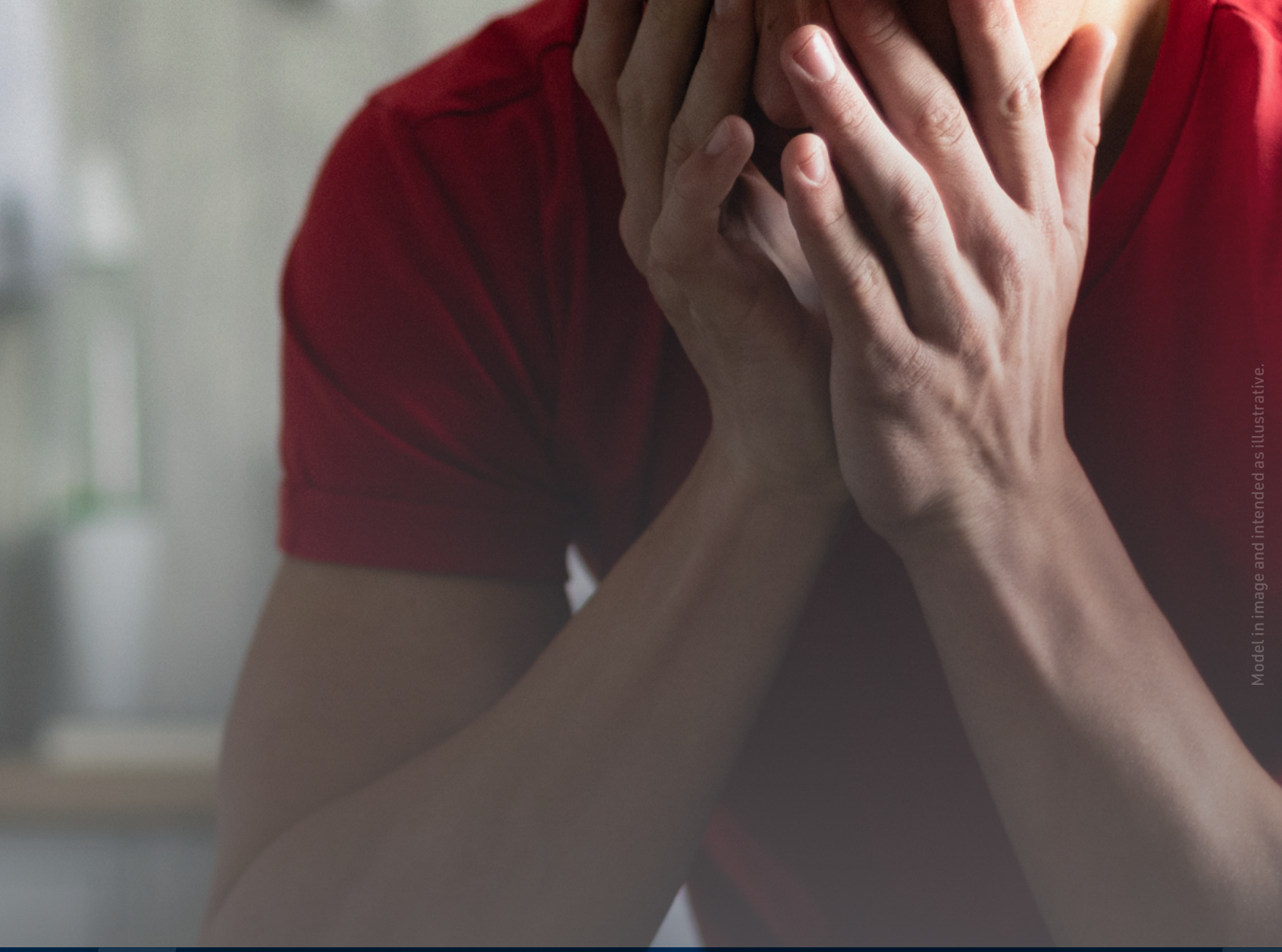


Model in image and intended as illustrative.

AN ANALYSIS OF FINANCIAL SEXTORTION VICTIM POSTS PUBLISHED ON R/SEXTORTION

Date: November 2022 | Author: Canadian Centre for Child Protection (C3P)

CANADIAN CENTRE *for* CHILD PROTECTION®
Helping families. Protecting children.

Model in image and intended as illustrative.

Table of Contents

Executive Summary 3

Background 6

Methodology 7

Findings 8

Conclusion 21

Appendix 22

EXECUTIVE SUMMARY

About this Study

This study was conducted by the Canadian Centre for Child Protection Inc. (C3P), a national charity dedicated to the personal safety of all children. C3P operates Cybertip.ca, Canada's tipline to report child sexual abuse and exploitation online. In addition to responding to concerns of child sexual abuse and its recording and distribution online, in recent years we have seen a massive increase in online sexual violence. This includes but is not limited to reports of sextortion, luring, non-consensual distribution of intimate images, doxing, and stalking.

This report presents analyses of one of the largest financial sextortion discussion/support forums on the internet, ***reddit.com/r/Sextortion***. Two forum data sources were analyzed for this study. One was open-source archives from July 2020 to September 2022, which provided historic forum trends. The second was 478 narratives of victims describing their experience of being financially sextorted, posted to r/Sextortion from June 10 to August 10, 2022.

Key Findings

The volume of new posts and subscribers to the r/Sextortion forum has been rising sharply since the spring of 2022. Analyses of these posts demonstrate that:

- **The primary targets of financial sextortion are boys and young men.** Of the forum posts that included information about the victim's gender, 98 percent were male.
- **Many extorters use a similar strategy involving Snapchat and Instagram.** Posing as a female, they first contact the victim on Instagram. They soon move the conversation to Snapchat, where they entice the victim to send a nude image. Then the extorter blackmails the victim: they demand that the victim send them money, and if not, they will send the victim's nudes to their friends and family. To legitimize their threats, extorters will send the victim screenshots of victim's social media contacts.
- **Popular platforms have design characteristics that create favourable conditions for predation.** Extorters weaponize social media platforms in that they can easily create fake accounts to access potential victims and their personal information and social networks. Victims also pointed to platform reporting functions that failed to provide them with options to accurately describe their situation and a lack of meaningful action being taken by platform operators.

- **Complying with extorters' demands for money typically leads to more demands for money.** When victims sent extorters money, in nearly all cases (93 percent) the extorters subsequently asked for *more* money.
- **Cybersecurity or reputation management firms and individuals claiming expertise overpromise their services, including the prevention of image distribution in exchange for significant sums of money.** Victims described negative interactions with these firms and individuals, likening their high-pressure sales tactics to those of extorters. Notably, victims who had employed fee-for-service firms or so-called "experts", sometimes for thousands of dollars, advised others against hiring these firms.

