RAPPORT D'ACTIVITÉ 2025 Trimestre 4

FRAUDE-ALERTE.CA

FRAUDE ALERTE

CRPC | Chaire de recherche en prévention de la cybercriminalité

Clinique de Cyber-Criminologie

Université de Montréal

FRAUDE ALERTE

FAITS SAILLANTS

661 SIGNALEMENTS

179 725 VISITES

5896 $ MONTANT MOYEN PERDU

Signalements

- Nombre de signalements analysés : 586
  - Exclusions :
    - Signalements provenant de l'étranger (notamment de France)
    - Signalements non pertinents ou incohérents

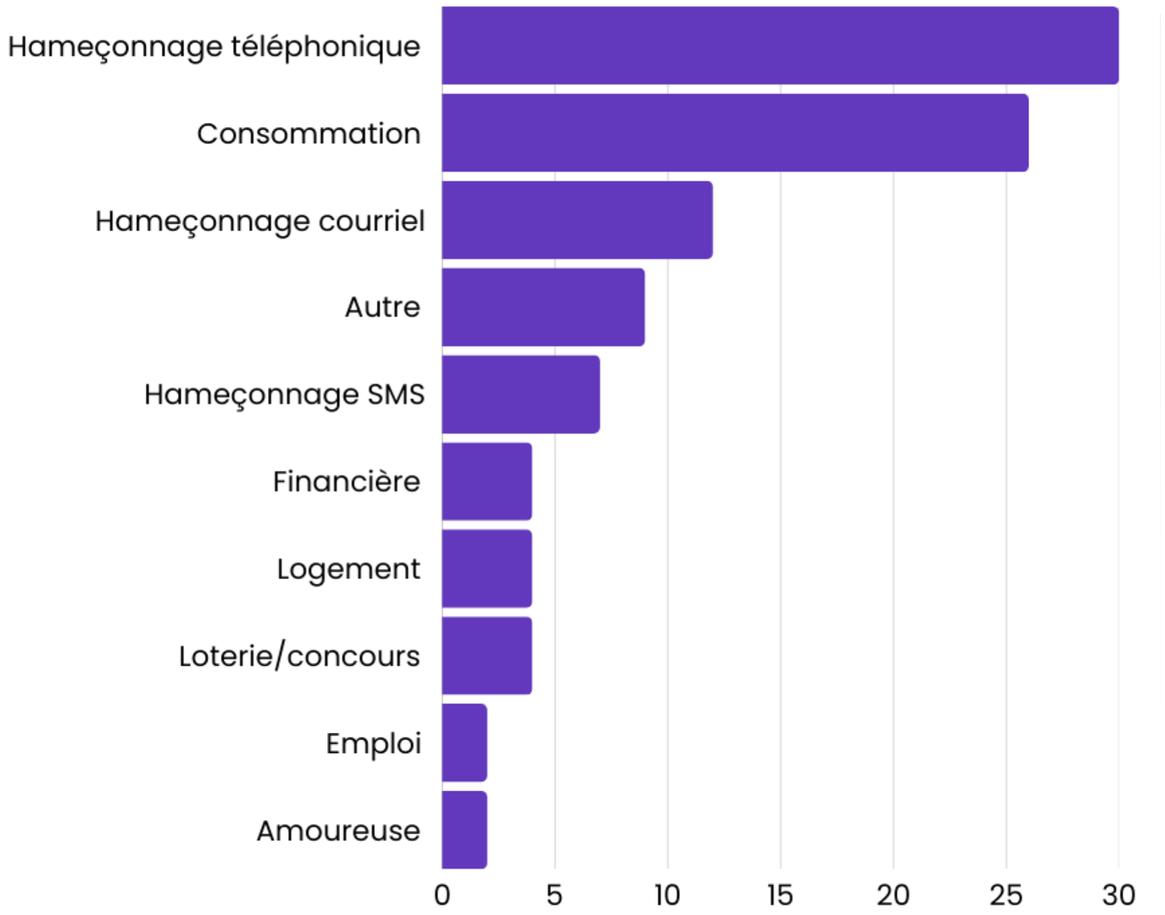
Montant perdus

- Perte médiane : 99 $
- Perte moyenne : 5896 $
  - *Note : Seuls 78 signalements (environ 13%) mentionnaient le montant perdu*
- Perte maximale : 150 000 $ (fraude amoureuse)
- Perte minimale : 1,6 $ (fraude liée à un faux service en ligne)

Observations

- Certains signalements exclus sont toujours disponibles sur Fraude-alerte mais n'ont pas été pris en compte pour l'analyse. Les montants des pertes sont difficiles à évaluer avec précision en raison du faible nombre de signalements mentionnant les montants.

