



Photo d'un mannequin. Pour illustrer le texte.

FORUM R/SEXTORTION : ANALYSE DES PUBLICATIONS DE VICTIMES DE SEXTORSION FINANCIÈRE

Date : Novembre 2022 | Auteur : Centre canadien de protection de l'enfance (CCPE)



CENTRE CANADIEN de PROTECTION DE L'ENFANCE™

Aider les familles. Protéger les enfants.

© 2022, Centre canadien de protection de l'enfance inc. (CCPE). Tous droits réservés. Il est permis de conserver et d'imprimer des copies du présent document au besoin pour des activités non commerciales (fins personnelles, recherche, etc.) à condition d'attribuer la source de l'information au CCPE lorsque des extraits sont cités ou référencés dans un autre document. Il est interdit de publier une copie du présent document sur Internet, en tout ou en partie.

Les données utilisées dans la production du présent document figurent telles quelles dans le texte et toutes les analyses ont été réalisées par le personnel du CCPE. Les références à des sources externes ne servent qu'à illustrer et à étayer le propos auquel elles se rapportent. Les opinions qui y sont exprimées ou les autres informations qui s'y trouvent appartiennent à leurs auteurs ou éditeurs et ne reflètent pas nécessairement les vues du CCPE. Nous avons fait des efforts raisonnables pour assurer l'exactitude de toutes les informations présentées, mais nous ne pouvons garantir que le contenu est exempt de toute erreur ou omission.

« CENTRE CANADIEN de PROTECTION DE L'ENFANCE » et « Projet Arachnid » sont utilisés comme marques de commerce du CCPE. Les autres marques citées appartiennent à leurs détenteurs respectifs, et leur mention ici ne constitue aucunement une marque d'approbation ou d'affiliation. Les marques de commerce de tierces parties sont indiquées par le symbole^{MD} lorsqu'elles sont déposées à la fois au États-Unis et au Canada, et par le symbole^{MC} lorsqu'elles sont déposées seulement au Canada ou aux États-Unis.

Remerciements

Le CCPE travaille en collaboration avec des survivant·es pour déceler des déficits de responsabilité à corriger pour mieux protéger les enfants. Le CCPE tient à remercier les personnes qui ont partagé leurs expériences de sextorsion financière sur le forum r/Sextortion. Nous n'aurions jamais pu réaliser la présente étude sans leurs contributions. Le courage dont ils font preuve en publiant des récits et des commentaires sur leurs expériences crée une source d'informations précieuses sur la sextorsion financière, aide les personnes dans le besoin et sensibilise la population à ce crime.

Table des matières

Sommaire.....	3
Contexte.....	6
Méthodologie.....	7
Constats.....	8
Conclusion.....	21
Annexe.....	22

SOMMAIRE

Présentation de l'étude

La présente étude est une réalisation du Centre canadien de protection de l'enfance inc. (CCPE), un organisme de bienfaisance national voué à la protection de tous les enfants. Le CCPE gère le programme Cyberaide.ca – la centrale canadienne de signalement des cas d'exploitation et d'abus sexuels d'enfants sur Internet. Acteur de la lutte contre les abus pédosexuels et les images d'abus pédosexuels, Cyberaide.ca observe depuis quelques années une augmentation fulgurante de la cyberviolence sexuelle, qui se manifeste notamment par des signalements de sextorsion, de leurre, de distribution non consensuelle d'images intimes, de divulgation de renseignements personnels et de harcèlement.

La présente étude offre des analyses d'un des plus grands forums de discussion et de soutien consacrés à la sextorsion financière sur Internet : **reddit.com/r/Sextortion**. Deux sources de données ont été utilisées pour la présente étude : 1) les archives ouvertes du forum pour la période de juillet 2020 à septembre 2022, qui permettent d'analyser l'évolution des tendances dans le temps; 2) les 478 publications de victimes de sextorsion financière parues dans le forum r/Sextortion durant la période du 10 juin au 10 août 2022.

Principaux constats

Le nombre de publications et d'abonnés sur le forum r/Sextortion est en forte augmentation depuis le printemps 2022. Voici ce qui ressort de l'analyse de ces publications :

- **Les garçons et les jeunes hommes sont les principales cibles de sextorsion financière.**
Dans les publications contenant des informations sur le sexe de la victime, celle-ci est de sexe masculin dans 98 % des cas.
- **De nombreux sextorqueurs appliquent une stratégie basée sur Instagram et Snapchat.**
Le sextorqueur contacte d'abord la victime sur Instagram en se faisant passer pour une fille. Il s'empresse ensuite de déplacer la conversation sur Snapchat, où il incite la victime à lui envoyer des photos nues. Le sextorqueur s'emploie alors à faire chanter la victime. Il exige une somme d'argent, sans quoi il transmettra les photos nues de la victime aux proches et amis de celle-ci. Pour donner du poids à ses menaces, le sextorqueur envoie à la victime des captures d'écran des contacts de celle-ci sur les médias sociaux.

- **Les plateformes grand public présentent des caractéristiques de conception qui en font des espaces propices à la prédation.** Les plateformes de médias sociaux sont transformées en armes par les sextorqueurs, qui peuvent facilement y créer de faux comptes pour trouver des victimes potentielles et accéder à leurs renseignements personnels et à leurs réseaux sociaux. Plusieurs victimes font aussi remarquer que les mécanismes de signalement de ces plateformes ne leur permettent pas de décrire précisément leur situation et que les opérateurs ne font pas grand-chose pour les aider.
- **Les sextorqueurs qui reçoivent de l'argent de leurs victimes vont souvent revenir à la charge avec d'autres demandes d'argent.** Dans la quasi-totalité des cas où une victime a envoyé de l'argent à un sextorqueur (93 %), le sextorqueur est revenu à la charge avec d'autres demandes d'argent.
- **Des entreprises de cybersécurité ou de gestion de réputation ainsi que de soi-disant experts font des promesses exagérées, dont celle de pouvoir empêcher la distribution des images moyennant des sommes importantes.** Plusieurs victimes font état d'interactions fâcheuses avec ce genre d'entreprises et d'individus, comparant leurs tactiques de vente sous pression à celles des sextorqueurs. Fait à souligner, les victimes qui ont retenu les services de ces entreprises ou soi-disant « experts » – parfois au prix de plusieurs milliers de dollars – déconseillent d'en faire autant.

Principaux points à retenir

- Les témoignages des victimes donnent à penser que, face à une tentative de sextorsion financière, mieux vaut ne pas céder aux demandes du sextorqueur et couper complètement la communication.
- Les plateformes de médias sociaux devraient s'assurer que les comptes d'utilisateurs mineurs soient privés par défaut, ne pas pousser les utilisateurs à multiplier les abonnés et ne pas les inciter à partager des renseignements personnels, comme leur position en temps réel.
- Les plateformes de médias sociaux devraient permettre aux victimes de signaler spécifiquement les cas de chantage et d'extorsion et de faire valoir l'urgence de la situation lorsqu'elles se font agressivement et activement harceler sur ces plateformes.
- Les informations recueillies sur le forum r/Sextorsion montrent que les sextorqueurs utilisent diverses formes de paiement en ligne, dont des cartes-cadeaux. Des recherches plus approfondies sont nécessaires pour trouver des moyens d'empêcher les sextorqueurs d'exploiter ces services pour commettre leurs crimes.

