A DIGITAL PANDEMIC: UNCOVERING THE ROLE OF ‘YAHOO BOYS’ IN THE SURGE OF SOCIAL MEDIA-ENABLED FINANCIAL SEXTORTION TARGETING MINORS

PRESENTED BY

NCRI

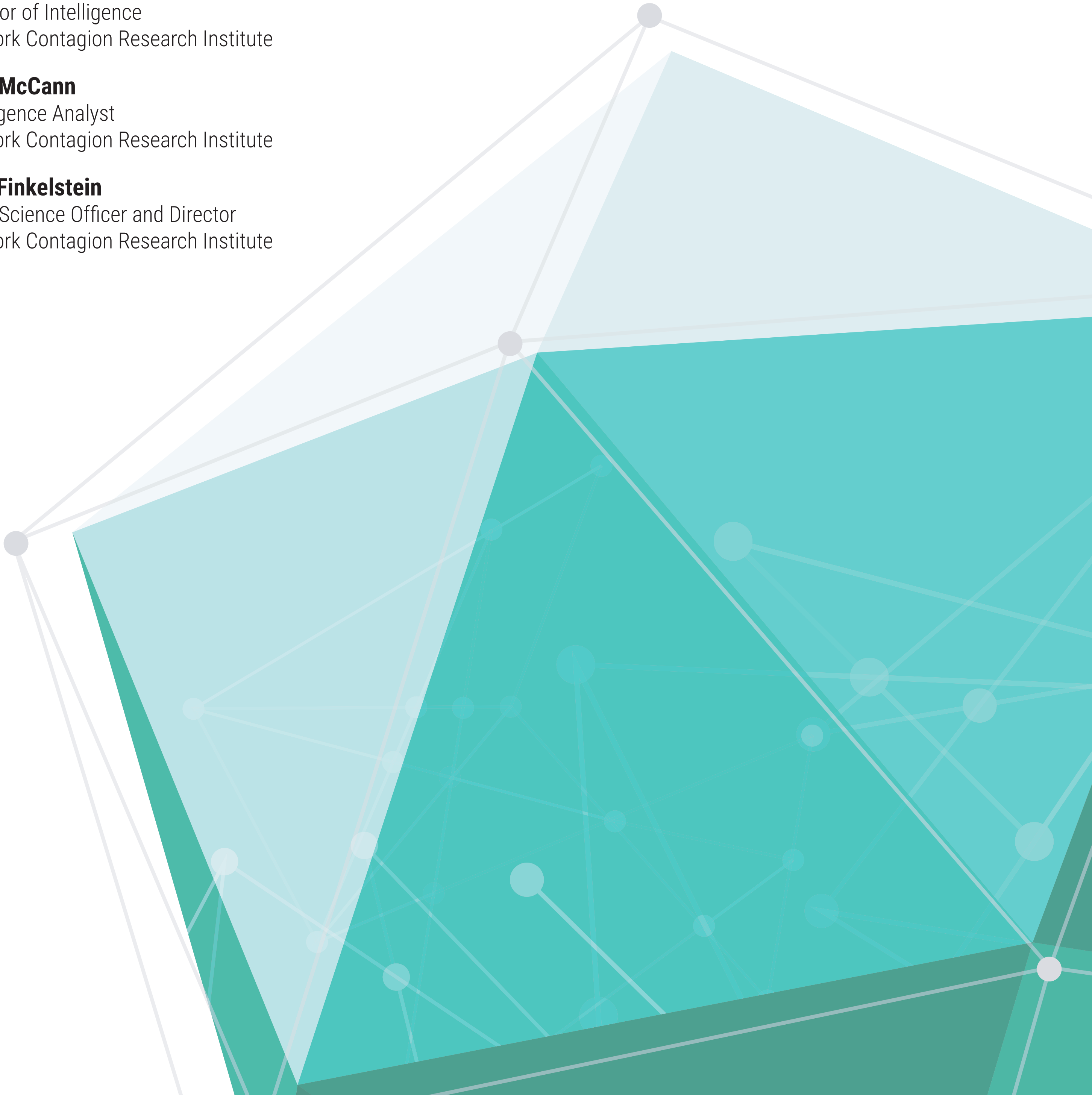
NETWORK CONTAGION
RESEARCH INSTITUTE

Paul Raffile
Senior Intelligence Analyst
Network Contagion Research Institute

Alex Goldenberg
Director of Intelligence
Network Contagion Research Institute

Cole McCann
Intelligence Analyst
Network Contagion Research Institute

Joel Finkelstein
Chief Science Officer and Director
Network Contagion Research Institute



NCRI
NETWORK CONTAGION
RESEARCH INSTITUTE

Threat Intelligence Report

A Digital Pandemic: Uncovering the Role of 'Yahoo Boys' in the Surge of Social Media-Enabled Financial Sextortion Targeting Minors

Financial sextortion is the fastest growing crime targeting children in North America and Australia—accelerating at an alarming rate, with incidents surging up 1,000% in the past 18 months. In a December 2023 hearing, FBI Director Wray warned Congress that sextortion is "a rapidly escalating threat," and teenage victims "don't know where to turn."[1]

Cybercriminals are using fake social media accounts to coerce victims, almost all of them boys, into sharing an explicit photo.[2] As soon as the criminal receives the photo, they threaten to (and sometimes do) expose the photo to the victim's friends, family, and followers unless a ransom is paid. These criminals employ ruthless tactics to intimidate their victims, inflicting lasting trauma and immense distress–which has led to more than 21 youth suicides.[3] [4]

This report reveals that virtually all of the financial sextortion targeting minors today is directly linked to a distributed West African cybercriminal group called the **Yahoo Boys.** Additionally, this investigation unveils previously unreported views into the social media platforms where these criminals share their sextorion scripts, tools, and methods, which has allowed this crime to proliferate at an exponential rate.