Key Takeaways

- Victim narratives suggest that when targeted by a financial sextortion attempt, an effective strategy is to not give in to an extorter's demands and cut off all communication.
- Social media platforms should ensure accounts for users under 18:
  - are by default private;
  - do not nudge them to add other users;
  - and do not incentivize them to share personal information, such as real-time location.
- Social media platforms should provide reporting options specific to blackmail and extortion that are responsive and capture the seriousness of users being aggressively and actively targeted.
- Information collected on the r/Sextortion forum shows extorters are using various online payment processors, including gift cards. Further research is needed to identify strategies to prevent extorters from exploiting these services to commit these crimes.

BACKGROUND

What is Reddit?

Reddit is a social media platform that consists of millions of forums known as "subreddits" dedicated to a variety of topics. Subreddits are also commonly referred to as "communities" or "sub-communities"[1], which users generally interact with based on personal interest. The name of each subreddit begins with "r/," as this is part of the URL that Reddit uses[2]. Reddit is comprised of user-generated content across subreddits. There are three ways in which users can interact with subreddits: posting, commenting on a post, and voting on a post. A new post to a subreddit, as well as any subsequent comments or votes on it, are collectively referred to as a thread.

What is r/Sextortion?

r/Sextortion is the largest known sextortion-specific support forum on Reddit. This community was created in February 2020 and, at the time of this report, had more than 6,300 members. Members who author posts or comments in the forum are nearly always victims of financial sextortion seeking support or offering advice. When Reddit users post experiences of being financially sextorted on other subreddits, such as r/Scams and r/Advice, it is common for other users to direct them to r/Sextortion for advice and support specific to sextortion.

What is Financial Sextortion?

Financial sextortion is a type of blackmail that typically involves a victim connecting with someone online who is unknown to the victim. The unknown individual often misrepresents their age and/or gender and manipulates the victim into sending nude images of themselves[3]. Almost immediately the victim receives demands for money (and sometimes also demands for more intimate images) while under constant threat that if they fail to comply, their images will be sent to friends, family, or distributed online. Some victims who are under 18 also report threats that they will be arrested for the imagery created. Targets of financial sextortion are reportedly often male youths who are deceived into believing they are communicating with a young female[4]; this communication often occurs over a short period of time, anywhere between minutes to hours.

---

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

[2] Widman, J. (2021, July 5). *What is Reddit?* Digital Trends. https://www.digitaltrends.com/computing/what-is-reddit/

[3] The Royal Canadian Mounted Police. (2022, August 22). *Tips to keep yourself safe from online sextortion* [News release]. https://bc-cb.rcmp-grc.gc.ca/ViewPage.action?siteNodeId=2087&languageId=1&contentId=76285

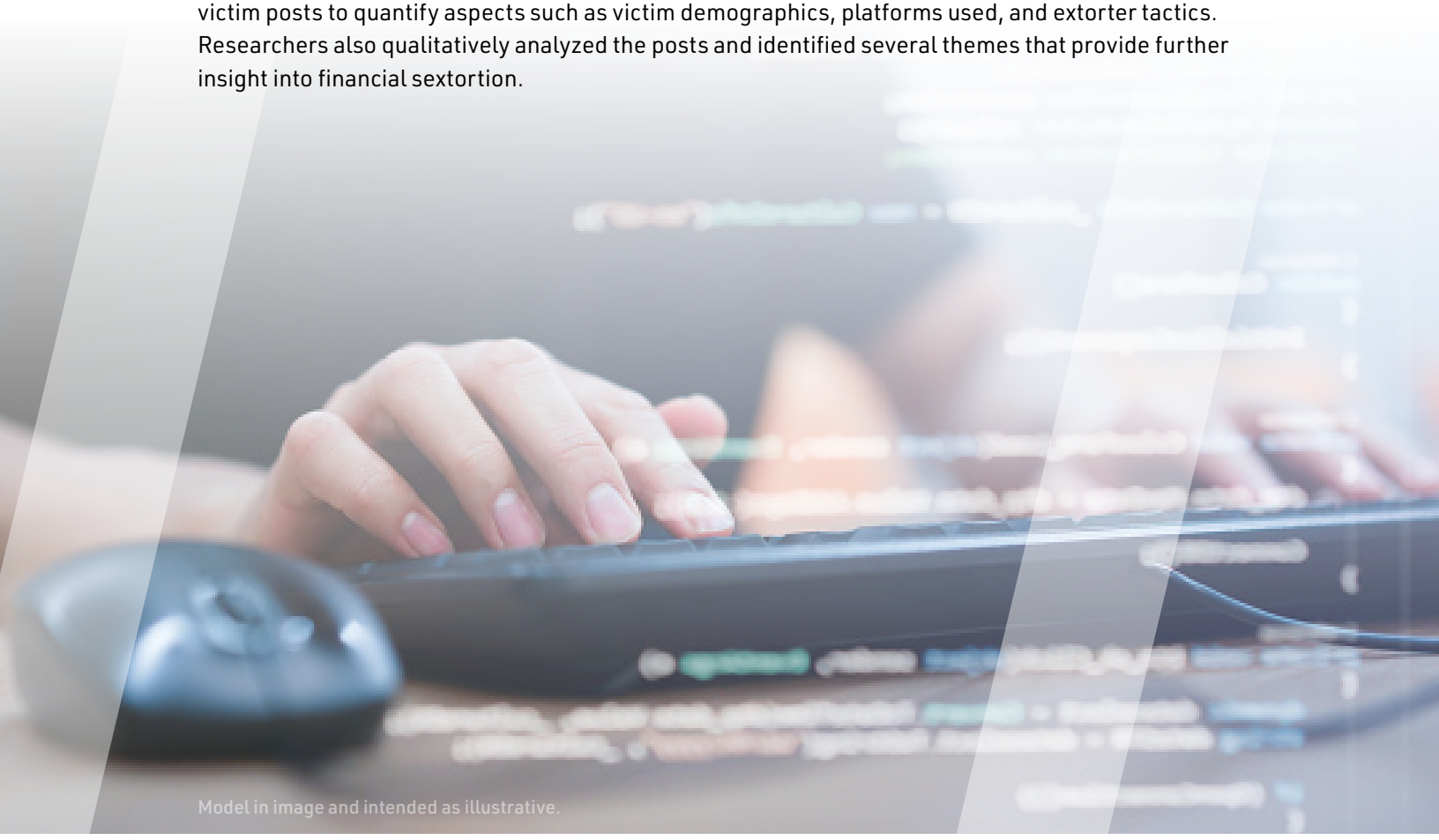
[4] Canadian Centre for Child Protection. (2022, August 4). *Boys aggressively targeted on Instagram and Snapchat, analysis of Cybertip.ca data shows* [Press release]. https://www.protectchildren.ca/en/press-and-media/news-releases/2022/sextortion-data-analysis

METHODOLOGY

C3P researchers analyzed one of the largest known sextortion discussion/support forums on the internet, ***reddit.com/r/Sextortion***. Two r/Sextortion data sources were analyzed for this study: forum archives and victim narratives.