TYPE DE FRAUDE



Habituellement, la **fraude à la consommation** constitue la catégorie la plus fréquente. Or, durant la période analysée, elle a été surpassée par l'**hameçonnage téléphonique**.

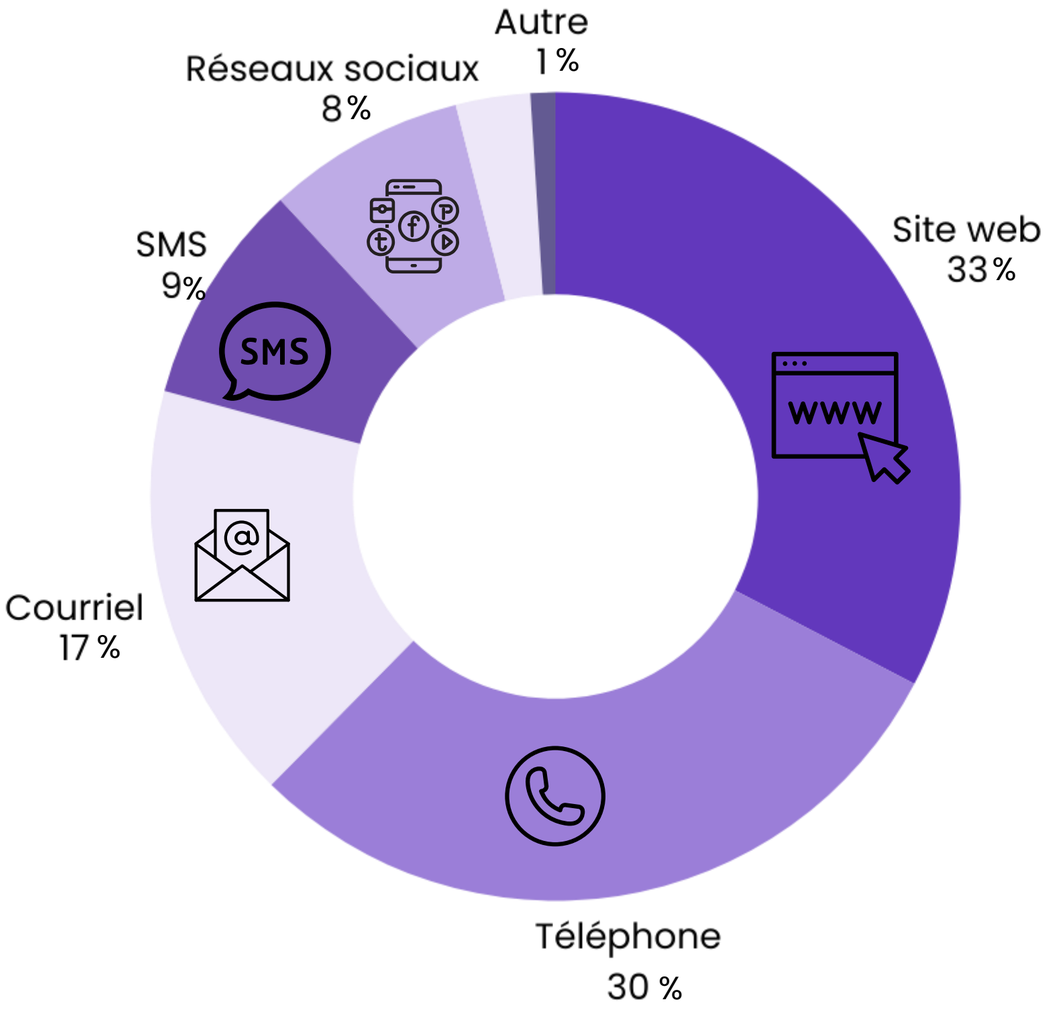
Concernant l'**hameçonnage téléphonique**, plusieurs **institutions financières** (p. ex. BMO, Desjardins) ainsi que des **organismes gouvernementaux** (p. ex. Revenu Canada, Habitation Québec) ont été usurpés, tout comme certaines grandes entreprises fréquemment mentionnées les trimestres précédents (p. ex. Google, fournisseurs de services de télécommunication). Dans le cas d'Habitation Québec, certains signalements faisaient état de fausses évaluations présentées comme permettant de réduire une facture d'électricité.

