

Rapport annuel

2025/2026

Par : La Clinique de Cyber-Criminologie

Date de dernière modification: Mars 2026

Note: Ce projet a été réalisé grâce au soutien financier de l'Autorité des marchés financiers. Les informations, opinions et avis exprimés n'engagent que la responsabilité de la Clinique de Cyber-Criminologie de l'Université de Montréal.

Table des matières

Sommaire exécutif	2
Introduction	3
Offre de service	4
Qui sont les usagers du service?	4
Types de fraude observés	5
Préjudices chez les usagers	7
Besoins des usagers	8
Conclusion	15
ANNEXE I : Lexique des principaux types de fraude.	17

SOMMAIRE EXÉCUTIF

Après une année complète d'opération, la Clinique de Cyber-Criminologie dresse un bilan détaillé de ses activités, des usagers servis et des principales tendances observées en matière de fraude en ligne. Ce sommaire exécutif présente les faits marquants de l'année, entre autres les types de fraudes les plus fréquents et les principaux impacts vécus par les personnes victimes.

Faits saillants de l'année :

- Au cours de l'année, **212** personnes victimes ou proches de personnes victimes ont été pris en charge par la Clinique de Cyber-criminologie;
- La **fraude à l'investissement** entraîne les pertes financières les plus importantes, pour un **total de 5 394 899 \$**;
- Plus d'un tiers des personnes rapportent un **endettement** lié à la fraude;
- Suite à l'expérience de victimisation, plus de la moitié des individus rapportent avoir fréquemment exprimé de **l'anxiété**, et environ 42% mentionnent s'être sentis **isolés**;
- Le besoin le plus fréquemment exprimé est d'obtenir des conseils pour **se protéger** et **éviter la revictimisation**.

Les constats tirés de cette première année d'activités offrent une vue d'ensemble sur l'évolution des menaces en ligne et serviront à orienter les priorités d'action pour l'année à venir.

INTRODUCTION

Depuis leur introduction, les **technologies de l'information** se sont immiscées dans la plupart des aspects de la vie quotidienne. Malgré les bénéfices qu'elles présentent, elles favorisent également l'émergence d'un environnement propice et lucratif pour des acteurs malveillants. Dans ce contexte, la **fraude en ligne** pose un enjeu d'ampleur, tel qu'illustré par des données récentes. Notamment, entre les mois de janvier et septembre 2025, le Centre antifraude du Canada a traité 33 854 rapports de fraude, révélant au moins 23 113 personnes victimes (Centre antifraude du Canada, 2025). De plus, les infractions ont entraîné des pertes financières totales d'environ 544 millions de dollars. Ces **pertes monétaires** sont fréquemment accompagnées de **conséquences psychologiques, émotionnelles et sociales** importantes (Button et al., 2014). Ainsi, face aux impacts multidimensionnels de l'expérience de victimisation à la fraude en ligne, l'offre de soutien devient un enjeu central.

Dans ce contexte, la Clinique de Cyber-Criminologie de l'Université de Montréal propose l'une des rares offres de services pour les individus qui ont vécu une expérience de fraude en ligne. Grâce à une **collaboration avec l'Autorité des marchés financiers (AMF)**, elle offre un service d'accompagnement aux personnes victimes de fraude en ligne et à leurs proches qui se structure en deux temps.

Premièrement, la personne recherchant un accompagnement fait état de la situation auprès d'un analyste clinique, via la ligne téléphonique de la Clinique ou un formulaire en ligne. Au travers de ce premier contact, divers éléments sont identifiés liés à l'expérience de victimisation, aux impacts qui en découlent, ainsi qu'aux attentes et aux besoins exprimés par la personne victime ou par son proche. La collecte de ces informations permet à l'analyste de construire un plan d'action personnalisé, offrant des informations, des ressources et des démarches à suivre adaptées à la situation. Le plan d'action peut simplement être communiqué par courriel ou expliqué en profondeur dans le cadre d'un appel téléphonique.

À la fin de sa première année complète d'opération (février 2025 à février 2026), ce rapport vise à documenter les caractéristiques des usagers ayant fait appel aux services de la Clinique.

OFFRE DE SERVICE

La **ligne téléphonique** de la Clinique est en opération dans son format actuel depuis février 2025. Les heures d'ouverture couvrent en moyenne **30 heures par semaine**. Les analystes cliniques en cyber-prévention sont des étudiants au premier cycle ayant suivi une formation initiale en criminologie (victimologie, relation d'aide, et cybercriminalité). Ils ont également tous suivi une formation hybride dispensée par la Clinique afin d'approfondir leurs connaissances liées à la fraude et de développer leurs compétences d'intervention dans une approche centrée sur les personnes victimes. Par ailleurs, les analystes ont accès à des activités de formation continue (supervision personnalisée, rencontres d'équipe, participation à des séminaires dispensés par des organismes partenaires, etc.).

QUI SONT LES USAGERS ?

