RAPPORT D'ACTIVITÉ
Trimestre 3 - 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

508 SIGNALEMENTS

143 940 VISITES

2 189$ DE PERTES MOYENNES

Signalements

- Total signalements reçus : 796
- Signalements analysés : 508
  - Exclusions :
    - Signalements provenant de l'étranger
    - Signalements non pertinents ou incohérents

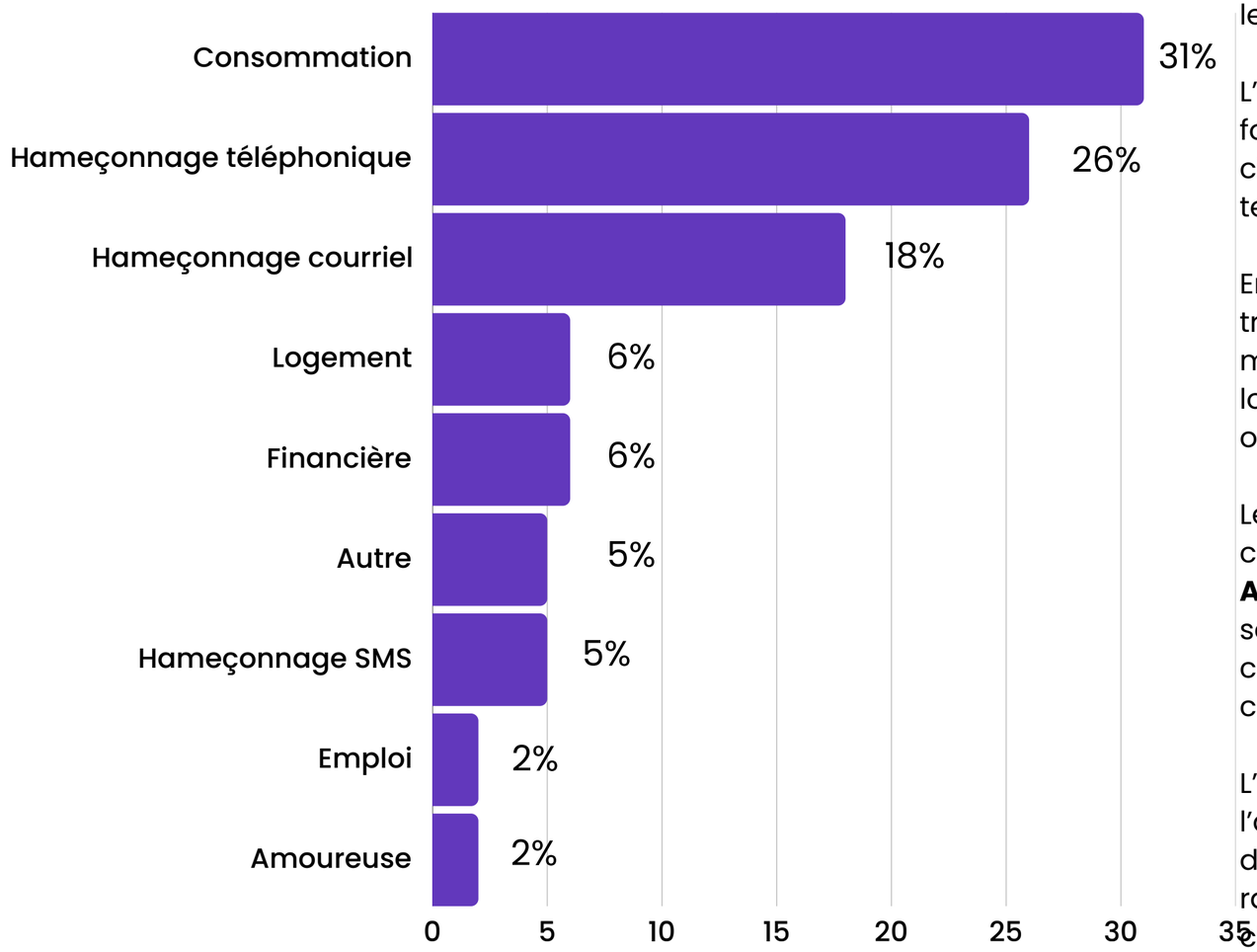
Montant perdus

- Perte médiane : 250 $
- Perte moyenne : 2 189 $
  - *Note* : Seuls 68 signalements (environ 13%) mentionnaient le montant perdu
- Perte maximale : 41 000 $ (fraude à l'investissement/crypto)
- Perte minimale : 14,95 $ (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 troisième trimestre de 2025, la tendance observée depuis le début de l'année se confirme : **la fraude à la consommation** demeure une part importante des signalements. De nombreux nouveaux sites de vente en ligne, souvent basés sur le modèle du parachutage (*dropshipping*), continuent d'émerger.

