

RAPPORT D'ACTIVITÉ

Trimestre 3 – 2024

FRAUDE 
ALERTE

FRAUDE-ALERTE.CA

748 SIGNALEMENTS

139 144 VISITES

**2 202\$ PERDU EN
MOYENNE**

FAITS SAILLANTS

Signalements

- Total signalements reçus : 885
- Signalements analysés : 748
 - Exclusions :
 - Signalements provenant de l'étranger (notamment de France)
 - Signalements non pertinents ou incohérents

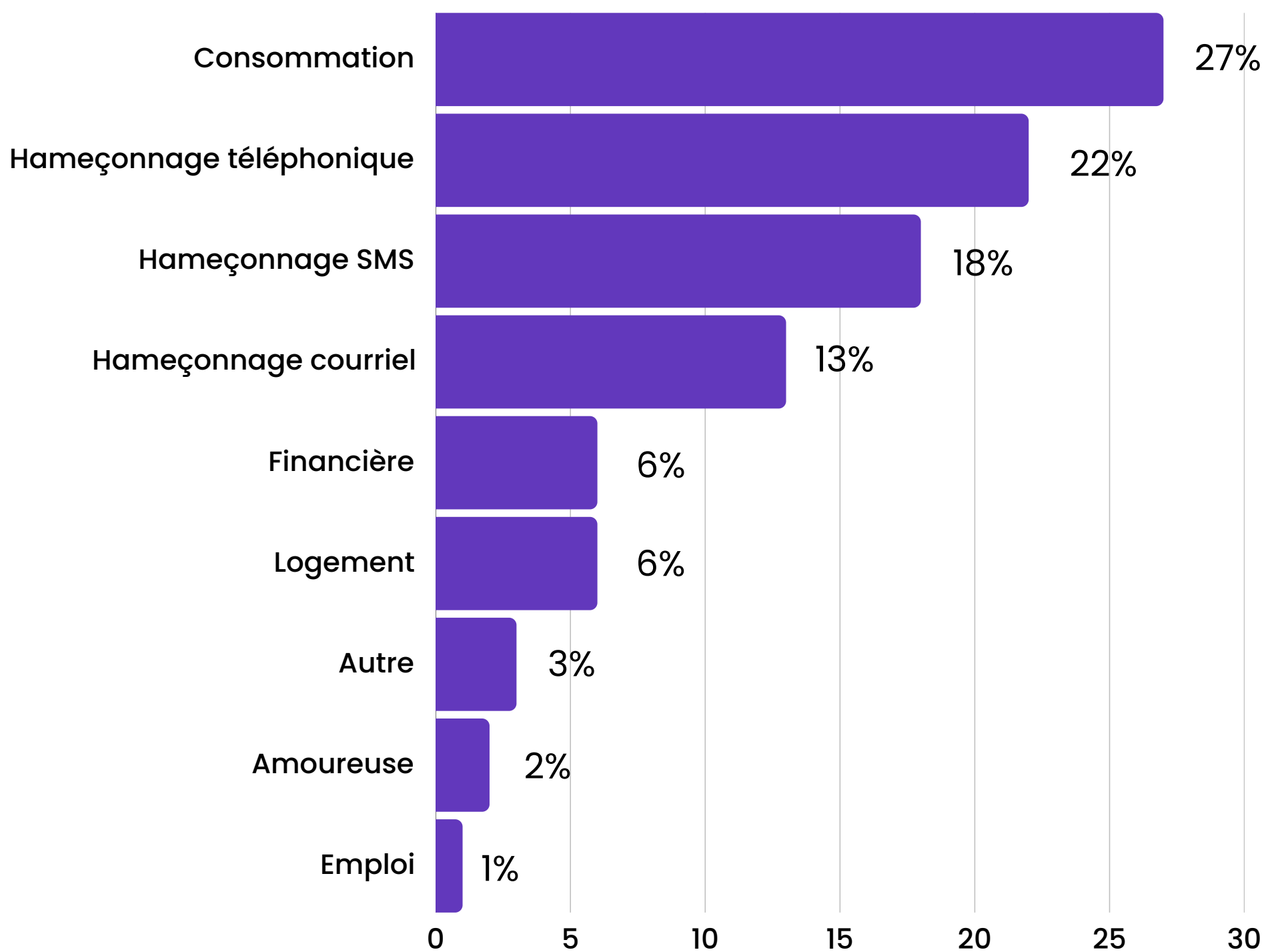
Montant perdu

- Perte médiane : 297\$
- Perte moyenne : 2 202\$
 - *Note* : Seuls 34 signalements mentionnaient le montant perdu
- Perte maximale : 20 000\$ (fraude à l'investissement/crypto)
- Perte minimale : 1,34\$ (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