Les autres types de fraude demeurent globalement stables. On observe toutefois une **légère diminution** des signalements liés à l'**hameçonnage par courriel** (- 6 %) et, à l'inverse, une **augmentation** de la catégorie « **Autres** » (+ 4 %). Cette hausse s'explique notamment par des signalements visant des sites proposant des services tels que des tests de QI ou la création de CV, lesquels dissimulaient des abonnements payants (par exemple, un paiement initial de 1 $ suivi d'un abonnement mensuel d'environ 30 $).

Le nombre de cas de **fraude amoureuse** demeure relativement faible, mais les montants fraudés associés à ces situations sont particulièrement élevés. Une tendance comparable est observée pour les **fraudes d'investissement**.

FRAUDE ALERTE

CANAL DE COMMUNICATION



Au cours du trimestre analysé, les fraudes sur **sites Web** sont devenues le principal canal utilisé par les fraudeurs, dépassant le téléphone. Ce canal est particulièrement associé aux fraudes à la consommation, aux fraudes liées à des services ainsi qu'aux fraudes d'investissement. Le **téléphone** demeure toutefois le deuxième moyen le plus fréquent, ce qui concorde avec la proportion élevée de signalements liés à l'hameçonnage téléphonique.

Le **courriel** constitue un autre vecteur important, notamment utilisé dans des stratagèmes d'intimidation ou de menace, comme de fausses accusations criminelles à caractère sexuel ou des avis frauduleux concernant des loyers prétendument impayés.

L'utilisation des **messages textes (SMS)** a connu une diminution marquée, passant de 19% à 9%. Malgré cette baisse, ce canal reste employé pour des stratagèmes similaires, notamment ceux liés à de prétendues erreurs de livraison de colis ou à des demandes de paiement pour de supposées infractions routières (p. ex. A25).

Les **réseaux sociaux** demeurent relativement stables comme canal de fraude et sont souvent associés à des fraudes à la consommation, par exemple des annonces Marketplace frauduleuses ou des publicités de produits offerts à prix très réduit.

