REPHRAIN

Protecting citizens online

Online sextortion: Characteristics of offences from a decade of community reporting

Matthew Edwards - University of Bristol

Nick M. Hollely - University of Bristol

November 2023

UK Research and Innovation · University of Bristol · UCL · The University of Edinburgh · King's College London · University of Bath

Journal of Economic Criminology 2 (2023) 100038

Contents lists available at ScienceDirect

Journal of Economic Criminology

journal homepage: www.journals.elsevier.com/journal-of-economic-criminology

Online sextortion: Characteristics of offences from a decade of community reporting

Matthew Edwards*, Nick M. Hollely

Bristol Cyber Security Group, University of Bristol, UK

ARTICLE INFO

Keywords:
Sextortion
Blackmail
Sex crime
Cybercrime
Online dating
Webcam
Fraud

ABSTRACT

Online sextortion is an organised form of blackmail which can have a serious financial and traumatic impact on its victims. Responding to a dearth of evidence about this crime, this study analyses patterns within a large dataset of over 23,000 anonymous victim reports, collected via an online support community. Using common responses within these reports, this study identifies the most typical patterns of offending, including the profile assumed by offenders, the platforms through which the offence is initiated and enabled, payment methods and amounts demanded, and the national origins of most offences. Analysis shows that the mix of social media and dating platforms being used to approach and communicate with victims is changing over time, but the tactics employed by offenders are remarkably standardised. Payment demands involved in the crime were previously centralised in a few key service providers, but are increasingly diversifying. The variety of platforms involved in online sextortion points towards enforcement and safeguarding challenges, motivating an analysis of common risk factors that can inform the design of broadly-applicable countermeasures.

1. Introduction

Sextortion is a form of blackmail in which images of the victim nude or engaged in sexual acts are used as leverage by the offender (Carlton, 2019). Typically, the offender will threaten the victim with public exposure of the images. Some offenders go so far as identifying and naming friends, family and coworkers of the victim as targets to whom they will disclose the images, maximising the potential reputational damage from disclosure. As a form of online image-based sexual abuse (IBSA) (Henry et al., 2021; Eaton and McGlynn, 2020), sextortion is related to but distinct from 'revenge porn', in which such images are released out of spite following an acrimonious break-up. While they can share a common outcome, the blackmail component is not present in revenge porn, and sextortion offenders do not necessarily carry out their threat. Sextortion can have a serious traumatic effect on its victims, with several prominent cases having led to suicides (Nilsson et al., 2019).

While early work on sextortion has primarily focused on sexual gratification and pornographic motivations for the offence (Wittes et al., 2016; Wolak et al., 2018), with several studies specifically targeting the sextortion of minors (Wolak et al., 2018; Patchin and Hinduja, 2020; Kopecky, 2017), more recent work has recognised a range of behaviour to be considered under the definition of sextortion (Carlton, 2019; O'Malley and Holt, 2022). O'Malley and Holt (2022) derive four distinct categories of sextortion offender from a survey of media and court documents related to sextortion cases: those focused on minors, cybercriminals who obtain blackmail material via computer intrusion, offenders who are former or current intimate partners, and transnational criminals who lure victims into sexual encounters online before then blackmailing them. To these categories we may also add a fifth: sextortion spammers, who have no genuine source of blackmail material at all, but make unevidenced threats via bulk email, and collect ransom via cryptocurrency transactions (Paquet-Clouston et al., 2019; Oggier et al., 2020).

This study relates primarily to the fourth of O'Malley and Holt's offender categories: transnational criminals engaged in an organised operation of meeting marks online, luring them into online sexual encounters, and then using recordings of these encounters to extort money from their victims. O'Malley and Holt (2022) noted that, unlike other forms of sextortion, offenders of this kind were not interested in extorting further sexually explicit material, but demanded money. This crime also appears distinct from other sextortion variants in that offenders primarily target males rather than females, and use a number of deceptive techniques, including fake webcam sessions.

This form of deceptive, organised sextortion[1] bears some similarity to the online romance scam, in which criminals approach victims

* Corresponding author.
E-mail address: matthew.john.edwards@bristol.ac.uk (M. Edwards).

[1] Henceforth, for simplicity, 'online sextortion'

https://doi.org/10.1016/j.jeconc.2023.100038
Received 31 July 2023; Received in revised form 29 September 2023; Accepted 1 November 2023

through online social media or dating platforms under a false identity, initiate a relationship, and then use that relationship to defraud victims of large sums of money (Whitty and Buchanan, 2012). Online sextortion mobilises some of the same methods: false relationships, initiating relationships using online communication platforms and making requests for payment using the same money transfer methods. However, online romance scams typically lack the explicit blackmail involved in online sextortion, leverage romance rather than sexual desire, and are known to target both genders at equivalent rates (Suarez-Tangil et al., 2019). Though the schemes can be distinct, cases of online romance scams developing into sextortion cases have been identified by Cross et al. (2022), with sextortion particularly associated with victims being young and male in one sample of reports (Cross et al., 2023).

A form of online fraud more closely aligned to online sextortion is the practice known as 'eWhoring'. As described by Hutchings and Pastrana (2019), eWhoring involves offenders pretending to be young women, and then convincing customers to pay for online sexual encounters, in which they distribute images and videos of those young women engaged in sexually explicit behaviour. These materials are often stolen from social media or pornographic websites, and repackaged into 'Video Cam Whores' – software-controlled video feeds that stitch recorded scenes together to give the illusion of a live-streaming model who can react to conversational prompts from the victim. Such materials are also used in online sextortion (Kopecky, 2016). As with online sextortion, eWhoring targets men, and much of the deceptive work involved in eWhoring would also enable online sextortion. Indeed, Hutchings and Pastrana (2019) identified several eWhoring tutorials which explicitly discussed extending the fraud via blackmail. Searches of underground forums readily retrieve such advice, which tends to centre on how to effectively threaten the victim:

> Find their facebook by finding their email and searching. Send them a link to their facebook to them and say that you'll post the chat logs on their facebook and, if you're whore is U18, report it to the police. Ask them to send you more money. Rinse and repeat.

with some tutorials even including excerpts of chat logs from successful extortion scripts, which weaponise claims of the model being underage:

> [12:30:44 AM] Angel: What would happen if I sent pictures of this chatlog, which includes you soliticing sexual pleasure from an underage 16 year old girl, and a picture of your cock, to your friends and family? Also, an anonymous report to the police department with your details? Don't even bother blocking me because I will go through with this if you do.

