RAPPORT D'ACTIVITÉ 2024

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

3 652 SIGNALEMENTS

607 001 VISITES

4 412$ PERDU EN MOYENNE

Signalements

- Total des signalements reçus : 3 974
- Nombre de signalements analysés : 3 652

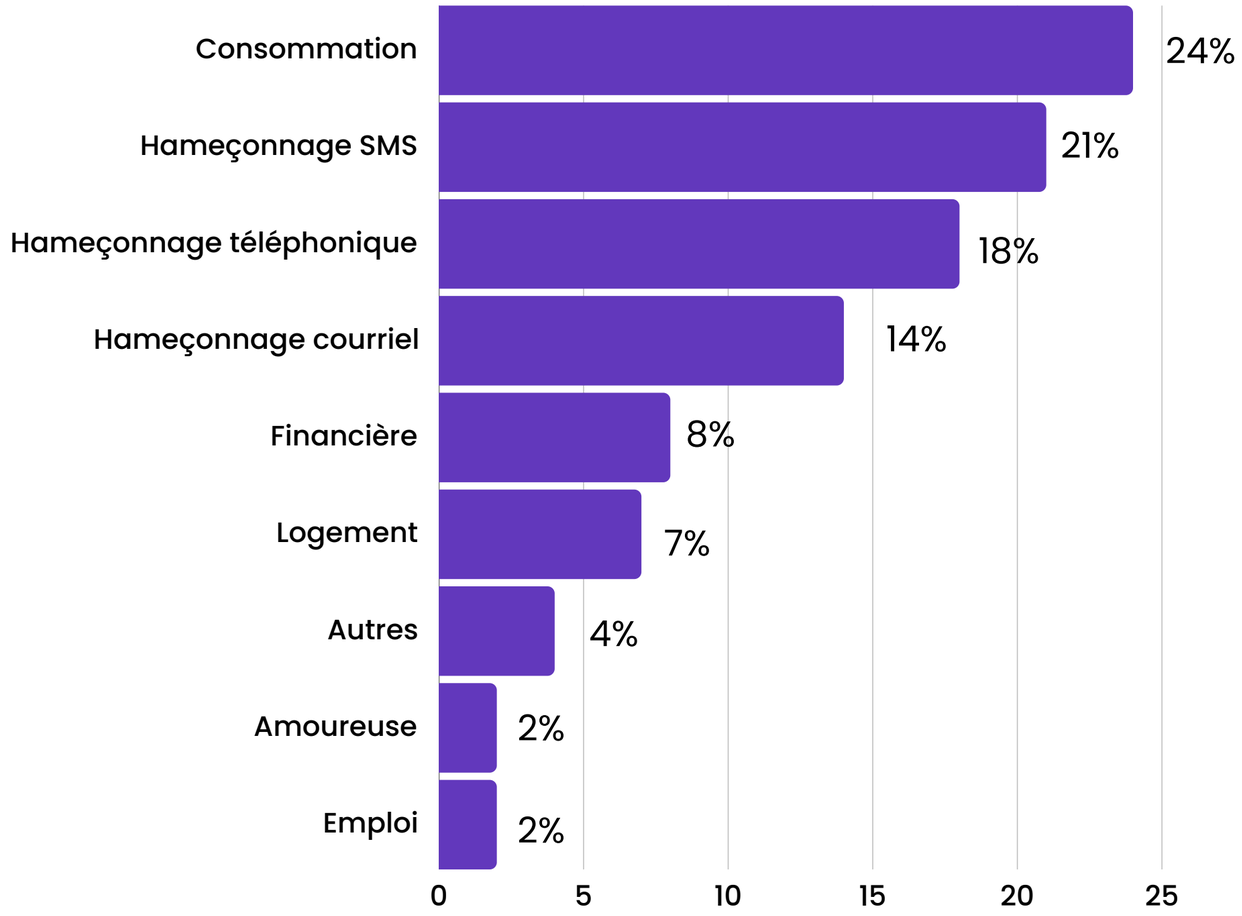
Montant perdus

- Perte médiane : 333 $
- Perte moyenne : 4 142 $
  - *Note* : Seuls environ 319 (9%) signalements mentionnaient le montant perdu
- Perte maximale : 200 000 $ (fraude à l'investissement liée aux cryptomonnaies)
- Perte minimale : 1,34 $ (site web frauduleux)

Observations

- Le nombre de signalements a presque doublé entre 2023 et 2024 et le nombre de visites a quant à lui également doublé, traduisant un intérêt accru du public à Fraude-alerte. En revanche, la perte moyenne a diminué, ce qui pourrait indiquer que les fraudes impliquant de très gros montants ont été moins nombreuses. Le montant maximal perdu a également diminué.
- Le montant moyen et médian des pertes a diminué alors que le taux de signalement mentionnant les montants perdus était presque similaire (8,4% en 2023 et 9% en 2024). Cela peut s'expliquer par un plus grand signalement des pertes liées à la fraude à la consommation dont les montants sont moindres que ceux engendré par la fraude à l'investissement.