Reddit limits the number of posts displayed on a forum. To assess historic forum trends, C3P researchers analyzed open-source r/Sextortion forum archives made available by the Pushshift.io Reddit API. Pushshift.io collects and disseminates public Reddit forum data on a monthly basis for research purposes. Using r/Sextortion forum archives from July 2020 to September 2022, C3P researchers wrote computer code to analyze forum user activity over time and assess the frequency with which victims reference key platforms and payment processors. The terms used for the keyword searches are set out in the Appendix.

To complement this timeseries analysis with rich, recent data, C3P researchers also analyzed victim narratives – the 478 posts from self-reported victims of financial sextortion that were publicly available on r/Sextortion between June 10 to August 10, 2022. Researchers manually coded the victim posts to quantify aspects such as victim demographics, platforms used, and extorter tactics. Researchers also qualitatively analyzed the posts and identified several themes that provide further insight into financial sextortion.



Model in image and intended as illustrative.

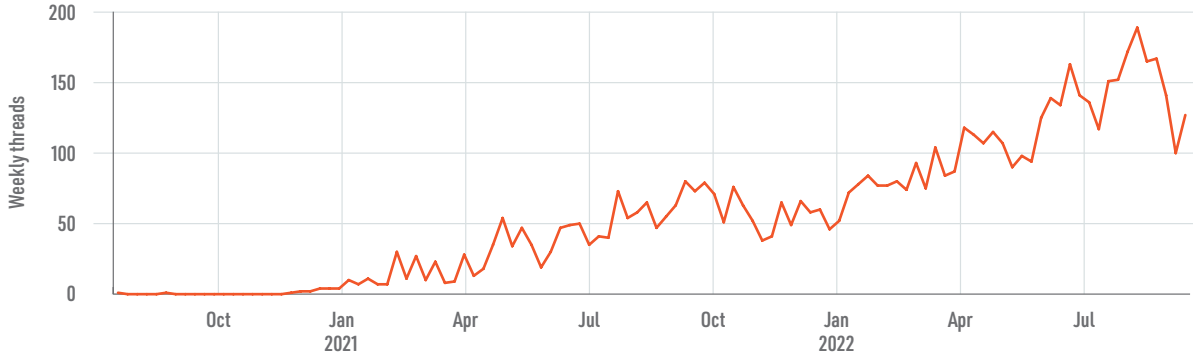
FINDINGS

Forum Archive Findings

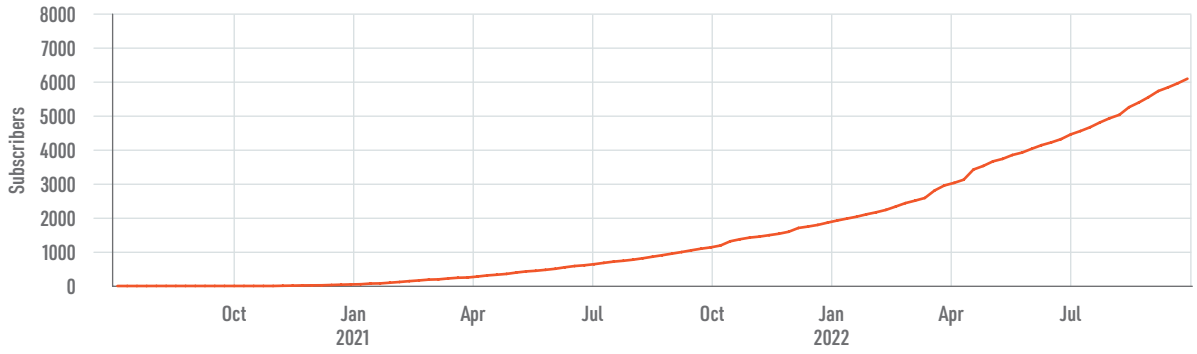
Forum User Activity

In total, 6,506 r/Sextortion threads were included in the archival analysis. At the time of this report, r/Sextortion had over 6,300 members, with hundreds of members joining weekly. The archive data shows the number of original posts (new threads) published each week has generally trended upward since January 2022, as has the number of active subscribers.

NEW WEEKLY THREADS POSTED TO R/SEXTORTION



CUMULATIVE R/SEXTORTION FORUM SUBSCRIPTIONS

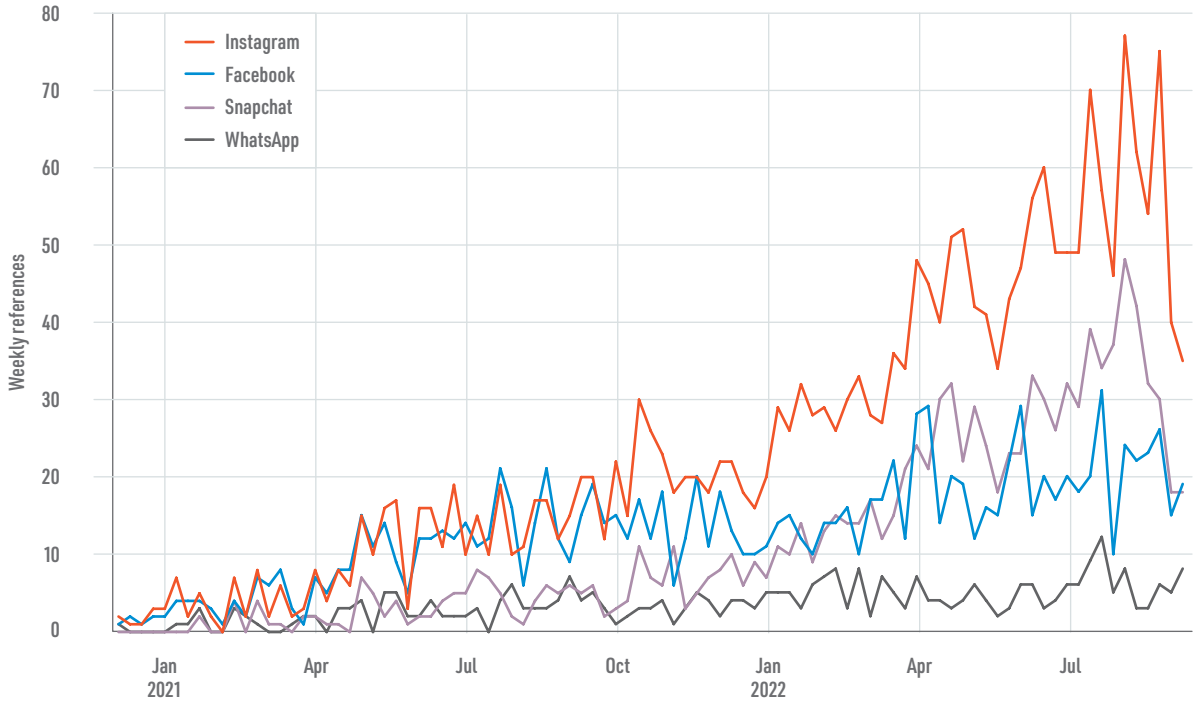


Platforms

We used keyword searches to identify the frequency with which victims referenced the major platforms on r/Sextortion since 2020. Note that the keyword search data reflects whether a platform was mentioned by the victim in the post; it does not necessarily indicate the named platform was used to facilitate the harm.