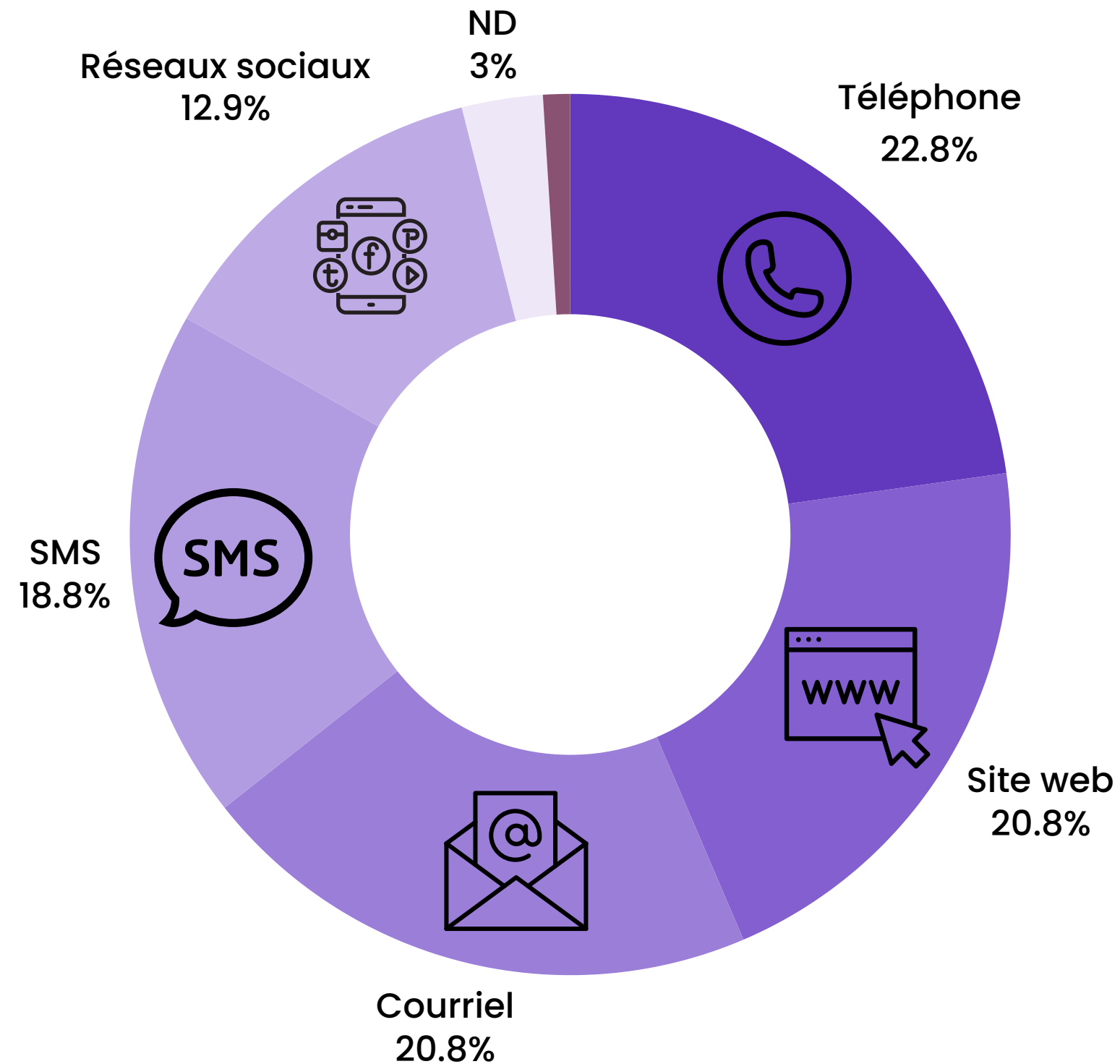


Au troisième trimestre 2024, la **fraude à la consommation** reste le type de fraude le plus fréquemment signalé sur la plateforme Fraude-Alerte. Cette tendance s'explique principalement par la multiplication des sites de vente exploitant le *dropshipping* et quelques annonces frauduleuses sur Marketplace.