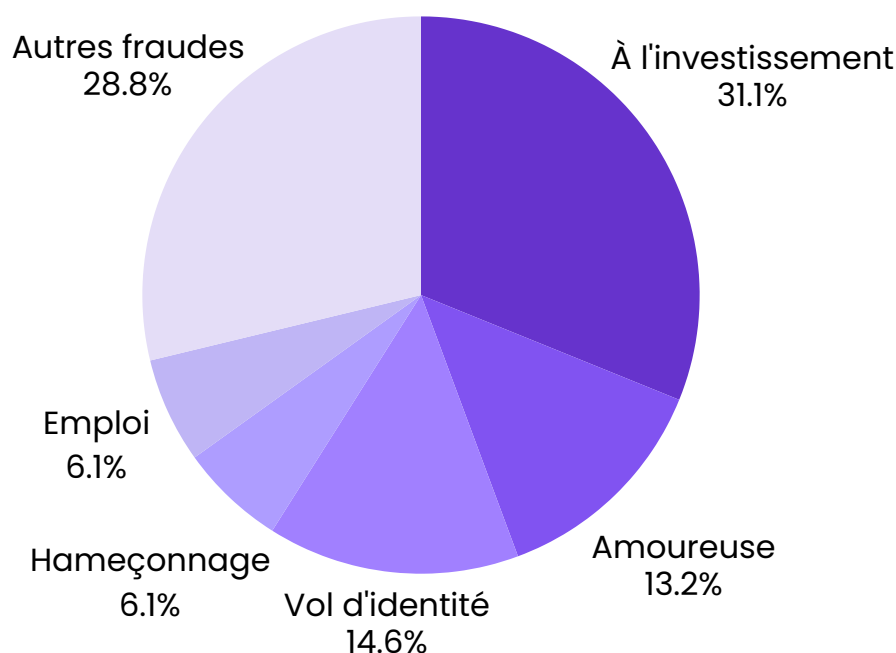
Un total de **212 personnes** (49,29 % d'homme; 48,82 % de femme; 1,9 % autre) a utilisé les services de la Clinique entre février 2025 et février 2026. La catégorie d'âge la plus représentée est le groupe des **35-44 ans avec 22,27 %** des demandes, suivi des 45-54 ans. Le total cumulé en perte financière des usagers est de 10 275 383,77 \$. La **somme moyenne individuelle perdue est de 66 723,27 \$** (écart-type=14 568,37) variant entre 89 \$ et 1,6 million \$. La médiane, soit la valeur qui partage l'ensemble de données ordonnées en deux parts égales, est de 16 965 \$.

La majorité des usagers de la Clinique a été **référée** par l'Autorité des marchés financiers (46,02 %), suivie par différents intervenants (p.ex. maison d'hébergement, maltraitance aînés, travailleur social, centre communautaire) (14,16 %) et les Centres d'aide aux victimes d'actes criminels (CAVAC) (12,62%). Une grande partie des usagers ont communiqué avec la Clinique de leur propre chef (48,34 %). Il est probable qu'ils aient pris connaissance de l'existence de la Clinique dans les médias ou à la suite d'une recherche sur internet.

TYPES DE FRAUDE OBSERVÉS

Cette section présente la **répartition des principaux types de fraude observés** parmi les usagers de la Clinique. La fraude à l'investissement constitue la forme la plus courante (31,1 %), suivie du vol d'identité (14,6 %) et de la fraude amoureuse (13,2 %). Ces trois types de fraude, comme l'illustre la *figure 1*, sont responsables d'une part substantielle des pertes financières totales déclarées par les victimes.

Figure 1. Statistiques descriptives des types de fraudes rapportés par les usagers (catégories peu fréquentes regroupées)



Tel que présenté dans le *tableau 1*, la **fraude à l'investissement** entraîne les pertes financières les plus importantes, pour un total de 5 394 899 \$. Le montant moyen perdu par victime s'élève à 84 295 \$, mais les pertes varient considérablement. En effet, la médiane est de 30 000 \$ de perte financière par personne. Celle-ci représente le montant qui sépare les données de manière égale. La **fraude amoureuse** représente 1 068 591 \$ des pertes totales, avec un montant moyen perdu par victime de 44 525 \$ et une médiane de 35 000 \$. Tout comme la fraude à l'investissement, la dispersion des montants perdus est élevée. Enfin, le **vol d'identité** occasionne des pertes totales de 231 502 \$, pour une perte moyenne par personne victime de 21 046 \$ et un montant médian de 3 800 \$.

Tableau 1. Montants moyens perdus selon le type de fraude (catégories peu fréquentes regroupées)

Types de fraude	n	Montant moyen perdu (\$)	ÉT (\$)	Médiane (\$)	Total perdu (\$)
Fraude à l'investissement	66	84 295	171 406	30 000	5 394 899
Fraude amoureuse	28	44 525	46 990	35 000	1 069 591
Vol d'identité	31	21 046	49 914	3 800	231 502
Hameçonnage	13	14 869	19 841	7 500	74 343
Emploi	13	11 975	15 133	5 000	131 726
Autres fraudes (< 12 cas + Autre)	61	55 563	—	—	3 389 322
Total	212	66 390	180 249	—	10 290 384

Note. M = moyenne; ÉT = écart-type; n = nombre de cas. La catégorie regroupée inclut toutes les fraudes ayant moins de 12 cas ainsi que la catégorie « Autre ».

Face à l'expérience de victimisation aux différents types de fraude énoncés ci-dessus, les usagers décrivent une variété d'impacts. Ceux-ci sont détaillés dans la section suivante, et affectent à la fois leur situation économique, leur bien-être physique et psychologique, ainsi que leurs relations interpersonnelles.

PRÉJUDICES CHEZ LES USAGERS

PRÉJUDICES FINANCIERS

La **perte d'argent directe est mentionnée par 75,83 % des usagers**. Par ailleurs, plus d'un **tiers des usagers (36,97 %) rapportent un endettement** lié à la fraude. Ce résultat indique que les effets financiers ne se limitent pas à une perte ponctuelle, mais peuvent entraîner des conséquences prolongées affectant la stabilité économique des personnes victimes. Au même titre, la perte de fonds d'épargne ou de pension est également notable (28,44 %). Ce type de préjudice peut avoir des implications importantes pour les finances futures des usagers. Les autres impacts financiers apparaissent nettement moins fréquemment, tels que les frais liés à la récupération de comptes (9,48 %), les coûts de réparation d'appareils (7,11 %) ou la perte d'emploi (6,64 %). Ces résultats montrent tout de même que la fraude peut générer des coûts indirects supplémentaires non négligeables.