While eWhoring, romance scamming and revenge porn are each conceptually linked to online sextortion, they have distinctive characteristics. eWhoring and romance scamming involve similar deceptive approaches and financial motives, but offenders in the majority of cases extract money through fraud rather than extortion. Revenge porn involves the distribution of nude or sexually explicit images of a victim, but does not contain the *threat* of such distribution (Carlton, 2019). Online sextortion should be considered a distinctive and serious organised cyber-sex crime (O'Malley and Holt, 2022). Sextortion as a research area lacks maturity (Nilsson et al., 2019; Wittes et al., 2016) and O'Malley and Holt (2022) have recently identified online sextortion in particular as both rapidly growing, and posing significant investigative hurdles. This has led to online sextortion rising on policy-making agendas in regions where there are high concentrations of victims. As such, evidence about online sextortion is urgently required in order to support regulatory and technical responses to offending.

This study responds to this need by analysing existing, public, but previously untapped data on cyber enabled sextortion, sourced from a NGO that offers web-based support for victims of online fraud. The NGO, Scam Survivors, has been receiving and publishing victim reports on cases of online sextortion since 2013. Using this data, this paper contributes to the IBSA literature by studying the dynamics of sextortion offences, how offenders can be characterised, and the major communication and payment platforms that enable online sextortion offending. The aim of this analysis is to detail how online sextortion has typically presented over the past decade in terms of the interactions between offender and victim online, the offenders' typical methods of operation, and the online platforms and geographic locations connected to sextortion offending. This overall view of the topic is then to be contrasted with a selection of more recent reports, to identify how online sextortion has changed in more recent years, and better inform attempts at combatting online sextortion offending.

2. Data and methods

Scam Survivors[2] is an online community reporting and support forum for victims of various forms of online fraud and malicious behaviour. Operating since 2012, one of its functions is to collect reports about scams and the offenders involved in perpetrating them. The forum contains boards for the reporting of romance scammers, advance-fee fraud emails, and phishing sites, as well as providing guidance and emotional support for victims. Since early 2013, Scam Survivors have also been collecting reports of online sextortion, also referred to on-site as 'webcam blackmail'. These reports are anonymous, follow a common structure, and, as they are released to the public, avoid capturing information directly pertaining to the victims themselves. Due to this, the geographic locations of the victims are not known, but people reporting to Scam Survivors are not confined to any particular jurisdiction. Reporting of online sextortion has grown rapidly, and it now forms one of the largest categories of report within the forum, second only to the reporting of advance-fee fraud emails.

After obtaining express permission from the forum's administrator, over 41,000 posts were downloaded from the public face of the forum for analysis, capturing all currently-available posts within the online sextortion subforum as of mid-July 2023. A Python toolchain was then developed against this corpus with the aim of extracting the semi-structured questionnaire data for analysis purposes. All data transformations were performed in a stand-off manner, avoiding any manual alteration of the data, and full raw and processed versions of the dataset are made available for other researchers.[3]

The posts were filtered to exclude unstructured commentary, retaining only posts which could be automatically determined to contain the structured questionnaire responses. A total of 23,705 responses were found, capturing answers to 19 common questions,[4] which are detailed in Table 1. Response rates varied for questions, from just 394 responses for Question 17 to 22,652 responses for Question 1. Questions 1 & 2 are currently required responses for form submission.

As almost all questions were implemented as free-text responses, significant effort was required to standardise responses for further analysis. Questions were judged not to have a response if the question did not appear in the post, if the answer was one of a number of common non-responses (e.g., "no","N/A","none","didn't get that far"), or contained patterns indicative of non-response to the current question. Answers were standardised to account for case, spelling errors and variant phrasings through an iterative process of parsing and tabulation, with all text responses that appeared more than once being considered for inclusion under a standardised code or exclusion as a non-response.

A number of additional values can be inferred from these responses, as detailed in the results below. Alongside the questions, the timestamp of the report's posting was also extracted, to enable temporal analyses.

[2] https://www.scamsurvivors.com/

[3] DOI: 10.17632/xp8n69sdtp.1

[4] Some evidence was found for other questions answered rarely in early versions of the questionnaire, but these were judged to have too few responses for a detailed analysis.

Table 1
Questions contained within the reports, and the number of valid responses found for each question. Question numberings and subheadings are not drawn from the data.

	Question	Responses
Offender presentation		
1	What name did the scammer use?	22,652
2	How old did the scammer say they were?	21,220
3	Please upload a photo of the scammer if they sent you one?	1971
Offence location/dynamics		
4	What site/app did you first meet the scammer on?	21,100
5	If they asked you to leave the site/app and go elsewhere, where did they take you?	17,833
6	If they showed you your video on a website, can you post the site and account they posted it with?	4210
7	Who made the first contact?[a]	4427
Payment demand		
8	Name you were told to send the money to?	13,860
9	How much money did they demand?	19,464
10	How were you to send the money?	15,271
11	What country/city were you told to send the money to?	13,275
Offender identifiers		
12	If they gave you a phone number, please add it here.	3452
13	Scammer's email address if you have it?	4946
14	Address of the scammer's Facebook, Google+ or other social media site page?	9781
15	Scammer's Skype name?	10,112
16	Scammer's Skype username?[b]	—
17	Scammer's Skype location?	394
Victim comment		
18	What steps, if any, have you already taken to block the scammer?	17,255
19	Are there any other details you wish to share?	6273
	Total	23,705

Question wordings given here reflect the most common of several variant phrasings. [a]This question only available since late 2018. [b]This question was a source of considerable confusion for respondents, with question variants showing multiple attempts to clarify the distinction between a display name and user id; correcting responses was not a priority for this study.

It is at this point worth noting a detail of the response submission and post release process: respondents first fill in an online form addressing the above questions as well as some private details that are not shared publicly, this is submitted and goes into a moderation queue. A forum administrator reviews the submission and then posts the resulting report to the public forum. This introduces the possibility of an unknown reporting delay. However, reports since June 2017 have included a 'Date Received' annotation. Analysis of the time differences between receipt and posting in this subset of 9,918 reports shows that the average delay is thirteen hours, 90.5% of reports are posted within 24 hours of receipt, and 98.2% of reports are posted publicly within 72 hours of receipt, suggesting little to no impact on aggregate monthly reporting.

The framing placed around reporting is also worth noting. Firstly, Scam Survivors exists primarily as an anti-fraud community, and so, while reports of other forms of sextortion are encouraged, reporting of sextortion can be expected to be biased towards financially-motivated online sextortion rather than other forms, such as intimate partner sextortion. Observation of the data confirms this, with just 25 reports of sexual exploitation motives for offences, to contrast with over 19,000 reports of financial motives. Secondly, Scam Survivors warns potential respondents that they will not provide assistance to respondents who knowingly engaged in sexual talk with a minor, defined as someone under the age of 18. This can be expected to bias responses about offender ages, and may also discourage reporting from victims under the age of 18.