The historic view illustrated in the chart below shows all references made by victims regarding Instagram® (n=2,263), Facebook® (n=1,212), Snapchat® (n=1,068), and WhatsApp® (n=329) over the past two years, broken down by weekly volume. These are the platforms that victims have referenced most often.

WEEKLY REFERENCES TO PLATFORMS POSTED TO R/SEXTORTION (BASED ON ARCHIVES)



Of note, TikTok®, which boasts over 1 billion active users[5], was seldom referenced by victims in the forum archives (n=33; not listed in chart). It is possible that the platform's policies and design characteristics make it such that extorters do not gravitate toward it. For example, direct messaging on the platform is only available to registered account holders aged 16 and older. This, coupled with the policy that content created outside of TikTok can't be shared in a direct message[6], suggests TikTok may be less suitable for carrying out sextortion tactics.

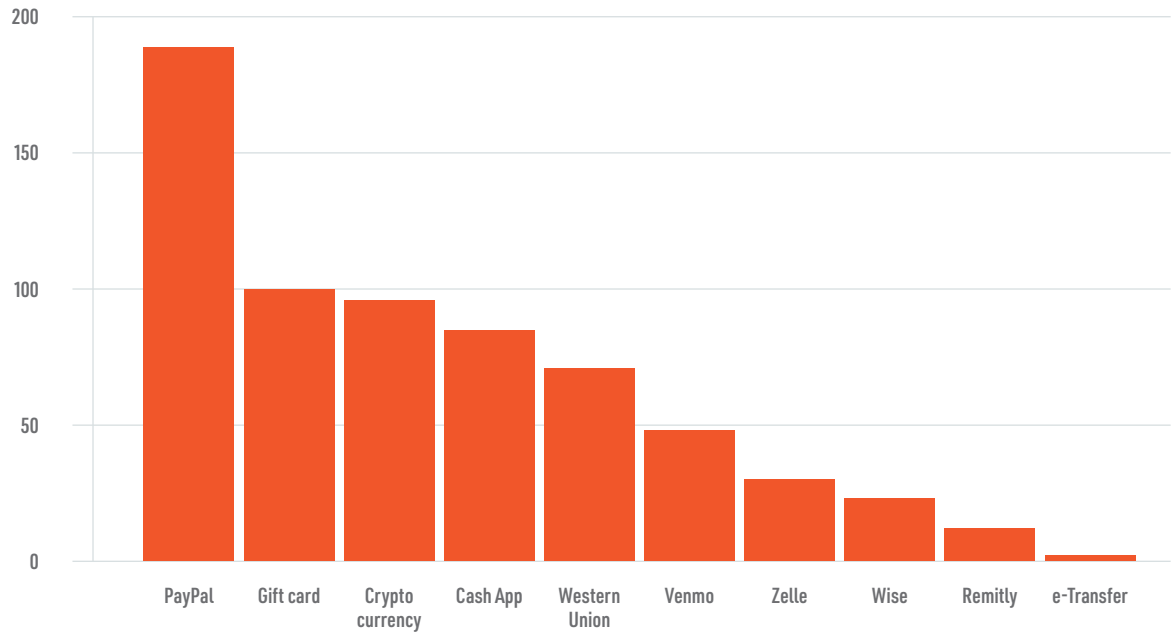
[5] Bursztynsky, J. (2021, September 27). TikTok says 1 billion people use the app each month. *CNBC*. https://www.cnbc.com/2021/09/27/tiktok-reaches-1-billion-monthly-users.html

[6] TikTok. (2022). *Direct messages*. Retrieved September 21, 2022, from https://support.tiktok.com/en/account-and-privacy/account-privacy-settings/direct-message

Payment Processors

Using keyword-based data, PayPal® (n=189), gift cards (n=100), Cryptocurrency (n=96), Cash App™ (n=85), and Western Union® (n=71) were the most frequently cited payment processors. Note that keyword search data reflects whether a platform was mentioned by the victim in the post; it does not necessarily indicate the named payment processor was ultimately used to send money to the extorter.

MOST REFERENCED PAYMENT PROCESSOR ON R/SEXTORTION (BASED ON ARCHIVES)

