A web of deceit

Financial sexual extortion of children and young people

BRIEFING PAPER

JUNE 2024

As highlighted in the WeProtect Global Alliance's 2023 Global Threat Assessment, cases of financial sexual extortion are growing dramatically, primarily targeting teenage boys, with the motivation to blackmail victims into providing money or gifts in kind.

It can progress rapidly, in some cases moving from initial message to coercion within a few hours. Tragically, there have also been media reports linking cases of financial sexual extortion to more than 20 children and young people taking their own lives.

This paper provides an overview of this rapidly growing threat, who is impacted, perpetrators and the typical pathways used to target children and young people.

Table of contents

What is financial sexual extortion?

Financial sexual extortion is a type of blackmail that typically involves a victim connecting with someone online who is unknown to the victim.[1] The unknown individual often misrepresents their age and/or gender and manipulates the victim into sending nude, sexual or intimate images of themselves. The victim may also be manipulated to join in a sexually explicit video call, after which the extorter takes screenshots or records the call.[2] Almost immediately the victim receives demands for money (and sometimes also demands for more intimate images) and is threatened that if they fail to comply, their images will be sent to friends, family or distributed online.

Analysis of reported cases by Europol suggests that the key elements of financial sexual extortion are likely to include:

- material — any content (information, photo or video) that the victim wishes to keep confidential
- threat — the undesirable outcome the victim aims to avert, typically the exposure of the confidential material
- value — the financial demands made by the perpetrator upon the victim.

The convergence of these factors in the digital realm is crucial for the perpetration of the crime, with the access to intimate material serving as a trigger for the entire process.[3]

Targets of financial sexual extortion are generally teenage boys who are deceived into believing they are communicating with a young female. Engaging victims often occurs over a short period of time, anywhere between minutes to hours.

While still a minority of all sexual extortion cases, financially motivated cases manifest differently. Seventy per cent of victims who ignore criminal demands for payment do not subsequently have their images distributed, suggesting that the primary motivation of perpetrators is financial.[4] Possession of the online intimate material is key as it uses threat of exposure to create psychological torment and quick decision-making by the victims to get them to pay immediately.[5]

Of increasing concern is access to generative artificial intelligence (AI) technology, which elevates the threat to children further as offenders can create credible images without needing to obtain intimate images (see section on Generative AI for more details).

A note on terminology

The Alliance uses the term 'financial sexual extortion' to highlight the specific nature of the crime. Other organisations also refer to the term 'financial sextortion'.

Europol uses the description economic or commercial sexual extortion to reflect the outcome where the victim, when threatened, provides something else other than money.

Europol also highlight problems with boys and men reconciling their masculine identity with the experience of being a sexual victim and suggests that deception might be a better word than extortion.[6]

Prevalence of a growing threat

While there is no definitive data source on financial sexual extortion, research from various sources paints a clear picture of this rapidly growing threat. For example, both the US based National Centre for Missing and Exploited Children (NCMEC) and the UK based Internet Watch Foundation (IWF) have reported exponential increases in reports in 2023 compared to 2022. NCMEC's CyberTipline saw 10,731 reports in 2022; this number jumped to 26,718 in 2023.[7]

In the first six months of 2023, the IWF received more reports involving financial sexual extortion than in the whole of 2022.[8] And in 2022, the Federal Bureau of Investigation (FBI) received 7,000 reports of financial sexual extortion against minors, prompting them to issue a national public safety alert.[9]

The Australian Federal Police's Australian Centre to Counter Child Exploitation receives about 300 reports a month of financial sexual extortion involving children.[10] However, Australian Federal Police Commander for Human Exploitation, Helen Schneider estimates "only one in 10 report it."[11] Children are particularly vulnerable; in a survey of over 1,500 victim-survivors, 46% were children.[12]

Who are the perpetrators?

Recent data and investigations by law enforcement authorities continue to shed light on the geographical origins of perpetrators and the evolving tactics they employ to exploit their victims both nationally and internationally. By understanding the perpetrators and their behaviours, we can develop more targeted response strategies.

Network Contagion Research Institute (NCRI)[13] has attributed the recent increase of financial sexual extortion cases as being driven by the Yahoo Boys, a distributed group of cybercriminals in West Africa adopting this tactic of financial gain. The Yahoo Boys are a major threat actor, actively targeting children and young people in the United States, Canada, United Kingdom, Australia, Europe, and elsewhere.[14]

Europol has also identified gangs operating from the Philippines, Nigeria and Côte d'Ivoire. English is the key language used to approach victims in the US, Canada and Australia, as well as the UK and the Netherlands. Similar crimes are emerging in other countries such as India where research suggests that there are around 500 cases of financial sexual extortion daily in India perpetrated by Indian nationals on other Indian nationals, but that only a small proportion of these are reported.[15] In 2020, a Korean national Cho Ju-bin was convicted of running a sex blackmail ring in Korea.[16] Financial sexual extortion crimes have also been uncovered in France[17], Germany,[18] Spain,[19] Morocco[20] and Mexico.[21]

According to Europol, the perpetrators are both male and female, working as part of organised criminal enterprises in teams largely based in developing countries.[22] They may act nationally and internationally, with the main goal of obtaining financial gain. They generally target young male victims in countries linked by language and do not know the victim in person.