Most recently, in November 2023, Olamide Oladosu Shanu, a Nigerian national, was indicted along with four co-conspirators in the largest known financial sextortion operation to date.[5] The indictment alleges that Shanu's criminal enterprise received upwards of $2.5 million U.S. dollars in Bitcoin from victim payments.[6]

[1] https://www.nbcrightnow.com/national/sextortion-is-a-rapidly-escalating-threat-fbi-director-says/video_4fb28c88-04ba-5131-89f3-082396fca798.html
[2] https://www.protectchildren.ca/en/press-and-media/news-releases/2022/sextortion-data-analysis
[3] https://www.missingkids.org/blog/2023/financial-sextortion-growing-crisis
[4] https://www.cbc.ca/news/canada/british-columbia/police-link-suicide-of-12-year-old-prince-george-b-c-boy-to-online-sexual-extortion-1.7041185
[5] USA v. Shanu (2023) | Case 1:23-mj-00258-REP via PACER
[6] USA v. Shanu (2023) | Case 1:23-cr-00296-BLW via PACER

Key Takeaways:

- Financial sextortion is the most rapidly growing crime targeting children in the United States, Canada, and Australia.
- Nearly all of this activity is linked to West African cybercriminals known as the Yahoo Boys, who are primarily targeting English-speaking minors and young adults on **Instagram**, **Snapchat**, and **Wizz**.
- The tenfold increase of sextortion cases in the past 18 months is a direct result of the Yahoo Boys distributing sextortion instructional videos and scripts on **TikTok**, **YouTube**, and **Scribd**, enabling and encouraging other criminals to engage in financial sextortion.
- The sextortion criminals are "**bombing**" high schools, youth sports teams, and universities with fake accounts, using advanced **social engineering tactics** to coerce their victims into a compromising situation.
- **Generative Artificial Intelligence** apps are already being used to target minors in a fraction of sextortion-at-scale operations.

These findings enhance our understanding of this emerging cyber threat and pave the way for more effective countermeasures to disrupt these cybercriminals. Additionally, the insights from this analysis form a basis for evidence-based policymaking and the development of prevention and support initiatives for victims.

Financial sextortion is the most rapidly growing crime targeting American, Canadian, and Australian youth.

The Network Contagion Research Institute (NCRI) has observed an exponential increase in sextortion cases targeting minors and youth on social media platforms over the past 18 months. During this period, the FBI reported a 1,000% increase in financial sextortion incidents,[7] while NCMEC reported a 7,200% increase in financial sextortion targeting children from 2021 to 2022.[8] This surge has been characterized by the FBI Director and international partners as a "global crisis that demands everyone's attention" [9]

[7] https://apnews.com/article/fbi-online-sexual-extortion-social-media-michigan-2a1fbfc0568fcb0d67da5474b22909f0
[8] https://www.weprotect.org/global-threat-assessment-23/data/
[9] https://www.fbi.gov/news/press-releases/international-law-enforcement-agencies-issue-joint-warning-about-global-financial-sextortion-crisis

To date, there have been at least 21 youth suicides linked to this sextortion surge—but this figure is likely a significant underreporting, given the shame and fear that prevent many victims from ever telling anyone about the incident.[10] [11]

For comparison, in a 2018 nationwide survey in the United States, 5% of teens had reported being a victim of sextortion online.[12] By the summer of 2023, 51% of Gen Z teens and young adults said they or their friends were catfished in online sextortion scams resulting in their intimate photos being used against them[13]—and half (47%) of respondents said they or their friends had been targeted in the past 3 months.[14]

According to Snapchat internal data, 31% of teens who are approached by a sextortion criminal ultimately share a compromising photo.[15] [16]

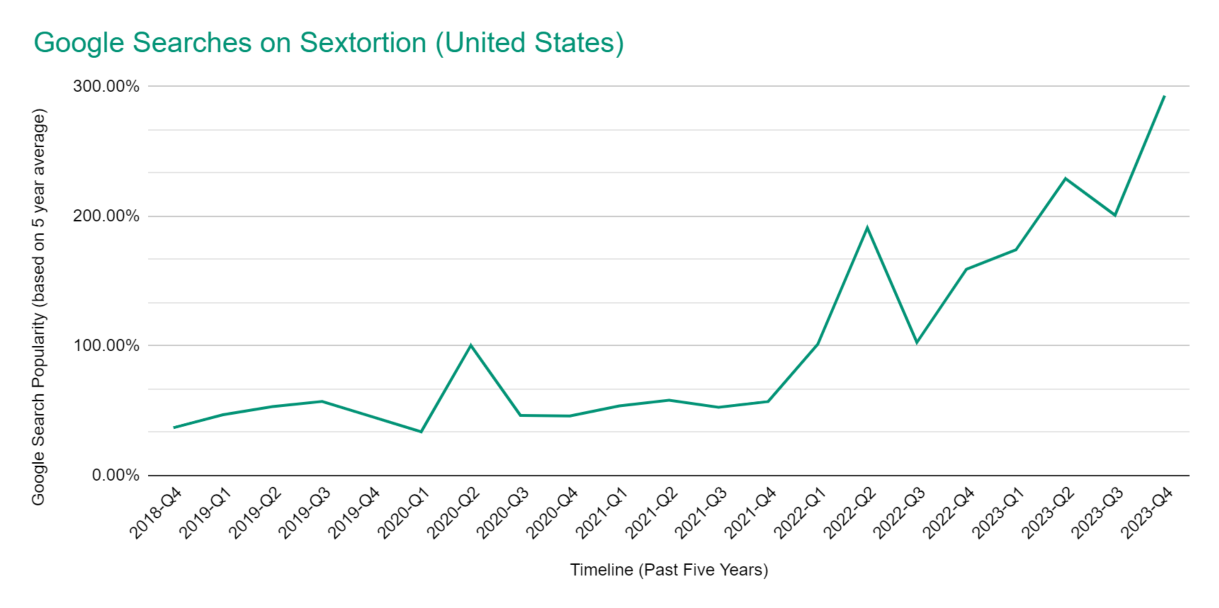
In the **United States**, the Federal Bureau of Investigation (FBI), Homeland Security Investigations (HSI), and the National Center for Missing and Exploited Children (NCMEC) issued a national Public Safety Alert on the “explosion” of sextortion incidents targeting teens.[17] At the time of this writing, NCMEC has received more than 20,000 reports related to financial sextortion.[18]