PRÉJUDICES PHYSIQUES, PSYCHOLOGIQUES ET RELATIONNELS

Les résultats mettent en évidence que les conséquences de la fraude dépassent largement l'aspect financier. Sur le **plan physique**, plus de la moitié des répondants rapportent des troubles du sommeil (54,50 %), ce qui constitue l'impact le plus fréquent de cette catégorie et suggère un niveau élevé de stress vécu. D'autres manifestations somatiques importantes sont également observées, notamment la fatigue excessive (34,12 %) et les maux de tête (31,28 %). Toutefois, près d'un tiers des participants (31,75 %) déclarent n'avoir subi aucun impact physique.

Les **impacts psychologiques** apparaissent importants. Plus de la moitié des répondants mentionnent un sentiment d'anxiété (50,71 %), tandis qu'une proportion importante rapporte un sentiment d'impuissance (42,65 %), d'humiliation ou de honte (40,76 %), de colère (38,39 %) et des difficultés à faire confiance aux autres (37,44 %). Ces résultats suggèrent que l'expérience de fraude peut être vécue comme un événement déstabilisant sur le plan émotionnel et relationnel puisque les conséquences observées ne se limitent pas aux pertes financières. La présence d'un

sentiment d'insécurité (33,65 %) et de peur d'être à nouveau victime (33,18 %) est aussi rapportée par le tiers des usagers. Fait particulièrement notable, 13,74 % des répondants indiquent avoir songé au suicide en lien avec leur victimisation.

Sur le **plan relationnel**, les résultats révèlent également des répercussions non négligeables. Le sentiment d'isolement est mentionné par 41,71 % des répondants, ce qui en fait l'impact le plus fréquent de cette catégorie. Près d'un quart rapportent des tensions avec leurs proches (24,17 %), tandis que des proportions plus faibles mentionnent des difficultés à faire confiance à leurs proches (17,06 %) ou des ruptures relationnelles (12,80 %). Néanmoins, 40,76 % indiquent n'avoir subi aucun impact relationnel.

Enfin, les **impacts numériques** apparaissent plus hétérogènes. Le vol de données constitue la conséquence la plus fréquente (31,75 %), suivi du piratage de compte (16,59 %) et de la perte d'accès à des comptes en ligne (15,17 %). Toutefois, plus de la moitié des répondants (51,18 %) déclarent n'avoir subi aucun impact numérique.

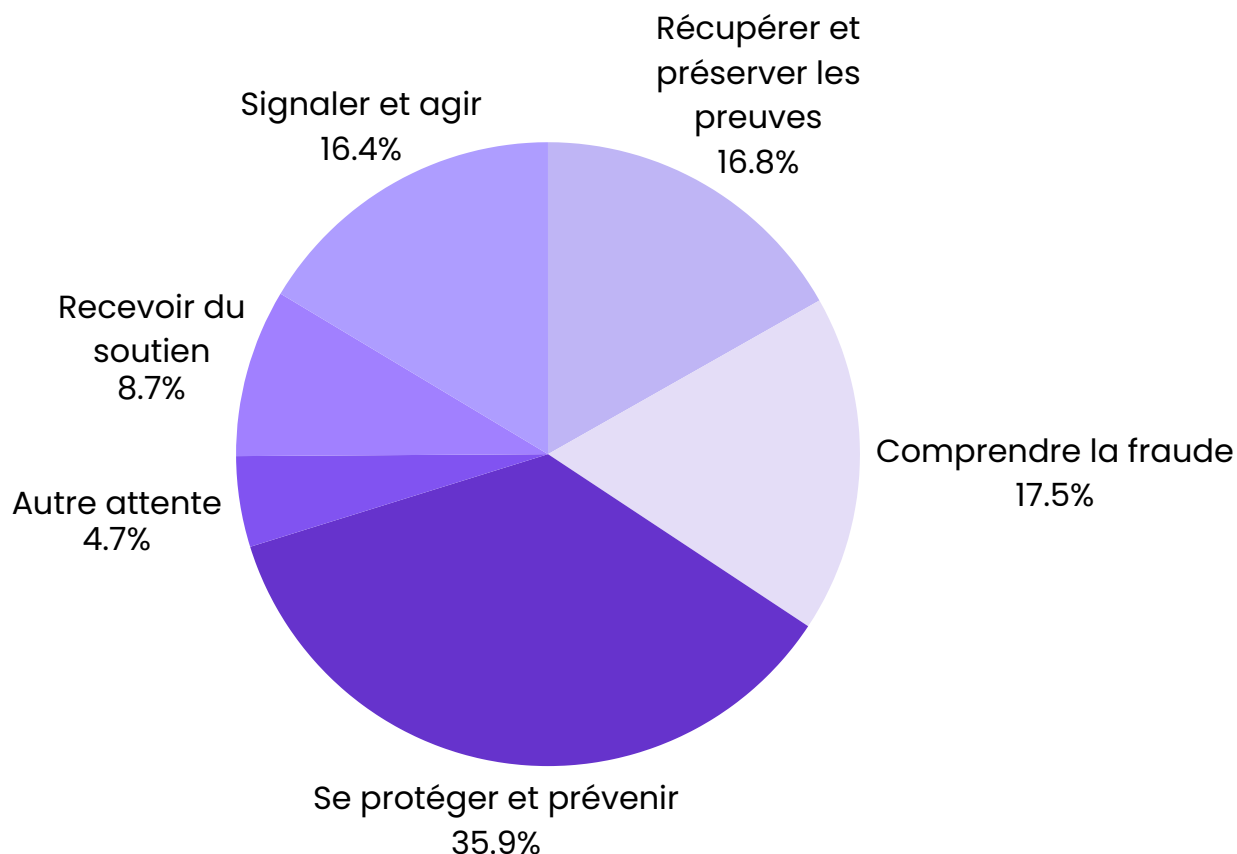
En somme, ces résultats montrent que la fraude doit être comprise comme une expérience aux répercussions multidimensionnelles. Ils soulignent ainsi la nécessité d'une prise en charge globale des personnes victimes qui intègre non seulement des solutions techniques et financières, mais aussi un soutien psychosocial.

