

**SIGNALER.**

**S'INFORMER.**

**S'ENTRAIDER.**