Given likely underreporting and limitations with current data, more research and data on financial sexual extortion perpetrators and their evolving tactics is crucial to developing effective prevention and intervention strategies.

Why are boys disproportionately targeted?

Historically, sexual extortion generally has primarily targeted women and girls.[23]

Although financial sexual extortion can impact anyone, current data suggests the main targets are teenage boys between 13 and 17 years. Boys are more likely to be lax with use of passwords and often communicate with strangers online in discussion forums, online dating sites, instant messaging and multi-player gaming.[24] Boys also claim to be more confident than girls in their ability to distinguish the real from the fake online. [25]

While girls also have a propensity to overshare online, girls see sending and receiving images as a high-risk activity, that is part of building and maintaining romantic relationships.[26]

What might make boys targets for this crime is their attitude to sending and receiving intimate images online with 'sexting' seen as a way to belong to and exercise power in friendship groups.[27]

For boys, there may also be barriers to disclosing extortion, including fear of not being believed, ridicule or stigma. For example, WeProtect Global Alliance research shows that several boys' groups expressed feeling particularly isolated, as culturally it was less acceptable to talk with peers about feelings and emotions.[28] This likely results in significant underreporting.

Tragically, there are also many documented cases of financial sexual extortion targeting children and young people which media have reported as contributing to them taking their own lives.

Further research needs to be undertaken to understand barriers to reporting and the factors which make children and young people more vulnerable to financial sexual extortion.

How are victims impacted?

Financial sexual extortion can cause serious harm to victims. Short-term impacts on victims included shame, stress, isolation, depression, anxiety and self-blame. Issues with trust may also develop.

Long-term impacts can include enduring episodes of anxiety, which may be further exacerbated by the religious or cultural environment of the victim.[29]
All of these impacts act as a barrier to seeking help.

Self-harm and suicide have also been identified as risks. In the US there were 20 known suicides linked to financial sexual extortion victims from October 2022 to March 2023.[30]

> *[Ryan's mother] said goodnight to Ryan at 10 p.m. and described him as her usually happy son. By 2 a.m., he had been scammed, and taken his life. Ryan left behind a suicide note describing how embarrassed he was for himself and the family.*[31]
>
> **17 year-old Ryan Last, California, USA**

> *[Daniel] was contacted by a financial sextortionist in February 2022. After being coerced into sending his explicit images, Daniel faced extortion within minutes. After intimidation, he complied with the offender's demands, and within three hours, Daniel took his own life.*[32]
>
> **17-year-old Daniel Lints, Manitoba, Canada**

Charting the typical online pathway enabling financial sexual extortion

Financial sexual extortion can involve the use of many platforms to identify potential victims, initiate private conversations and exchange images and transfer money.

Research cited in this briefing suggests, perpetrators favour three platforms in particular: Instagram, Snapchat and Wizz[33]. However, following pressure from law enforcement agencies, Wizz was removed from the App Store and Google Play Store in February 2024 over the use of the app in financial sexual extortion scams.[34]

1. Identifying and connecting with potential victims

Criminals target high schools, sports teams and youth groups on social media and gaming apps with follow requests in order to have mutual friends within their focus.[35] They typically use stolen or hacked Instagram accounts and use files of amateur, self-produced imagery sometimes stolen or bought from OnlyFans models, to appear more authentic.[36]

The moment a user accepts a request their following list is compromised, and the criminals can grab personal information about the victim and screenshot the victim's social media followers and following lists. Getting access to this information is important so that the criminal can later threaten the victim that the nude photos will be shared with friend and family members.

Perpetrators use bots, scripts and hacked accounts to manufacture evidence of account usage and engagement, leading victims to believe the criminal is an authentic user.[37]

2. Threats and coercion

Once the perpetrator has been accepted as a follower by the victim, they then encourage the victim to move to an encrypted platform. Intimate images and videos - purportedly of the "girl" that the victim is interacting with - are sent, with coaxing messages for the victim to send nude images and videos back. According to Snapchat commissioned research in Australia, France, Germany, India, UK and the US, 31% of teens who are approached by a sexual extortion criminal ultimately share a compromising photo.[38]

Perpetrators use widely circulated scripts to escalate the threat level. This includes sharing screenshots with followers and sending screenshots of draft messages to friends and family to apply pressure.

