RAPPORT D'ACTIVITÉ
Trimestre 1 - 2025

FRAUDE ALERTE

FRAUDE-ALERTE.CA

CRPC | Chaire de recherche en prévention de la cybercriminalité

Clinique de Cyber-Criminologie

Université de Montréal

FRAUDE ALERTE

FAITS SAILLANTS

742 SIGNALEMENTS

143 007 VISITES

5 554$ DE PERTES MOYENNES

Signalements

- Total signalements reçus : 799
- Signalements analysés : 742
  - Exclusions :
    - Signalements provenant de l'étranger (notamment de France)
    - Signalements non pertinents ou incohérents

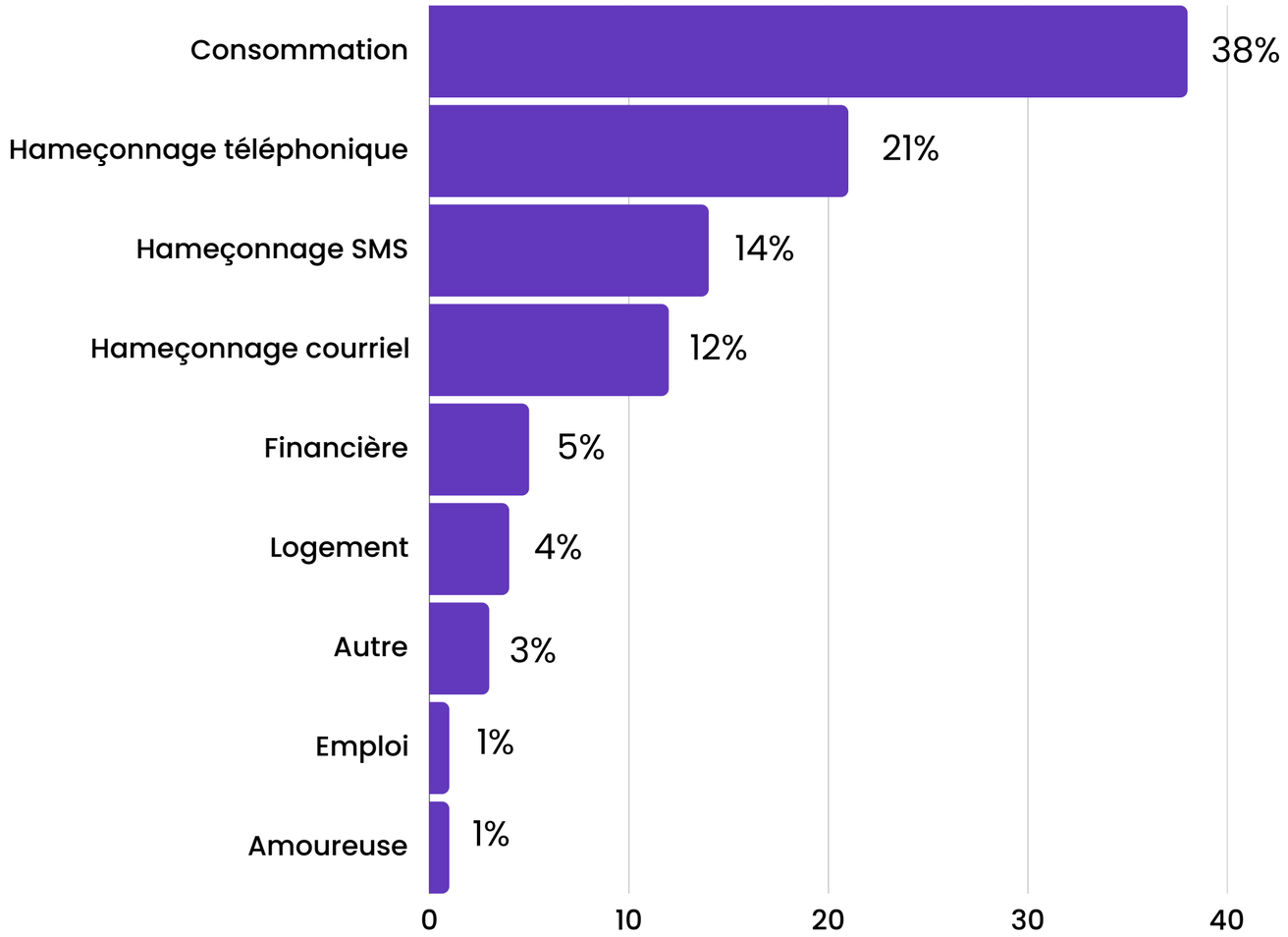
Montant perdus

- Perte médiane : 165 $
- Perte moyenne : 5 554$
  - *Note* : Seuls 83 signalements mentionnaient le montant perdu
- Perte maximale : 100 000 $ (hameçonnage/ fraude au président)
- Perte minimale : 39,99 $ (fraude à la consommation)