3. Results

3.1. Offender presentation

Victims reported the presented age of offenders, either elicited by them from the offender during their conversation, or inferred from the physical appearance they were shown. Of the 21,220 valid responses, some 742 gave age ranges, explicitly indicated that the age given was an estimate, or gave imprecise non-numeric responses (e.g., "legal adult" (N = 18)). As shown in Fig. 1, of the remaining 20,478 reports, the average offender age is 23%, and 88% of offenders gave the impression of being in their 20s, with much of this mass lying in the early twenties (the interquartile range was 21–25). Very few (N = 26) reports mentioned encountering offenders who presented themselves as under 18, as might be expected given the warnings issued by the forum. However, a small number of reports indicated here that offenders had

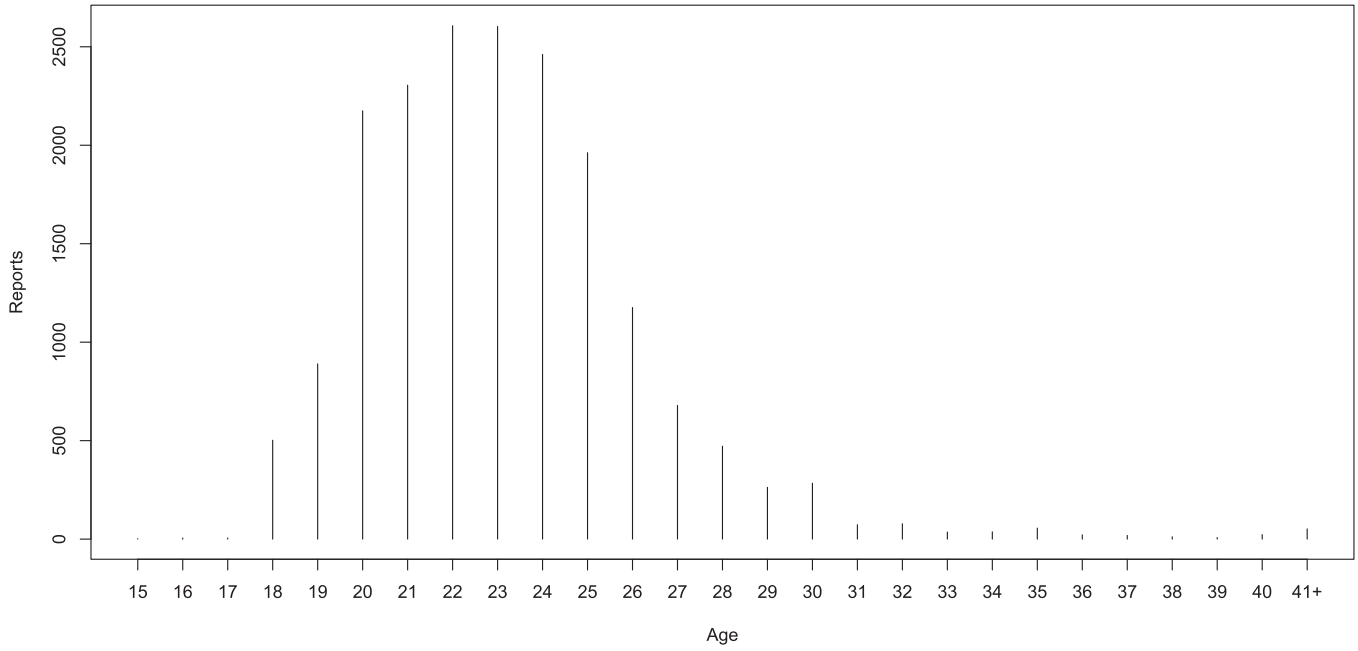

Fig. 1. Apparent offender ages as reported by victims (N = 18, 826).

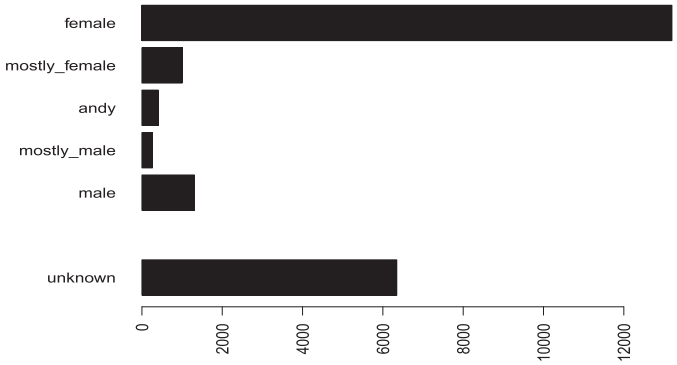

Fig. 2. Inferred presented genders of offenders, based on reported first name ($N = 22,652$).

first pretended to be over 18 while entrapping their victim, before then claiming to actually be younger as part of the sextortion script launched after the victim has sent sexually graphic content to the offender. This highlights a bait-and-switch tactic which makes cynical use of the stigma associated with sexual encounters with under-18s.

Offender gender was not explicitly recorded in reports. However, gender can commonly be inferred from names. The Python package `gender-guesser` was used to infer the gender for each name given in response to Question 1, using a large database of name-gender associations. No nationality was specified as a parameter. As shown in Fig. 2, results indicated an overwhelming preference for using female identities, at approximately 10× the rate for male identities. In total, 88% of reports where a gender could be inferred indicated a female or mostly female name used by the offender. These results combined indicate that offenders for the most part present themselves as young females, findings which are consistent with earlier reports of online sextortion mostly targeting males (O'Malley and Holt, 2022).

3.2. Offence locations & dynamics

The questionnaire asked victims about three different online locations involved in the offence: the meeting-place where they first met the offender, the secondary location the conversation was moved to (if any), and the site used to host the video of the victim in order to make a credible threat.

Of the 21,100 responses regarding the initial meeting-place, the largest origin (37%) was Facebook, followed by video-chat site ChatRoulette (11%), dating site OkCupid (6%) and social/dating app Skout (5%). The remainder of common origins were dominated by an assortment of random-meeting chat and hookup applications, mixed in with dating sites and a few general-purpose messaging and social networking sites. One noteworthy case is that of Ashley Madison ($N = 331$), and a small number of other sites aimed at enabling flings and secret encounters, which might naturally lend themselves to a blackmail script. Of the 4,427 responses to the 2018-onward question asking victims which party initiated online contact, 3,588 (81%) indicated that the offender initiated contact.

Within the 17,833 responses reporting a secondary location for conversation, a significant majority (63%) indicated that the offenders invited them to talk on Skype. The next largest platforms were Facebook (9%), Google Hangouts (8%), WhatsApp (3%), phone conversations (2%) and chat apps like Kik (2%), WeChat (2%) IMO (1%) and Line (1%), with some representation of other social networks such as Instagram (1%). Approximately 1% of users indicated the second contact mechanism was via email. Some of the most common transitions between meeting-place and conversation platform are presented in Table 2. Facebook, the most common meeting place, also had the greatest diversity of secondary locations. Skype was the dominant historic aggregator for conversations initiated on other platforms, with notable transitions including 81% of all interactions that started on ChatRoulette being moved to Skype.