Criminals will also threaten to frame the victim for sending intimate images to a child, create wanted posters with a victim's intimate image, name and number, or threaten that the sharing of the photos will have consequences such as school expulsion or the job loss of parents.

Despite the most popular sexual extortion scripts being publicly accessible since 2021, according to NCRI, texts have not been blacklisted by key platforms including TikTok, Instagram and YouTube.[39]

3. Financial transfers and payment in kind

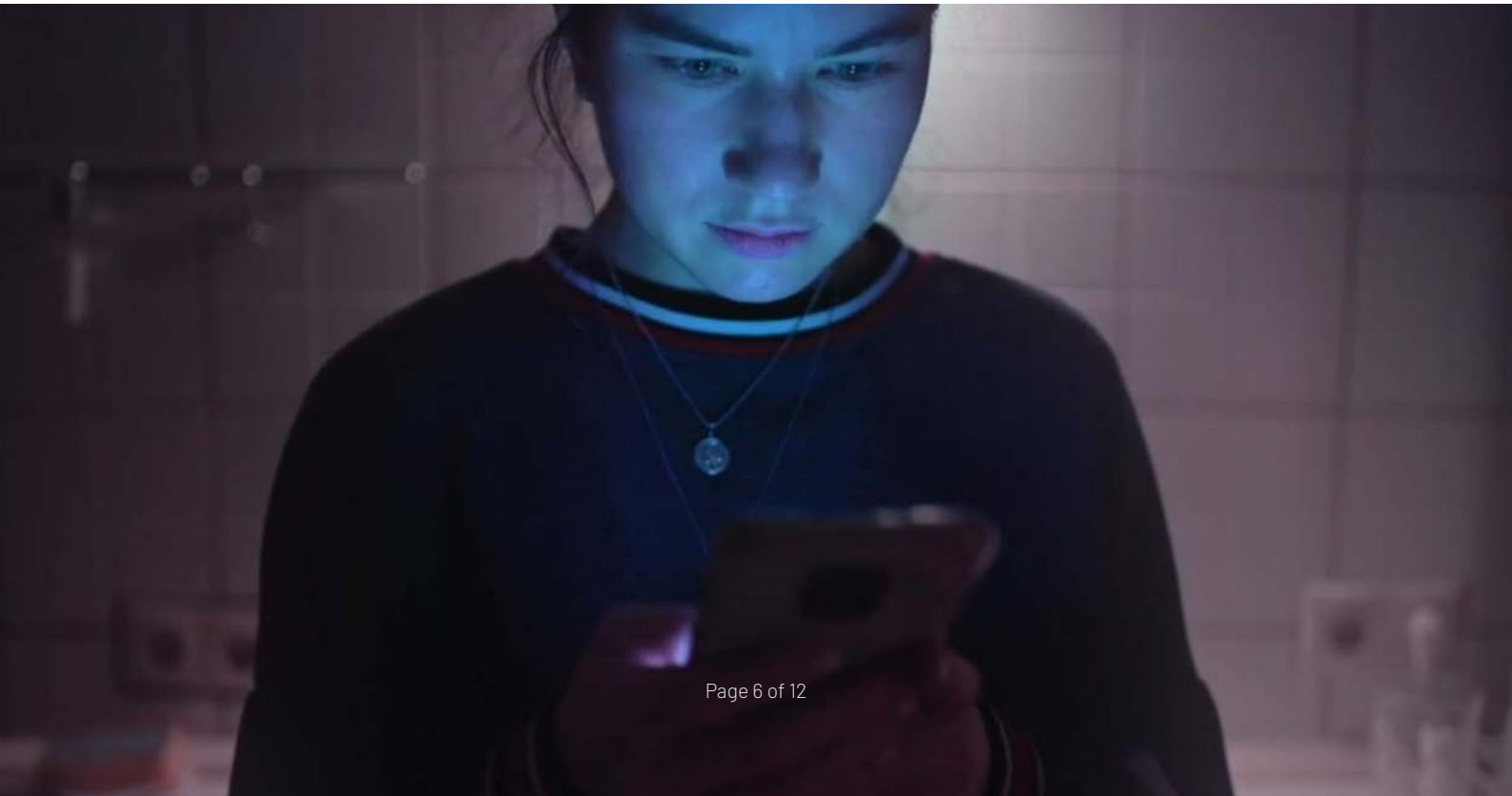
More research is needed about the role of payment platforms in financial sexual extortion. According to research on the Reddit support forum r/Sextortion, which has more than 20,000 members, PayPal was the most mentioned payment mechanism, along with gift cards and cryptocurrency,[40] fee and payment processors Venmo and Zelle. Transactions made via banks, and other platforms such as Cash App and Remitly, accounted for a small portion of known payment processors.