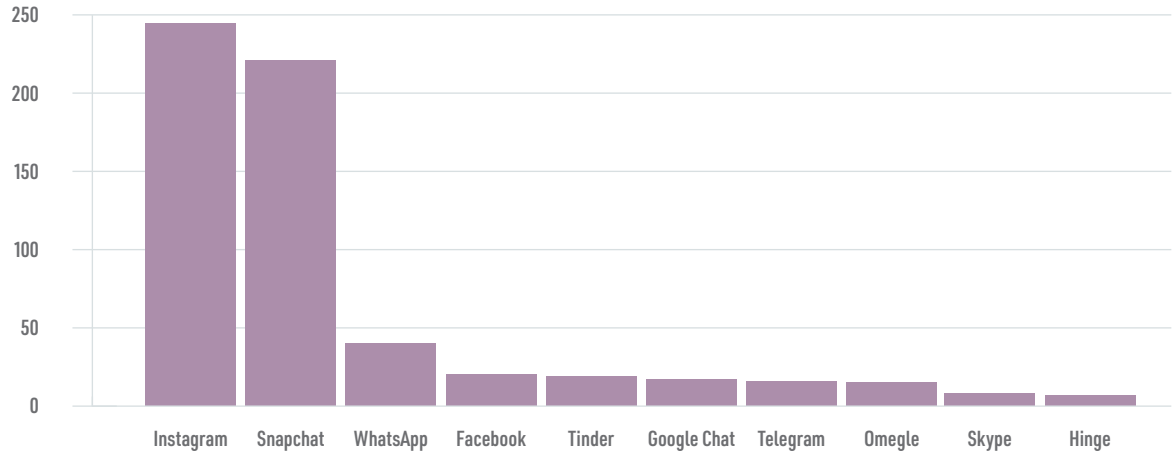


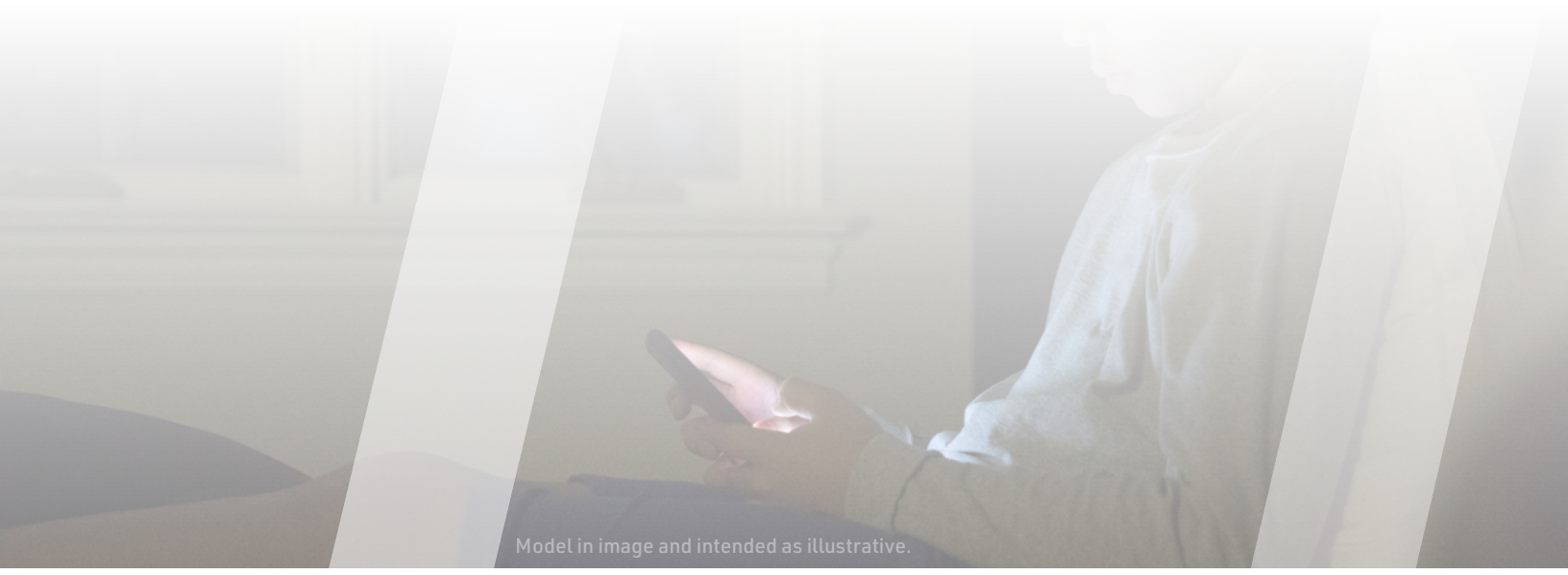
Victim Narrative Findings: Numeric Analyses

Platforms

Based on the sample of manually reviewed victim posts (n=478) from June to August 2022, the most frequently identified platforms used to facilitate financial sextortion tactics were Instagram (n=245) and Snapchat (n=221) followed by WhatsApp (n=40), Facebook (n=20), and Tinder® (n=19). Victims frequently described initial contact occurring on Instagram, which then migrated over to Snapchat where images were exchanged. Some extorters used Facebook to take screenshots of a victim's Facebook contacts and send them to the victim to illustrate they had the means to send victim's images to their friends, family, and so on. Reflective of the archival analysis, TikTok was rarely identified by victims as a platform in which sextortion occurred (n=2).

PLATFORMS IDENTIFIED BY VICTIMS ON R/SEXTORTION (TOP 8 ONLY | BASED ON VICTIM NARRATIVES)





Model in image and intended as illustrative.

Victim Demographics

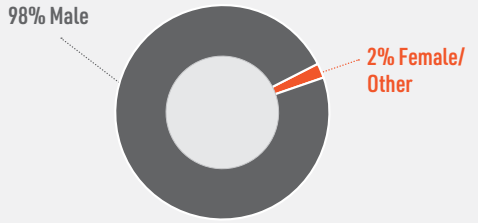
Gender

In nearly half of cases (n=231), the victims did not include information about their gender. Of the victims whose gender was clear, males were significantly over-represented (n=241). This pattern is mirrored in reports made Canada-wide to Cybertip.ca describing financial sextortion[7] as well as reports received by law enforcement agencies across Canada[8], the U.S.A.[9], and Australia[10].

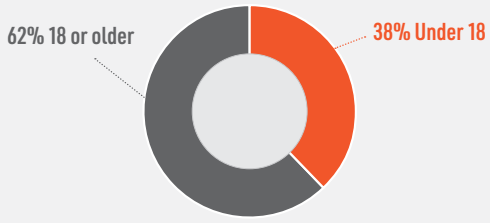
Age

In most cases, victims did not provide information about their age (n=302). Of the remaining cases, over 60 percent of financial sextortion victims were 18 and older (n=109) and nearly 40 percent (n=67) of victims identified as minors.

GENDER OF FINANCIAL SEXTORTION VICTIMS[11]



AGE OF FINANCIAL SEXTORTION VICTIMS



[7] Canadian Centre for Child Protection. (2022, August 4). *Boys aggressively targeted on Instagram and Snapchat, analysis of Cybertip.ca data shows* [Press release]. https://www.protectchildren.ca/en/press-and-media/news-releases/2022/sextortion-data-analysis

[8] Dormer, D. (2022, June 2). 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, May 31). 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, September 10). *Police warning: Sextortion for profit on the rise*. https://www.afp.gov.au/news-media/media-releases/police-warning-sextortion-profit-rise

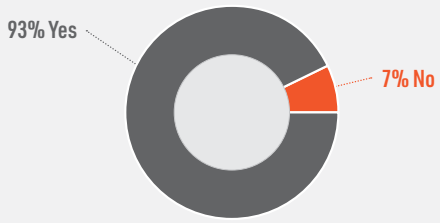
[11] Charts and figures in this section are based only on known or available data. For example, this chart only includes the data for the 245 victims who provided information about their gender; not displayed are the 231 victims who did not provide information about their gender.

How Victim Compliance Impacted Extorters' Demands and Threat Follow Through

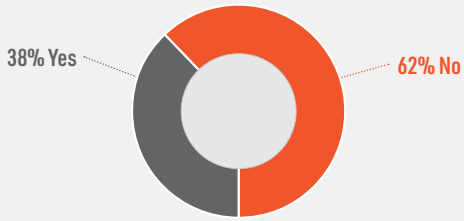
There were 174 victims who reported complying with extorters' demands for money with many noting how complying impacted the extorters' demands (n=133) or threat follow through (n=81). Almost all (93 percent) victims who paid the extorter received further demands for money, and nearly 40 percent had their images distributed anyways. Taken together, these findings support the prevailing recommendation given by many experts in this space, which is to never pay the extorter.

WHEN VICTIMS COMPLIED WITH EXTORTERS' DEMANDS FOR MONEY...

DID EXTORTERS DEMAND MORE MONEY?[12]

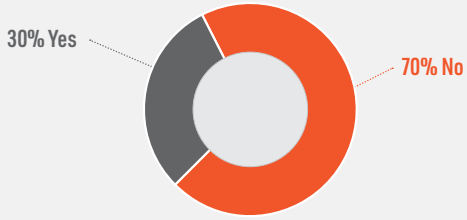


DID EXTORTERS FOLLOW THROUGH ON THEIR THREATS OF IMAGE DISTRIBUTION?