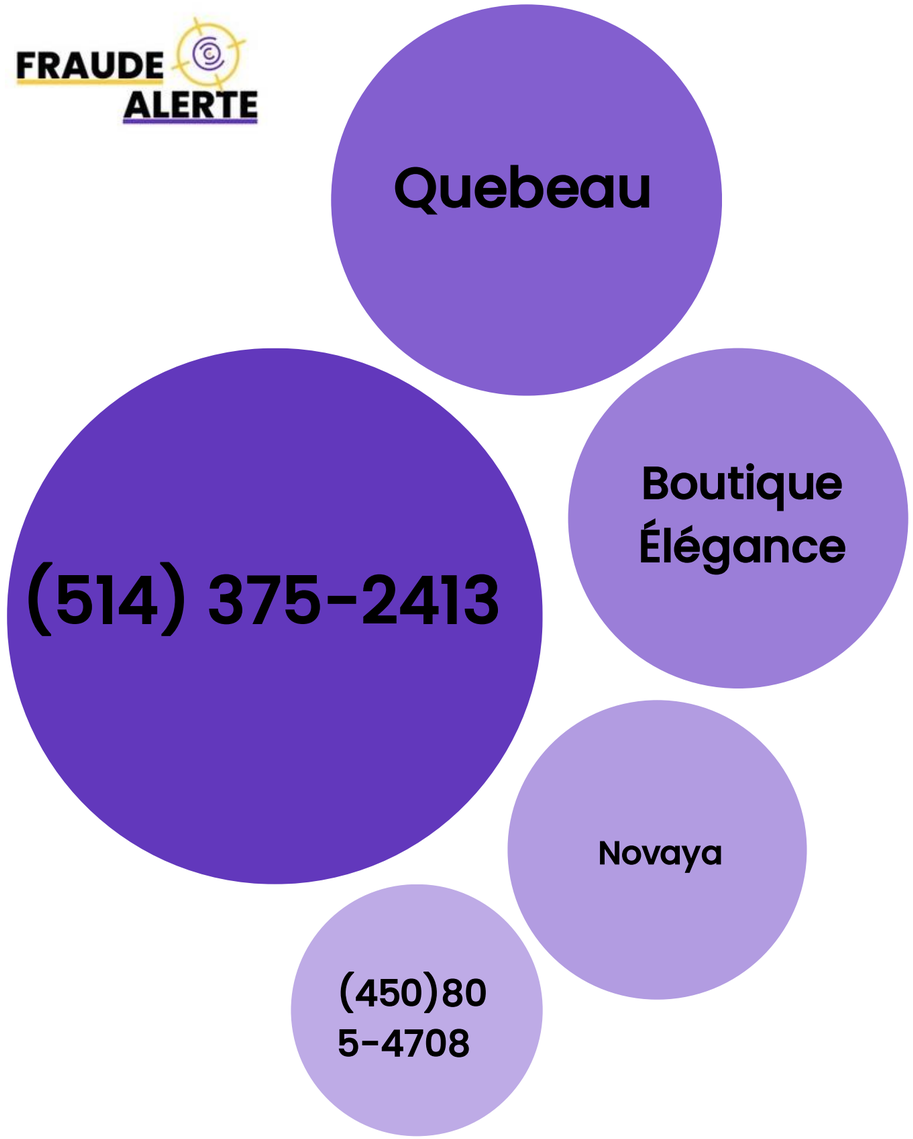
FRAUDE ALERTE

ORGANISATION PERSONNIFIÉE

Au cours de la période analysée, **25 %** des signalements faisaient état de l'**usurpation de l'identité d'une organisation connue**. Les **agences gouvernementales** représentaient **6 %** des cas, tandis que **5 %** concernaient des **institutions financières**, notamment BMO et Desjardins. Les **entreprises technologiques** comptaient pour **4 %** des signalements, suivies des **services de livraison** (**3 %**), tels que Purolator, FedEx et Postes Canada, ainsi que des **fournisseurs de télécommunications** (**2 %**), dont Bell, Rogers, Telus et Fido.

Plus précisément, Google a été usurpé dans 3 % des situations recensées. Des avocats ont également été personnifiés dans 2 % des cas, principalement dans des scénarios liés à de fausses accusations criminelles. Enfin, Desjardins et Amazon ont chacun été utilisés comme façade frauduleuse dans 2 % des signalements.

Ces résultats illustrent la **diversité des organisations exploitées** par les fraudeurs, qui misent sur la crédibilité et la notoriété d'entités reconnues afin de renforcer l'apparence de légitimité de leurs stratagèmes.



REQUÊTES

Au dernier trimestre de 2025, les internautes ont accédé à la plateforme Fraude-Alerte principalement par le biais de moteurs de recherche, en formulant des requêtes visant à vérifier la légitimité de sites de vente en ligne ou de numéros de téléphone.

Parmi ceux-ci, le **514-375-2413** (7 006 requêtes) et le **450-805-4708** (1 430 requêtes) ont particulièrement été objets de recherche. Tous deux sont associés à des appels silencieux ou à des appels empruntant l'identité d'organismes légitimes (firme de sondage, institution financière, etc.). Plusieurs sites de commerce en ligne, prétendument québécois, ont également été recherchés, dont **Quebeau** (3 299 requêtes), **Boutique Élégance** (2 862 requêtes) et **Novaya** (2 420 requêtes). Finalement, **Fraude-alerte** (1 144 requêtes) a fait l'objet de plusieurs recherches de la part des internautes.

D'autres sites de vente en ligne ont également suscité un volume important de vérifications, incluant Quebecool, Quebecelle, CloudHug et Tendance Montréal. La plupart semblent prétendre vendre des produits d'origine québécoise à des fins de marketing.

FRAUDE ALERTE

GLOSSAIRE ET RESSOURCES

- **Fraude à la consommation**: fraudes impliquant les site 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 pou 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 le 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.