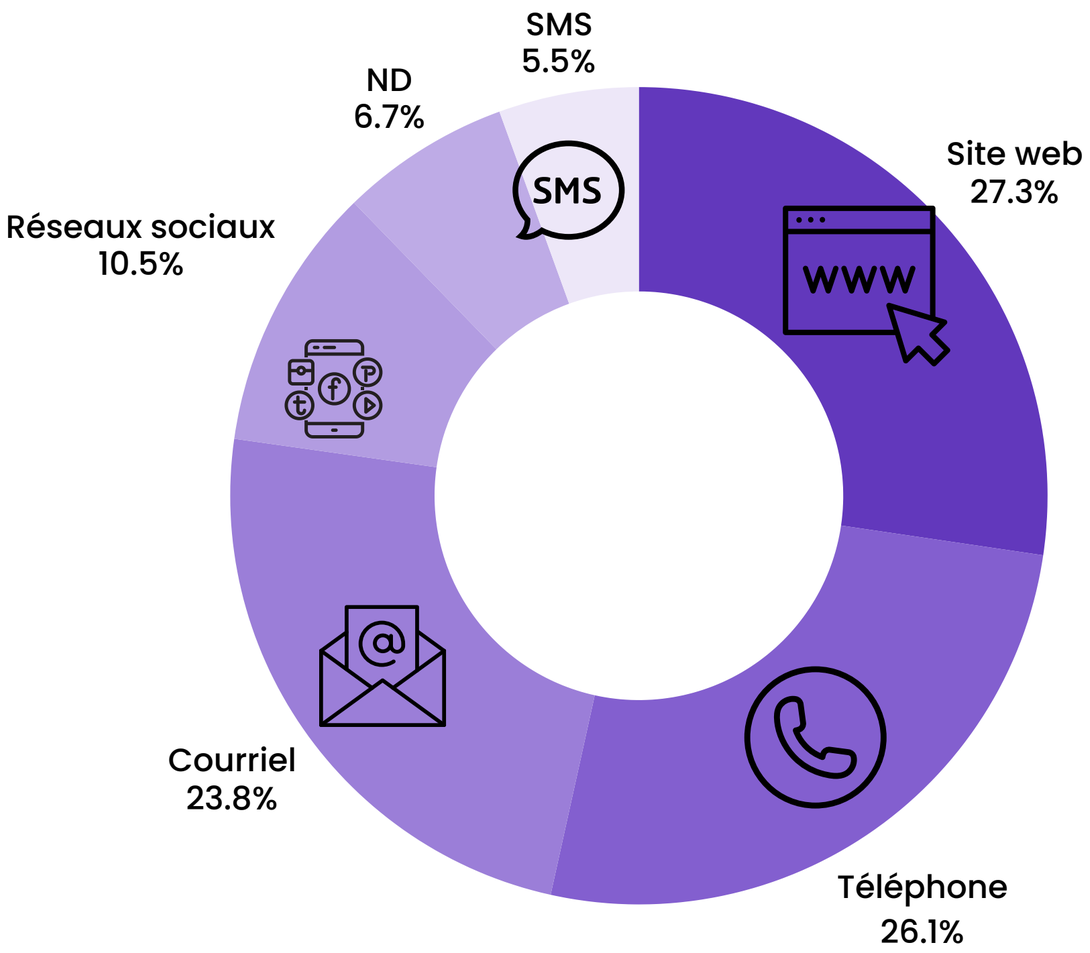
L'**hameçonnage téléphonique** se maintient à un niveau stable et demeure la forme de fraude où l'usurpation d'identité d'entreprises est la plus fréquente, ciblant notamment des institutions financières et des entreprises technologiques, telles que Google.