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 premier trimestre de 2025, la tendance observée à la fin de l'année 2024 se maintient, avec une forte proportion des signalements liés à la **fraude à la consommation**. De nombreux nouveaux sites de vente en ligne, souvent basés sur le modèle du parachutage (*dropshipping*), continuent d'émerger. On observe également une multiplication de faux sites usurpant l'identité de commerces légitimes, souvent dans le cadre de ventes de liquidation fictives.

La période est également marquée par une recrudescence de l'**hameçonnage téléphonique**, après une baisse notable l'année précédente. Ce type de fraude demeure celui où l'usurpation d'identité d'entreprises est la plus fréquente, touchant des institutions financières, des entreprises de télécommunications et des entreprises technologiques.

En revanche, l'**hameçonnage par courriel et par SMS** a connu un net recul ce trimestre, alors qu'il s'agissait des formes de fraude les plus signalées en 2024. Certaines campagnes amorcées l'an dernier se poursuivent néanmoins.

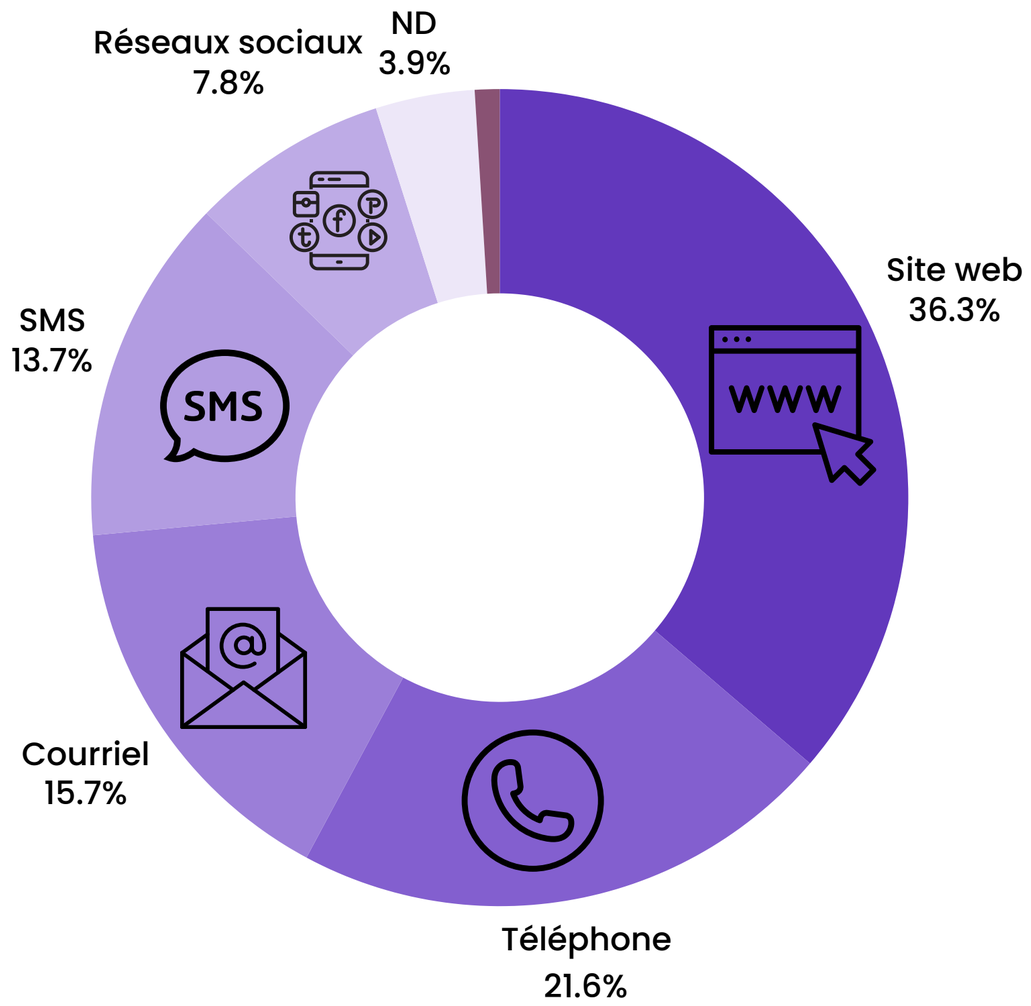
Les **fraudes financières** demeurent centrées sur les investissements en cryptomonnaies. À l'inverse, les faux prêts enregistrent une baisse des signalements. La **fraude à l'emploi**, notamment les fausses offres nécessitant un investissement préalable pour réaliser des tâches rémunérées (connue sous le nom d'« arnaque à la tâche »), est en hausse et suscite de vives inquiétudes.