CONTEXTE

Un mot sur Reddit

Reddit est une plateforme de médias sociaux formée de millions de forums (appelés « subreddits ») consacrés à une foule de sujets. Les subreddits, appelés aussi « communautés » ou « sous-communautés »¹, réunissent les utilisateurs en fonction de leurs intérêts. Le nom d'un forum commence toujours par « r/ », car cet élément fait partie de l'adresse URL que Reddit utilise². Les utilisateurs de Reddit alimentent les subreddits en contenu. Il y a trois façons de contribuer à un subreddit : mettre une publication en ligne, commenter une publication ou voter sur une publication. Une publication dans un subreddit ainsi que tous les commentaires et les votes qui s'y rattachent forment ensemble un fil de discussion (*thread*).

Un mot sur r/Sextortion

r/Sextortion est le plus grand forum de soutien connu dédié à la sextorsion sur Reddit. Cette communauté créée en février 2020 comptait plus de 6300 membres en date de la présente étude. Les auteurs des publications et des commentaires mis en ligne sur ce forum sont presque toujours des victimes de sextorsion financière qui ont besoin d'aide ou qui ont des conseils à offrir. Lorsque des utilisateurs de Reddit racontent des expériences de sextorsion financière dans d'autres subreddits (p. ex. r/Scams et r/Advice), il n'est pas rare qu'ils se fassent diriger vers r/Sextortion pour obtenir des conseils et du soutien en matière de sextorsion.

Un mot sur la sextorsion financière

La sextorsion financière est un type de chantage généralement exercé par une personne inconnue de la victime à travers Internet. Cette personne, qui se fera souvent passer pour une personne plus jeune ou du sexe opposé, manipulera la victime pour la convaincre de lui envoyer des images d'elle nue³. Presque aussitôt, la victime se fera demander de l'argent (et parfois aussi, de nouvelles images intimes) sous la menace constante de voir ses images retransmises à ses proches et amis ou mises en circulation sur Internet si elle n'obtempère pas. Certaines victimes mineures disent également avoir été menacées d'arrestation pour les images qu'elles ont produites. Les cibles de sextorsion financière seraient souvent des garçons qui se font prendre au piège en croyant communiquer avec une jeune femme⁴; ces conversations sont souvent de courte durée – de quelques minutes à quelques heures.

¹ Reddit. (2020, 16 janvier). *Frequently asked questions*. https://www.reddit.com/wiki/faq/#wiki_what_is_reddit.3F

² Lerman, J. (2021, 5 juillet). *What is Reddit?* Digital Trends. <https://www.digitaltrends.com/computing/what-is-reddit/>

³ Gendarmerie royale du Canada (2022, 22 août). *Conseils pour se protéger de la sextorsion en ligne* [Communiqué de presse]. <https://bc-cb.rcmp-grc.gc.ca/ViewPage.action?languageId=4&siteNodeId=2087&contentId=76285>

⁴ Centre canadien de protection de l'enfance (2022, 4 août). *Sextorsion : Les garçons sont la cible de tactiques agressives sur Instagram et Snapchat, selon une analyse de Cyberaide.ca* [Communiqué de presse]. <https://www.protegeonsnosenfants.ca/fr/zone-medias/communiqués/2022/analyse-donnees-sextorsion>

MÉTHODOLOGIE

Les chercheurs du CCPE ont analysé l'un des plus grands forums connus de discussion et de soutien consacrés à la sextorsion sur Internet : [reddit.com/r/Sextortion](https://www.reddit.com/r/Sextortion). Deux sources de données du forum r/Sextortion ont été analysées dans le cadre de cette étude : les archives du forum et les récits des victimes.

Reddit limite le nombre de publications affichées sur un forum. Pour évaluer l'évolution des tendances dans le temps, les chercheurs du CCPE ont analysé les archives ouvertes du forum r/Sextortion obtenues au moyen de Pushfit.io de Reddit, une interface API qui recueille et diffuse mensuellement les données des forums publics de Reddit à des fins de recherche. Ayant obtenu les archives du forum r/Sextortion pour la période de juillet 2020 à septembre 2022, les chercheurs du CCPE ont créé un code informatique pour analyser l'activité des utilisateurs dans le temps et mesurer la fréquence à laquelle les victimes font mention des principales plateformes et formes de paiement en ligne. Les termes utilisés pour les recherches par mots-clés sont indiqués dans l'annexe.

Pour apporter un complément de données riches et récentes à l'analyse des archives, les chercheurs du CCPE ont aussi analysé des récits de victimes, à savoir les 478 publications de victimes autodéclarées de sextorsion financière qui étaient publiquement accessibles sur r/Sextortion pour la période du 10 juin au 10 août 2022. Les chercheurs ont codé manuellement les publications des victimes afin de pouvoir quantifier certaines caractéristiques comme leur profil sociodémographique, les plateformes utilisées et les tactiques des sextorqueurs. Les chercheurs ont aussi procédé à une analyse quantitative des publications et dégagé plusieurs thèmes qui permettent d'approfondir le phénomène de la sextorsion financière.

Photo d'un mannequin. Pour illustrer le texte.

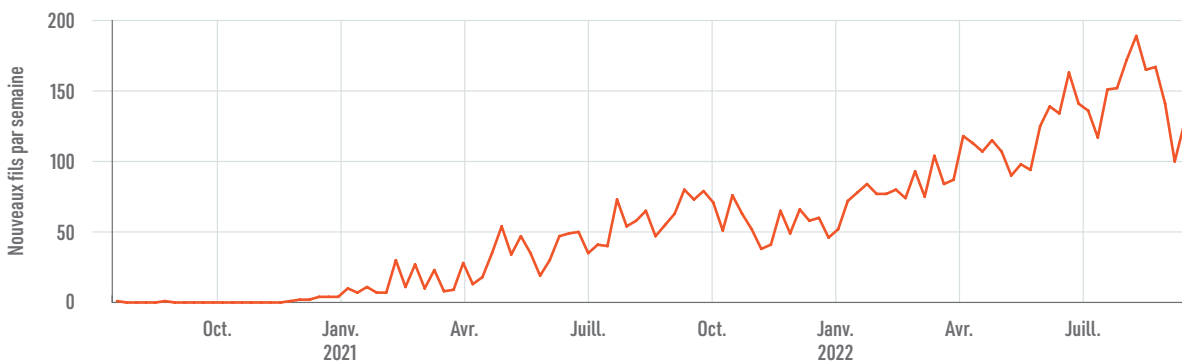
CONSTATS

Constats de l'analyse des archives du forum

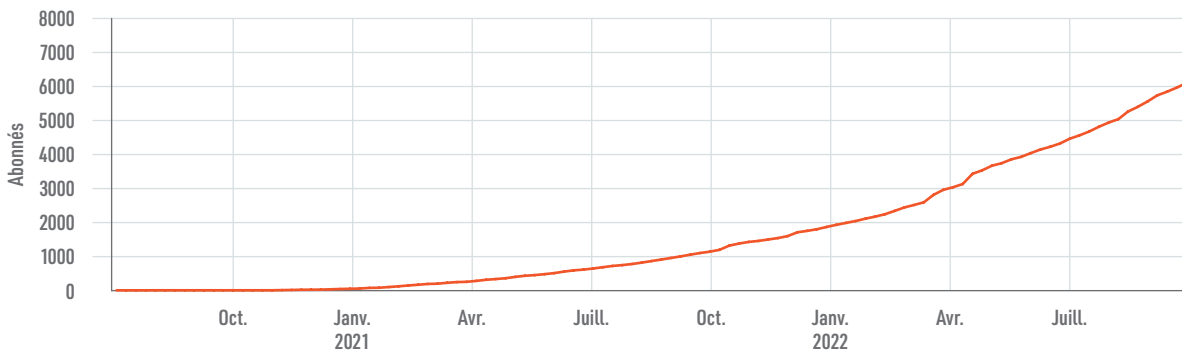
Activité des utilisateurs du forum

Au total, 6506 fils de discussion du forum r/Sextortion ont été inclus dans l'analyse des archives. En date de la présente étude, le forum r/Sextortion comptait quelque 6300 abonnés et ce nombre augmentait de plusieurs centaines par semaine. Les données d'archives montrent que le nombre de publications originales (nouveaux fils de discussion) parues chaque semaine affiche une tendance à la hausse depuis janvier 2022, tout comme le nombre d'abonnés actifs.