L'**hameçonnage téléphonique** arrive en deuxième position parmi les fraudes les plus signalées, en raison d'une vaste campagne usurpant l'identité d'Amazon et de Google. Les fraudeurs prétendaient détecter des transactions suspectes sur la plateforme d'Amazon ou exigeaient un paiement pour l'indexation d'une entreprise sur Google. L'**hameçonnage par SMS** a également connu une hausse des signalements, notamment à cause de la résurgence de la campagne d'hameçonnage utilisant l'identité de l'A25 et de plusieurs institutions financières. En revanche, l'**hameçonnage par courriel** a diminué.

Les **fraudes financières** restent celles qui entraînent les plus grandes pertes, principalement sous forme d'investissements frauduleux en cryptomonnaies. La **fraude au logement** demeure stable, mais elle est majoritairement liée à des courriels frauduleux réclamant des loyers impayés.

Enfin, la catégorie « **Autre** », qui regroupe des cas de fraude à l'immigration, de services d'escortes ou informatiques frauduleux, d'usurpations d'identité, de piratages sur les réseaux sociaux, ainsi que les **fraudes amoureuses et à l'emploi** été moins signalées ce trimestre.



CANAL DE COMMUNICATION

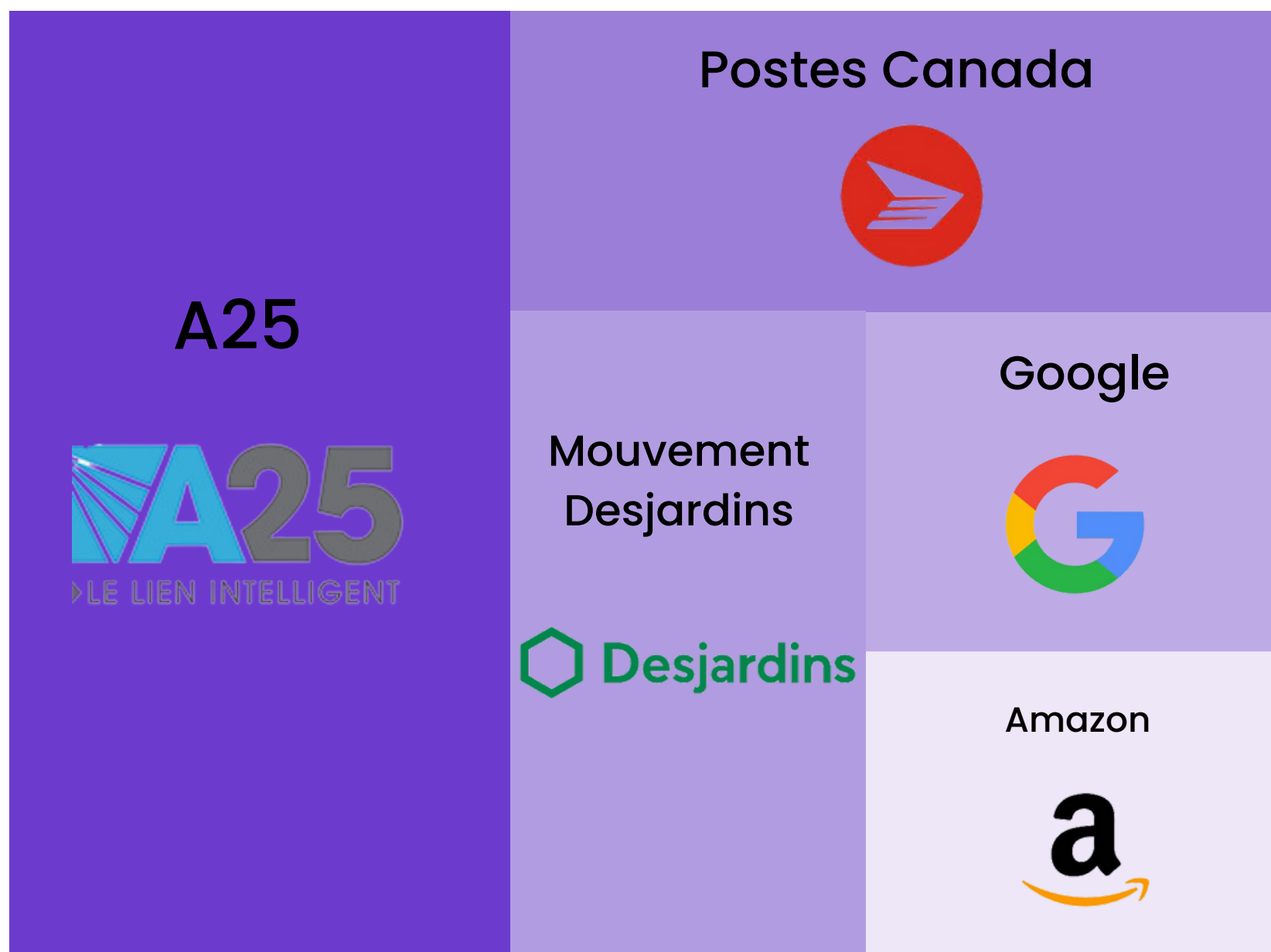
Le **téléphone** demeure l'un des canaux les plus exploités par les fraudeurs, tel que constaté par l'augmentation de l'hameçonnage téléphonique. En parallèle, les **sites web** continuent d'être un levier privilégié par les fraudeurs, notamment dans les cas de fraude à la consommation, où ils sont largement mobilisés pour tromper les victimes.