In **Canada**, the Canadian Centre for Child Protection’s Cybertip program currently receives an average of 50 sextortion reports per week,[19] calling it "an unprecedented volume”[20] and “a public safety emergency.” Several recent tragedies in Canada have sparked renewed calls for child safety regulation on social media platforms. In October 2023, a 12 year old boy in British Columbia died by suicide after being sextorted on Snapchat and Instagram.[21] Another 17 year old from Manitoba died last year only three hours after he was targeted by the sextortion criminal.[22]

In **Australia**, the Federal Police say they've seen sextortion cases grow by 300% in the past year and now receive about 300 complaints per month—although authorities estimate only 1 in 10 victims actually report the crime to police.[23] [24] [25]

[10] https://www.missingkids.org/blog/2023/financial-sextortion-growing-crisis
[11] https://www.cbc.ca/news/canada/british-columbia/police-link-suicide-of-12-year-old-prince-george-b-c-boy-to-online-sexual-extortion-1.7041185
[12] https://journals.sagepub.com/doi/full/10.1177/1079063218800469
[13] https://www.weprotect.org/blog/two-thirds-of-gen-z-targeted-for-online-sextortion-new-snap-research/
[14] https://www.weprotect.org/blog/two-thirds-of-gen-z-targeted-for-online-sextortion-new-snap-research/
[15] https://www.foxbusiness.com/technology/sextortion-schemes-target-two-out-every-three-teens-snap-research-shows
[16] https://www.weprotect.org/blog/two-thirds-of-gen-z-targeted-for-online-sextortion-new-snap-research/
[17] https://www.cbsnews.com/video/financial-sextortion-scams-targeting-teen-boys/
[18] https://www.missingkids.org/blog/2023/financial-sextortion-growing-crisis
[19] https://www.cybertip.ca/en/online-harms/sextortion/
[20] https://www.cbc.ca/news/canada/british-columbia/sextortion-recovery-scams-1.6774652
[21] https://www.cbc.ca/news/canada/british-columbia/police-link-suicide-of-12-year-old-prince-george-b-c-boy-to-online-sexual-extortion-1.7041185
[22] https://www.cbc.ca/news/canada/manitoba/manitoba-sexploitation-suicide-1.6494054
[23] https://www.theguardian.com/australia-news/2023/nov/09/australia-federal-police-facebook-meta-young-people-scams-esafety
[24] https://www.abc.net.au/listen/programs/illawarra-breakfast/helen-schneider/103163730
[25] https://www.abc.net.au/news/2023-10-22/snapchat-extortion-explicit-photo-victim-speaks-out/102932958

It’s worth emphasizing that the percentage of victims who ultimately report the incident to authorities is low, given the shame and fear that many victims experience.[26] These organizations recognize their metrics are likely only the tip of the iceberg. To better understand the larger scale at which financial sextortion is occurring, two additional sources may be examined. The first measure is a surge of Google Searches about sextortion and highly-correlated search inquiries expected of new victims. The second is the exponential growth of the world’s largest sextortion support community.



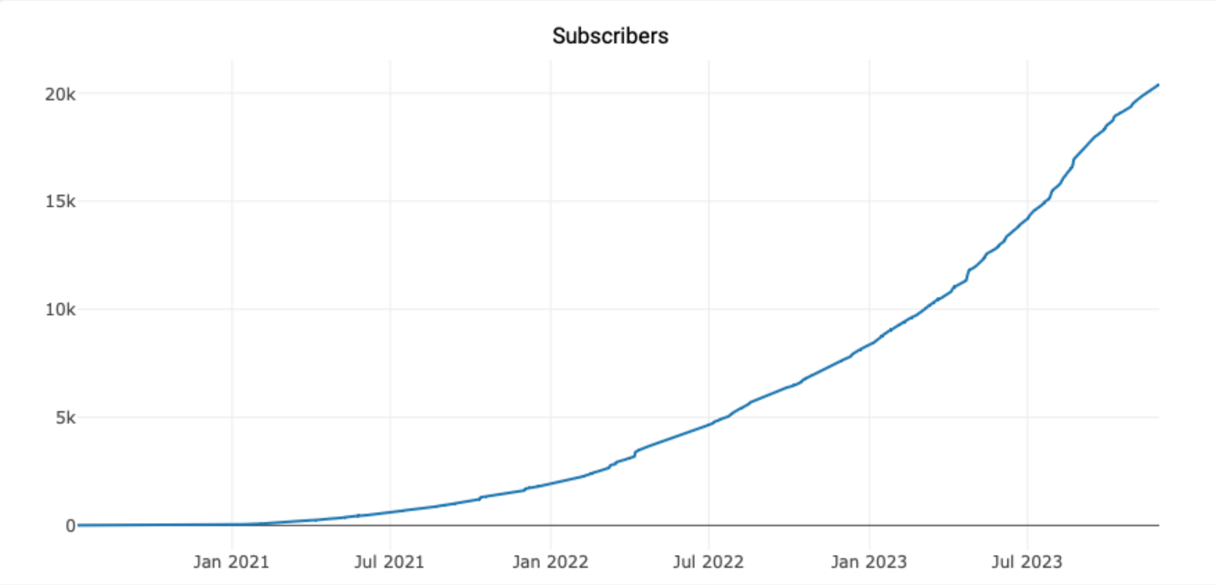
The staggering amount of Google searches related to sextortion is largely driven by new victims seeking help for their situation. Closely related search queries by similar users include “how to delete Instagram account” and “how to report sextortion”.[27]

r/Sextortion is the world’s largest sextortion support forum. This Reddit community was created in February 2020 and, at the time of this report, has more than 20,000 members (subscribers) and surpassed 1 million monthly unique viewers in November 2023.[28] It is now among the Top 5% largest Reddit communities.[29] Members who author posts or comments in the forum are nearly always victims of financial sextortion seeking support or offering advice.[30] The moderated forum creates a safe haven for victims to give and receive support. Its growth highly suggests an exponential growth in victimization rates