BESOINS DES USAGERS

Les besoins exprimés par les usagers sont variés et, tout comme les impacts vécus, couvrent plusieurs dimensions de leur expérience. Globalement, le besoin le plus exprimé est d'**obtenir des conseils pour se protéger et éviter la revictimisation** (43,70%). À l'opposé, une infime minorité d'individus indiquent n'avoir aucun besoin (1,68%).

Afin de mieux analyser l'ensemble des besoins, ils ont été classés en cinq catégories : comprendre la fraude, se protéger et prévenir, signaler et agir, recevoir du soutien, et récupérer ou préserver les preuves. Les sous-sections suivantes présentent ces catégories de manière davantage détaillée.

Figure 2. Répartitions des besoins des usagers par catégories principales.



Note : Les pourcentages dépassaient initialement 100 % car chaque répondant pouvait exprimer plusieurs besoins au sein d'une même catégorie. La figure présente donc la part relative de chaque catégorie par rapport au volume total de besoins exprimés (928 mentions au total) afin d'obtenir un total de 100%.

L'analyse de la répartition pondérée des attentes exprimées par les usagers de la Clinique révèle une prédominance marquée des **stratégies de protection de de prévention**. La catégorie « se protéger et prévenir » représente 35,9% des besoins nommés. Ce chiffre suggère une préoccupation importante à ne pas vivre de revictimisation.

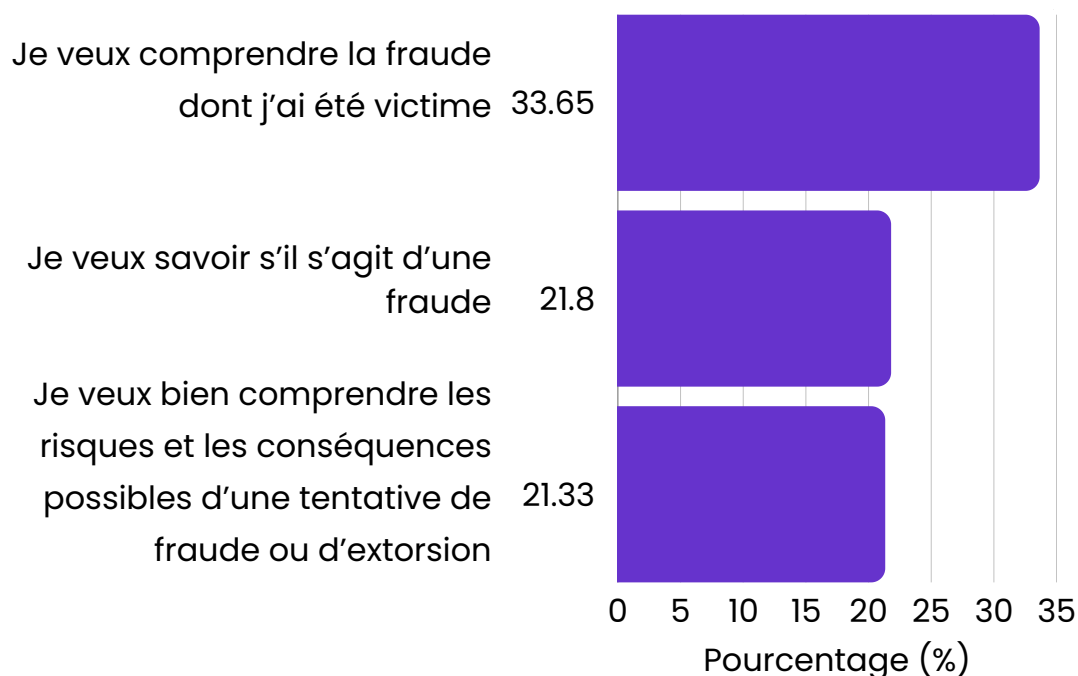
Par ailleurs, les **besoins de compréhension de la victimisation (17,5%), de recours institutionnel (16,4%) et de récupération et préservation de preuves (16,4%)** suivent à quasi-égalité. Ces résultats suggèrent une pluralité de préoccupations concomitantes caractérisant la phase post-victimisation.

Enfin, le **soutien psychosocial (8,7%)** occupe une place proportionnellement secondaire dans les besoins immédiats. Cette tendance peut refléter une priorisation des enjeux techniques liés à la résolution de la situation. Afin d'approfondir l'interprétation de ces tendances, une analyse de chacune de ces grandes catégories de besoins a été réalisée pour permettre de préciser la nature et la fonction des besoins exprimés.

