

# RAPPORT D'ACTIVITÉ Trimestre 1 – 2024

**FRAUDE**   
**ALERTE**

# FRAUDE-ALERTE.CA

**1016 SIGNALEMENTS**

**158 865 VISITES**

**3 237\$ MONTANT  
MOYEN PERDU**

# FAITS SAILLANTS

## Signalements

- Total signalements reçus : 1221
- Signalements analysés : 1016
  - Exclusions :
    - Signalements provenant de l'étranger (notamment de France)
    - Signalements non pertinents ou incohérents

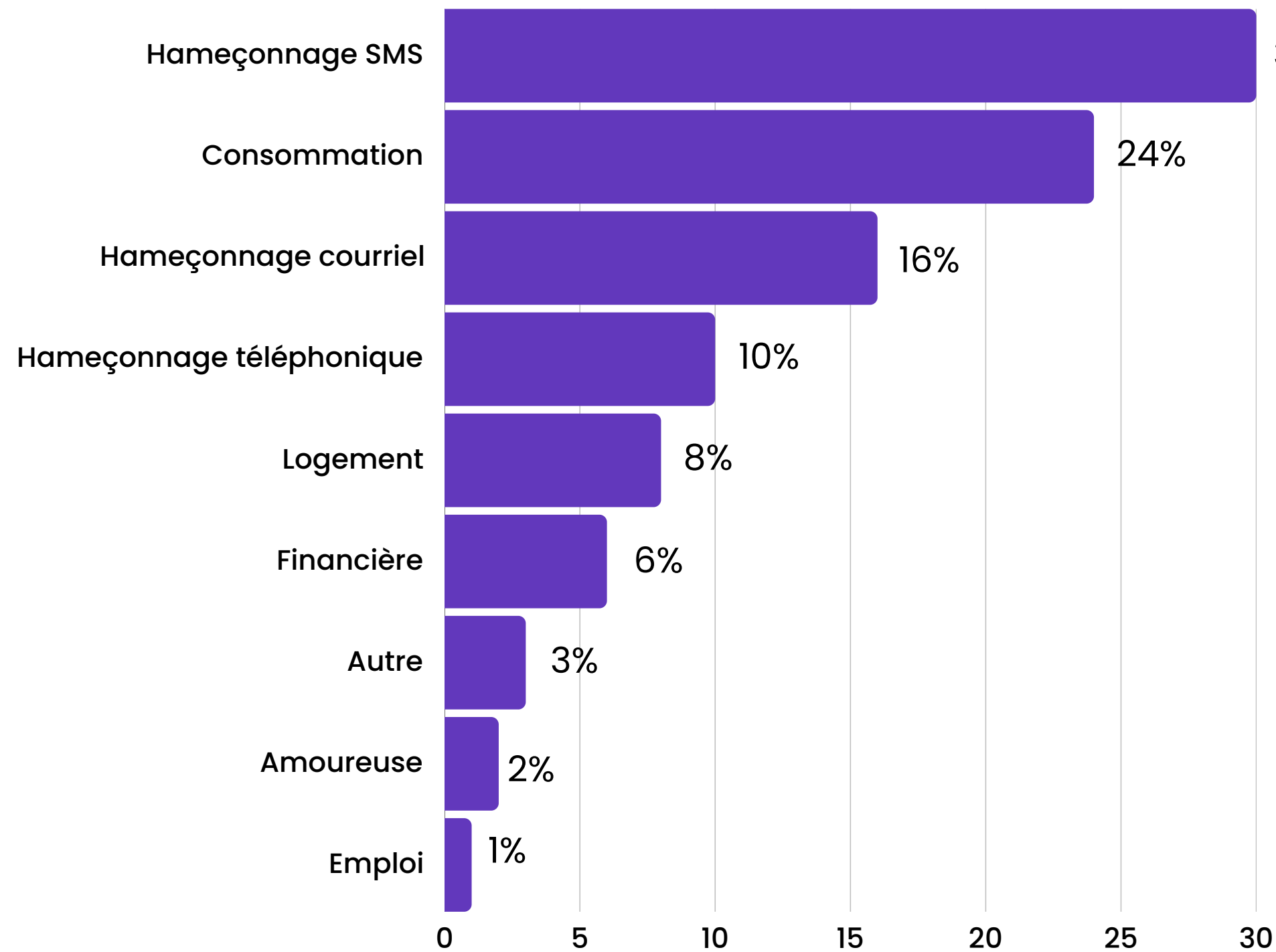
## Montant perdu

- Perte médiane : 253 \$
- Perte moyenne : 3 237\$
  - *Note* : Seuls 95 signalements mentionnaient le montant perdu
- Perte maximale : 90 000 \$ (fraude à l'investissement/crypto)
- Perte minimale : 20 \$ (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 2024, l'**hameçonnage par SMS** s'est imposé comme la fraude la plus fréquemment signalée sur la