For cases where the amount of money paid to extorters was known, most victims (40%) paid between $100 and $500. Just over one third (36%) of victims paid $100 or less. Despite each individual payment being relatively small, criminals are raising significant sums from extortion because of the scale of the activity. For example, a group accused of trying to blackmail young men and boys swindled $1.7 million from victims in the US, UK and Canada.[41] Similarly, NCRI cites the indictment of Olamide Oladosu Shanu, a Nigerian whose financial sexual extortion enterprise had received US $2.5m in Bitcoin from victim payments.[42]

Even if the victim pays, the photos might not be deleted, and the criminals might continue to demand multiple payments over an extended period. If the victim pays the criminal, they are often put on scheduled weekly or monthly payment plans.

If the victim cannot pay the perpetrator because, as a child, they do not have access to money, they may then be asked to hand over their social media accounts or create new accounts for criminals to use. Evidence of this has been found in the US on websites such as Login.gov and IRS.gov. The criminal may also try to obtain a guardian's credit card information from a child either directly or by getting the child to sign up for a particular website that requires this information. Children can also be blackmailed to become money mules to transfer funds from victims to other members of the criminal network.

One of the most shocking characteristics of this type of abuse is the speed with which the extortion unfolds. Criminals put intense and rapid pressure on victims to gain payment quickly. This precludes any but the most rudimentary grooming techniques from the perpetrators, who may trick the victim into believing that they and the victim share mutual friends, go to the same school, or live in the same city. Sophisticated grooming techniques are typically not used because they take too long, as the crime is time-sensitive and financially motivated.[43]



How generative AI is being used in financial sexual extortion schemes

With the availability of low-cost or free-to-use generative AI (Gen AI) tools to create deepfakes, an extortionist no longer needs to trick a child into sharing an intimate picture. With access to the victim's photos and videos on social media platforms, offenders can easily generate an intimate image that looks like the victim.

Gen AI technology is used in two main ways to perpetrate financial sexual extortion:

- to enhance a fake or stolen online identity by manipulating photographs to falsely show proof of life, or to create a credible life-like synthetic identity, making it easier to deceptively befriend the victim.
- to create a deepfake based on a clothed Instagram picture to nudify the victim.

Gen AI apps are already being used to target children in a small number of cases. For example, NCMEC's CyberTipline received a report relating to a financial sexual extortion plot using Gen AI technology to create explicit images from innocuous images in which the offender threatened the child victim.

The report said: "I recently had an intriguing idea to create a video where you'd be pleasuring yourself on one side of the screen, while looking at photos of your acquaintances on the other side. Using AI and your data it wasn't hard to make it happen. I was amazed by the outcome. With one click I can send this video to all of your friends via email, social networks and instant messengers. If you don't want me to do it, sent [sic] me $850 in my Bitcoin wallet."

Another report to the CyberTipline revealed a stranger engaged a child online and then sent fake explicit photos threatening to share the images with the child's Instagram friends unless the child paid money. The child said: "[t]he images look SCARY real and there's even a video of me doing disgusting things that also look SCARY real. I don't know how the person managed to make them look that real. I did end up sending ...my debit card information".[44]

Since the use of Gen AI does not require authentic intimate images to commit financial sexual extortion, this is a threat which has significant potential to evolve and grow quickly at scale and move from primarily targeting teen boys to using deepfake imagery to increasingly target girls.

Responding to financial sexual extortion

Public awareness campaigns and alerts

Given the exponential increase in the prevalence of financial sexual extortion, several public awareness campaigns have been launched to educate and protect children and young people.

One such campaign is Know2Protect, launched by the United States' Department of Homeland Security, which provides resources, workshops, and community events to raise awareness about the dangers of financial sexual extortion. The campaign emphasises digital literacy and safe online practices, offering practical advice to children, parents, and educators on how to recognise and respond to potential threats. The campaign also highlights the importance of support networks for victims, helping them to seek help and recover from their experiences.

Another impactful initiative is No Escape Room[45], an interactive online experience designed by NCMEC to simulate the tactics used by extortionists. This platform allows participants to safely navigate scenarios similar to real-life extortion attempts, thereby equipping them with the knowledge and skills to identify and avoid such threats.

There have also been official warnings from various law enforcement agencies. In February 2023, a joint warning about the threat of financial sextortion was issued by the FBI, NCMEC, Royal Canadian Mounted Police, the UK National Crime Agency (NCA) and the Toronto Police Service. This warning promoted the message that, "law enforcement around the world wants victims to know they are not in trouble, they are not alone, and there is life after pictures."[46]

Additionally, the NCA issued an alert to hundreds of thousands of education professionals following a considerable increase in global cases of financially motivated sexual extortion. Specialists from the NCA's education team produced the alert, which was issued to teachers across the UK on Monday 29 April 2024.[47] The alert provides advice on spotting the signs of this type of abuse, supporting young people and encouraging them to seek help. It also includes guidance to be disseminated to parents and carers on how to talk to their child about sextortion and how to support them if they become a victim. These initiatives aim to reduce the stigma surrounding the topic and, in turn, take away power away from those who wish to harm.