Les fraudeurs recourent également aux **courriels**, en particulier pour des cas de fraude au logement, sous prétexte de loyers impayés, ainsi que pour de faux concours prétendument organisés par de grandes enseignes.

Contrairement au trimestre précédent, le **SMS** a connu une augmentation, principalement en raison d'une vaste campagne d'hameçonnage usurpant l'identité de l'A25.

Enfin, les **réseaux sociaux**, et plus particulièrement Facebook, jouent un rôle central dans plusieurs types de fraudes. Cette plateforme demeure prisée par les fraudeurs pour les fraudes à la consommation.

ORGANISATION PERSONNIFIÉE



Au troisième trimestre 2024, **36 %** des signalements concernaient des cas d'usurpation d'identité d'organisations. En tête de liste, l'**A25** a été la plus ciblée (15 %), victime d'une vaste campagne d'hameçonnage par SMS. Elle est suivie par **Postes Canada** (7 %) et le **Mouvement Desjardins** (6 %), ce dernier ayant été usurpé dans plusieurs fraudes, notamment via de l'hameçonnage par SMS et des arnaques téléphoniques de type « fraude aux grands-parents ».

Google et **Amazon** (5 % chacun) ont également été imités dans des campagnes d'hameçonnage téléphonique. Dans le cas de Google, des fraudeurs demandaient aux entreprises de payer pour leur indexation sur le moteur de recherche. Quant à Amazon, les appels frauduleux évoquaient de prétendues charges appliquées aux comptes des victimes.

Par ailleurs, de nombreuses **organisations gouvernementales** (19 %), comme la Ville de Montréal et la Gendarmerie royale du Canada, ainsi que des **commerces** (13 %) et des **institutions financières** (10 %), ont aussi été ciblées. Dans une moindre mesure, les fraudeurs ont également usurpé des **services de télécommunications** (4 %) et de **livraison** (4 %), illustrant la diversité des entités exploitées pour tromper le public.

438-809-2414

514-375-2413

Fraude-alerte

800-672-7339

450-805-4708

Les internautes ont accédé à Fraude-Alerte en effectuant diverses recherches sur les moteurs de recherche. Comme lors des deux trimestres précédents, la majorité de ces requêtes visaient à vérifier l'identité d'un appelant.

De nombreux utilisateurs ont cherché des informations sur divers numéros de téléphone, notamment le **514-375-2413** (6 932 requêtes), le **800-672-7339** (2 940 requêtes) et le **450-805-4708** (2 642 requêtes), tous associés à des appels silencieux. Le numéro **438-809-2414** (6 651 requêtes) a quant à lui été signalé pour la diffusion d'un message préenregistré annonçant l'ouverture d'un magasin.

Le terme "**Fraude-Alerte**" (2 940 requêtes) a également été fréquemment recherché par les internautes. Par ailleurs, plusieurs sites de vente en ligne frauduleux, tels que Koliza Québec, Emma Québec Cuir, Nyzara et Fabula, ont suscité un grand nombre de recherches au cours du troisième trimestre.



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.