Table 2
Most commonly reported meeting-place to conversation location transitions, including the proportion this represents of all interactions from the initial meeting-place.

	transitions	proportion
Facebook → Skype	3197	41%
ChatRoulette → Skype	1843	81%
OkCupid → Skype	798	56%
Skout → Skype	643	64%
Facebook → Facebook	569	7%
Facebook → Google Hangouts	494	6%
Facebook → WeChat	273	3%
OkCupid → Google Hangouts	258	18%
Badoo → Skype	248	65%
Omegle → Skype	242	45%
MeetMe → Skype	233	62%

A comparatively smaller number of reports (4,210) answered the question about the site hosting the threat video, possibly reflecting a large number of cases where the sextortion attempt reported was identified before an online sexual encounter took place. Of the parseable responses amongst these, over half (57%) indicated that the threat video was hosted on YouTube, with the next-largest host being Facebook (12.2%). A large number of respondents (at least 17.6%) indicated that their blackmailer sent the video to them directly, either via the chat channel they were communicating over (e.g., Skype), or via other direct methods such as email. Other common video hosts were SendVid (2%), Vimeo (2%) and DailyMotion (1%). 58 responses indicated videos were hosted on porn websites. Six responses indicated that videos were uploaded to apparent anti-child-abuse vigilante websites. Several responses misinterpreted the question as being about where the video was threatened to be sent for disclosure, leading to some strange results, e.g., five responses mentioned the Ellen Degeneres show.

3.3. Payment demands

Of the 19,464 responses regarding the money demanded in sextortion, 18,771 responses reported identifiable currency amounts. Of the excluded 693, the majority were parsing failures on unusual formatting or respondent explanations, but 25 appeared to report the offender demanding further sexual material or actions rather than money. Some 99 reported that the offender demanded a non-specific money transfer (e.g., "Whatever you can afford."). A further 61 indicated that the offender demanded their card details, and 129 reported that they were instructed to sign up to an adult cam-site – both strategies seeming to indicate an effort at extorting ongoing rather than one-off payments.

A described in Fig. 3, while the majority (81%) of the 18,771 responses reported demands in USD, a variety of other currencies were also used, with the most common being EUR (8%), GBP (5%) and MYR (the Malaysian ringgit; 2%). Where no currency was specified, the bare figure was interpreted as referring to USD; this occurred in 32% of reports. Amounts in other currencies were converted to USD for analysis purposes, using recorded currency conversion rates for the date the report was published. Conversion rates for the New Taiwan dollar (NTD; $N = 104$) and the Emirati dirham (AED; $N = 103$) were not available, and these figures were thus excluded from the analysis below.

Of the 18,563 demand amounts successfully converted, 32 were identified as aberrant values greater than 500,000 USD, and excluded. Six amounts reported a demand of 0 USD and were also excluded, for a total of 18,525 payment demands. The average payment demand was 2,218 USD, but this figure is skewed by a few large demands (14 demands > 100,000 USD). The median demand was 700 USD, with an

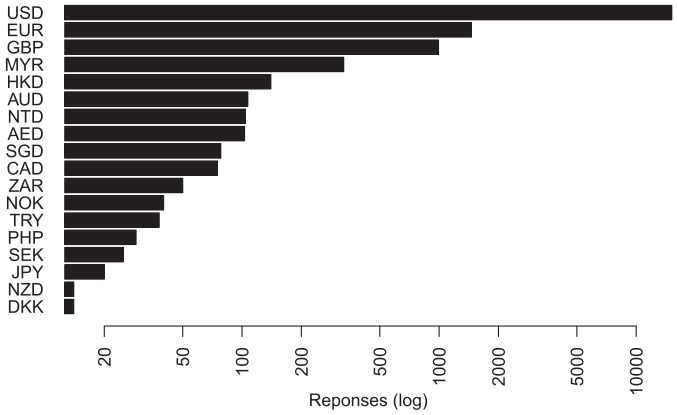

Fig. 3. Currencies of reported payment demands (log scale).

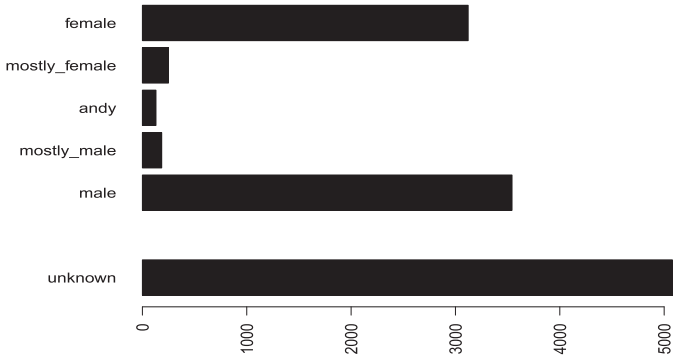

Fig. 5. Genders of payees, inferred from first name on payment delivery instruction (N = 12, 308).

interquartile range of 400–2000 USD. As shown in Fig. 4, this figure has been rising over time, from 500 USD in 2013 to 1000 USD in 2020, with some deflation back to 700 USD as of 2023.

A total of 15,271 respondents reported how money was to be sent to the offender. In the majority of cases (74%), payment was to be delivered through Western Union, with the second most popular method being MoneyGram (12%). A variety of payment methods including Paypal (3%), direct-payment apps, bank transfers, gift cards and cryptocurrencies constituted the remainder of responses.

The dominant use of addressed payments through Western Union and MoneyGram enables some indirect insight into the origins of offending, by revealing a payee name and location (Questions 8 & 11). Fig. 5 presents the inferred gender of payees, following the same methodology as previously applied to the responses to Question 1. Contrasting Fig. 5 with Fig. 2, two key observations can be made. Firstly, payee names included many more names unknown to the name-gender association database, suggesting poor coverage of some populations. Secondly, the gender balance in payee names differs significantly from that in presented names, with more male or mostly male names (42%) than female or mostly female names (38%). While payee names may yet be handlers or intermediaries for payment, this evidence is suggestive of a large number of male offenders presenting themselves as female in order to extort funds from victims.

A total of 13,275 responses were available regarding the location to which money should be addressed, of which 326 were excluded as unidentifiable. Responses were standardised and collected at the national level, with some exceptions. Fig. 6 presents the 20 most frequent national destinations reported. A notable limitation was that some reports were highly underspecific, with e.g., 1.5% referring only to 'Africa'. The Philippines was the largest single destination by some distance, accounting for 48% of all reported locations. A number of northern and western African nations (Ivory Coast, Morocco, Mali, Burkina Faso, Ghana, Cameroon) in combination comprise a similar proportion of reported locations, with other notable payment destinations including the United States (3%) and France (1%).