[26] https://www.thorn.org/wp-content/uploads/2019/12/Sextortion_Wave2Report_121919.pdf
[27] https://trends.google.com/trends/explore?date=today%205-y&geo=US&q=sextortion&hl=en-US
[28] https://www.reddit.com/r/Sextortion/
[29] Ibid.
[30] https://content.c3p.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf

and the forum provides insight into some of the methods and tactics used by the criminals.

r/Sextortion Growth



r/Sextortion is currently growing at an exponential rate, surpassing 20,000 subscribers in Q4 2023. The community is now viewed by 1 million unique users each month—many of whom are new victims seeking guidance and support.

Instagram, Snapchat, and Wizz are the leading platforms where youth are being targeted by financial sextortion.

According to the most recent NCMEC data, minors are most often victimized by sextortion on the following apps.[31]

- **Instagram** is the most common vector that sextortion criminals use to target their victims. Instagram's design and features make it the most accessible platform for blackmailers to quickly attain personal information about the victim to initiate a successful sextortion attack. Specifically, nearly all financial sextortion attacks on minors involve the screenshotting of the victim's Instagram followers/following lists and using those lists as leverage, threatening to send the victim's intimate

[31] https://www.nbcnews.com/tech/social-media/friend-finding-app-offered-safe-space-teens-sextortion-soon-followed-rcna91172

photos to all these accounts. Unlike Meta's Facebook, where users can opt to make their connections private, Instagram does not offer this privacy safeguard.

- **Snapchat** is most frequently utilized to coerce victims into sending a compromising photo. While the conversation may start on Instagram or Wizz, the criminals usually direct victims to Snapchat to exchange photos. Snapchat is the preferred app by criminals because its design features provide a false sense of security to the victim that their photos will disappear and not be screenshotted. Criminals effectively exploit Snapchat's safety features that are intended to keep users safe, circumventing the screenshot notification feature, and Snapchat's "live photo" indicator despite using a prerecorded video.

- **Wizz** is the third-most prevalent, but fastest rising social media platform for sextortion of minors.[32] This trending app has similar features to Tinder, but is marketed towards children 13+ and has been downloaded 15 million times.[33] In a poll of 500 English-speaking Wizz users, 40% reported being sextorted on Wizz. Among those victims, 77% of them are minors.[34] Some victims report being targeted by sextortion within minutes of joining the app, suggesting that criminals have saturated Wizz.[35] In the Google Play Store and the App Store, dozens of minors have reported that they were coerced into producing self-generated child sexual exploitation material (SG-CSEM) and blackmailed on Wizz[36]—alongside other child safety concerns, including a high frequency of complaints that the app is serving pornographic ads to minors.[37] Wizz is owned by French appmaker Voodoo[38] and does not report incidents of child sexual exploitation on its platform to NCMEC.

These alarming trends and statistics beg the question: what has caused financial sextortion to skyrocket over the past 18 months?

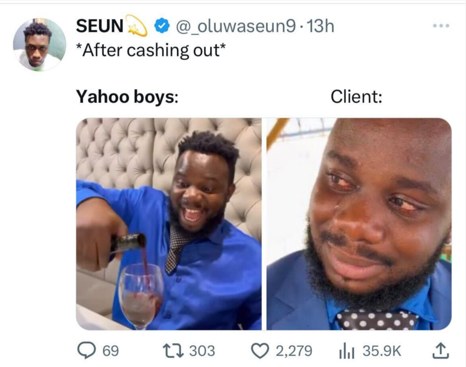
[32] https://www.nbcnews.com/tech/social-media/friend-finding-app-offered-safe-space-teens-sextortion-soon-followed-rcna91172
[33] https://apps.apple.com/us/app/wizz-app-chat-now/id1452906710
[34] https://www.reddit.com/r/Wizz_app/comments/15bt3v1/have_you_been_blackmailed_over_nudes_on_wizz/
[35] https://www.reddit.com/r/Sextortion/comments/18679it/help/
[36] https://play.google.com/store/apps/details?id=info.wizzapp&hl=en&gl=US
[37] https://apps.apple.com/us/app/wizz-app-chat-now/id1452906710
[38] https://www.voodoo.io/apps

West African cybercriminals known as the “Yahoo Boys” are responsible for the surge of the financial sextortion targeting minors on Instagram, Snapchat, and Wizz.

The exponential increase of sextortion cases is driven by the Yahoo Boys, a financially-motivated, distributed group of overseas cybercriminals[39], adopting this tactic as a primary method of financial gain. The Yahoo Boys, nicknamed after their use of Yahoo.com emails to conduct phishing scams decades ago,[40] are a distributed group of cybercriminals, mostly in Nigeria, who have been associated with many online scams.[41] [42] They are the original “Nigerian Princes”, who have shifted in recent years to conduct elderly fraud, fake job scams, romance scams[43]—and now the mass sexual extortion of children for profit.[44]

The Yahoo Boys are a major threat actor, actively targeting youth in the United States, Canada, United Kingdom, Australia, Europe, and elsewhere.[45] The Yahoo Boys openly share their tactics and tradecraft among their social media networks, which has resulted in the alarming uptick in sextortion cases and subsequent suicides.

1.