En revanche, l'**hameçonnage par courriel** poursuit sa baisse marquée ce trimestre. La **fraude au logement** enregistre une légère hausse, bien que la majorité des signalements concernent des courriels frauduleux réclamant des loyers impayés. À noter que plusieurs cas de fraude liée à la location de chalets ont été signalés au troisième trimestre.

Les **fraudes financières** restent dominées par les investissements en cryptomonnaies, tandis que les faux prêts continuent de reculer.La catégorie « **Autre** » est en nette progression et regroupe, entre autres, des fraudes liées aux services, des usurpations d'identité sur les réseaux sociaux et des piratages de courriels et d'appareils personnels, avec une augmentation notable des cas concernant les services de voyance et d'escorte.

L'**hameçonnage par SMS** continue sa baisse, en raison possiblement de l'absence de campagnes d'hameçonnage massives observables l'année dernière. La **fraude à l'emploi** a également connu une nette augmentation en raison d'une recrudescence de cas usurpant l'identité de Randstad et ciblant les chercheurs d'emploi. Enfin, plusieurs cas de **fraude amoureuse** ont été signalés.

FRAUDE ALERTE



CANAL DE COMMUNICATION

Les **sites web** constituent un vecteur majeur, notamment dans les fraudes à la consommation. Le **téléphone**, qui avait retrouvé la faveur des fraudeurs au premier et au deuxième trimestre 2025, demeure leur canal privilégié 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, ils cherchent à instaurer un climat de confiance auprès des victimes.

Le **courriel** est particulièrement répandu dans les fraudes au logement, notamment pour exiger de faux loyers impayés. Les **réseaux sociaux**, et en particulier Facebook, jouent également un rôle central dans la diffusion de publicités redirigeant fréquemment les victimes vers de faux sites de vente, tandis que la section Marketplace. À noter que plusieurs signalements mentionnent l'utilisation d'Instagram pour la diffusion de ces publicités frauduleuses.

Le **SMS** reste moins sollicité au troisième trimestre. Notons également qu'un nombre important de signalements ne permettent pas d'identifier le canal de communication utilisé par les fraudeurs, et ce, notamment dans les cas de fraude à l'investissement.