This offender location information is partially corroborated by geocoding of the phone numbers provided in the smaller selection of 3452 reports where victims obtained offender phone numbers. Of the 2818 cases where a national dialling code was included, 52% contained a Philippines country code, with other common locations being the USA (26%), Ivory Coast (4%) and France (2%). As the victims have all reported anonymously, there is no data on whether some of these cases are conducted with both offender and victim in the same legal jurisdiction.

3.4. Time sensitivity

As shown in Fig. 7, online sextortion reporting showed a consistent increase between 2013 and 2016, rising to over 400 reports each month. Between 2018 and 2023, reporting to Scam Survivors fell significantly, and for the recorded 6 months of 2023 a volume of approximately 20 reports per month can be observed. This effect may be attributable to the increased availability of alternative reporting locations since 2016, rather than an actual decrease in the rate of online sextortion offending.

Online platforms are involved in constant cycles of popularity; since at least 2020, there has been a significant global shift in the use of

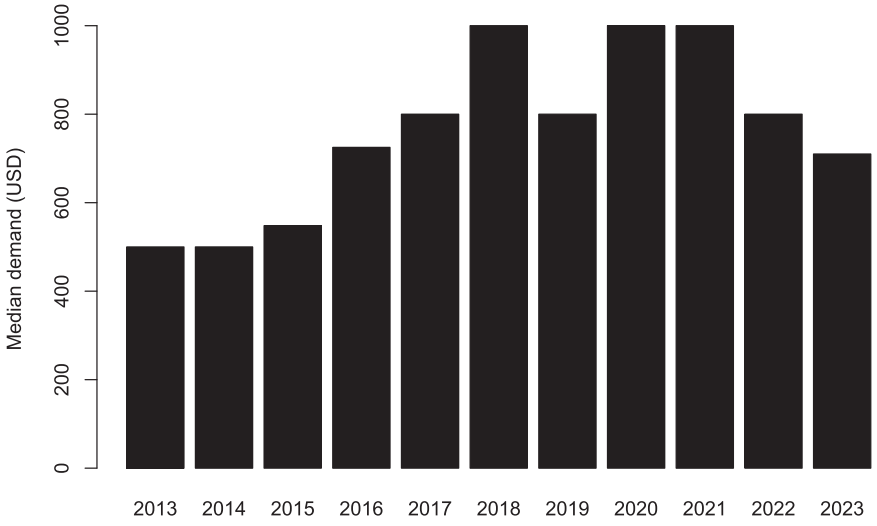

Fig. 4. Median value of demanded payments per year, 2013–2023.

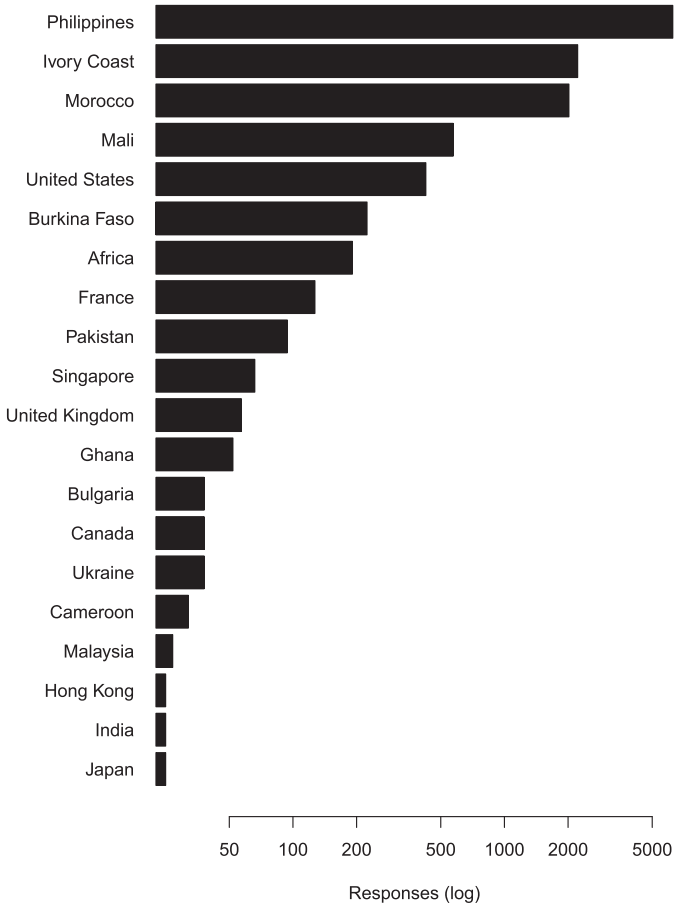

Fig. 6. Most commonly-reported locations to which extorted payment was to be addressed (log scale).

technologies for online communication, the effects of which may be obscured in a sample composed heavily of pre-2018 reports. As such, the data was re-examined to study the past 1.5 years specifically, to identify any differences in modern patterns of offending and newly implicated platforms for offences reported since the start of 2022. A total of 517 reports fall within this period.

3.4.1. Offender presentation

Offender presentation within the recent reports subset remains consistent with the offender presentation in the wider dataset. A total of 39 reports gave inexact age estimates, with the other reports yielding a mean age of 24 (median 23) and only 1 report of an offender presenting as under 18, with the victim's additional comment clarifying that this age (15) was reported only after blackmail material was obtained. Where a gender could be inferred from the name given by the scammer, in 77% of cases it was a female or mostly female name.

3.4.2. Offence locations and dynamics

Offence locations show some substantial shifts in the recent reports relative to the overall dataset. Most notably, the most common initial meeting place in the past 1.5 years was Instagram (23%), beating out Facebook (11%) and followed by Omegle (10%), Tinder (5%) and OkCupid (4%). Instagram was also the most common secondary location for conversation, at 19% of recent reports, edging out Skype (16%) and followed by Google Hangouts (13%), WhatsApp (13%), SnapChat (10%), Facebook (7%) and Telegram (5%). The location of Instagram as a newly emerging key location for sextortion offending makes it central to the most significant platform transitions reported, both as a conversation platform for interactions started elsewhere (most commonly Omegle, the primary meeting place for 24% of incidents with Instagram as the secondary location) and as a launching-point for conversations on a variety of other platforms (most notably SnapChat and WhatsApp). As within the overall data, in the majority of cases (76%) the offender contacted the victim first. Only two recent reports mentioned a specific hosting location for blackmail videos, which may be due to increased support for video content within other conversation platforms.