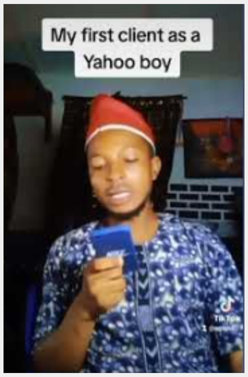


SEUN💫 @_oluwaseun9 · 13h

After cashing out

Yahoo boys: Client:

2.



My first client as a Yahoo boy

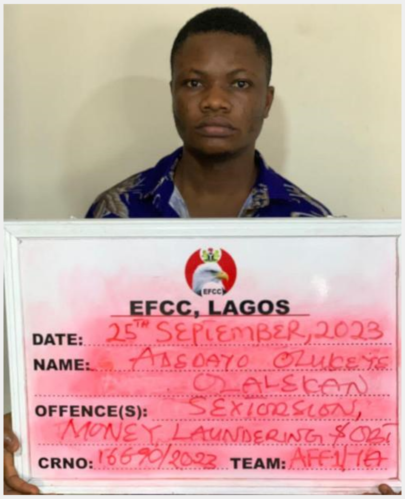
Photo 1 This meme posted on X (formerly Twitter) depicts a representation of a Yahoo Boy and his “client” (victim) after cashing out from a scam.

Photo 2 This TikTok depicts a self-identified Yahoo Boy creating a meme of his experience as a sextortion criminal, and makes reference to blackmailing a “client” (victim) over their nudes.

[39] https://www.proquest.com/docview/1350307576?sourcetype=Scholarly%20Journals
[40] https://therecord.media/for-a-former-yahoo-boy-romance-is-a-cut-and-paste-proposition
[41] https://www.proquest.com/docview/1350307576?sourcetype=Scholarly%20Journals
[42] https://longreads.com/2023/07/11/inside-the-world-of-nigerian-yahoo-boys-atavist-excerpt/
[43] https://www.walshmedicalmedia.com/open-access/narrative-of-illicit-money-yahoo-boy-format-of-cyber-scams-and-governance-challenges-in-africa.pdf
[44] https://www.foxnews.com/us/expert-warns-growing-social-media-sextortion-schemes-targeting-boys
[45] https://www.theguardian.com/australia-news/2023/nov/09/australia-federal-police-facebook-meta-young-people-scams-esafety

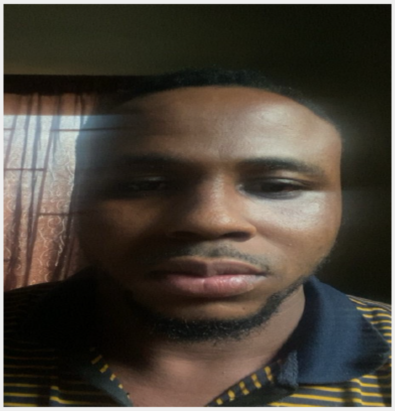
The Yahoo Boy subculture has become a part of the Nigerian internet landscape.[46] These individuals are known for their lavish lifestyles fueled by ill-gotten gains. The subculture is often associated with flaunting wealth, displaying expensive items like cars, designer clothes, and jewelry on social media to showcase their success.[47]

There has been little published about the criminals involved in the current financial sextortion surge. To date, there are only three known indictments of these criminals in court records and public reporting. In August 2023, two Nigerian men were extradited to the United States for sextorting numerous American boys, and causing the death of 17 year old Jordan DeMay[48]; local reporting in Nigeria identified them and four other co-conspirators as Yahoo Boys.[49] In September 2023, Nigeria's Economic and Financial Crimes Commission arrested a man for the sextortion of a 14 year old Canadian boy who died by suicide.[50] Most recently, in November 2023, Olamide Shanu and unidentified co-conspirators in Nigeria, were indicted for receiving more than $2.5 million dollars in Bitcoin transactions amid a large-scale financial sextortion operation.[51]


EFCC
EFCC, LAGOS
DATE: 25TH SEPTEMBER,2023
NAME: ADEDAYO OLUKEYE OLALEKAN
OFFENCE(S): SEXTORTION, MONEY LAUNDERING & OBT
CRNO: 16690/2023 TEAM: AFF1/TA

Olukeye Adedayo Olalekan was arrested in September 2023 for his role in the sextortion of a 14 year old Canadian boy who died by suicide.

In August 2023, three men from Nigeria were extradited to the U.S. for their involvement in sextortion schemes targeting American boys, which led to the death by suicide of 17 year old Jordan DeMay.



Olamide Oladosu Shanu was indicted in November 2023 for his role in a financial sextortion conspiracy that involved more than two million dollars paid by victims.

[46] https://www.researchgate.net/publication/343432593_Social_Values_and_the_Yahooboys'_Subculture_in_Nigeria_Towards_A_Paradigm_Shift_for_National_Value_Re-Orientation

[47] https://www.cybercrimejournal.com/pdf/adebusuyiijccdec2008.pdf

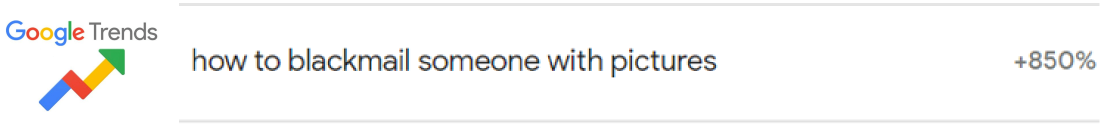
[48] https://www.justice.gov/usao-wdmi/pr/2023_0813_Two_Nigerian_Men_Extradited_To_The_United_States

[49] https://gazettengr.com/sextortion-fbi-hails-efcc-for-nabbing-six-yahoo-boys-tied-to-suicide-of-american-teenager/