Further awareness of the problem is required, involving open conversations with carers and parents and with schools, youth groups and sports teams.

This will help erode the power of the threats propagated by criminals. These conversations should discuss that it is best not to comply with the threats and to cut off communication with the criminal, while retaining the interactions for potential law enforcement follow-up.

The classic pathway taken by the perpetrators should be widely publicised and discussed with children and young people. Awareness campaigns should consult with children and young people to explore ways for them to continue to enjoy being young, enabling them to explore sexuality, without making themselves vulnerable to extortionists.

International law enforcement cooperation

Law enforcement is crucial to addressing financial sexual extortion and other forms of child exploitation.

The transnational nature of financial sexual extortion means that perpetrators and victims often reside in different countries, allowing criminals to use jurisdictional boundaries to their advantage and evade detection and prosecution.

Collaborative efforts, such as the FBI's cooperation with Nigerian authorities, enable law enforcement agencies to work across borders, ensuring that criminals cannot easily escape justice. This cross-border coordination is vital in tackling the complexities of global crime networks involved in financial sexual extortion.

> In 2023 FBI Michigan (US) travelled to Nigeria to conduct a co-operative investigation with Nigerian law enforcement officials[47]. The US Department of Justice's Office of International Affairs and the US Department of State requested the provisional arrest of three Nigerian nationals involved in a financial sextortion ring. Working with the Nigerian law enforcement agency, the Economic and Financial Crimes Commission, arrests were made on domestic Nigerian charges based on shared information. This then enabled the extradition of the suspects to the US.

Many countries lack the specialised resources and expertise necessary to combat financial sexual extortion effectively. By collaborating, law enforcement agencies can share resources such as digital forensics capabilities and advanced training programmes. Enhanced intelligence sharing ensures timely exchange of critical information, leading to swift actions against perpetrators and providing comprehensive protection for victims.

An example of this is Project Boost, set up by the International Justice Mission, Meta and NCMEC. The project helps train law enforcement around the world to identify and investigate cases of online sexual exploitation of children and is already working in Kenya, Ghana and Nigeria to arrest criminals suspected of the sexual exploitation of children.[48]

Financial services ability to flag suspicious activity

Experts have highlighted the critical role of financial institutions in addressing financial sexual extortion, despite its perception as a family matter.[49] Victims often go to great lengths to hide extortion attempts from family and peers, making external intervention vital.

For instance, gift cards and prepaid cards are frequently used in financial sexual extortion schemes. Extortionists, whether domestic or international, can easily access the value stored on these cards by coercing the victims to share account codes over text. Unusually large purchases of gift cards or significant cash withdrawals intended to buy gift cards should be treated with suspicion.

Implementing periodic audits and reviews of their profiling and transaction monitoring programmes are other ways in which financial services can flag suspicious activities.

Offenders often exhibit identifiable patterns in their financial transactions that can signal involvement in financial sexual extortion. For example, extorters will have patterns of small amounts paid irregularly into their accounts from victims who may live close to each other, since extorters "bomb" schools, youth and sports groups to exploit social connectedness.

Peer-to-peer transfers to new recipients and outgoing payments from minors' accounts to cryptocurrency platforms could also be indicators for sexual extortion.[50]

Monitoring these low-value transactions typical in children's accounts can be challenging. Experts recommend setting lower alert thresholds to detect potential signs of sexual extortion effectively.[51] For instance, transactions as small as $100 in a minor's account should be treated with the same scrutiny as $10,000 in an adult's account, helping to identify and address extortion attempts more swiftly.

Social media platform mitigations

Meta has recently announced that it is testing new features to help protect young people from financial sexual extortion and intimate image abuse.[52] These features aim to make it more difficult for potential scammers and criminals to find and interact with teens. It is also experimenting with ways to help users identify potential sexual extortion scams, encouraging them to report suspicious activities and empowering them to refuse uncomfortable requests. Additionally, Meta has started sharing more signals about sexual extortion accounts with other tech companies through Lantern[53], a cross-platform sharing programme run by the Tech Coalition.