BESOINS DE COMPRÉHENSION ET D'INFORMATION

Les **besoins liés à la compréhension de la fraude** semblent marqués. Près du tiers (33,65 %) des répondants souhaitent comprendre comment la fraude dont ils ont été victimes a été exécutée pour mieux en comprendre les mécanismes. Environ un cinquième souhaitent mieux comprendre les risques et conséquences possibles d'une tentative de fraude (21,33 %). Enfin, une proportion similaire (21,80 %) cherche d'abord à confirmer s'il s'agit bien d'une fraude.

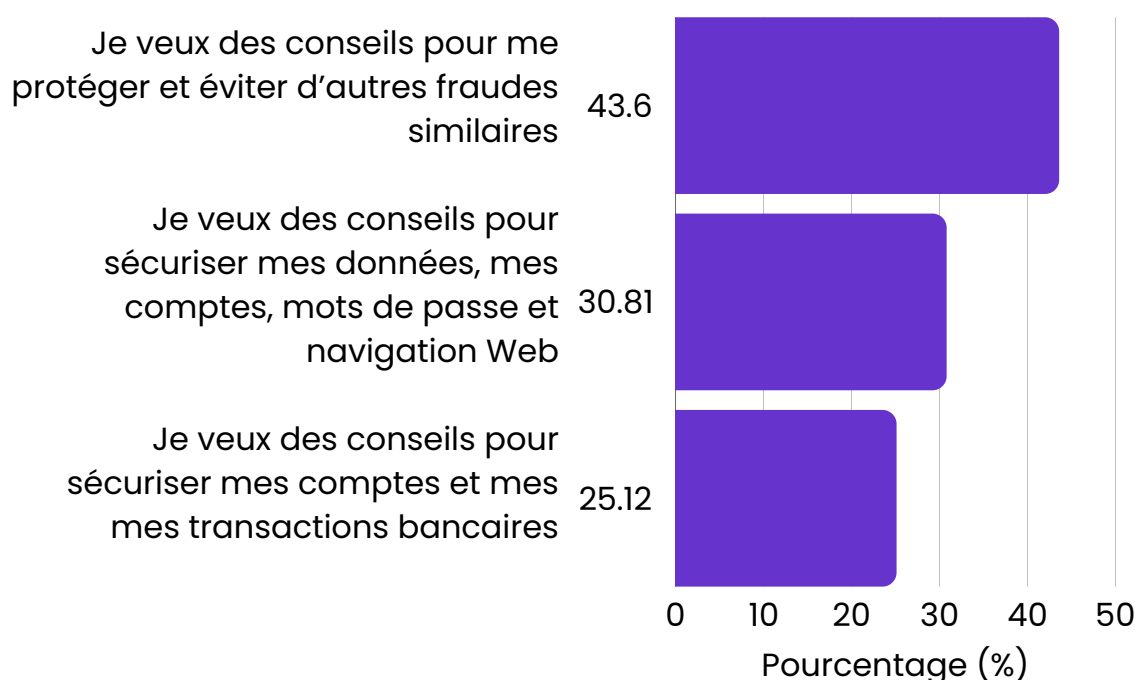
Figure 3. *Besoins de compréhension et d'information (%)*



BESOINS DE PROTECTION ET DE PRÉVENTION

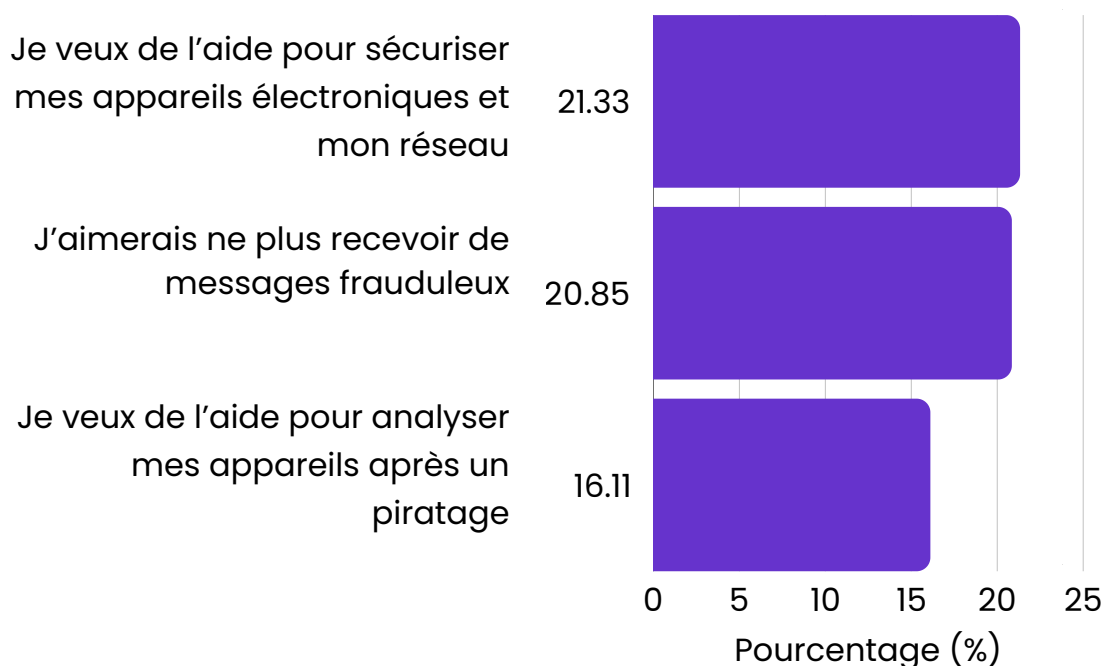
Les **besoins liés à la protection et à la prévention** sont parmi les plus fréquemment exprimés. L'analyse détaillée des sous-catégories met en évidence certains besoins spécifiques davantage rapportés par les usagers. La demande la plus fréquente concerne **l'obtention de conseils généraux visant à se protéger et à éviter d'autres fraudes similaires (43,60 %)**. Ceci témoigne d'une mobilisation proactive centrée sur la prévention de la revictimisation et démontre l'importance de l'éducation et de la sensibilisation. Les besoins associés à la **sécurisation technique** sont les seconds plus rapportés. Près d'un tiers des répondants souhaitent des conseils pour sécuriser leurs données, comptes, mots de passe et navigation Web (30,81 %), tandis qu'un quart mentionnent la sécurisation des comptes et transactions bancaires (25,12 %).