plateforme Fraude-alerte. Cette hausse est principalement attribuable à une vaste campagne d'hameçonnage usurpant l'identité de l'autoroute A25, de la Ville de Montréal, et du gouvernement, ciblant les citoyens sous prétexte de fausses amendes pour excès de vitesse ou de stationnement.

La **fraude à la consommation** reste, elle aussi, largement répandue, notamment via des sites de vente en ligne frauduleux exploitant le *dropshipping*, ainsi que des annonces trompeuses sur Facebook Marketplace.

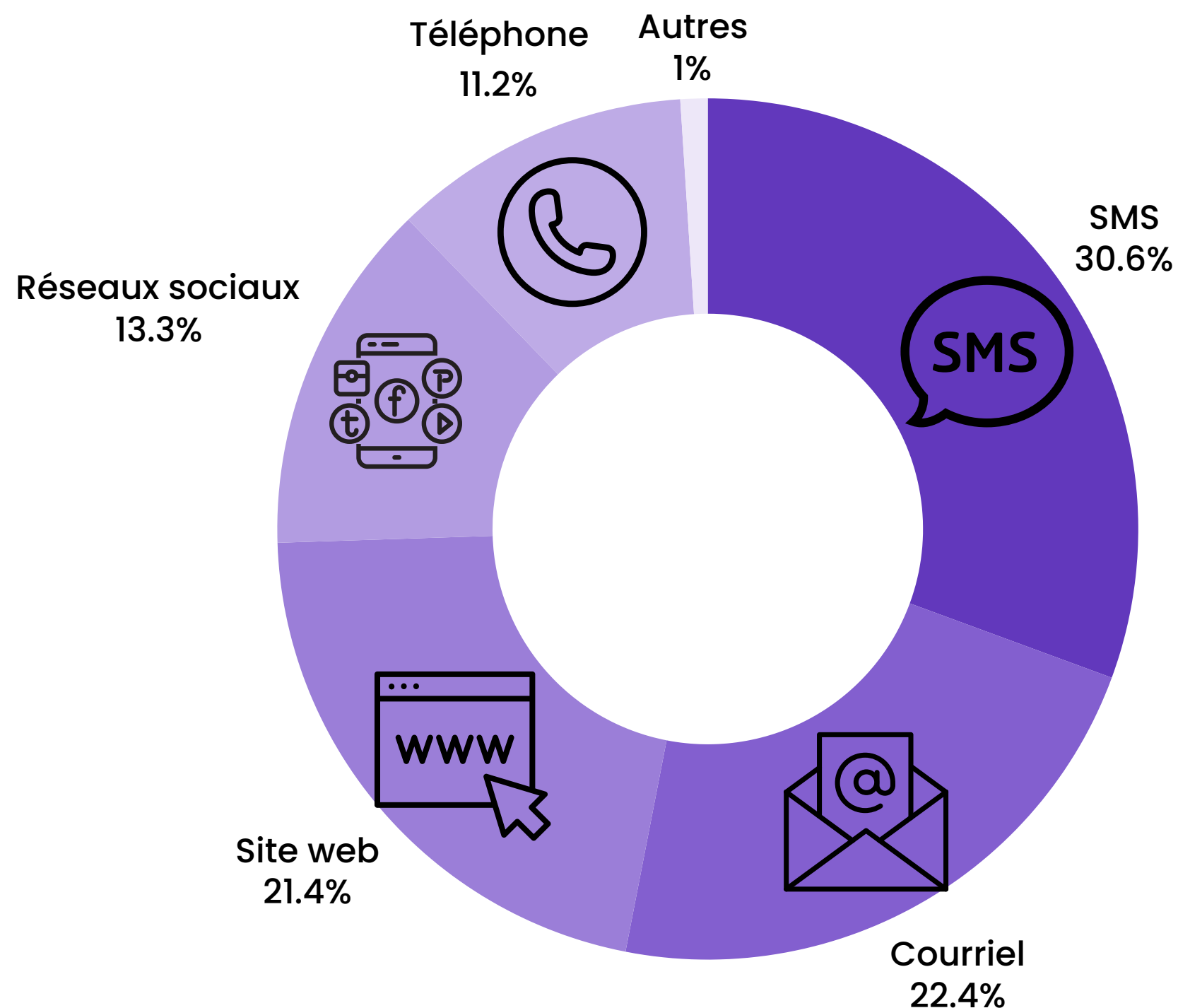
En revanche, contrairement à l'année 2023 où l'**hameçonnage par courriel** occupait la deuxième place, ce type de fraude a connu une baisse significative au cours des premiers mois de 2024. Les signalements d'**hameçonnage téléphonique** ont eux aussi reculé durant cette période.