Other social media platforms are also taking steps to combat financial sexual extortion. For example, Snapchat uses signal-based detection to identify and remove bad actors. Additionally, Snapchat has expanded its in-app reporting tools to include a specific reason for financial sexual extortion. Once identified, Snapchat takes action against the content, accounts, or devices involved, and reports offenders to NCMEC and law enforcement where appropriate.[54]

There are other mitigations that can be implemented by social media platforms to disrupt financial sexual extortion criminals. First, making accounts for users under 18 private by default can significantly reduce their exposure to potential offenders. Algorithms should not nudge young users to add others or incentivise them to share personal information. Platforms should also make it easier to specifically report financial sexual extortion incidents, providing direct links to resources such as NCMEC's Take it Down service of the UK's Report Remove service. By implementing these measures, social media platforms can create a safer environment for young users and help prevent financial sexual extortion.

Footnotes

1 - An Analysis of Financial Sextortion Victim Posts Published on r/Sextortion, November 2022, https://protectchildren.ca/en/resources-research/an-analysis-of-financial-sextortion-victim-posts-published-on sextortion/#:~:text=In%20an%20open%2Dsource%20analysis,Canadians%20and%20online%20users%20abroad

2 - Sexual extortion trends and challenges – position statement, August 2021, https://www.esafety.gov.au/industry/tech-trends-and-challenges/sextortion

3 - Online Sexual Coercion and Extortion as a Form of Crime Affecting Children: Law Enforcement Perspective, May 2017, https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children_0.pdf

4 - The Cyber Pandemic: Exploring the Financial Sextortion of Young Males, April 2023, https://arcabc.ca/islandora/object/mru%3A862/datastream/PDF/view

5 -Understanding the psychological impact of rape and serious sexual assault of men: a literature review, August 1997, https://pubmed.ncbi.nlm.nih.gov/9362829/

6 -Online Sexual Coercion and Extortion as a Form of Crime Affecting Children: Law Enforcement Perspective, May 2017, https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children_0.pdf

7 - NCMEC releases new sextortion data, April 2024. Accessed here: https://www.missingkids.org/blog/2024/ncmec-releases-new-sextortion-data

8 - Hotline reports 'shocking' rise in the sextortion of boys, September 2023, https://www.iwf.org.uk/news-media/news/hotline-reports-shocking-rise-in-the-sextortion-of-boys/

9 - FBI and Partners Issue National Public Safety Alert on Financial Sextortion Schemes, December 2022, https://www.fbi.gov/news/press-releases/press-releases/fbi-and-partners-issue-national-public-safety-alert-on-financial-sextortion-schemes

10 - ACCCE partners with Meta and Kids Helpline to increase sextortion support for young people, December 2023, https://www.afp.gov.au/news-centre/feature/accce-partners-meta-and-kids-helpline-increase-sextortion-support-young-people

11 - Sextortion: A Growing Concern for Schools, March 2024, https://www.schoolgovernance.net.au/news/sextortion-a-growing-concern-for-schools

12 - Sextortion of Minors: Characteristics and Dynamics (Wolak, J. et al., 2017) Accessed from: https://www.unh.edu/ ccrc/sites/default/files/media/2022-02/sextortion-ofminors-characteristics-and-dynamics.pdf

13 - A digital pandemic: uncovering the role of 'yahoo boys' in the surge of social media-enabled financial sextortion targeting minors, January 2024, https://networkcontagion.us/wp-content/uploads/Yahoo-Boys_1.2.24.pdf

14 - A digital pandemic: uncovering the role of 'yahoo boys' in the surge of social media-enabled financial sextortion targeting minors, January 2024, https://networkcontagion.us/wp-content/uploads/Yahoo-Boys_1.2.24.pdf

15 - The sextortion scammers of rural India, December 2022, https://restofworld.org/2022/sex-scam-village-india/

16 - Welcome to cyber hell: How Korean journalists shined a light on an online sextortion ring, May 2022, https://english.hani.co.kr/arti/english_edition/e_national/1044708

17 - Chantage intime : le nombre de cas de "sextorsion" explose en France, March 2024, https://www.francebleu.fr/infos/societe/chantage-intime-le-nombre-de-cas-de-sextorsion-explose-en-france-9042144

Sextorsion : «Si je ne répondais pas assez vite, il me rappelait que, de toute façon, il allait tout diffuser", February 2024, https://www.radiofrance.fr/franceinter/podcasts/le-zoom-de-la-redaction/le-zoom-de-la-redaction-du-mercredi-07-fevrier-2024-4478028

Réseaux sociaux: les victimes de chantage à la vidéo intime se multiplient en France, February 2024, https://www.francetvinfo.fr/societe/harcelement-sexuel/reseaux-sociaux-les-victimes-de-chantage-a-la-video-intime-se-multiplient-en-france_6388039.html

18 - Mit Penis-Foto erpresst: Sextortion-Opfer spricht über seinen Fall, August 2023, https://www.ndr.de/nachrichten/niedersachsen/Mit-Penis-Foto-erpresst-Sextortion-Opfer-spricht-ueber-seinen-Fall,sextortion104.html