ÉVOLUTION HEBDOMADAIRE DU NOMBRE DE NOUVEAUX FILS DE DISCUSSION SUR R/SEXTORTION



ÉVOLUTION CUMULATIVE DU NOMBRE D'ABONNEMENTS AU FORUM R/SEXTORTION

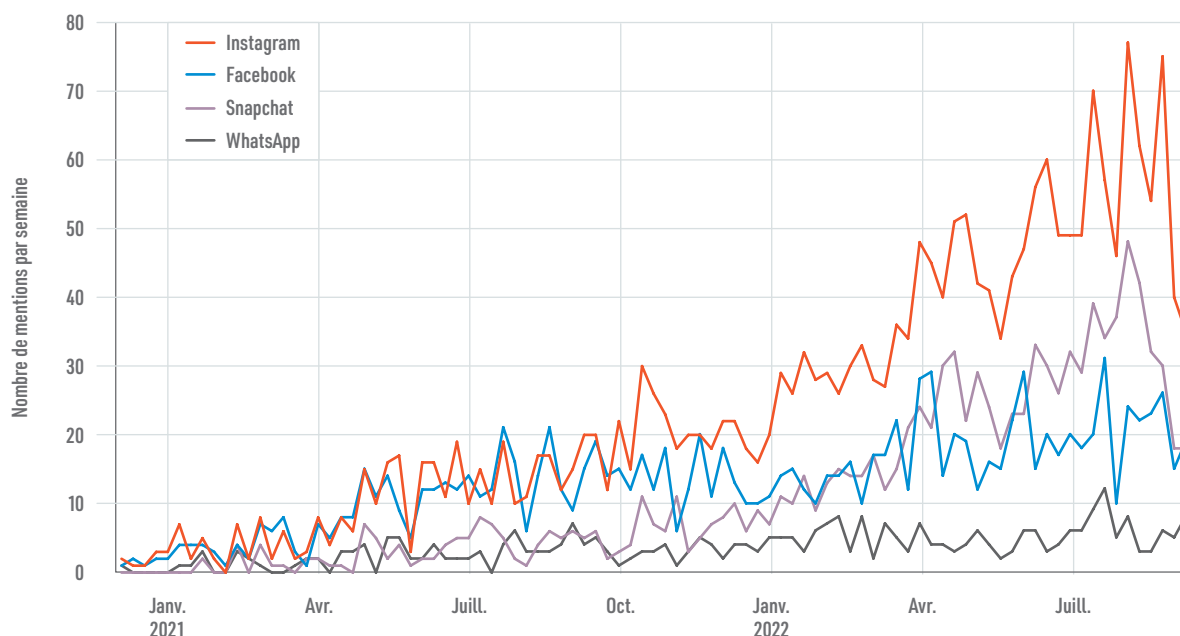


Plateformes

Nous avons utilisé des recherches par mots-clés pour déterminer la fréquence à laquelle les victimes ont fait mention des principales plateformes sur le forum r/Sextortion depuis 2020. Précisons que les résultats de ces recherches indiquent le nombre de mentions des différentes plateformes relevées dans les publications des victimes, ce qui ne signifie pas nécessairement que la plateforme en question a été utilisée pour sextorquer la victime.

Le graphique ci-dessous montre l'évolution hebdomadaire du nombre de mentions relevées pour chacune des plateformes les plus souvent mentionnées par les victimes dans les deux dernières années, à savoir Instagram^{MD} (n=2263), Facebook^{MD} (n=1212), Snapchat^{MD} (n=1068) et WhatsApp^{MD} (n=329).

ÉVOLUTION HEBDOMADAIRE DES MENTIONS RELEVÉES SUR R/SEXTORTION, PAR PLATEFORME (D'APRÈS LES ARCHIVES)



Signalons que TikTok^{MD}, qui dit compter plus d'un milliard d'utilisateurs actifs⁵, est rarement mentionnée par les victimes dans les archives des forums (n=33; absente du graphique). Il est possible que les politiques et les caractéristiques de conception de cette plateforme la rendent moins attrayante pour les sextorqueurs. Par exemple, l'envoi de messages directs n'est possible que pour les utilisateurs enregistrés de 16 ans et plus. À cela s'ajoute l'impossibilité de transmettre par message direct des contenus produits en dehors de TikTok⁶. Par conséquent, cette plateforme s'avère peut-être moins propice à une utilisation dans un contexte de sextorsion.

⁵ Bursztynsky, J. (2021, 27 septembre). TikTok says 1 billion people use the app each month. *CNBC*. <https://www.cnn.com/2021/09/27/tiktok-reaches-1-billion-monthly-users.html>

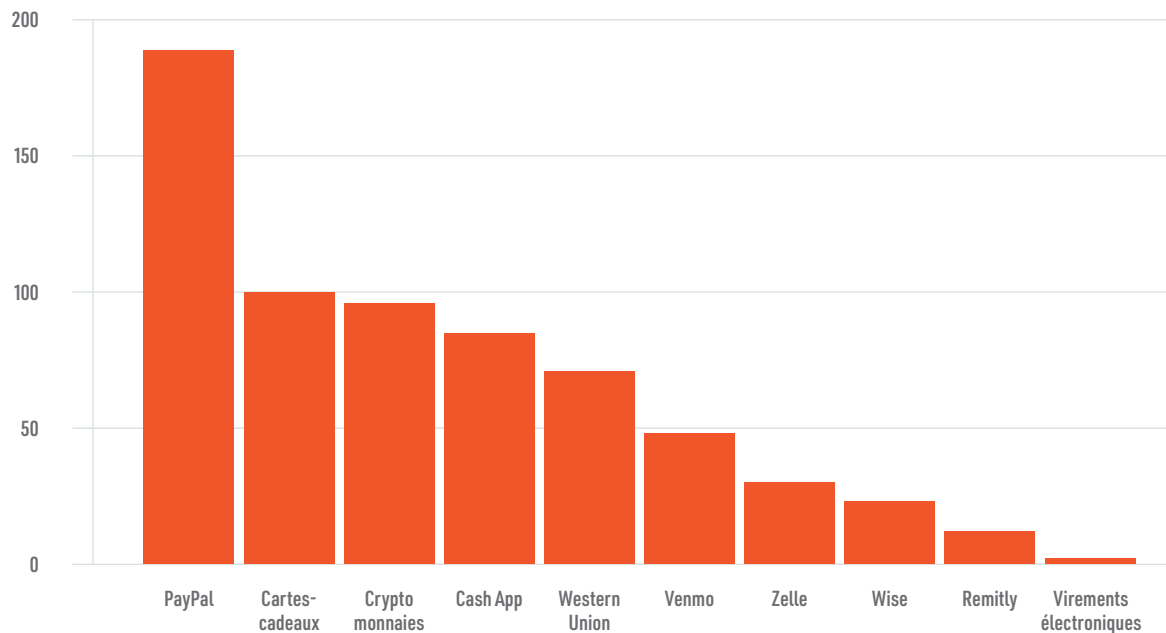
⁶ TikTok (2022). *Messages directs*. Source consultée le 21 septembre 2022 au <https://support.tiktok.com/fr/account-and-privacy/account-privacy-settings/direct-message>

Photo: iStockphoto.com. Pour illustrer le texte.