TYPE DE FRAUDE



En 2024, la **fraude à la consommation** a connu une forte augmentation, en grande partie due à la prolifération de sites de vente se présentant comme québécois, mais en réalité basés sur le *dropshipping*, proposant des produits importés de Chine. Bien que plusieurs de ces sites (Orthoconfortable, L'atelier d'Émelie, Nyzara) aient déjà été signalés en 2023, ils ont continué à faire de nombreuses victimes et de nouveaux sites ont fait leur apparition (Fabula, Allure Québec, Idole Québec). Les fraudes liées aux petites annonces sur Marketplace ont également été fréquemment signalées au cours de la première moitié de l'année, avant de diminuer par la suite.

L'**hameçonnage par SMS** demeure l'un des types de fraude les plus répandus, notamment à travers de vastes campagnes menées au début et à la fin de l'année, ciblant l'A25 et la SAAQ. Cette tendance confirme l'intérêt croissant des fraudeurs pour ce mode d'hameçonnage, au détriment du **courriel** qui a considérablement baissé par rapport à 2023.

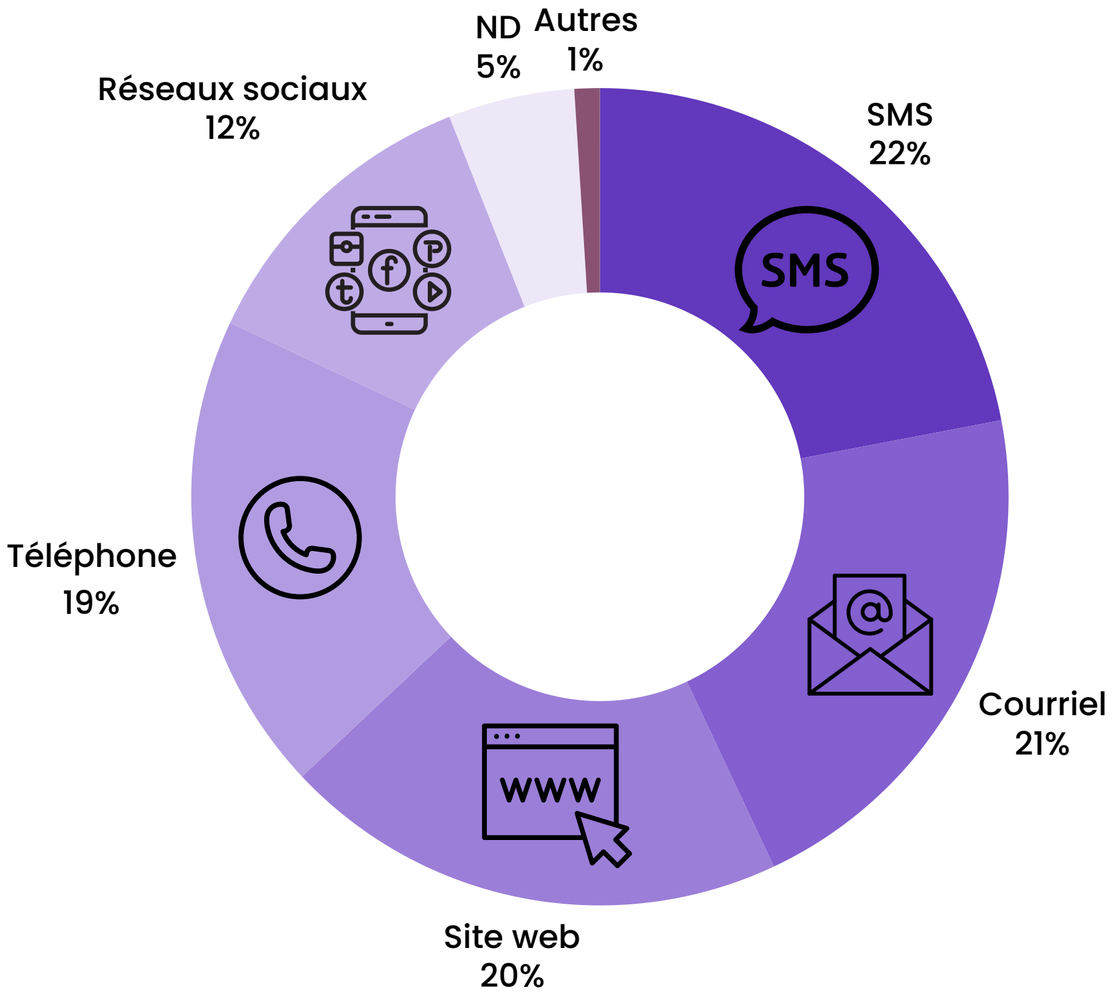
L'**hameçonnage téléphonique** est également resté courant, incluant des appels sans sonnerie, des messages préenregistrés et des sollicitations frauduleuses usurpant notamment l'identité d'Amazon et de Google. En fin d'année, une vague d'appels frauduleux se faisant passer pour Google a été signalée, prétendant résoudre des problèmes d'indexation d'entreprise sur le moteur de recherche et exigeant un paiement.