La **fraude au logement**, bien qu'en diminution, reste présente. Les méthodes restent similaires à celles observées l'an dernier : courriels réclamant des loyers impayés et de fausses annonces sur des plateformes comme Facebook Marketplace.

Enfin, plusieurs cas de **fraude amoureuse** ont été signalés. La catégorie « **Autre** » regroupe notamment des fraudes liées à des services d'escortes, des usurpations d'identité sur les réseaux sociaux ainsi que des piratages de courriels personnels.

FRAUDE ALERTE

CANAL DE COMMUNICATION



Au premier trimestre 2025, comme pour les types de fraude, les **sites web** représentent le vecteur principal, en particulier dans la fraude à la consommation s'appuyant sur le parachutage (*dropshipping*). Toutefois, les **réseaux sociaux** – et plus particulièrement Facebook – jouent un rôle central dans la diffusion de ces fraudes. Les publicités diffusées sur la plateforme redirigent fréquemment les victimes vers de faux sites de vente.

Le **téléphone** connaît un regain d'intérêt chez les fraudeurs, qui l'utilisent pour entrer directement en contact avec leurs cibles. En se faisant passer pour des représentants d'institutions financières, de services gouvernementaux ou encore de compagnies de télécommunications, les fraudeurs tentent de gagner la confiance des victimes.

Les **courriels** et les **SMS** restent également des canaux prisés, bien qu'un peu moins mobilisés en ce début d'année. Le courriel est particulièrement utilisé dans les cas de fraude au logement, notamment pour réclamer de faux loyers impayés, ou encore pour promouvoir de prétendus concours organisés par de grandes chaînes commerciales. Quant aux SMS, ils continuent de servir dans des campagnes d'hameçonnage usurpant l'identité d'organismes comme l'A25 ou la SAAQ, un phénomène déjà observé à la fin de l'année 2024.