Tausende werden mit Nacktbildern erpresst, December 2023, https://www.zdf.de/nachrichten/panorama/kriminalitaet/nacktbilder-erpressung-100.html

Sextortion: Erpressungen mit Nacktaufnahmen treffen vermehrt Jugendliche, January 2024, https://www.derstandard.de/story/3000000204190/sextortion-erpressungen-mit-nacktaufnahmen-treffen-vermehrt-jugendliche

19 - Sextorsión: cuando los adolescentes se convierten en el principal objetivo de los ciberdelincuentes, February 2024, https://www.rfi.fr/es/sociedad/20240220-sextorsi%C3%B3n-cuando-los-adolescentes-se-convierten-en-el-principal-objetivo-de-los-ciberdelincuentes

20 - Meet the men behind Morocco's 'sextortion' racket, October 2016, https://www.bbc.co.uk/news/av/magazine-37705678

21 - Fraude amoroso y sextorsión, principal preocupación entre jóvenes de generaciones Z y Millennial, February 2024, https://www.cronica.com.mx/nacional/fraude-amoroso-sextorsion-principal-preocupacion-jovenes-generaciones-z-millennial.html

22 - Online Sexual Coercion and Extortion as a Form of Crime Affecting Children: Law Enforcement Perspective, May 2017, https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children_0.pdf

23 - Warning Issued to Thousands of US Teenage Boys, April 2024, https://www.newsweek.com/teen-boys-risk-sextortion-online-social-media-1885627

24 - The Cyber Pandemic: Exploring the Financial Sextortion of Young Males, August 2023, https://arcabc.ca/islandora/object/mru%3A862/datastream/PDF/view

25 - Children and Parents: Media Use and Attitudes Report, April 2024. Accessed here: https://www.ofcom.org.uk/__data/assets/pdf_file/0025/283048/Childrens-Media-Literacy-Report-2024.pdf

26 - Conduct problems and sexting: Gender differences, Computers in Human Behaviour, May 2024, https://www.sciencedirect.com/science/article/abs/pii/S0747563224000190#:~:text=A%20recent%20study%20found%20that,across%20distinct%20types%20of%20sexting.

27 - A digital pandemic: uncovering the role of 'yahoo boys' in the surge of social media-enabled financial sextortion targeting minors, January 2024, https://networkcontagion.us/wp-content/uploads/Yahoo-Boys_1.2.24.pdf

28 - Child 'self-generated' sexual material online: children and young people's perspectives, https://www.weprotect.org/wp-content/uploads/WP-Report-Praesidio-Safeguarding-.pdf

29 - Short-Term and Long-Term Impacts of Financial Sextortion on Victim's Mental Well-Being, March 2023, https://journals.sagepub.com/doi/abs/10.1177/08862605231156416

30 - Tackling the rising incidence of financial sexual extortion, Takeaways from a cross-sector innovation forum, 2024, https://www.weprotect.org/wp-content/uploads/FSE-Post-Event-Report-PA-Consulting.pdf

31 - A 17-year-old boy died by suicide hours after being scammed. The FBI says it's part of a troubling increase in 'sextortion' cases, May 2022, https://edition.cnn.com/2022/05/20/us/ryan-last-suicide-sextortion-california/index.html

32 - 'World lost a good person': Manitoba parents warn of global sextortion targeting teenage boys, June 2022, https://www.cbc.ca/news/canada/manitoba/manitoba-sexploitation-suicide-1.6494054

33 -A friend-finding app offered a 'safe space' for teens — sextortion soon followed, July 2023, https://www.nbcnews.com/tech/social-media/friend-finding-app-offered-safe-space-teens-sextortion-soon-followed-rcna91172

A digital pandemic: uncovering the role of 'yahoo boys' in the surge of social media-enabled financial sextortion targeting minors, January 2024, https://networkcontagion.us/wp-content/uploads/Yahoo-Boys_1.2.24.pdf

An Analysis of Financial Sextortion Victim Posts Published on r/Sextortion, November 2022, https://protectchildren.ca/en/resources-research/an-analysis-of-financial-sextortion-victim-posts-published-on sextortion/#:~:text=In%20an%20open%2Dsource%20analysis,Canadians%20and%20online%20users%20abroad

34 - Wizz, a Tinder-like app aimed at teenagers, removed from Apple App Store and Google Play, February 2024, https://www.nbcnews.com/tech/social-media/wizz-tinder-app-aimed-teens-removed-apple-google-stores-rcna136607

35 - A digital pandemic: uncovering the role of 'yahoo boys' in the surge of social media-enabled financial sextortion targeting minors, January 2024, https://networkcontagion.us/wp-content/uploads/Yahoo-Boys_1.2.24.pdf

Sexual extortion trends and challenges – position statement, August 2021, https://www.esafety.gov.au/industry/tech-trends-and-challenges/sextortion