Figure 4. Principaux besoins de protection et de prévention (%)



Par ailleurs, une proportion notable de répondants exprime le besoin de sécuriser les appareils électroniques et le réseau (21,33 %) et de ne plus recevoir de messages frauduleux (20,85 %), ce qui renvoie davantage à une dimension immédiate de protection et de réduction de l'exposition aux sollicitations malveillantes.

Figure 5. Autres besoins de protection et de prévention (%)



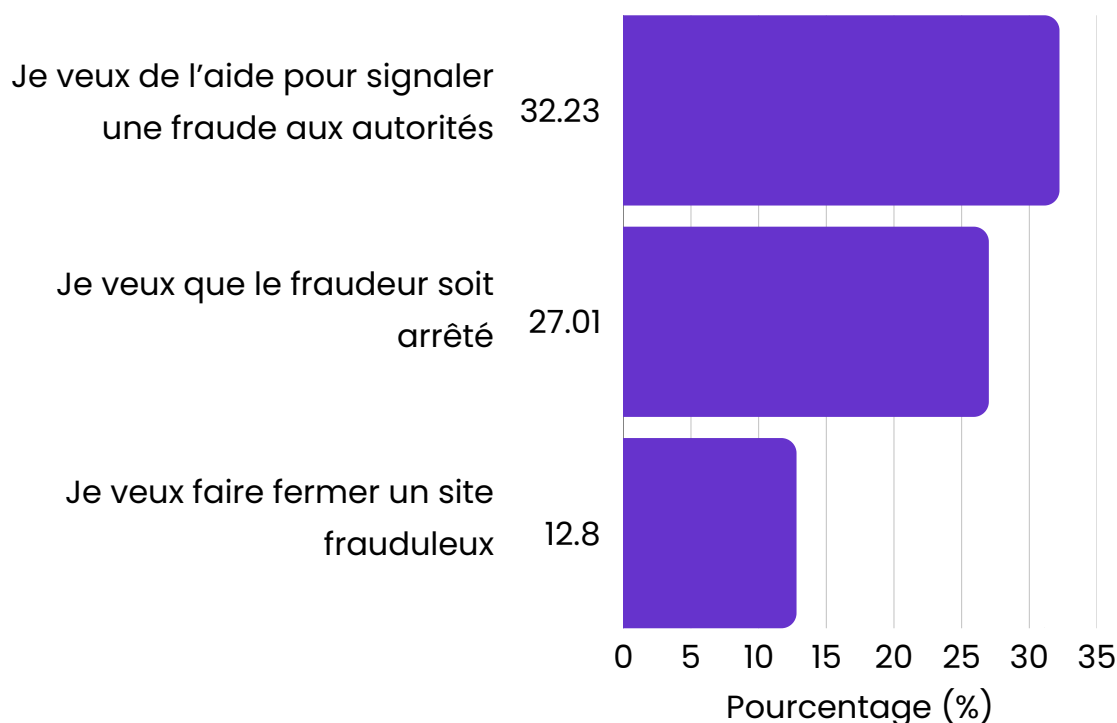
BESOINS DE SIGNALEMENT ET D'INTERVENTION

Les **besoins liés au signalement et à l'intervention** démontrent un désir de justice et de reconnaissance. Près d'un tiers des usagers (32,23 %) souhaitent obtenir de l'aide pour signaler la fraude aux autorités. Cette donnée met en évidence que les démarches de signalement ne sont pas perçues comme simples ou intuitives et qu'un accompagnement est souvent nécessaire pour naviguer les procédures administratives, juridiques ou institutionnelles.

Par ailleurs, plus d'un quart des usagers (27,01 %) expriment l'attente que le fraudeur soit arrêté. Ce résultat suggère que les victimes ne recherchent pas uniquement une résolution pratique de la situation, mais également une reconnaissance officielle du tort subi et une sanction à l'encontre de l'auteur.

Enfin, une proportion moindre (12,80 %) indique vouloir faire fermer un site frauduleux. Bien que moins fréquente, cette demande traduit une préoccupation tournée vers la protection collective.