Comme l'année précédente, la **fraude au logement** a continué d'être notable avec les mêmes stratagèmes, soit les courriels réclamant des loyers impayés et un nombre croissant de fausses annonces de logement sur Facebook Marketplace.

Les **fraudes financières**, en tête des pertes les plus lourdes, concernent surtout les investissements en cryptomonnaies et les faux 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.

Enfin, plusieurs cas de **fraude amoureuse** ont été signalés. La catégorie "**Autre**" englobe des cas de fraude à l'immigration, des services d'escortes, de rénovation ou informatiques frauduleux, ainsi que des usurpations d'identité et piratages sur les réseaux sociaux.

# CANAL DE COMMUNICATION



Au premier trimestre 2024, à l'instar des types de fraude, le **SMS** s'est imposé comme le canal privilégié des fraudeurs, notamment dans les campagnes d'hameçonnage par SMS et les fraudes à l'emploi. 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 **sites web**, presque tout aussi important que les courriels, restent un vecteur fréquent de fraudes, en particulier pour celles liées au *dropshipping*, aux faux prêts et aux cryptomonnaies.

Les **réseaux sociaux**, et plus spécifiquement Facebook, ont joué un rôle central dans plusieurs types de fraudes. En effet, parmi l'ensemble des réseaux sociaux, dans 98 % des cas, les fraudeurs ont utilisé cette plateforme pour attirer leurs victimes, soulignant ainsi sa popularité auprès des cybercriminels. Enfin, le **téléphone** reste un canal toujours exploité par les escrocs, que ce soit pour des appels silencieux, des services de voyance ou des offres de courtage dans les cryptomonnaies.

# ORGANISATION PERSONNIFIÉE



Au premier trimestre 2024, plus d'un tiers (34 %) des signalements portaient sur des cas d'usurpation d'identité d'une organisation. En tête de liste figure la **Ville de Montréal** (11 %), prise pour cible dans une vaste campagne d'hameçonnage par SMS. L'**autoroute A25** (7%), largement usurpée fin 2023 a continué d'être mobilisée par les fraudeurs.

**Poste Canada** (9 %) reste une cible fréquente des fraudeurs, particulièrement via SMS, tandis qu'**Amazon** (7 %) a été régulièrement usurpée, principalement dans des arnaques téléphoniques. Vers la fin du trimestre, la **SAAQ** (7 %) a également été usurpée pour une campagne d'hameçonnage par SMS, prétextant des remboursements aux automobilistes

Par ailleurs, de nombreuses institutions financières (18 %), agences gouvernementales (11 %), services de livraison (8 %) et commerces (6 %) ont également été usurpés par les fraudeurs, confirmant la diversité des cibles exploitées pour tromper le public.

514-375-2413

Fraude-alerte

450-805-4708

438-738-1424

581-781-7510

Les internautes se sont rendus sur Fraude-alerte en utilisant diverses requêtes sur les moteurs de recherche. 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 téléphones tels que, **450-805-4708** (36 855 requêtes) un appel téléphonique invitant à participer à un sondage, loin devant le **514-375-2413** (7 285 requêtes) et le **581-781-7510** (2 295 requêtes) associés à des appels silencieux et le **438-738-1424** (3 506 requêtes) correspondant à un appel faisant la promotion de services de voyance.

"**Fraude-alerte**" a également fait l'objet d'un nombre de requêtes (6 846 requêtes) démontrant une fois de plus la curiosité des utilisateurs envers la plateforme.



# 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.**