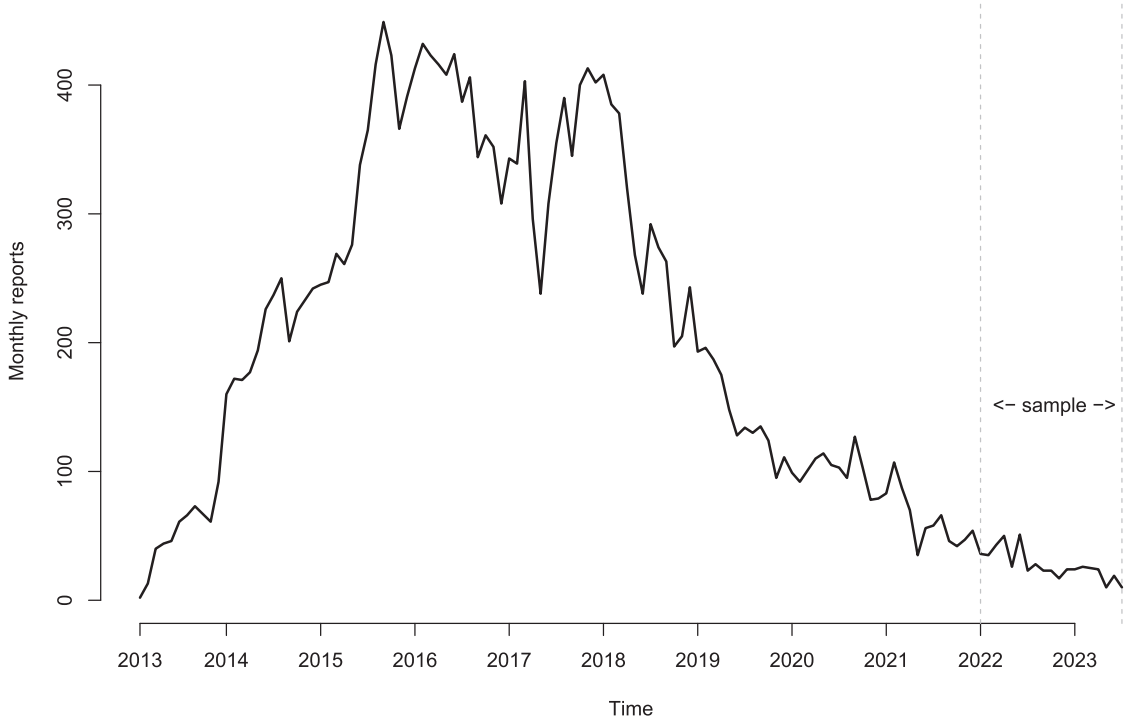

Fig. 7. Total monthly reports over time, with recent subset period marked.

3.4.3. Payment demands

Of the 517 recent reports, 412 reported identifiable currency amounts, of which 1 value was 0 and 2 were aberrent values over 500,000 USD. The average demand over this period was 3,274 USD, but this is highly skewed by one large demand, with a median demand of 800 USD. The majority of demands (74%) were in USD, followed by EUR (13%) and GBP (9%), with MYR demanded in 1% of cases.

Western Union remains the most preferred payment method for offenders, but its share of payments is drastically reduced in recent reports (26%, compared to 74% overall), and is nearly coeval with Paypal, the use of which is rising (also 26%, compared to 3% overall). Moneygram is mentioned in 8% of recent reports, while the combination of a variety of different gift card schemes and direct-payment apps makes up the bulk of reported methods, with the most common being Remitly (4%), CashApp (4%) and Wise (3%). The increased diversity of payment methods in recent offending poses potential enforcement challenges.

The locations of offenders discernable from recent money demands (240 reports) show commonalities with the overall sample, with 63% drawn from the Philippines, 15% from the Ivory Coast and smaller numbers reported from the United States (8%) and Morocco (5%). The dominance of the Philippines is more pronounced in recent reports, with fewer reports of West African origins, and proportionately more incidents involving the US, Pakistan, Burkina Faso, India and France (each 2%). The names associated with payment demands continue to show a more equal split of genders, slightly biased towards males (52%) rather than females (46%).

4. Discussion

The resource analysed in this study does suffer from several important limitations. Firstly, the reporting does not explicitly capture the degree of exposure a victim had to an offender, or the success of the crime: while victims can indicate how much money was demanded by an offender, no question asks if they have paid this amount. Therefore, future analyses seeking to differentiate offender tactics by their effectiveness would need to attempt to identify cases where victims have or have not paid the offender based upon interpretation of additional comments from the victim. Second, no information about the victims themselves is made available. This is a privacy-preserving measure on the part of the report publishers, protecting victims of a crime type which heavily leverages shame, but it does mean that a direct understanding of victim demographics and risk factors cannot be obtained from this data. Third, the information about offences is provided as reported by victims, rather than established through other means, and so victims' own interpretation or partial recollection of events could be expected to colour reporting. Victims also do not always have a full understanding of the crime event to which they were a participant, and may not understand the degree to which they were targeted by a criminal, or which aspects of an offender's conversation with them were truthful. Victims have information about how an offender presented themselves in conversation (Questions 1–3), but these presentations are unlikely to be truthful, and even information revealed in later stages of the crime, such as the name on a payment demand, may only be a secondary false persona. As such, while trends within such a large body of reports can be useful in characterising offending, any specific report should be treated with caution.

Much of the previous literature on sextortion has focused on offences motivated by sexual gratification that are directed primarily at women. For example, the telephone survey of Walsh and Tener (2022) covered mostly female victims, nearly half of whom were minors at the time of offending, and Dolev-Cohen et al. (2022) focused specifically on the experiences of female minors. However, as outlined from analysis of news reports by O'Malley and Holt (2022), sextortion offending comes in a number of different varieties, and some forms of sextortion are more commonly targeted at males. Cross et al. (2023) found that sextortion victimisation within online dating fraud was associated with being young and male, and with contact made via social media, a result that concurs with the dominant offender tactic in this study's data, in which offenders mostly present themselves as a female between the ages of 21 and 25. The volume of reporting in the Scam Survivors dataset suggests that this form of financially-motivated online sextortion may be being overlooked, and a heavily-targeted demographic may be underserved by both past research on this topic and victim support agencies.

Our main predecessors in identifying this demographic, Cross et al. (2023), studied online sextortion only within the context of online dating fraud, whereas our analysis includes interactions with victims or near-victims that did not view the online interaction as part of an extended romantic relationship. Viewing sextortion as a distinct crime type may be important for recognising its full impact, as aspects of the crime could be viewed variously as fraud, blackmail or online harrassment. Offender locations also appear to differ between online sextortion and romance fraud offences; Edwards et al. (2018) present a prominently West African origin for online dating fraud, differing from the dominantly Filipino origin appearing in this study's data. Differentially mapping the occurrence of online crimes has been identified as a major challenge (Lusthaus et al., 2020) and online sextortion may prove an important additional dimension to this problem.