This advice is further underscored in the outcomes of the 145 victims who did **not** comply with extorters' demands for money[13]: compared to those who complied, those who didn't had a similar likelihood of having their images distributed with the benefit of not receiving further threats or demands from the extorter.

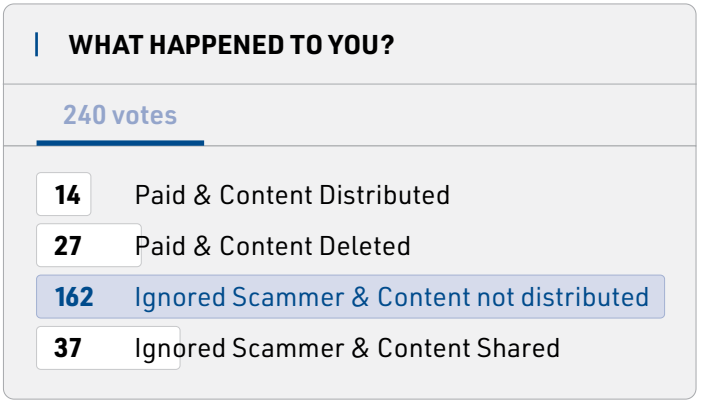
DID EXTORTERS FOLLOW THROUGH ON THEIR THREATS OF IMAGE DISTRIBUTION WHEN VICTIMS *DID NOT COMPLY?*



[12] "Demands" in the context of this table are defined as the additional demands that followed compliance. As a result, "demands" was not an applicable data field for those who did not comply with extorters' demands.

[13] An additional 115 victims did not comply with extorter demands for money. These victims did not state whether the extorter followed through on their threats of image distribution.

We believe the collection of forum posts analyzed underestimates the true proportion of victims who did not comply with extorters' demands and did not have their images distributed. In cases such as these (where threats subsided after not complying/cutting off further communication), the victims may be less motivated to return to the forum and provide updates to their previous posts about their experiences, as they may no longer be in a state of crisis. This theory is supported by the results of several informal polls taken on the forum itself over the past several months, which routinely showed higher proportions of no threat follow-throughs for those who did not comply (see image below)[14].



Payment Amounts

For cases where the amount of money paid to extorters was known (n=112), most victims paid between $100 and $500 (40 percent). Just over one third (36 percent) of victims paid $100 or less. Since it is impossible to know the currency type of the reported payments in all cases, this table assumes all values are in U.S. dollars.

AMOUNT OF MONEY VICTIMS PAID TO EXTORTERS

< $100	40	36%
$100 to $500	45	40%
$500 to $1000	15	13%
$1000 to $5000	12	11%
Total	**112**	**100%**

Payment Processors

When victims identified the payment processor used to pay the extorter (n=73), PayPal was named the most (n=23). This was followed by Venmo® (n=10) and Zelle® (n=7). Transactions made via banks, gift cards, and other platforms such as Cash App and Remitly™ accounted for a small portion of known payment processors. In many cases (n=131), victims who complied with the demand for money did not list a payment processor.

[14] AtomicDuckiez. (2022, April 8). *What happened to you?* [Online forum post]. Reddit. https://www.reddit.com/r/Sextortion/comments/tz36mj/what_happened_to_you/

Model in image and intended as illustrative.

Victim Narrative Findings: Thematic Insights

Extorter Strategy

The victim posts analyzed for this report often described similar extortion strategies. The following quote captures key elements of many experiences on r/Sextortion, which mirror trends in reports to Cybertip.ca[15]:

> **"Early today I had accepted this person on my Instagram page. After talking a few minutes, we moved on to snapchat. Then the scammer sent some nude images and I stupidly sent some back. After that they had screenshots of my whole following list from Instagram, most of them were my family members and they threatened that they will expose me if I didn't send them money."[16]**

Victims often note they had or should have had suspicions they were being targeted by a scam, acknowledging red flags such as poor grammar, moving the conversation to different platforms, and the speed at which the conversation turned sexual. However, mutual followers, the appearance of high engagement (including high follower counts or Snapchat scores[17]) helped convince victims that extorter accounts were legitimate.

> **"I know all the usual tells of a scam like this but the scammer made it very believable, they had normal amount of followers on insta, a high snapscore and a consistent face from the snaps. so, I was convinced that it wasnt a scam. I was wrong."[18]**

As indicated above, extorters often engage with victims across more than one social media platform. This cross-platform tactic provides greater access to the victim's followers and personal information, intensifying the threat and consequences in the event of image distribution.

---

[15] Canadian Centre for Child Protection. (2022). *Online harms: Sextortion*. https://www.cybertip.ca/en/online-harms/sextortion/

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

[17] A Snapchat score ("Snapscore") is the sum of images and videos sent and received on Snapchat. A low Snapscore would indicate a new or rarely used account, which can be a sign of a fraudulent accounts.

[18] DickCheed. (2022, April 1). *Last few days have been traumatic, need guidance* [Online forum post]. Reddit. https://www.reddit.com/r/Sextortion/comments/ttk7l0/last_few_days_have_been_traumatic_need_guidance/