Formes de paiement en ligne

Les formes de paiement en ligne le plus souvent relevées dans les recherches par mots-clés sont PayPal^{MD} (n=189), les cartes-cadeaux (n=100), les cryptomonnaies (n=96), Cash App^{MC} (n=85) et Western Union^{MD} (n=71). Précisons que les résultats des recherches par mots-clés indiquent le nombre de mentions des différentes formes de paiement relevées dans les publications des victimes, ce qui ne signifie pas nécessairement que la forme mentionnée a été utilisée pour transmettre des fonds au sextorqueur.

FORMES DE PAIEMENT LES PLUS SOUVENT MENTIONNÉES SUR R/SEXTORTION (D'APRÈS LES ARCHIVES)



Constats de l'analyse des récits de victimes

Plateformes

Sur la base de l'échantillon de publications de victimes examinées manuellement (n=478) pour la période de juin à août 2022, les plateformes les plus souvent mentionnées pour leur utilisation dans un contexte de sextorsion financière sont Instagram (n=245) et Snapchat (n=221), suivies de WhatsApp (n=40), Facebook (n=20) et Tinder^{MD} (n=19). Les victimes rapportent souvent avoir été contactées pour la première fois sur Instagram, après quoi la conversation s'est poursuivie sur Snapchat, où des images ont été échangées. Certains sextorqueurs utilisent Facebook pour faire des captures d'écran des contacts Facebook de la victime et les envoyer à cette dernière pour montrer qu'ils ont les moyens d'envoyer ses images à ses amis, à sa famille, etc. Comme dans l'analyse des archives, très peu de victimes disent s'être fait sextorquer au moyen de la plateforme TikTok (n=2).

PLATEFORMES MENTIONNÉES PAR LES VICTIMES SUR R/SEXTORTION (TOP-8 SEULEMENT | D'APRÈS LES RÉCITS DES VICTIMES)

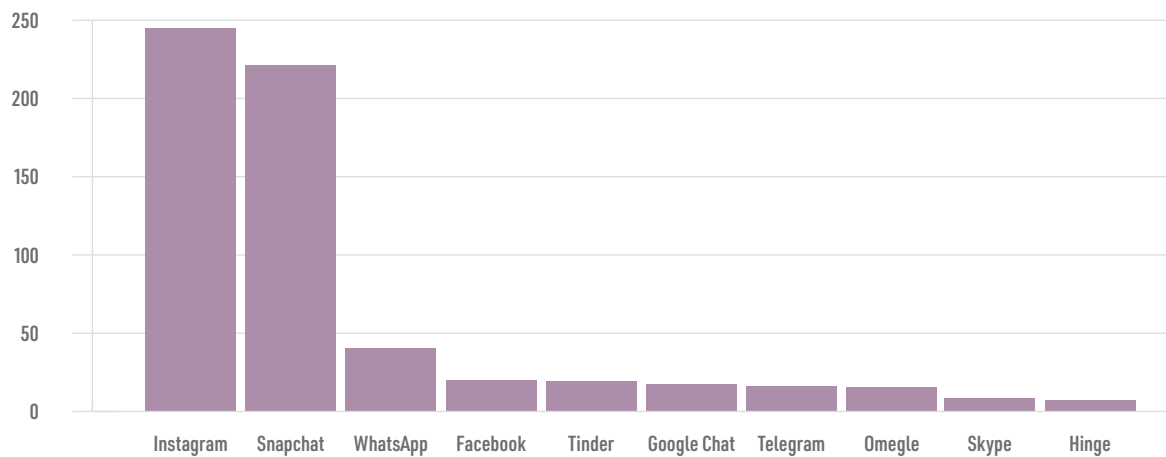


Photo d'un mannequin. Pour illustrer le texte.

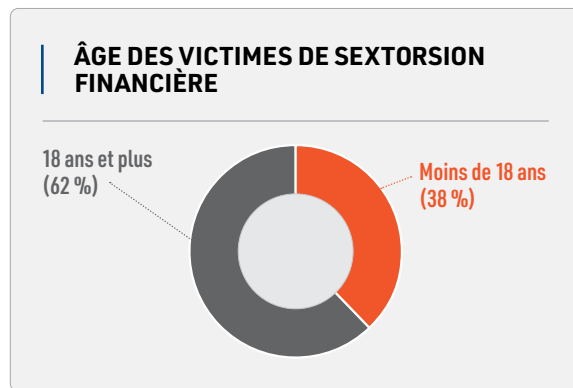
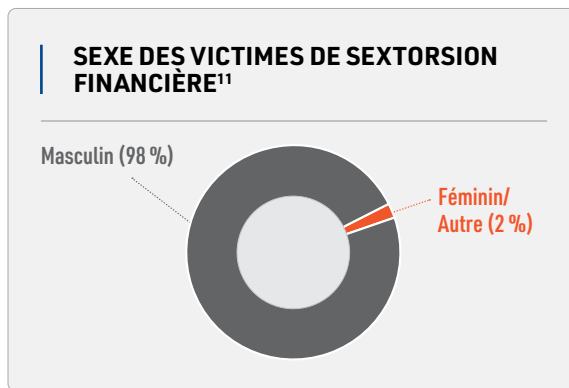
Profil sociodémographique des victimes

Sexe

Dans près de la moitié des cas (n=231), la victime ne donne aucune information sur son sexe. Dans les cas où le sexe de la victime ne fait aucun doute, les victimes masculines sont nettement surreprésentées (n=241). Cette tendance se reflète dans les signalements d'origine canadienne transmis à Cyberaide.ca au Canada⁷ ainsi que dans les signalements reçus par les forces policières canadiennes⁸, américaines⁹ et australiennes¹⁰.

Âge

Dans la plupart des cas, les victimes ne donnent aucune information sur leur âge (n=302). Parmi les autres cas, plus de 60 % des victimes de sextorsion financière sont âgées de 18 ans ou plus (n=109) et près de 40 % (n=67) disent être mineures.



⁷ Centre canadien de protection de l'enfance (2022, 4 août). *Sextorsion : Les garçons sont la cible de tactiques agressives sur Instagram et Snapchat, selon une analyse de Cyberaide.ca* [Communiqué de presse]. <https://www.protegeonsnosenfants.ca/fr/zone-medias/communiques/2022/analyse-donnees-sextorsion>

⁸ Dormer, D. (2022, 2 juin). Calgary police warn of online 'sextortion' scam targeting young boys. *CTV News*. <https://calgary.ctvnews.ca/calgary-police-warn-of-online-sextortion-scam-targeting-young-boys-1.5929588>

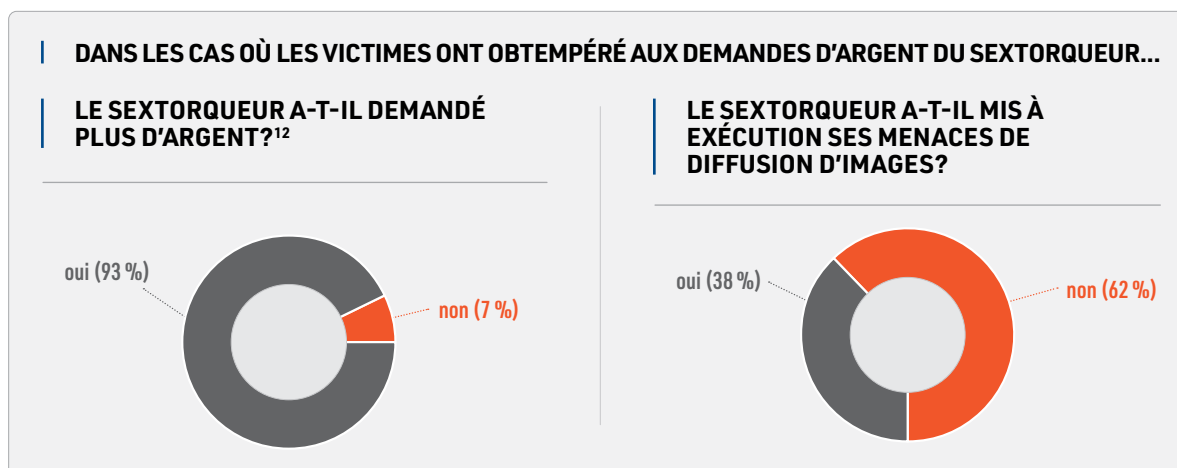
⁹ Lynch, S. (2022, 31 mai). FBI Charlotte warns of increase in sextortion schemes targeting teenage boys. *FBI Charlotte*. <https://www.fbi.gov/contact-us/field-offices/charlotte/news/press-releases/fbi-charlotte-warns-of-increase-in-sextortion-schemes-targeting-teenage-boys>