Figure 6. *Besoins de signalement et d'intervention*

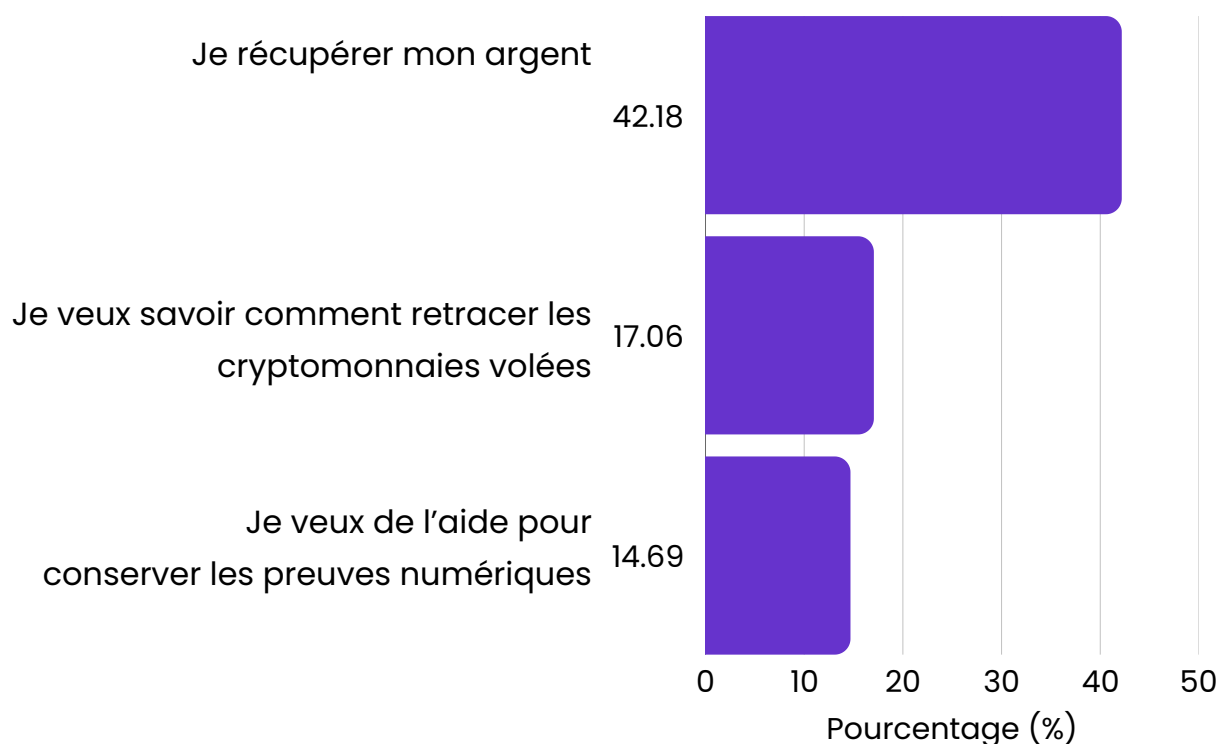


BESOINS DE RÉCUPÉRATION ET DE PREUVES

En termes de besoins de récupération et de preuves, la demande la plus fréquente concerne la **récupération de l'argent perdu (42,18 %)**, ce qui reflète l'importance des préjudices financiers dans l'expérience de victimisation. Une proportion plus restreinte des usagers souhaite savoir comment **retracer les cryptomonnaies volées (17,06 %)**. Cette demande met en évidence l'émergence de besoins spécifiques liés à la complexification des modalités de fraude numérique.

Enfin, 14,69 % des répondants expriment le besoin d'aide pour conserver les preuves numériques. Bien que moins fréquent, ce résultat est important, car il renvoie à une étape cruciale dans les démarches de signalement et de poursuite éventuelle.

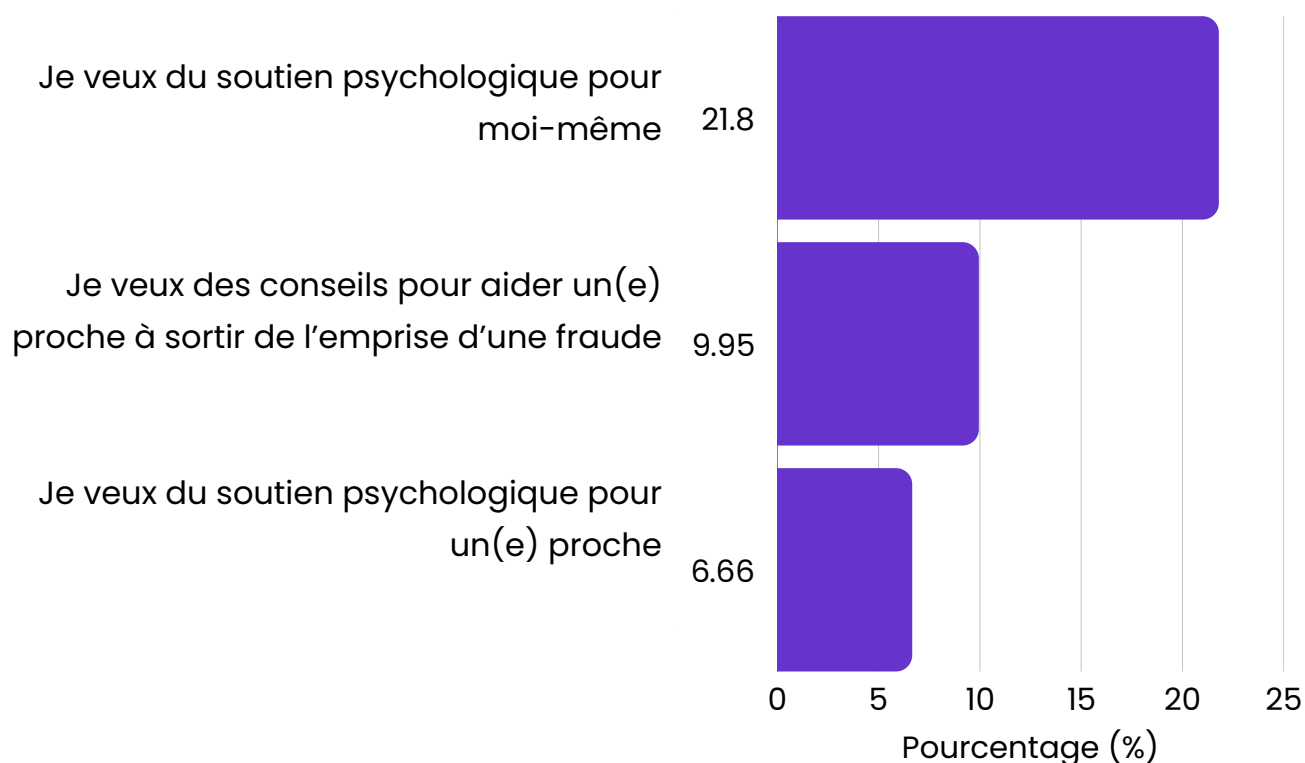
Figure 7. *Besoins de récupération et de preuves (%)*