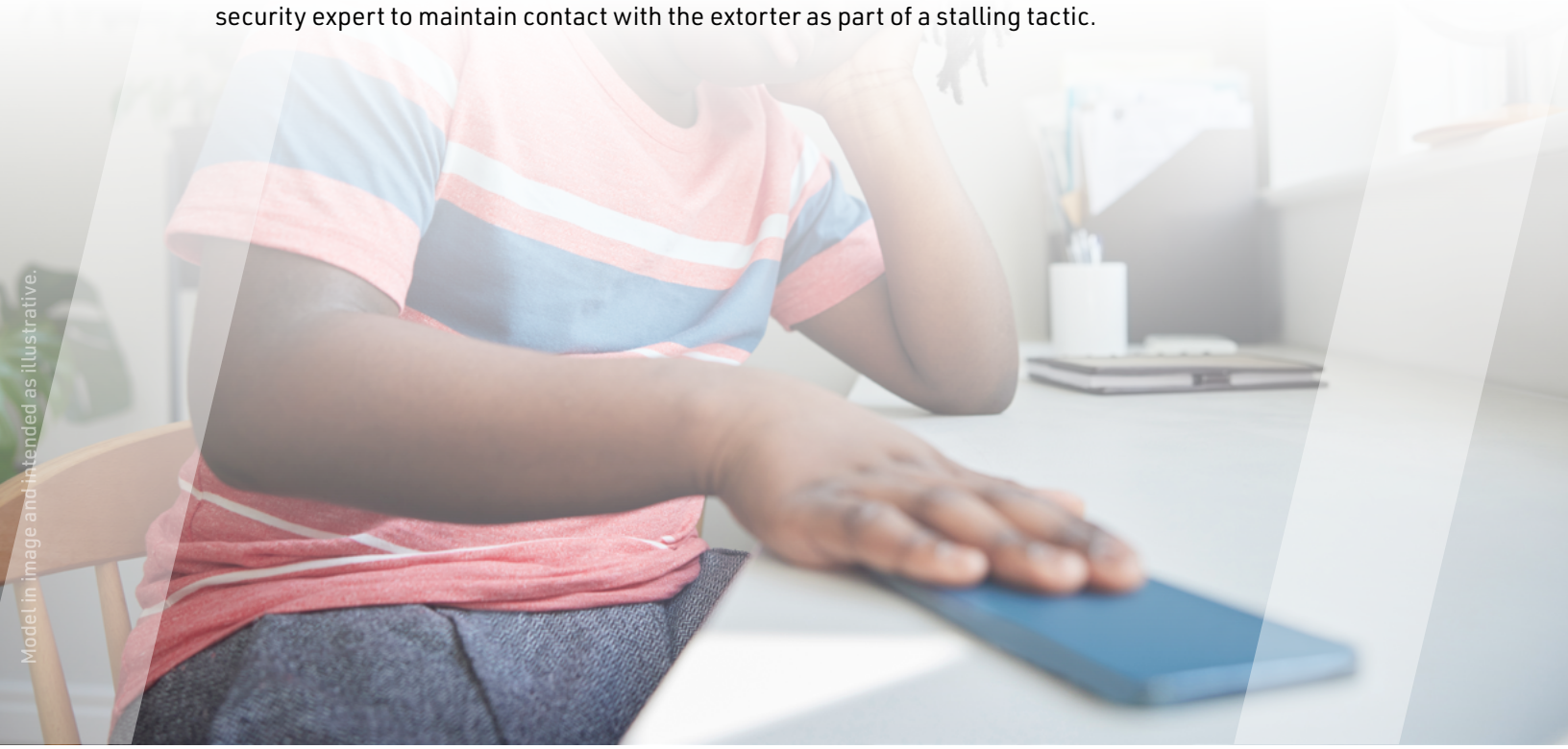
Communication with the Extorter

Despite the r/Sextortion community's repeated advice to block extorters, victims tended to be reluctant to do so, for several reasons. Many felt blocking would aggravate the extorter, increasing the likelihood of their images being distributed. Many victims also expressed a fear of losing some form of control over the outcome of the crisis, should they cut off communication with the extorter. Also common were concerns of losing the ability (or perceived ability) to monitor whether their images were ultimately distributed.

> **"I've seen all the advice in here to just block them everywhere and cut off all communication and don't worry about it, but my anxiety knowing this person might follow through and send these DMs to people I know is legitimately crippling."** [19]

Many victims described how continued communication with the extorter such as paying, negotiating, stalling, and antagonizing, were likely to aggravate the extorter, in some cases leading to image distribution. This further supported the r/Sextortion moderators' repeated advice to immediately block extorters.

In addition to the instinctive reluctance for many to break off communication, at least one victim who reported into Cybertip.ca said they were advised by an individual who purports to be a cyber-security expert to maintain contact with the extorter as part of a stalling tactic.



Model in image and intended as illustrative.

[19] bigstud1891. (2022, June 12). *I need help* [Online forum post]. Reddit. https://www.reddit.com/r/Sextortion/comments/vanz1z/i_need_help/

Extorter's Payment Demands and Victim Refunds

Victims generally did not provide insight regarding if and how the extorter instructed victims to pay them. While PayPal was referenced most often by victims, extorters relied on a wide variety of payment methods. Some victims were able to receive a refund from the payment processor or cancel the transaction; however, many were unaware this was possible, or were concerned that cancelling it would aggravate the extorter. It is worth noting that refunds may not be possible in some circumstances. For example, if a victim were to send an extorter a personal payment (i.e. not one sent to a registered business) using PayPal, they would not be eligible for a refund[20].

Cybersecurity and Reputation Management Firms, and "Recovery Scammers"

Several victims described negative interactions with two groups of people who provide help for a fee: for-hire cybersecurity and reputation management firms and individuals claiming expertise, as well as "recovery scammers" who reached out to the victim directly.

Such firms include private investigators or private consultants often promote their services through sophisticated-looking websites. Their websites showcase success stories and claims such as: preventing the distribution of intimate images; locating, identifying and bringing the extorter to justice; protecting personal information; and securing online accounts.

Victims on the forum described finding and contacting these firms or so-called "experts" when in crisis with several echoing a feeling of being taken advantage of given their state of panic. These victims detailed the use of high-pressure and fear-based sales tactics to encourage victims to pre-pay, in some cases, thousands of dollars for service packages with escalating expenses and service claims. For example, with one firm, a service to prevent image distribution – the primary objective of nearly all victims – was only available for the most expensive service package, which could only be accessed following the purchase of other services.

[20] PayPal. (2021, December 10). *PayPal's Purchase Protection Program*. https://www.paypal.com/us/webapps/mpp/ua/buyer-protection?locale.x=en_US#top

When victims on r/Sextortion expressed they were considering hiring such firms, subsequent comments from experienced forum users advised against this. In fact, some users likened these companies to the extorters, saying the companies were "scammers" who used the same "scare tactics."

In addition to the above firms and individual "experts", victims also described encountering offers of help from "recovery scammers." Recovery scammers refers to individuals who reach out to victims who have posted to the forum, offering to connect them with a "hacker" who could access the extorter's accounts or device and delete the victim's images – an offer contingent on upfront payment. The r/Sextortion moderators are aware of these tactics and warn against them in a permanent introductory post[21] as well as an automated comment that appears on every new post on the forum[22].

Suspected Use of Bots and Automation by Extorters

Many victims described encountering accounts that they suspected to be a "bot". For example:

> **"Despite being able to tell something was off with the supposed "girl", I still sent nudes. My assumption was that I was talking to a bot but I went along with it anyways."[23]**

There is limited information to support the idea that extorters are using bots or other automation methods to extort victims; however, we discovered several online tools and pre-written scripts (computer code) on software developer forums that could facilitate the creation of accounts and the artificial inflation of account engagement measures such as Instagram followers and Snapchat scores.

---

[21] the_orig_odd_couple. (2021, May 4). *New victims: Please read first* [Online forum post]. Reddit. https://www.reddit.com/r/Sextortion/comments/n4yorq/new_victims_please_read_first/

[22] AutoModerator. (2022, October 17). *Please read the post: New Victims: Please read first WARNING...Beware of recovery scammers: It is likely that you will* [Comment on the online forum post *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, November 4). *Hinge/Snapchat scam* [Online forum post]. Reddit. https://www.reddit.com/r/Sextortion/comments/qmvs3n/hingesnapchat_scam/

Platform Design Risk Factors

Analyses of victims' posts highlighted four platform design characteristics that create favorable conditions for financial sextortion.