¹⁰ Australian Federal Police (2022, 10 septembre). *Police warning: Sextortion for profit on the rise*. <https://www.afp.gov.au/news-media/media-releases/police-warning-sextortion-profit-rise>

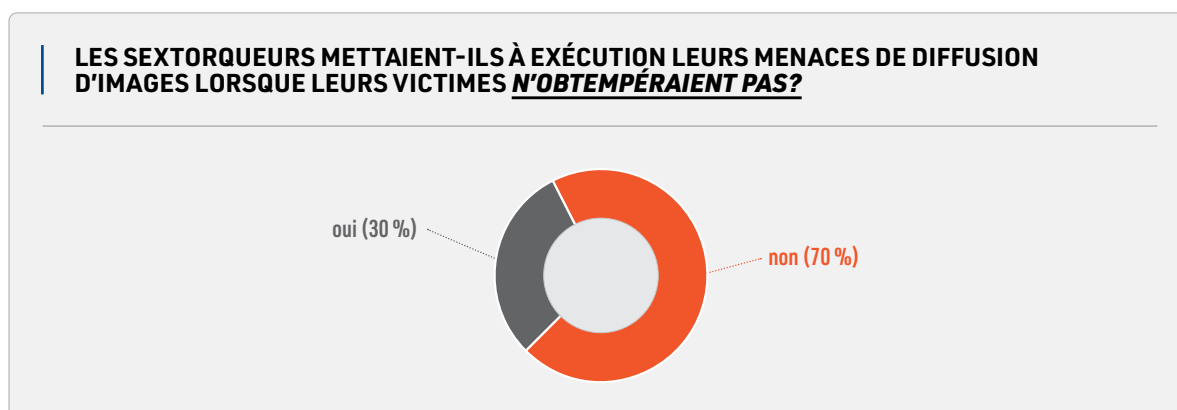
¹¹ Les graphiques et les chiffres présentés dans cette section sont basés uniquement sur des données connues ou disponibles. Par exemple, ce graphique n'est basé que sur les 245 victimes dont le sexe ne fait aucun doute et fait abstraction des 231 victimes qui ne donnent aucune information sur leur sexe.

L'obéissance des victimes et son effet sur les demandes des sextorqueurs et la mise à exécution de leurs menaces

Parmi les victimes qui déclarent avoir obtempéré aux demandes d'argent du sextorqueur (n=174), beaucoup rapportent que leur obéissance a eu un effet sur les demandes du sextorqueur (n=133) ou la mise à exécution de ses menaces (n=81). La quasi-totalité (93 %) des victimes qui ont versé de l'argent au sextorqueur ont reçu d'autres demandes d'argent, et près de 40 % ont vu leurs images diffusées malgré tout. Ces résultats donnent du mérite à la recommandation de nombreux experts en la matière, soit de ne jamais verser d'argent à un sextorqueur.



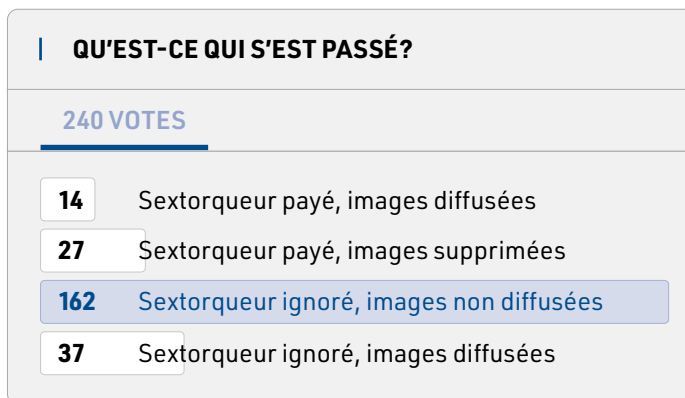
Les mérites de cette recommandation se reflètent aussi dans les résultats des 145 victimes qui **n'ont pas obtempéré** aux demandes d'argent des sextorqueurs¹³: comparativement à celles qui leur ont versé de l'argent, celles qui ne l'ont pas fait ont vu leurs images diffusées dans des proportions similaires, mais n'ont plus reçu d'autres menaces ou demandes de la part du sextorqueur.



¹² Dans ce graphique, « demandes » s'entend des demandes additionnelles faites par le sextorqueur après que la victime eut obtempéré. Dès lors, le champ « demandes » ne s'applique pas aux victimes qui n'ont pas obtempéré aux demandes du sextorqueur.

¹³ 115 autres victimes n'ont pas obtempéré aux demandes d'argent du sextorqueur. Ces victimes n'ont pas précisé si le sextorqueur avait mis à exécution ses menaces de diffusion d'images.

Nous sommes d'avis que l'analyse des publications relevées sur le forum sous-estime la proportion réelle de victimes qui n'ont pas obtempéré aux demandes des sextorqueurs et qui n'ont pas vu leurs images diffusées. En pareilles situations (c.-à-d. lorsque les menaces se sont calmées après que les victimes eurent refusé d'obtempérer ou eurent coupé la communication), les victimes sont peut-être moins motivées à retourner sur le forum et à mettre à jour leurs publications antérieures à propos de leurs expériences, car elles ne sont plus en état de crise. Cette théorie est étayée par les résultats de plusieurs sondages informels réalisés sur le forum lui-même dans les derniers mois, lesquels révèlent systématiquement une proportion plus élevée de non-mise à exécution des menaces contre les victimes qui n'obtempèrent pas (voir image ci-dessous)¹⁴.



Sommes versées

Dans les cas où les sommes d'argent versées aux sextorqueurs sont connues (n=112), la plupart des victimes ont versé entre 100 et 500 dollars (40 %). Un peu plus du tiers (36 %) des victimes ont payé 100 \$ ou moins. Il est impossible de savoir en quelle devise ces sommes ont été versées; on suppose ici qu'elles ont été versées en dollars américains.

SOMMES D'ARGENT VERSÉES AUX SEXTORQUEURS PAR LES VICTIMES

< 100 \$	40	36 %
De 100 \$ à 500 \$	45	40 %
De 500 \$ à 1000 \$	15	13 %
De 1000 \$ à 5000 \$	12	11 %
Total	112	100 %

Formes de paiement en ligne

Dans les cas où la victime a fait mention de la forme de paiement utilisée pour payer le sextorqueur (n=73), PayPal est la forme la plus souvent citée (n=23). Viennent ensuite Venmo^{MD} (n=10) et Zelle^{MD} (n=7). Les transactions effectuées par l'entremise d'une banque ou au moyen de cartes-cadeaux et d'autres plateformes dont Cash App et Remitly^{MC} ne représentent qu'une petite partie des formes de paiement relevées. Dans de nombreux cas (n=131), les victimes qui ont donné suite à une demande d'argent n'ont pas fait mention d'une quelconque forme de paiement.