This study's results enable typification of offences both historically over the past decade and in more recent data. Historically speaking, the most common case would involve an offender that approaches a victim on Facebook, transitions a conversation to Skype, records blackmail material from a webcam session on that platform, and then makes a demand, perhaps uploading a video to YouTube as part of making the threat. The offender would then demand that payments be made via Western Union to an address in the Philippines. The approach via Facebook often simplifies the blackmail process for the offender – a Facebook connection provides access to the victim's intimate circle, including the friends and family members which it would be maximally damaging for an offender to contact with an explicit video of the victim. Meanwhile, Skype's prominence as a location for offending is explained by the platform's historic dominance in the online video call market. Skype was so common as a medium for offending that questions specific to Skype (Questions 15, 16 & 17) were integrated into the Scam Survivors form for online sextortion reports. However, this position appears to have been contingent upon there being few popular competitors for video calls or similar chat applications that facilitate the extraction of blackmail material.

In general, the differences in dynamics between historic reports and reports in the past 1.5 years seem to point to an increasing diversity of platforms used for offending. A wide variety of dating sites, hookup apps, chat systems and social media platforms are represented within reporting, both as initial meeting places and secondary locations for sextortion conversations. This poses enforcement hurdles: it is no longer the case that technical or other countermeasures implemented on one social platform would have an impact on the majority of online sextortion. The approach taken in situational crime prevention (Clarke, 1995) is to decrease the attractiveness of a crime within a situation where it is commonly occurring, by reducing opportunities for the crime to take place. At least as construed narrowly, this approach will struggle to be effective when the opportunities are widespread across many online platforms, and affordances within those platforms are generally conducive to the crime. For example, decreased reporting of video hosting sites suggests that where blackmail material is being extracted, this may now be demonstrated to the victim directly on the conversation platform, negating the possibility of countering most offending at the video delivery stage through collaboration with major video hosts. Within payment platforms, too, offending diversity creates limitations for analyses: our data shows that methods for tracing cryptocurrency payments from sextortion, such as those of Oggier et al. (2020), will apply to only a thin slice of online sextortion offending.

Future countermeasures to online sextortion will need to be adaptive to this diverse range of enabling platforms.

One platform does appear to be growing in significance for online sextortion: Instagram. While it does not dominate recent reporting to the same extent that Facebook and Skype did previously, Instagram's appearance as a leading meeting-place and conversation platform for online sextortion may make it suitable location for future studies and for effective deployment of awareness or prevention campaigns in the short term. However, this is also likely to change in the longer term, and research should focus on the common features of platforms that are useful to online sextortion offenders, in order to predict which platforms are likely to attract offending. The notion of 'risky places' for crime, and of identifying the factors that contribute to risk, is often studied in offline contexts (Kennedy and Caplan, 2012; Irvin-Erickson, 2014; Lersch, 2017; Kennedy et al., 2018), and can also be studied in the context of certain online dangers that are tied to online platforms or types of platform (Ybarra and Mitchell, 2008).

The meeting-places for online sextortion are generally social platforms designed for facilitating meeting new people, and especially when the online context is one related to dating or sexual encounters, or the target demographic includes the young males that would appear to be the main targets of this form of financially-motivated online sextortion. As offenders typically approach the victim, any platform that supports initiating such unmediated connections with strangers is potentially a platform for online sextortion. A risk terrain modelling approach would usually suggest altering the environment to interrupt such risky interactions (Kennedy et al., 2018, p. 30). However, rejecting such behaviour entirely cannot be recommended in earnest: in many cases, including when using dating sites and hookup apps, this form of interaction is precisely what users want to achieve, and the basis of many platforms' business models. Effective management of risky behaviour may be a more realistic goal. As mentioned above, a hurdle for offenders is gaining access to a victim's circle of friends and family, in order to most effectively threaten the release of explicit materials. Platforms could help prevent the collection of such information with better privacy controls, and behavioural interventions could focus on helping users keep various online identities separate, so that an identity used on a hookup site is difficult to link to a user's more general social media identity. This would allow for interactions to continue to take place in these online environments in the manner users intend, while reducing offenders' ability to make credible threats of reputational damage.

The secondary locations for offending are for the most part conversation platforms, with video chat features being common components but not entirely essential to offending. Data on such platforms is intentionally non-public and increasingly end-to-end encrypted, suggesting that any interventions would need to be located primarily at the network end-points. A routine activities theory approach would suggest that the absence of a capable guardian in these interactions may be productive of crime (Cohen and Felson, 1979). Yet interventions that involve the introduction of guardians into such point-to-point communication systems could be unwelcome if they are seen to impact the privacy of such communications. Platforms could however address the suitability of their users as targets, by implementing controls to facilitate blocking users and reporting of offender behaviour, and offering resources that support victims in protecting themselves online. Resources explaining online sextortion specifically could be placed alongside more general guidance on safe online behaviour, helping to raise awareness and reduce victims' sense of isolation. To avoid duplication of effort, these resources should be developed by independent online safety organisations, to which social media sites can become affiliates in order to co-design best practices and support systems.

Online locations are not the only locations of interest when considering environmental factors promoting online sextortion. Approximately half of all payment demands in the dataset were to be sent to an address in the Philippines, with this proportion increasing to close to two thirds of more recent reports. The Philippines thus plays a major role in online sextortion offending for victims who have reported to Scam Survivors, and international law enforcement operations focused on this crime would benefit from collaboration with local authorities, both in prosecuting and in preventing the crime. Other major locations where targeted campaigns could be most beneficial would include the Ivory Coast, the United States, and Morocco. In many cases, including the Philippines, countries connected to online sextortion offending score poorly on indices of corruption (Transparency Internationa, 2022). Public corruption has been linked directly to the commission of online fraud in previous work (Tade and Aliyu, 2011) and our data is suggestive that a similar connection may be found for online sextortion. Addressing crimogenic factors such as corruption in countries that are originating transnational offending could be considered a major target for long-term responses to online sextortion.

While in some cases very large sums of money are extracted, including cases where recurring payments were demanded, the median payment demand was for 700 USD, a relatively small figure that highlights the mass-market nature of this crime type. While many reports in the data were from victims who did not pay the offender, the total amount demanded by offenders within this community reporting reaches 41 million USD. Online sextortion is a crime which by its nature exploits the shame of victims, suggesting a large under-reporting bias, and so the magnitude of damages from this crime are likely substantially under-estimated. A key danger here is that the comparatively low value of individual losses could lead to online sextortion being deprioritised by policymakers, which would have knock-on effects for law enforcement. Officers assigned to online sextortion cases may struggle to justify allocation of resources to expensive transnational investigations, which could explain the extremely low rates of prosecution for financially-motivated online sextortion. This is differentiated from other forms of sextortion that are primarily motivated by sexual gratification, where victims and extortioners are more often in the same jurisdiction and the demands are often for further content or other actions rather than money. While in many cases now carried out online, such sextortion is more closely linked to sexual harrassment and the abuse of power to extract sexual favours (Mumporeze et al., 2021), and presents a different victim demographic.