FRAUDE ALERTE

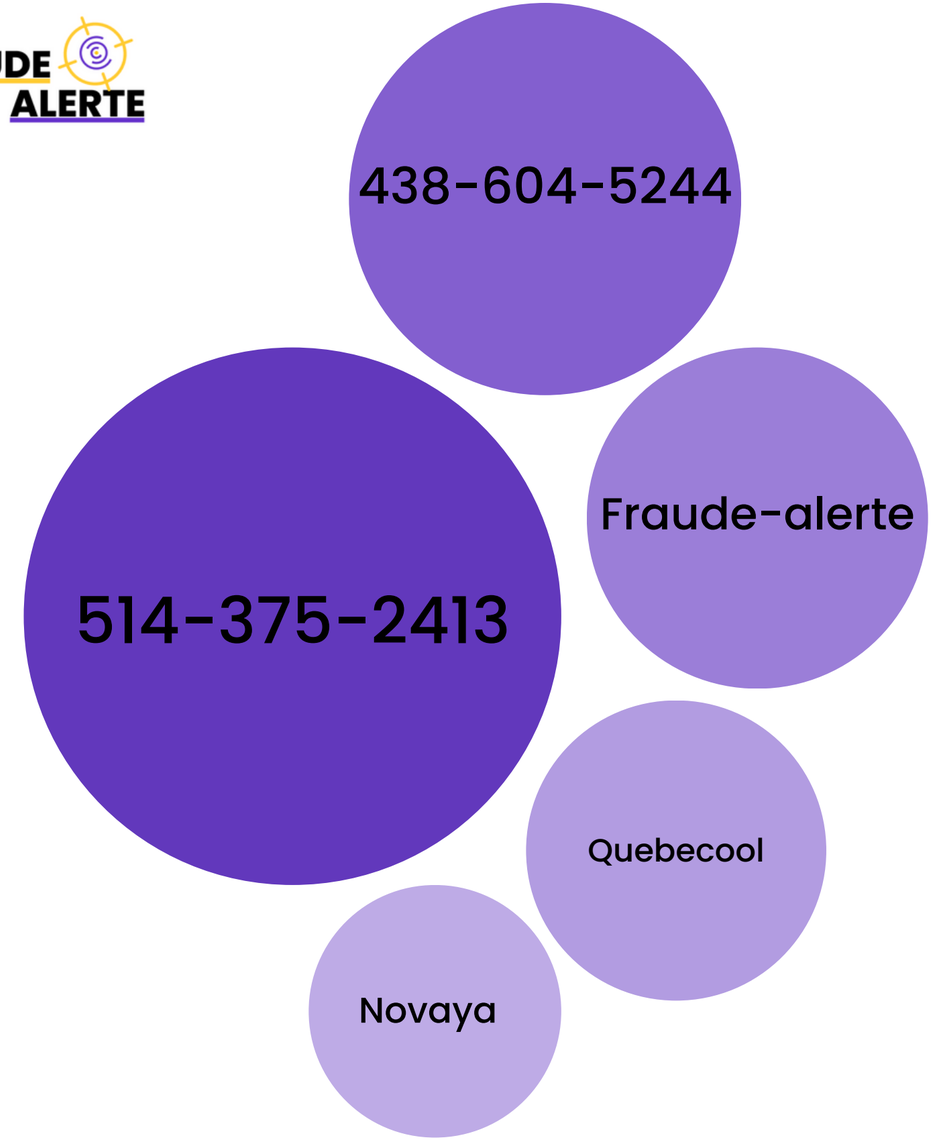
ORGANISATION PERSONNIFIÉE

Au troisième trimestre 2025, 20 % concernaient des cas d'usurpation d'identité d'organisations. En tête de liste figure **Equifax**, ciblée dans 12% des signalements, au cœur d'une vaste campagne d'hameçonnage téléphonique. Les fraudeurs prétendaient informer les victimes qu'une alerte à la fraude avait été levée sur leurs comptes. La **Gendarmerie royale du Canada** a également été usurpée dans près de 9% des signalements, et ce, pour des cas d'hameçonnage prétendant des accusations de pornographie juvénile. **Amazon** (9%) a également été usurpée pour une campagne d'hameçonnage téléphonique prétendant des achats frauduleux.

Le **Mouvement Desjardins** (7 %) a été usurpé dans le cadre d'une fraude au faux représentant, où les fraudeurs se faisaient passer pour des employés de Desjardins et demandaient aux victimes leur NIP ainsi que leur carte de débit. Enfin, **Purolator** (5%) a également fait l'objet d'usurpation dans le cadre d'une campagne d'hamçonnage par courriel prétendant la livraison de colis.

Outre ces organisations, d'autres types de cibles ont été identifiés : des **entreprises technologiques**, telles que Google ou Apple (17%), des **institutions financières** (14 %), des **agences gouvernementales** (7 %) ainsi que des **commerces** (8 %). Dans la grande majorité des cas, ces usurpations étaient menées par hameçonnage téléphonique ou par courriel, confirmant la persistance de ces vecteurs dans les campagnes frauduleuses.

FRAUDE ALERTE



REQUÊTES

Au troisième 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 numéros de téléphone afin de vérifier l'identité des appelants. Parmi ces numéros, les suivants ont fait l'objet d'importantes requêtes: **514-375-2413** (10 454 requêtes) relié à des appels silencieux et le **438-604-5244** (7 533 requêtes) qui correspond à un message préenregistré demandant de peser sur un chiffre du clavier. **Fraude-alerte** (6 108 requêtes) a également fait l'objet de plusieurs recherches de la part des internautes. Enfin, deux sites de commerce en ligne, **Novaya** (1 907 requêtes) et **Quebecool** (1 605 requêtes), prétendant vendre des produits de confection québécois, ont également fait l'objet de nombreuses recherches par les internautes.

D'autres sites de vente en ligne ont également suscité un volume important de vérifications, notamment Quebecelle, Boutique Élégance, La Belle Courbe ou encore Aloha Towels, ce qui indique 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.