¹⁴ AtomicDuckiez (2022, 8er avril). *What happened to you?* [publication relevée sur le forum]. Reddit. https://www.reddit.com/r/Sextortion/comments/tz36mj/what_happened_to_you/

Constats de l'analyse des récits de victimes : Perspectives thématiques

Stratégies des sextorqueurs

Les publications des victimes analysées ici révèlent de nombreuses similitudes dans les stratégies des sextorqueurs. La citation suivante fait état des principales caractéristiques de nombreuses expériences relevées sur r/Sextortion, lesquelles se reflètent dans des signalements transmis à Cyberaide.ca¹⁵:

« En début de journée, j'avais accepté cette personne sur ma page Instagram. On s'est parlé quelques minutes, puis on a poursuivi sur Snapchat. C'est là que cet escroc m'a envoyé des photos nues, et j'ai bêtement fait pareil. Après ça il m'a envoyé des captures d'écran de toute ma liste d'abonnés sur Instagram (dont la plupart étaient des membres de ma famille) en me disant qu'il mettrait mes images en circulation si je refusais de lui envoyer de l'argent¹⁶. [traduction libre]

Les victimes admettent souvent qu'elles se doutaient ou auraient dû se douter qu'elles étaient visées par une arnaque eu égard à certains signaux d'alarme, dont la syntaxe déficiente des messages reçus, le déplacement de la conversation vers une autre plateforme et la vitesse à laquelle la conversation a pris un tour sexuel. Toutefois, l'existence d'abonnés en commun et l'apparence d'un niveau d'engagement élevé (à en juger notamment par un nombre d'abonnés ou un score Snapchat¹⁷ élevés) ont amené les victimes à estimer que les comptes des sextorqueurs étaient légitimes.

« Je connais tous les signes habituels d'une arnaque comme celle-ci, mais l'arnaqueur s'était arrangé pour tromper les apparences. Son nombre d'abonnés sur insta était normal, son snapscore était élevé et son visage était toujours le même d'un snap à l'autre. J'étais donc convaincu que ce n'était pas un arnaqueur. J'étais dans le champ¹⁸. [traduction libre]

Comme nous l'avons mentionné précédemment, les sextorqueurs communiquent souvent avec leurs victimes sur plusieurs plateformes de médias sociaux. Cette tactique multiplateforme leur procure un meilleur accès aux abonnés et aux renseignements personnels des victimes, ce qui a pour effet de rendre les menaces et les conséquences plus redoutables en cas de diffusion d'images.

¹⁵ Centre canadien de protection de l'enfance (2022). *Dangers d'Internet : Sextorsion*. <https://www.cyberaide.ca/fr/dangers-internet/sextorsion/>

¹⁶ Stonehedge (2022, 17 août). *I have just been a victim of sextortion and idk what to do* [publication relevée sur le forum]. Reddit. https://www.reddit.com/r/Sextortion/comments/wr9oce/i_have_just_been_a_victim_of_sextortion_and_idk/

¹⁷ Le score Snapchat (snapscore) est la somme des photos et des vidéos envoyées et reçues par un utilisateur de Snapchat. Un score faible indiquerait un compte nouveau ou rarement utilisé, signe qu'il s'agit peut-être d'un compte frauduleux.

¹⁸ DickCheed. (2022, 1^{er} avril). *Last few days have been traumatic, need guidance* [publication relevée sur le forum]. Reddit. https://www.reddit.com/r/Sextortion/comments/ttk7l0/last_few_days_have_been_traumatic_need_guidance/

Communications avec le sextorqueur

Même si la communauté r/Sextortion répète sans cesse le même conseil de bloquer les sextorqueurs, les victimes sont réticentes à le faire, et ce pour plusieurs raisons. Beaucoup craignent d'exaspérer le sextorqueur et de risquer davantage de voir leurs images diffusées si elles coupent la communication avec lui. Beaucoup disent aussi craindre que cela ne les prive d'une certaine influence sur l'issue de la crise. Certaines victimes craignent aussi de perdre la capacité (réelle ou perçue) de savoir si leurs images ont finalement été diffusées.

« **J'ai vu tous les conseils disant de simplement les bloquer partout et de couper toute communication et de ne plus y penser, mais j'étais légitimement paralysé par la peur que cette personne mette ses menaces à exécution et transmette mes images par message direct à des gens que je connais**¹⁹. [traduction libre]

De nombreuses victimes font valoir que le maintien des communications avec le sextorqueur (pour le payer, négocier, essayer de gagner du temps, lui faire entendre raison, etc.) risque d'exaspérer le sextorqueur et, dans certains cas, de se solder par la diffusion des images. Cela donne encore ici du mérite au conseil maintes fois répété par les modérateurs de r/Sextortion, à savoir de bloquer immédiatement les sextorqueurs.

En plus de la réticence naturelle de nombreuses victimes à couper la communication avec le sextorqueur, au moins une victime rapporte dans un signalement à Cyberaide.ca qu'un individu se faisant passer pour un expert en cybersécurité lui avait conseillé comme tactique dilatoire de garder contact avec le sextorqueur.

¹⁹ bigstud1891 (2022, 12 juin). *I need help* [publication relevée sur le forum]. Reddit. https://www.reddit.com/r/Sextortion/comments/vanz1z/i_need_help/

Méthodes de paiement et remboursements aux victimes

Les victimes ne donnent généralement pas de détails sur les moyens que les sextorqueurs leur dictent d'utiliser pour leur envoyer de l'argent. PayPal est la plateforme la plus souvent citée par les victimes, mais les sextorqueurs ont aussi recours à de nombreuses autres formes de paiement en ligne. Certaines victimes ont réussi à annuler la transaction ou à se faire rembourser par l'entreprise qui avait traité le paiement, mais beaucoup ne connaissaient pas l'existence de cette possibilité ou redoutaient la colère du sextorqueur si elles annulaient le paiement. Il est bon de souligner qu'il n'est pas toujours possible d'obtenir un remboursement. Par exemple, les paiements personnels (destinés à des particuliers plutôt qu'à des entreprises enregistrées) au moyen de PayPal ne sont pas remboursables²⁰.

Entreprises de cybersécurité et de gestion de réputation, et « escrocs du recouvrement »

Plusieurs victimes font état d'interactions fâcheuses avec des entreprises de cybersécurité et de gestion de réputation, de soi-disant experts et des « escrocs du recouvrement » qui les ont contactées directement.

Ces entreprises disposent de consultants ou de détectives privés et présentent souvent leurs services sur des sites de belle facture. Témoignages à l'appui, elles disent pouvoir empêcher la diffusion d'images intimes, repérer les sextorqueurs, les identifier et les traduire en justice, protéger les renseignements personnels et sécuriser les comptes.

Sur le forum, des victimes racontent comment elles en sont venues à trouver et à contacter ces entreprises ou ces soi-disant « experts » lorsqu'elles étaient en détresse, et plusieurs disent avoir eu le sentiment de se faire exploiter en raison de leur état de panique. Elles disent avoir fait l'objet de tactiques de pression et de peur destinées à leur faire payer d'avance des sommes allant parfois jusqu'à plusieurs milliers de dollars pour des forfaits et des services toujours plus chers. Une entreprise, par exemple, offrait un service censé empêcher la diffusion des images – le souhait le plus cher de presque toutes les victimes – mais ce service n'était inclus que dans son forfait le plus cher, lequel nécessite l'achat préalable d'autres services.