5. Conclusion

This study has reviewed the dynamics of online sextortion offending as detailed in the largest collection of victim reports studied to date. In evidence spanning a decade of reports, offences have been characterised in terms of the common presentation of offenders, the platforms used to initiate and carry out sextortion, and the probable national origins of offending. Whilst online sextortion has historically been linked to particular platforms (e.g., Skype and Facebook), offenders are now diversifying in response to the changing technological landscape, posing increased difficulties for law enforcement and other bodies attempting to combat this crime in the future.

Financially-motivated online sextortion is being addressed by multiple institutions in different countries, including educational establishments who are responsible for the empowerment of potential victims. Educators can help people to proactively identify the variety of ever-changing online threats and also inform media awareness campaigns. The technology industry that enables transnational communications and provides platforms used by sextortion offenders is populated by many different organisations, many of whom are in competition with one another. Attempting to develop collaborations amongst the whole array of different institutions around the world that are currently operating as a loosely coupled network to disrupt sextortion remains an ongoing challenge. Further research should focus on how the full suite of institutions with an interest in disrupting sextortion can make more efficient use of the scarce resources being mobilised to aid victims and potential victims.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This research would not have been possible without the work of the Scam Survivors forum and the associated community.

This research is part of the Sextortion Offending: Locations & Dynamics (SOLD) project, supported by REPHRAIN: The UK National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online, under UKRI grant EP/V011189/1.

References

Carlton, A., 2019. Sextortion: the hybrid cyber-sex crime. North Carol. J. Law Technol. 21, 177–215.
Clarke, R.V., 1995. Situational crime prevention. Crime. Justice 19, 91–150.
Cohen, L.E., Felson, M., 1979. Social change and crime rate trends: a routine activity approach. Am. Sociol. Rev. 44, 588–608.
Cross, C., Holt, K., O'Malley, R.L., 2022. "If U Don't Pay they will Share the Pics": exploring sextortion in the context of romance fraud. Vict. Offenders 1–22.
Cross, C., Holt, K., Holt, T.J., 2023. To pay or not to pay: an exploratory analysis of sextortion in the context of romance fraud. Criminol. Crim. Justice 1–16.
Dolev-Cohen, M., Nezer, I., Zumt, A.A., 2022. A qualitative examination of school counselors' experiences of sextortion cases of female students in Israel. Sex. Abus. 1–24.
Eaton, A.A., McGlynn, C., 2020. The psychology of nonconsensual porn: Understanding and addressing a growing form of sexual violence. Policy Insights Behav. Brain Sci. 7 (2), 190–197.
Edwards, M., Suarez-Tangil, G., Peersman, C., Stringhini, G., Rashid, A., Whitty, M. 2018. The geography of online dating fraud. In: Workshop on Technology and Consumer Protection.
Henry, N., McGlynn, C., Flynn, A., Johnson, K., Powell, A., Scott, A.J., 2021. Image-based sexual abuse: a study on the causes and consequences of non-consensual nude or sexual imagery. Routledge, Abingdon, UK.
Hutchings, A., Pastrana, S. 2019.Understanding eWhoring. In: Proceedings of the 2019 IEEE European Symposium on Security and Privacy (EuroS&P), 201–214.
Irvin-Erickson, Y. 2014.Identifying risky places for crime: An analysis of the criminogenic spatiotemporal influences of landscape features on street robberies (Unpublished doctoral dissertation). Rutgers University Graduate School.
Kennedy, L.W., Caplan, J.M., 2012. A theory of risky places. Research brief. Rutgers Center on Public Security.
Kennedy, L.W., Caplan, J.M., Piza, E.L., 2018. Risk-based policing: evidence-based crime prevention with big data and spatial analytics. University of California Press.
Kopecky`, K., 2016. Misuse of web cameras to manipulate children within the so-called webcam trolling. Telemat. Inform. 33 (1), 1–7.
Kopecky`, K., 2017. Online blackmail of Czech children focused on so-called` "sextortion" (analysis of culprit and victim behaviors). Telemat. Inform. 34 (1), 11–19.
Lersch, K.M., 2017. Risky places: an analysis of carjackings in Detroit. J. Crim. Justice 52, 34–40.
Lusthaus, J., Bruce, M., Phair, N. 2020.Mapping the geography of cybercrime: A review of indices of digital offending by country. In: 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 448–453.
Mumporeze, N., Han-Jin, E., Nduhura, D., 2021. Let's spend a night together; i will increase your salary: an analysis of sextortion phenomenon in Rwandan society. J. Sex. Aggress. 27 (1), 120–137.
Nilsson, M.G., Pepelasi, K.T., Ioannou, M., Lester, D., 2019. Understanding the link between sextortion and suicide. Int. J. Cyber Criminol. 13 (1), 55–69.
O'Malley, R.L., Holt, K.M., 2022. Cyber sextortion: an exploratory analysis of different perpetrators engaging in a similar crime. J. Interpers. Violence 37, 258–283.
Oggier, F., Datta, A., Phetsouvanh, S., 2020. An ego network analysis of sextortionists. Soc. Netw. Anal. Min. 10 (44), 1–14.
Paquet-Clouston, M., Romiti, M., Haslhofer, B., Charvat, T. 2019.Spams meet cryptocurrencies: Sextortion in the Bitcoin ecosystem. In: Proceedings of the 1st ACM Conference on Advances in Financial Technologies, 76–88.
Patchin, J.W., Hinduja, S., 2020. Sextortion among adolescents: Results from a national survey of US youth. Sex. Abus. 32 (1), 30–54.
Suarez-Tangil, G., Edwards, M., Peersman, C., Stringhini, G., Rashid, A., Whitty, M., 2019. Automatically dismantling online dating fraud. IEEE Trans. Inf. Forensics Secur. 15, 1128–1137.
Tade, O., Aliyu, I., 2011. Social organization of Internet fraud among university undergraduates in Nigeria. Int. J. Cyber Criminol. 5, 2.
Transparency International. 2022. Corruption Perceptions Index 2022.〈https://www.transparency.org/en/cpi/2022〉.
Walsh, W.A., Tener, D., 2022. "If you don't send me five other pictures i am going to post the photo online": a qualitative analysis of experiences of survivors of sextortion. J. Child Sex. Abus. 31 (4), 447–465.
Whitty, M.T., Buchanan, T., 2012. The online romance scam: a serious cybercrime. Cyber, Behav., Soc. Netw. 15 (3), 181–188.
Wittes, B., Poplin, C., Jurecic, Q., Spera, C. 2016. Sextortion: Cybersecurity, teenagers, and remote sexual assault (Tech. Rep.).
Wolak, J., Finkelhor, D., Walsh, W., Treitman, L., 2018. Sextortion of minors: characteristics and dynamics. J. Adolesc. Health 62 (1), 72–79.
Ybarra, M.L., Mitchell, K.J., 2008. How risky are social networking sites? a comparison of places online where youth sexual solicitation and harassment occurs. Pediatrics 121 (2), 350–357.