1. Ease of Access to Victims' Social Media Accounts and Contacts

Several platform design aspects make it easy for extorters to immerse themselves in a victim's social network (e.g., to "friend" or "follow" them) and access the victim's contact list (e.g., seeing their other "friends" or "followers"). Both aspects are key to deploying financial sextortion tactics. Once an extorter can directly message a user, they can initiate the exchange of intimate images. And once in possession of these, they may leverage their access to the victim's contact list to amplify and lend credence to their threat of sending the intimate images to the victim's contacts. Extorters also use victim contact lists to grow their pool of potential victims.

Consider Snapchat's "Quick Add" feature. This feature finds other accounts that are connected in some fashion to a user's account, such as through a mutual friend, and then presents the user with a list of accounts to consider adding as contacts. Many victims noted this very functionality is how they became connected with an extorter: some said they saw the extorter's account listed under "Quick Add" and added the extorter, whereas others noted that the extorter had added them using "Quick Add".

Facebook's "friends" list function and Instagram's "following" list function have similar implications. On Instagram, for example, anyone can see a user's "following" or "friend" list if the user's settings are such that this information is visible publicly; if their account is private, their following or friend list can be viewed by anyone they allow to follow or friend them. With minimal effort, extorters have unfettered access to other users connected to their victim, and the opportunity to carefully curate their accounts to appear more authentic by establishing mutual connections.

> **"Yesterday, I got a follow request from a random girl on Instagram with 1.1 k followers and +500 following. *She had 12 mutual friends as me so I ended up accepting her account*."[24]**

2. Incentives to Share Personal Information

Many platforms have design features that encourage and even incentivize users to share significant amounts of personal information. As a result, extorters have easy access to information that may be weaponized against victims.

For example, Snapchat uses nudging functions to encourage users to "improve your Snap Map by enabling precise location". When users agree to this, additional platform features are unlocked, allowing others to see their real-time location. Several victims expressed that their extorter had accessed and sent screenshots of the victim's Snap Map to prove they knew the victim's location, further intensifying the threats.

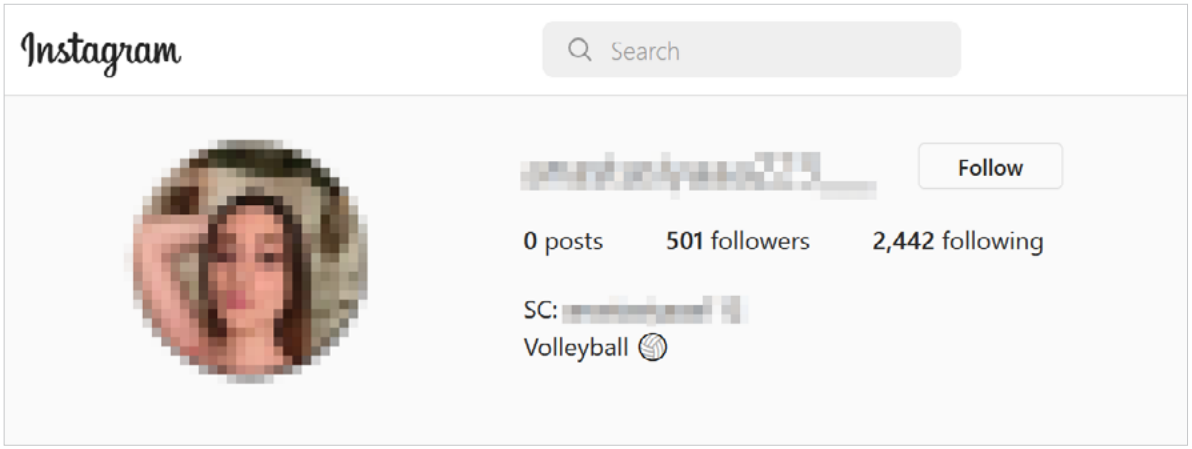
---

[24] 7T9I7. (2022, June 13). *I am a victim of sextortion* [Online forum post]. Reddit. https://www.reddit.com/r/Sextortion/comments/vbra6y/i_am_a_victim_of_sextortion/

3. The Proliferation of Fraudulent or Fake Accounts

Extorters can seemingly create multiple accounts that appear legitimate through careful curation or by hacking/taking over an existing account and repurposing it for their use[25]. We believe extorters may also purchase stolen or hacked accounts from online communities dedicated to cybercrime. Victims have remarked that extorters often recycle the likeness of a profile, using the same images and name construction to operate multiple accounts simultaneously. For example, over the last two months, Cybertip.ca analysts became aware of at least 19 unique Instagram accounts used to extort victims that all use a profile picture that appears to depict the same female, and in some cases recycle the same picture, such as the example shown in the below image. This suggests social media platforms are failing to intercept relatively obvious patterns used by extorters.

AN INSTAGRAM PROFILE PHOTO COMMONLY REUSED BY EXTORTERS



4. Lack of Reporting Options and Inaction

Several victims expressed frustration over reporting menus/options that are not specifically related to sextortion and fail to capture the urgency of the matter when users are being aggressively (and actively) targeted on these platforms. Several victims noted that despite reporting offending accounts, the accounts either remained active or the extorter was able to access the victim through separate accounts when the initial account was blocked, deleted, or removed by the platform operators.

[25] O'Flaherty, K. (2019, February 12). 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

This report presented historical trends and keyword analyses of archival forum data and in-depth analyses of victim narratives from one of the largest financial sextortion discussion/support forums on the internet, r/Sextortion. Findings from the in-depth analyses indicated that most victimization was facilitated using a combination of Instagram and then Snapchat, the primary targets of financial sextortion were boys and young men (when gender was known), and that certain design characteristics of social media platforms create favorable conditions for extorters. These findings highlight the need for enhanced safety and privacy features as well as better reporting mechanisms to combat the increase in sexual violence occurring online.

We thank those who publicly shared their personal experiences in the r/Sextortion community. We believe these contributions have and will continue to inform policy, spread awareness, and help those who have been victimized by this crime.

Model in image and intended as illustrative.

APPENDIX: TERMS USED FOR KEYWORD SEARCHES IN REDDIT ARCHIVE POSTS

Keyword searches were performed using Regular Expression (Regex) and case insensitive string matching. Regex is a string of text that lets a user create patterns that help match and locate text using computer programming techniques. Decisions on which platforms and payment processors to include in each search terms list was based on the most commonly encountered technologies listed in the sample of posts that were manually reviewed and general knowledge of online offending patterns.

The following are the Regex strings used for identifying references to platforms in the forum posts:

```
'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':['\bviber\b']}
```

The following are the Regex strings used for identifying references to payment processors in the forum posts:

```
‘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’:[‘\brevolut\b’]}
```

Model in image and intended as illustrative.

CANADIAN CENTRE *for* CHILD PROTECTION®

Helping families. Protecting children.

protectchildren.ca @CdnChildProtect Canadian Centre for Child Protection @cdnchildprotect