²⁰ PayPal (2021, 10 décembre). *Programme de protection des achats de PayPal*. https://www.paypal.com/ca/webapps/mpp/ua/buyer-protection?locale.x=fr_CA

Lorsque des victimes indiquent sur r/Sextortion leur intention de faire appel à de telles entreprises, les habitués du forum répondent en le leur déconseillant. De fait, certains utilisateurs assimilent ces entreprises aux sextorqueurs, affirmant qu'il s'agit d'« escrocs » qui utilisent les mêmes « tactiques de peur ».

En plus des entreprises susmentionnées et des soi-disant experts, des « escrocs du recouvrement » offrent aussi leurs services aux victimes. L'expression « escrocs du recouvrement » désigne ici des personnes qui entrent en contact avec des victimes sur le forum et qui offrent de les mettre en relation avec un pirate informatique (*hacker*) capable de s'introduire dans les comptes ou l'appareil du sextorqueur pour y effacer les images de la victime – à condition de se faire payer d'avance. Les modérateurs de r/Sextortion sont au courant de ces tactiques et mettent les utilisateurs en garde dans un texte d'introduction permanent²¹ ainsi que dans un commentaire qui apparaît automatiquement dans toutes les nouvelles publications sur le forum²².

Utilisation possible de robots et de processus automatisés par les sextorqueurs

De nombreuses victimes disent avoir vu des comptes qu'elles soupçonnent être des « robots ». Par exemple :

« **Même si je trouvais que quelque chose ne tournait pas rond avec cette « fille », je lui ai quand même envoyé des photos nues. J'ai supposé que je parlais à un robot, mais je me suis quand même plié au jeu²³. [traduction libre]**

Les preuves manquent pour étayer l'idée que les sextorqueurs utilisent des robots ou d'autres processus automatisés pour extorquer leurs victimes; cependant, nous avons découvert sur des forums de développeurs de logiciels de nombreux outils en ligne ainsi que des scripts tout faits (code informatique) qui pourraient servir à créer des comptes et à gonfler artificiellement certaines mesures d'engagement, dont le nombre d'abonnés Instagram et le score Snapchat.

²¹ the_orig_odd_couple (2021, 4 mai). *New victims: Please read first* [publication relevée sur le forum]. Reddit. https://www.reddit.com/r/Sextortion/comments/n4yorq/new_victims_please_read_first/

²² AutoModerator (2022, 17 octobre). *Please read the post: New Victims: Please read first WARNING...Beware of recovery scammers: It is likely that you will* [Commentaire relevé sur la publication intitulée *How to protect yourself from and IG sextortion scam*]. Reddit. https://www.reddit.com/r/Sextortion/comments/y63ewf/how_to_protect_yourself_from_and_ig_sextortion/

²³ Acceptable-Waltz-518. (2021, 4 novembre). *Hinge/Snapchat scam* [publication relevée sur le forum]. Reddit. https://www.reddit.com/r/Sextortion/comments/qmvs3n/hingsnapchat_scam/

Facteurs de risque liés à la conception des plateformes

L'analyse des publications des victimes a mis en évidence quatre caractéristiques de conception qui rendent une plateforme propice à la sextorsion financière.

1. Facilité d'accès aux comptes de médias sociaux et aux contacts des victimes

Plusieurs caractéristiques de conception des plateformes permettent aux sextorqueurs de s'immiscer facilement dans les réseaux sociaux des victimes (p. ex. en devenant leur « ami » ou en les « suivant ») et d'accéder à leurs listes de contacts (p. ex. en examinant la liste de leurs autres « amis » ou de leurs « abonnés »). Ces deux éléments sont indissociables de toute tactique de sextorsion financière. Dès qu'un sextorqueur peut envoyer un message direct à un utilisateur, l'échange d'images intimes peut commencer. Et dès qu'il a des images de la victime en sa possession, le sextorqueur peut brandir son accès à la liste de contacts de celle-ci pour donner du poids à ses menaces de transmettre lesdites images aux contacts de la victime. Les sextorqueurs utilisent aussi les listes de contacts des victimes pour agrandir leur bassin de victimes potentielles.

Prenons la fonction « Ajout rapide » de Snapchat. Cette fonction présente à l'utilisateur une liste de personnes avec lesquelles il a des amis en commun et lui permet de les ajouter à sa liste de contacts. De nombreuses victimes font remarquer que c'est par cette même fonction qu'elles ont été mises en contact avec un sextorqueur. Certaines disent avoir ajouté le sextorqueur après l'avoir vu dans l'ajout rapide, d'autres rapportent que c'est le sextorqueur qui les a ajoutées à partir de l'ajout rapide.

La liste d'« amis » sur Facebook et la liste d'« abonnements » sur Instagram fonctionnent un peu de la même manière. Sur Instagram, par exemple, n'importe qui peut voir la liste d'« abonnements » ou d'« abonnés » d'un utilisateur si son profil est public; si son profil est privé, seuls ses abonnés peuvent voir la liste des personnes qu'il suit ou qui le suivent. Avec un minimum d'effort, il est facile pour un sextorqueur de voir le réseau de ses victimes et de donner une apparence d'authenticité à ses comptes en établissant minutieusement des connexions communes.



Hier, j'ai reçu une demande de suivi sur Instagram venant d'une inconnue qui avait 1100 abonnés et qui suivait plus de 500 personnes. Comme elle avait 12 amis en commun avec moi, j'ai fini par accepter sa demande²⁴. [traduction libre]

2. Incitatifs à partager des renseignements personnels

De nombreuses plateformes présentent des caractéristiques de conception qui encouragent les utilisateurs à partager des quantités importantes de renseignements personnels, renseignements dont les sextorqueurs peuvent ensuite se servir aisément pour s'en prendre à leurs victimes.

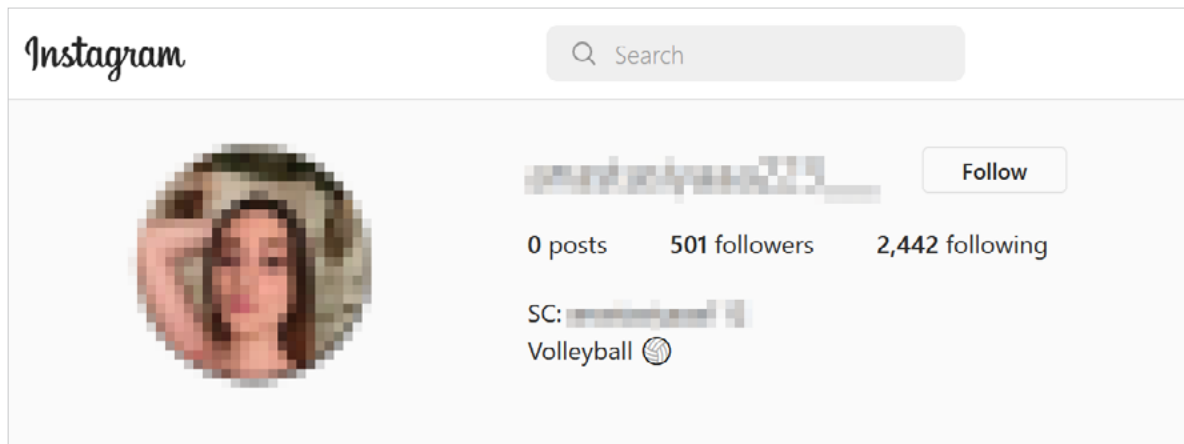
Par exemple, Snapchat utilise des fonctions de notification pour encourager les utilisateurs à améliorer leur Carte Snap en activant la localisation exacte. Ce paramètre a pour effet de débloquent certaines fonctions et de permettre à d'autres personnes de voir la position de l'utilisateur en temps réel. Plusieurs victimes rapportent que leur sextorqueur avait consulté leur Carte Snap et leur en avait envoyé des captures d'écran pour leur montrer qu'il connaissait leur position, donnant ainsi plus de crédibilité à ses menaces.