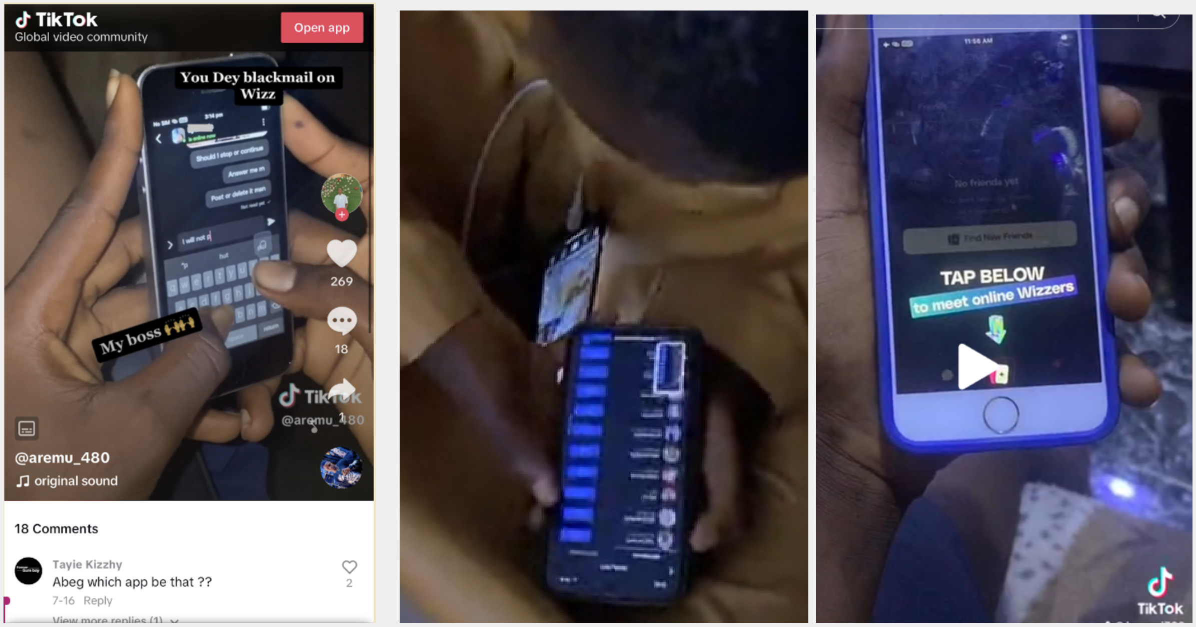
[50] https://www.efcc.gov.ng/efcc/news-and-information/news-release/9496-efcc-arraigns-man-for-alleged-sextortion-in-lagos

[51] USA v. Shanu (2023) | Case 1:23-mj-00258-REP via PACER

According to Google Search Trends in Nigeria, the phrase "how to blackmail someone with pictures" is trending up 850% at the time of this writing.[52]



how to blackmail someone with pictures +850%



18 Comments

Tayie Kizzhy
Abeg which app be that ??
7-16 Reply

Dozens of videos posted to TikTok and YouTube show individuals self-identified as Yahoo Boys actively engaged in sextorting minors on Instagram, Snapchat, and Wizz.

The Yahoo Boys are widely sharing sextortion scripts and instructional videos on TikTok, YouTube, and Scribd, encouraging other criminals to partake in sextortion.

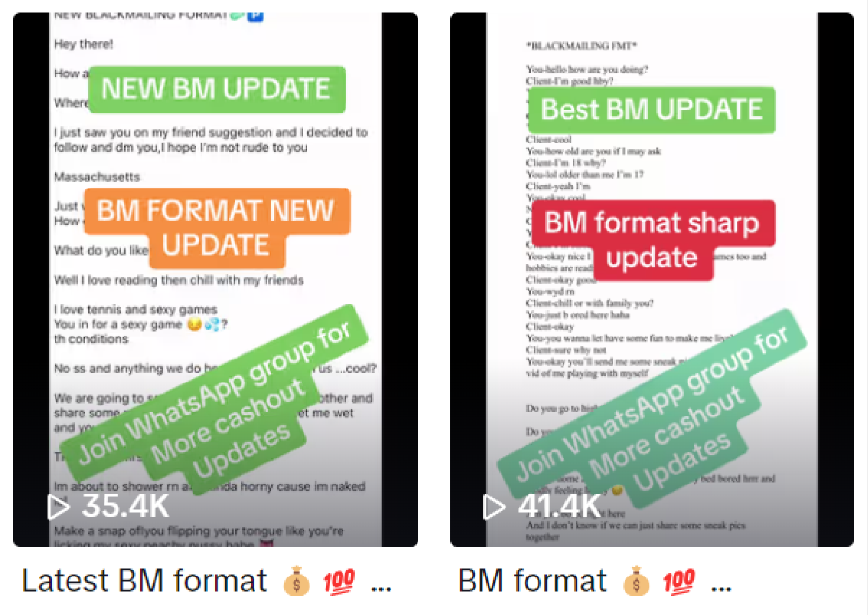
These sextortion scripts have been viewed more than half a million times on **TikTok**, **YouTube**, and **Scribd**. Comments on these videos are filled with criminals eagerly asking to download the sextortion script and tools. Most of the comments on these videos appear to be other from cyber scammers, often commenting in Nigerian Pidgin dialect.

[52] https://trends.google.com/trends/explore?geo=NG&q=how%20to%20blackmail&hl=en-US

These videos and scripts are publicly accessible under the titles “**Blackmail Format**” and “**BM Format**”. These posts often using the tags **#YahooBoys**, **#YahooFormat**, **#YahooUpdates**, and **#ElonMuskBoys** to connect with others within this group.

Yahoo Boys refer to their victims as **“clients”**, a term they use to evade getting banned on social media platforms.

These videos provide detailed instructions and incentives for other cybercriminals to engage in financial sextortion against minors.



NEW BLACKMAILING FORMAT

Hey there!