BESOINS DE SOUTIEN SOCIAL OU PSYCHOLOGIQUE

Le besoin le plus rapporté par les usagers dans cette catégorie est le souhait de **soutien psychologique pour eux-mêmes (21,80 %)**. Ce résultat suggère qu'une certaine proportion d'usagers reconnaît explicitement les répercussions psychologiques de l'événement. Par ailleurs, **9,95 % des répondants recherchent des conseils pour aider un proche** à sortir de l'emprise d'une fraude. Cette donnée met en évidence que les conséquences de la fraude peuvent dépasser la personne directement touchée et s'étendre à son entourage.

Figure 8. *Besoins de soutien social ou psychologique (%)*



CONCLUSION

Ce rapport permet de dresser le profil des usagers de la Clinique de Cyber-Criminologie au cours de sa première année d'opération, soit entre février 2025 et février 2026. Particulièrement, la pertinence et l'utilité du service d'accompagnement personnalisé, fortement sollicité par les personnes victimes de fraude en ligne et leurs proches, sont soutenues par les données présentées dans le rapport qui mettent en évidence la diversité d'impacts et de besoins liés à l'expérience de victimisation.

Les profils des usagers varient selon l'âge, la situation financière et le type de fraude vécu, ce qui permet également de démontrer la complexité du phénomène. Les impacts sont diversifiés et incluent fréquemment des préjudices financiers importants, en plus d'impacts émotionnels, physiques et relationnels.

Les données mettent en évidence les besoins liés à l'accompagnement qui découlent des impacts vécus. Entre autres, les usagers expriment le besoin d'être mieux outillés pour se protéger et pour prévenir la revictimisation. Le besoin de comprendre la fraude vécue, ainsi que des besoins plus techniques liés au soutien, au signalement et à la sécurisation des appareils électroniques sont également exprimés, démontrant l'importance d'un accompagnement personnalisé qui tient compte des différentes dimensions liées à l'expérience de victimisation. Ceci s'inscrit dans les objectifs de la Clinique de Cyber-Criminologie, soit de redonner le contrôle aux personnes victimes en leur offrant un espace d'écoute et les ressources dont elles ont besoin.

Ainsi, l'évaluation continue des différentes dimensions de l'expérience de victimisation liée à la fraude en ligne apparaît nécessaire afin d'assurer un service adapté et cohérent avec les besoins exprimés, tout en nourrissant la réflexion sur l'évolution du phénomène et les réponses pouvant y être apportées.

Informations de contact



Sites webs:

- Clinique de Cyber-Criminologie: <https://www.clinique-cybercriminologie.ca/>
- Fraude-Alerte: <https://www.fraude-alerte.ca/>



de téléphone:

Contacter un.e analyste clinique : (438) 901-4395

Lundi : 13h00 à 17h00

Mardi : 13h à 17h

Mercredi : 10h à 14h

Jeudi : 9h à 17h

Vendredi: 13h à 17h

Samedi: 10h-14h



Adresse courriel:

Info@clinique-cybercriminologie.ca

ANNEXE I

Fraude à l'investissement. Stratagème visant à inciter une personne à investir dans une opportunité inexistante ou trompeuse (cryptomonnaie, actions, projets fictifs). Les fraudeurs promettent habituellement des rendements élevés et utilisent de faux conseillers financiers.

Fraude amoureuse ou sentimentale. Forme de manipulation émotionnelle où le fraudeur établit une relation de confiance et/ou amoureuse afin d'obtenir de l'argent, des informations personnelles ou un transfert de services.

Fraude de type crypto-romance. Stratagème combinant la fraude amoureuse et la fraude à l'investissement par cryptomonnaies, où un fraudeur gagne la confiance d'une victime par une relation sentimentale en ligne, puis l'incite à investir dans de prétendues plateformes de cryptomonnaies.

Vol d'identité. Utilisation frauduleuse de renseignements personnels pour ouvrir des comptes ou effectuer des achats sans l'autorisation de la victime.

Récupération de fonds. Fraude secondaire qui revictimise les victimes d'une première fraude. Le fraudeur prétend pouvoir récupérer l'argent perdu moyennant des frais initiaux.

Fraude à l'emploi. Annonce d'emploi fictive ou offre mensongère où la victime est amenée à fournir des informations personnelles, à payer des frais de formation ou à effectuer des transferts d'argent sous prétexte d'une éventuelle embauche.

Fraude hybride. Combinaison de plusieurs formes de fraude (ex. amoureuse et investissement).

Autres fraudes. Catégorie regroupant les fraudes moins fréquentes (sextorsion, hameçonnage, escroquerie immobilière, faux représentants, etc.).