²⁴ 7T917 (2022, 13 juin). *I am a victim of sextortion* [publication relevée sur le forum]. Reddit. https://www.reddit.com/r/Sextortion/comments/vbra6y/i_am_a_victim_of_sextortion/

3. Prolifération de comptes frauduleux ou bidons

Une pratique des sextorqueurs consisterait à créer plusieurs comptes auxquels ils donnent une apparence légitime par des associations minutieuses avec d'autres comptes ou par le piratage ou la prise de contrôle de comptes existants qu'ils réaffecteront pour leur usage²⁵. Il nous apparaît possible aussi que des sextorqueurs achètent des comptes volés ou piratés auprès de communautés en ligne spécialisées dans la cybercriminalité. Certaines victimes ont constaté que les sextorqueurs créent souvent des profils similaires à des profils existants en réutilisant les mêmes images et en modifiant subtilement le nom de l'utilisateur, ce qui leur permet d'exploiter plusieurs comptes simultanément. Par exemple, dans les deux derniers mois, les analystes de Cyberaide.ca ont appris l'existence d'au moins 19 comptes Instagram uniques dédiés à la sextorsion et arborant sensiblement le même visage de jeune femme sur la photo de profil ou la même photo, comme dans l'exemple ci-dessous. Cela donne à penser que les plateformes de médias sociaux ne parviennent pas à déjouer les stratagèmes relativement flagrants des sextorqueurs.

PHOTO DE PROFIL INSTAGRAM SOUVENT RÉUTILISÉE PAR LES SEXTORQUEURS



4. Manque d'options de signalement et inaction

Plusieurs victimes déplorent le fait que les plateformes de médias sociaux ne leur permettent pas de signaler spécifiquement les cas de sextorsion et de faire valoir l'urgence de la situation lorsqu'elles s'y font agressivement (et activement) harceler. Plusieurs victimes rapportent que des comptes sont restés actifs même après qu'elles les eurent signalés ou que le sextorqueur soit parvenu à les recontacter au moyen d'un autre compte après que les opérateurs de la plateforme eurent bloqué, effacé ou fermé le compte utilisé initialement.

²⁵ O'Flaherty, K. (2019, 12 février). Hackers have just put 620 million accounts up for sale on the dark web - - Are you on the list? *Forbes*. <https://www.forbes.com/sites/kateoflahertyuk/2019/02/12/hackers-have-just-put-620-million-online-account-details-up-for-sale-is-yours-on-the-list/?sh=25748d874418>

CONCLUSION

La présente étude offre des analyses de tendances historiques et de mots-clés relevés dans les données d'archives du forum r/Sextortion – l'un des plus grands forums de discussion et de soutien consacrés à la sextorsion financière sur Internet – ainsi que des analyses approfondies de récits de victimes trouvés au même endroit. Les résultats de ces analyses approfondies montrent que la plupart des incidents impliquent l'utilisation combinée d'Instagram et ensuite de Snapchat, que les principales cibles de sextorsion financière sont des garçons et de jeunes hommes (lorsque le sexe de la victime est connu) et que certaines caractéristiques de conception des plateformes de médias sociaux rendent celles-ci propices à la sextorsion. Ces résultats soulignent la nécessité de renforcer la sécurité et la protection de la vie privée sur les plateformes de médias sociaux et d'améliorer les mécanismes de signalement pour lutter contre l'augmentation de la cyberviolence sexuelle.

Nous remercions les personnes qui ont partagé publiquement leurs expériences personnelles dans la communauté r/Sextortion. Nous sommes d'avis que ces contributions permettent d'éclairer les politiques publiques, de sensibiliser la population et d'aider les victimes de ce crime.



Photo d'un mannequin. Pour illustrer le texte.

ANNEXE : TERMES UTILISÉS POUR LES RECHERCHES PAR MOTS-CLÉS DANS LES ARCHIVES DE REDDIT

Des recherches par mots-clés ont été effectuées au moyen d'expressions rationnelles (Regex) et de correspondances de chaînes insensibles à la casse. Une expression rationnelle est une suite de caractères typographiques chargée de décrire une chaîne de caractères à trouver dans un bloc de texte. Nous avons déterminé les plateformes et les formes de paiement en ligne à inclure dans les différentes listes de termes de recherche en fonction des technologies les plus souvent relevées dans l'échantillon de publications examinées manuellement et de notre connaissance générale des pratiques des sextorqueurs.

Les expressions rationnelles suivantes ont été utilisées pour trouver des mentions de plateformes dans les publications du forum :

```
'Instagram':[r'\binsta\b',r'\binstagram\b',r'\big\b',r'\bgram\b'],
'WhatsApp':[r'\bwhatsapp\b',r'\bwhats app\b'],
'Facebook':[r'\bfacebook\b',r'\bface book\b',r'\bfb\b'],
'Tinder':[r'\btinder\b'],
'Telegram':[r'\btelegram\b'],
'TikTok':[r'\btiktok\b',r'\btik tok\b'],
'Snapchat':[r'\bsnapchat\b',r'\bsnapchat\b',r'\bsnap\b',r'\bsc\b'],
'Omegle':[r'\bomegle\b'],
'Wink':[r'\bwink\b'],
'Hinge':[r'\bhinge\b'],
'Skype':[r'\bskype\b'],
'Grindr':[r'\bgrindr\b',r'\bgrinder\b'],
'Discord':[r'\bdiscord\b'],
'Hoop':[r'\bhoop\b'],
'LinkedIn':[r'\blinkedin\b',r'\blinked in\b'],
'Badoo':[r'\bbadoo\b'],
'Bumble':[r'\bbumble\b'],
'Viber':[r'\bviber\b']}]
```

Les expressions rationnelles suivantes ont été utilisées pour trouver des mentions de formes de paiement en ligne dans les publications du forum :

```
'PayPal':[r'\bpaypal\b',r'\bpay pal\b'],
'Venmo':[r'\bvenmo\b'],
'Zelle':[r'\bzelle\b'],
'Remitly':[r'\bremitly\b'],
'Wise':[r'\bwise\b'],
'Cash App':[r'\bcash app\b',r'\bcashapp\b'],
'Western Union':[r'\bwestern union\b',r'\bwesternunion\b',
r'\bwestern-union\b'],
'Gift card':[r'\bgift card\b', r'\bgift cards\b',
r'\bgiftcards\b', r'\bgiftcard\b'],
'e-Transfer':[r'\be-transfer\b',r'\be transfer\b',r'\betransfer\b'],
'Crypto currency':[r'\bcrypto\b',r'\bcryptocurrency\b',
r'\bcrypto currency\b',r'\bcrypto-currency\b',
r'\bbitcoin\b',r'\bbitcoin\b',r'\bethereum\b',
r'\btether\b',r'\busdt\b'],
'Revolut':[r'\brevolut\b']}]
```



Photo d'un mannequin. Pour illustrer le texte.



CENTRE CANADIEN *de* PROTECTION DE L'ENFANCE™
Aider les familles. Protéger les enfants.

 [Protegeonsnosenfants.ca](https://protegeonsnosenfants.ca)

 [@CCPEenfance](https://twitter.com/CCPEenfance)

 [Centre canadien de protection de l'enfance](https://www.facebook.com/CentreCanadienDeProtectionDeL'Enfance)

 [@cdnchildprotect](https://www.instagram.com/cdnchildprotect)