Les **fraudes financières** ont été particulièrement répandues, notamment les arnaques à l'investissement en cryptomonnaie et les faux prêts, qui représentent les pertes financières les plus importantes. La **fraude au logement**, toujours sous formes de courriels réclamant des loyers impayés et de fausses annonces de location publiées sur Facebook Marketplace ont continué à être signalés même si pour cette dernière forme, plusieurs cas ont été recensés en début d'année, aucun signalement n'a été fait en fin d'année, contrairement à l'année précédente où de fausses annonces de logement à louer avaient été signalées tout au long de l'année.

Enfin, la catégorie "**Autres**" regroupe divers types de fraudes, notamment celles liées aux services d'escortes, à l'assistance informatique, à l'immigration, ainsi qu'aux cas de piratage et d'usurpation d'identité sur les réseaux sociaux. Quelques cas de **fraude amoureuse** ont également été rapportés. La **fraude à l'emploi**, impliquant de faux recrutements demandant l'achat de cartes cadeaux ou d'investissements en échange de tâches rémunérées, a également été observée.

FRAUDE ALERTE

CANAL DE COMMUNICATION



En 2024, les fraudeurs ont exploité plusieurs canaux pour entrer en contact avec leurs victimes. Le **SMS** a été le principal moyen utilisé, notamment lors de campagnes massives visant des services publics et bancaires, tels que l'A25, la SAAQ, Postes Canada et diverses institutions financières.

Bien que l'**hameçonnage par courriel** ait diminué, il demeure un canal privilégié pour certains types de fraudes, notamment la fraude au logement. Les **sites web** ont également joué un rôle clé, en particulier pour héberger des sites de vente frauduleux ainsi que pour des cas de fraudes aux faux prêts et aux cryptomonnaies.

Le **téléphone** reste largement utilisé pour divers types d'appels frauduleux, tandis que les **réseaux sociaux** ont servi à promouvoir des sites de *dropshipping* frauduleux et à publier de fausses annonces sur Marketplace. Il est important de souligner que l'ampleur de l'utilisation des réseaux sociaux est probablement sous-estimée : dans de nombreux cas, les fraudeurs attirent leurs victimes via des publicités en ligne, un élément souvent négligé dans les signalements.

Par ailleurs, un certain nombre de signalements n'ont pas précisé le canal de communication utilisé, notamment en ce qui concerne les fraudes financières. D'autres moyens, comme **WhatsApp**, ont également été employés pour des escroqueries ciblées, telles que la fraude à l'emploi.