How a

Where

I just saw you on my friend suggestion and I decided to follow and dm you,I hope I'm not rude to you

Massachusetts

Just
How

What do you like

Well I love reading then chill with my friends

I love tennis and sexy games
You in for a sexy game 😉💦?
th conditions

No ss and anything we do h us ...cool?

We are going to s other and share some et me wet and y

Im about to shower rn a nda horny cause im naked

Make a snap of|you flipping your tongue like you're

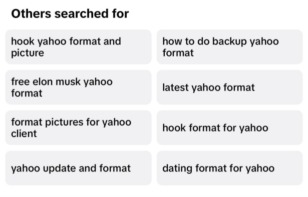
BLACKMAILING FMT

You-hello how are you doing?
Client-I'm good hby?
Client-cool
You-how old are you if I may ask
Client-I'm 18 why?
You-lol older than me I'm 17
Client-yeah I'm
You-okay cool
You-okay nice I ames too and hobbies are read
Client-okay good
You-wyd rn
Client-chill or with family you?
You-just b ored here haha
Client-okay
You-you wanna let have some fun to make me liv
Client-sure why not
You-okay you'll send me some sneak vid of me playing with myself

Do you go to hi

Do y

And I don't know if we can just share some sneak pics together



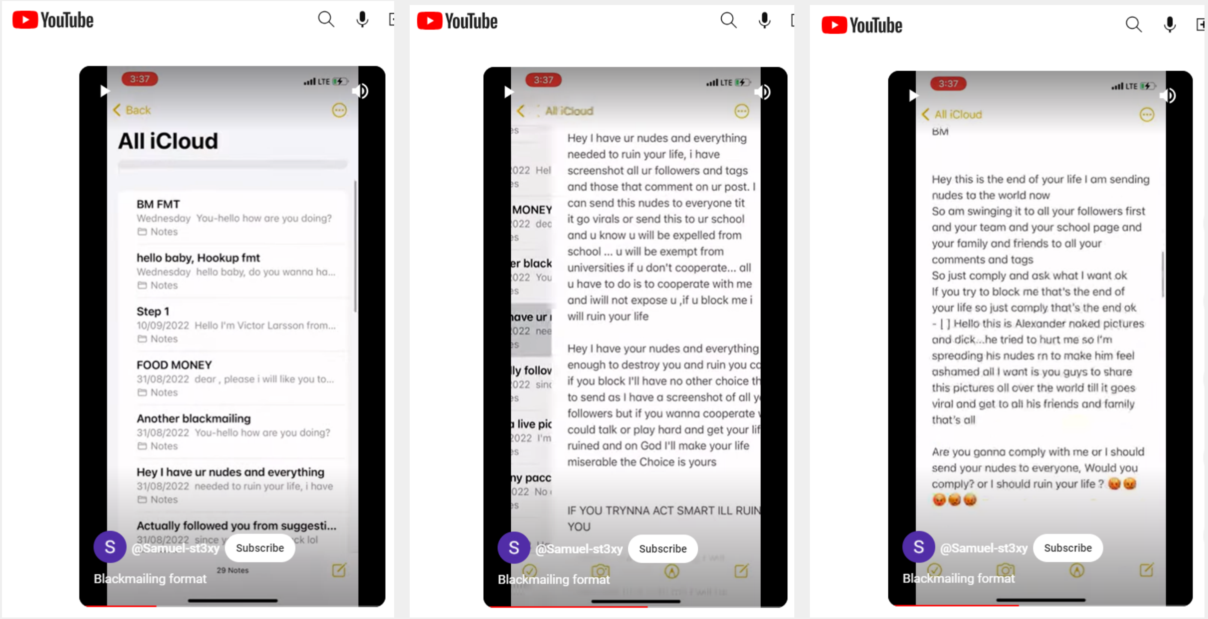
Others searched for

hook yahoo format and picture	how to do backup yahoo format
free elon musk yahoo format	latest yahoo format
format pictures for yahoo client	hook format for yahoo
yahoo update and format	dating format for yahoo

One cybercriminal was selling sextortion manuals and scripts on TikTok, garnering over 75,000 views before the videos were removed following NCRI’s reporting.

Upon viewing this material once, TikTok began to recommend other “Yahoo formats” consisting of various illegal scam methods, materials, and how-to guides.

All sextortion manuals and scripts identified during this investigation were linked to the Yahoo Boys and nearly all accounts commenting on the videos spoke in Nigerian Pidgin, used slang specific to the same region, or were attributable to the region via an examination of their profile.



All iCloud

BM FMT
Wednesday You-hello how are you doing?
Notes

hello baby, Hookup fmt
Wednesday hello baby, do you wanna ha...
Notes

Step 1
10/09/2022 Hello I'm Victor Larsson from...
Notes

FOOD MONEY
31/08/2022 dear , please i will like you to...
Notes

Another blackmailing
31/08/2022 You-hello how are you doing?
Notes

Hey I have ur nudes and everything
31/08/2022 needed to ruin your life, i have
Notes

Actually followed you from suggesti...
31/08/2022 since y ck lol

Hey I have ur nudes and everything needed to ruin your life, i have screenshot all ur followers and tags and those that comment on ur post. I can send this nudes to everyone tit it go virals or send this to ur school and u know u will be expelled from school ... u will be exempt from universities if u don't cooperate... all u have to do is to cooperate with me and iwill not expose u ,if u block me i will ruin your life

Hey I have your nudes and everything enough to destroy you and ruin you co if you block I'll have no other choice th to send as I have a screenshot of all y followers but if you wanna cooperate could talk or play hard and get your lif ruined and on God I'll make your life miserable the Choice is yours