36 - A digital pandemic: uncovering the role of 'yahoo boys' in the surge of social media-enabled financial sextortion targeting minors, January 2024, https://networkcontagion.us/wp-content/uploads/Yahoo-Boys_1.2.24.pdf

37 - https://github.com/useragents/Snapchat-Snapscore-Botter

An Analysis of Financial Sextortion Victim Posts Published on r/Sextortion, November 2022, https://protectchildren.ca/en/resources-research/an-analysis-of-financial-sextortion-victim-posts-published-on sextortion/#:~:text=In%20an%20open%2Dsource%20analysis,Canadians%20and%20online%20users%20abroad

38 - Two-thirds of Gen Z targeted for online "sextortion" – New Snap research, June 2023, https://www.weprotect.org/blog/two-thirds-of-gen-z-targeted-for-online-sextortion-new-snap-research/ ; Digital Well-Being Index – Year Two, February, 2024, https://values.snap.com/safety/dwbi

39 - A digital pandemic: uncovering the role of 'yahoo boys' in the surge of social media-enabled financial sextortion targeting minors, January 2024, https://networkcontagion.us/wp-content/uploads/Yahoo-Boys_1.2.24.pdf

40 - An Analysis of Financial Sextortion Victim Posts Published on r/Sextortion, November 2022, https://protectchildren.ca/en/resources-research/an-analysis-of-financial-sextortion-victim-posts-published-on sextortion/#:~:text=In%20an%20open%2Dsource%20analysis,Canadians%20and%20online%20users%20abroad

41 - Delaware woman accused in sextortion plot to blackmail $6M from victims in US and UK, April 2024, https://www.independent.co.uk/news/world/americas/crime/sextortion-plot-delaware-woman-arrested-b2528001.html

42 - A digital pandemic: uncovering the role of 'yahoo boys' in the surge of social media-enabled financial sextortion targeting minors, January 2024, https://networkcontagion.us/wp-content/uploads/Yahoo-Boys_1.2.24.pdf

43 - A digital pandemic: uncovering the role of 'yahoo boys' in the surge of social media-enabled financial sextortion targeting minors, January 2024, https://networkcontagion.us/wp-content/uploads/Yahoo-Boys_1.2.24.pdf

44 - Addressing Real Harm Done by Deepfakes, March 2024, https://www.missingkids.org/content/dam/missingkids/pdfs/final-written-testimony-john-shehan-house-oversight-subcommittee-hearing.pdf

45 - "No Escape Room" Launches with New Data: Interactive Experience Exposes Dangers of Financial Sextortion, April 2024, https://www.missingkids.org/blog/2024/no-escape-room-launches-with-interactive-experience

46 - International Law Enforcement Agencies Issue Joint Warning about Global Financial Sextortion Crisis. February 2023, https://www.fbi.gov/news/press-releases/international-law-enforcement-agencies-issue-joint-warning-about-global-financial-sextortion-crisis

47 - NCA issues urgent warning about 'sextortion', April 2024, https://www.nationalcrimeagency.gov.uk/news/nca-issues-urgent-warning-about-sextortion

48 - International Justice Mission Partners with NCMEC, Law Enforcement, and Tech to Protect Children Online through Training in Côte d'Ivoire, May 2024, https://www.ijm.org/news/international-justice-mission-partners-ncmec-law-enforcement-tech-protect-children-online-training

49 - In Stopping 'Sextortion' Attacks Against Minors, Banks Have Role to Play, March 2024, https://www.moneylaundering.com/news/in-stopping-sextortion-attacks-against-minors-banks-have-role-to-play/

50 - How to follow the money of a sextortion victim, Jan 2024, https://5522198.fs1.hubspotusercontent-na1.net/hubfs/5522198/RFA_Infographic_Sextortion.pdf

51 - In Stopping 'Sextortion' Attacks Against Minors, Banks Have Role to Play, March 2024, https://www.moneylaundering.com/news/in-stopping-sextortion-attacks-against-minors-banks-have-role-to-play/

52 - New Tools to Help Protect Against Sextortion and Intimate Image Abuse, April 2024, https://about.fb.com/news/2024/04/new-tools-to-help-protect-against-sextortion-and-intimate-image-abuse/

53 - Tech Coalition Releases its First Lantern Transparency Report and 2023 Annual Report, April 2024, https://www.technologycoalition.org/newsroom/tech-coalition-release-its-first-lantern-transparency-report-and-2023-annual-report; New Tools to Help Protect Against Sextortion and Intimate Image Abuse, April 2024, https://about.fb.com/news/2024/04/new-tools-to-help-protect-against-sextortion-and-intimate-image-abuse/

54 - What you need to know about Financial Sextortion, Snapchat, https://values.snap.com/safety/financial-sextortion