FRAUDE ALERTE

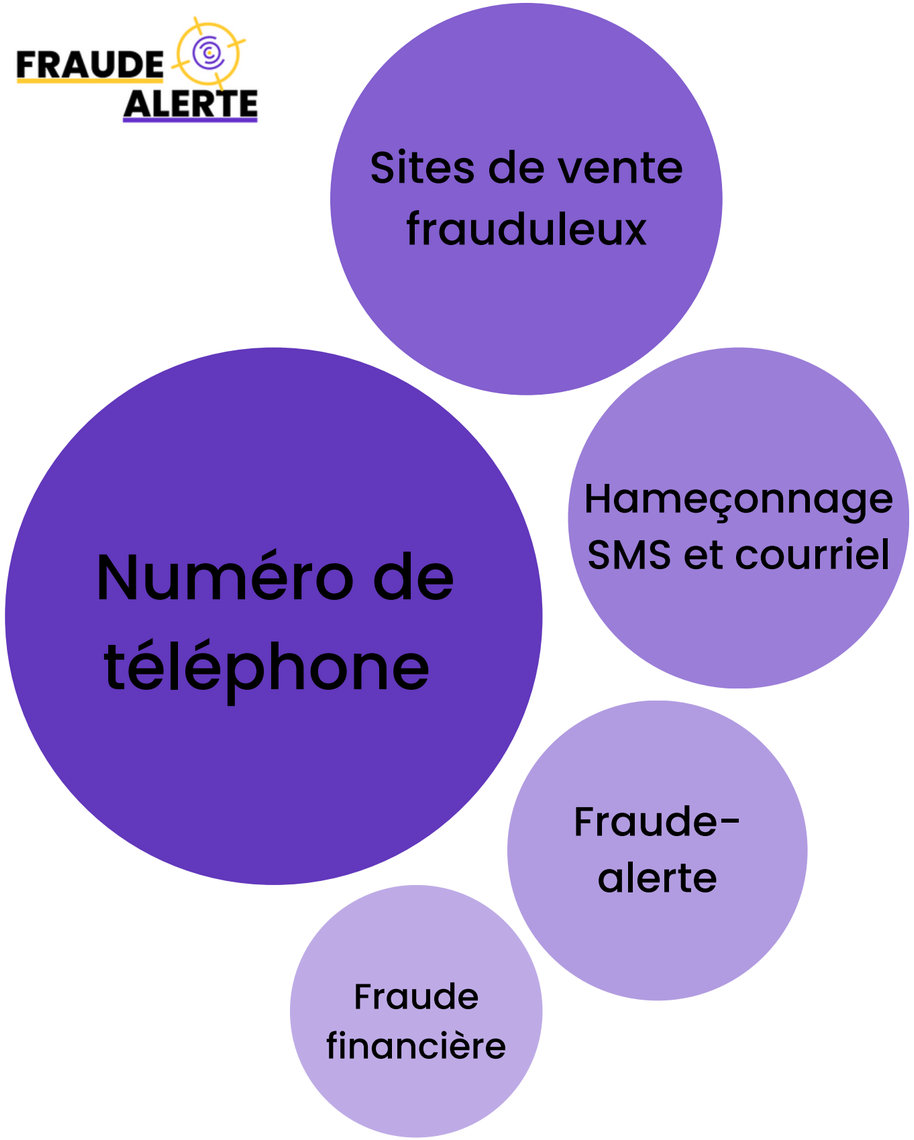
ORGANISATION PERSONNIFIÉE

En 2024, l'**A25** a été l'organisation la plus usurpée, principalement réalisée via des campagnes d'hameçonnage par SMS, exigeant frauduleusement des paiements de péage. À noter que la **Ville de Montréal** a également été mobilisée en début d'année dans ce type de campagnes prétextant le paiement d'amendes de stationnement. **Postes Canada** a également été une cible fréquente, notamment dans des fraudes liées à des colis inexistants où des frais de livraison supplémentaires étaient exigés des victimes.

Amazon a été largement usurpée dans des cas d'hameçonnage téléphoniques, où les fraudeurs contactaient les victimes sous prétexte de transactions suspectes nécessitant une confirmation ou une annulation. La **Société de l'assurance automobile du Québec (SAAQ)** a aussi été exploitée dans des fraudes prétendant offrir des remboursements.

Les institutions financières n'ont pas été épargnées surtout en fin d'année. **Desjardins** a été utilisée dans des cas de fraude "grand-parents" et d'hameçonnage bancaire. La **Banque de Montréal (BMO)** a également été usurpée dans des cas d'hameçonnage par SMS tout comme le portail gouvernemental québécois **ClicSÉQUR**.

Enfin, en fin d'année, la marque **La Vie en Rose** a été détournée dans des fraudes à la consommation via des sites frauduleux prétendant organiser des ventes de liquidation.



REQUÊTES

Les internautes se sont rendus sur Fraude-alerte en utilisant diverses requêtes sur les moteurs de recherche. Les requêtes les plus fréquentes ont porté sur des **numéros de téléphone** (190 646 requêtes, et près de 1 125 233 impressions), de nombreuses personnes ayant cherché à vérifier l'identité des appelants.

Les requêtes impliquant des **sites de vente frauduleux** (ex: Nyzara, Orthoconfortable, Allure Québec, etc.) ou des **adresses courriel liés à des site de vente frauduleux** ont également fait l'objet d'un grand nombre de requête (65 918 requêtes et 441 378 impressions).

D'autres requêtes ont concerné des cas d'**hameçonnage par SMS et courriel** (ex: gigadat, mafacturea25.com, Michael Duheme, etc.)(16 508 requêtes, 120 687 impressions) pour lesquels les internautes ont cherché à vérifier la véracité du contenu de SMS ou de courriel.

Fraude-alerte (16 014 requêtes, 26 375 impressions) reste une requête populaire auprès des internautes, que ce soit pour se rendre directement sur la plateforme ou après en avoir entendu parler via les médias.

Enfin, plusieurs **plateforme d'investissement en cryptomonnaies**, **sites web de prêts financiers** et **noms de courtier en investissement** (ex: tradiora, matrollo, etc.) (2 620 requêtes, 19321 impressions) ont fait l'objet de requêtes qui ont amené les internautes vers Fraude-alerte.

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.