FRAUDE ALERTE

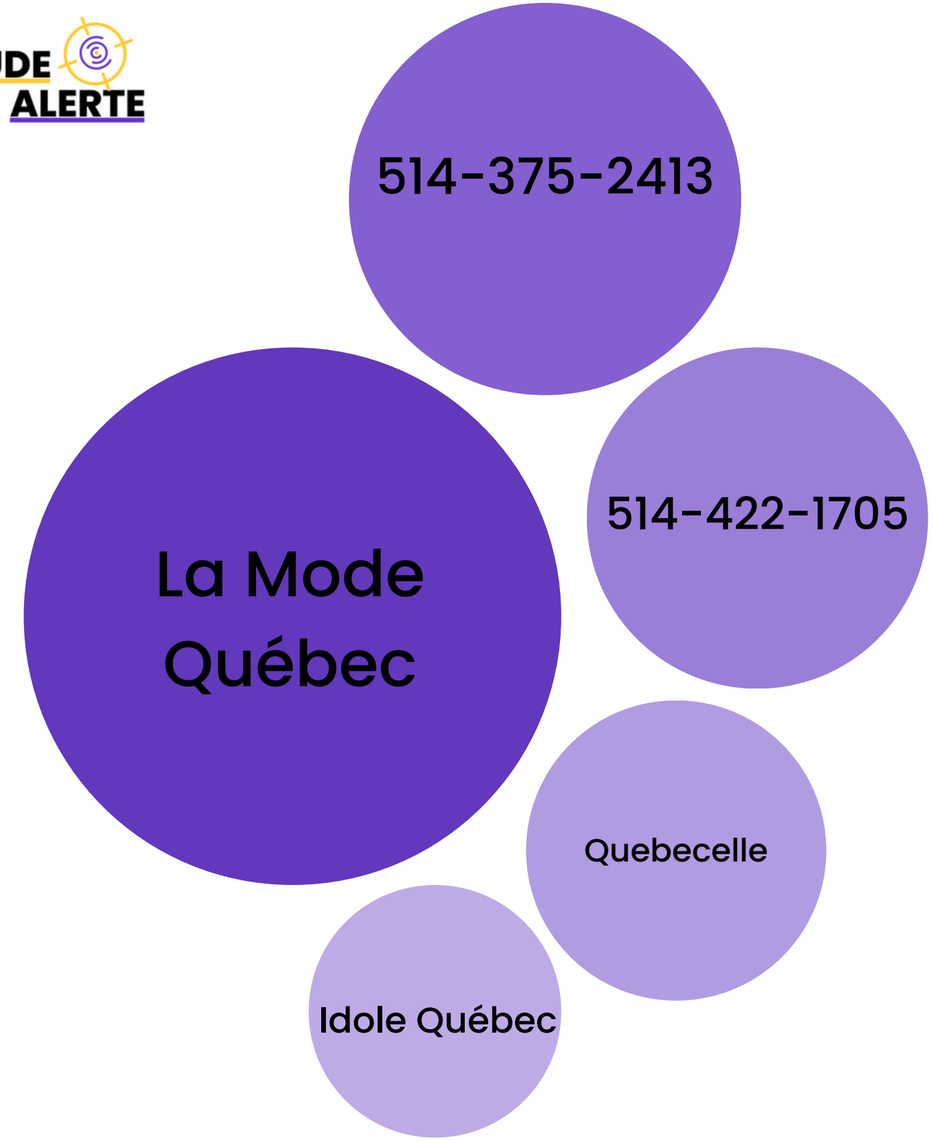
ORGANISATION PERSONNIFIÉE

Au premier trimestre 2025, plus d'un quart des signalements (27 %) concernaient des cas d'usurpation d'identité d'organisations. En tête de liste figure l'**autoroute A25** (11 %), ciblée dans une vaste campagne d'hameçonnage par SMS amorcée l'année précédente.

Amazon (8 %) reste une organisation fréquemment usurpée, notamment dans le cadre d'arnaques téléphoniques, tout comme la **Banque de Montréal (BMO)** (8 %), le **Mouvement Desjardins** (7 %) et **Equifax** (5 %). Cette tendance s'explique en partie par un regain d'intérêt pour le téléphone comme vecteur privilégié de contact pour les fraudeurs, qui misent sur l'usurpation d'institutions financières afin d'instaurer un climat de confiance, souvent renforcé par un sentiment d'urgence.

D'autres types d'organisations ont également été ciblés : des agences gouvernementales (18 %), des services de télécommunications (9 %), des entreprises technologiques (9 %) ainsi que des commerces (7 %). Ces usurpations s'opèrent par différents moyens, principalement l'hameçonnage téléphonique, par SMS et par courriels.

FRAUDE ALERTE



REQUÊTES

Au premier trimestre 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 suspects.

Une majorité de ces recherches portaient sur des sites de commerce en ligne, notamment **La Mode Québec** (13 196 requêtes), **Quebecelle** (3 237 requêtes) et **Idole Québec** (2 128 requêtes). Cette tendance est cohérente avec les données de signalement sur Fraude-Alerte, où les fraudes liées à ce type de sites figurent parmi les plus fréquemment rapportées.

Par ailleurs, plusieurs requêtes visaient à vérifier des numéros de téléphone associés à des pratiques douteuses. Le numéro **514-375-2413**, souvent relié à des appels silencieux, a été recherché à 7 941 reprises. Le **514-422-1705**, utilisé dans des tentatives de fraude se faisant passer pour la Banque de Montréal (BMO), a quant à lui généré 4 906 requêtes.

D’autres sites de vente en ligne ont également suscité un volume important de vérifications, notamment Aloha Towel, Louis Québec, Allure Québec ou encore Cuistel, indiquant une vigilance accrue de la part des internautes face à la recrudescence des sites de vente frauduleux.

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 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.