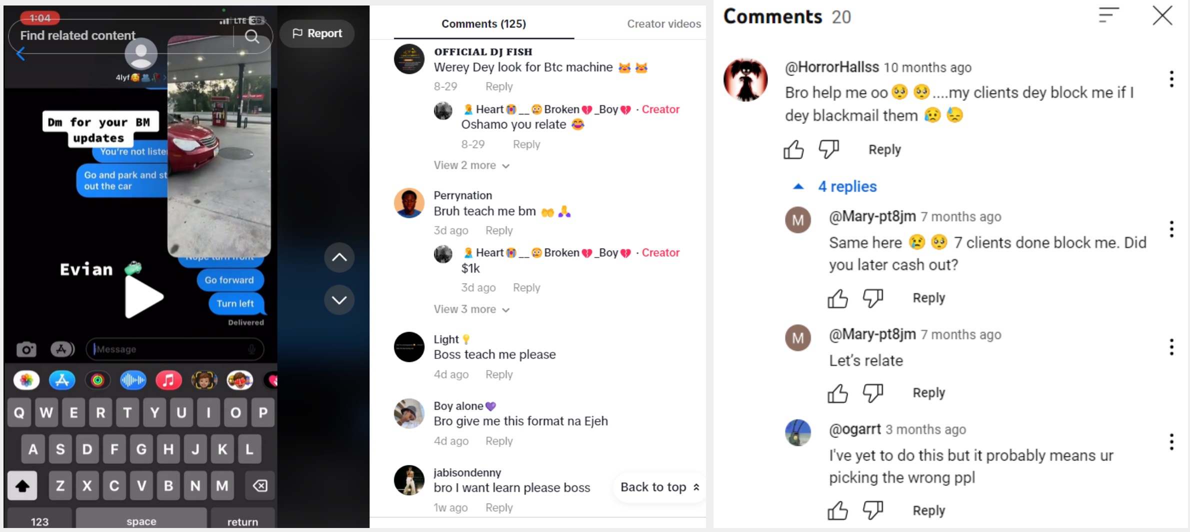
IF YOU TRYNNA ACT SMART ILL RUIN YOU

BM

Hey this is the end of your life I am sending nudes to the world now
So am swinging it to all your followers first and your team and your school page and your family and friends to all your comments and tags
So just comply and ask what I want ok
If you try to block me that's the end of your life so just comply that's the end ok
- [ ] Hello this is Alexander naked pictures and dick...he tried to hurt me so I'm spreading his nudes rn to make him feel ashamed all I want is you guys to share this pictures all over the world till it goes viral and get to all his friends and family that's all

Are you gonna comply with me or I should send your nudes to everyone, Would you comply? or I should ruin your life ? 😡😡😡😡😡

In a series of videos called “Blackmailing format” uploaded to YouTube in September 2022, one cybercriminal shared four sextortion scripts.



You're not liste
Go and park and st out the car
Nope turn front
Go forward
Turn left

OFFICIAL DJ FISH
Werey Dey look for Btc machine 😹😹
8-29 Reply

Heart😭__😢Broken💔_Boy💔 · Creator
Oshamo you relate 😂
8-29 Reply

View 2 more

Perrynation
Bruh teach me bm 👐🙏
3d ago Reply

Heart😭__😢Broken💔_Boy💔 · Creator
$1k
3d ago Reply

View 3 more

Light 💡
Boss teach me please
4d ago Reply

Boy alone💜
Bro give me this format na Ejeh
4d ago Reply

jabisondenny
bro I want learn please boss
1w ago Reply

@HorrorHallss 10 months ago
Bro help me oo 🥺🥺....my clients dey block me if I dey blackmail them 😢😓
Reply

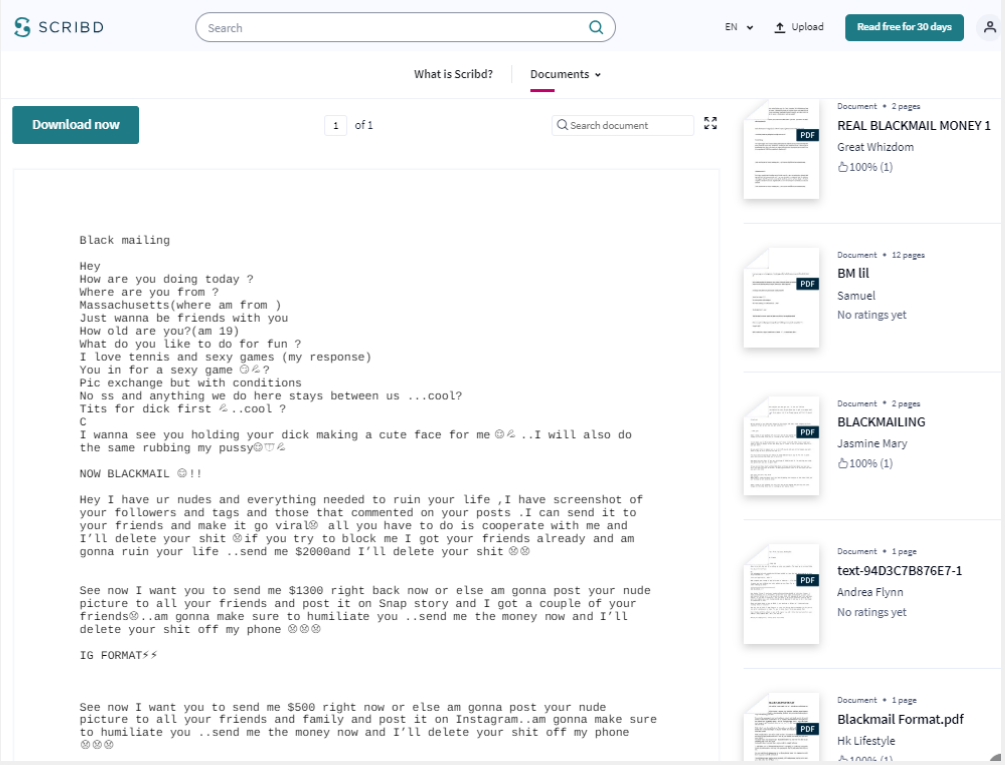
@Mary-pt8jm 7 months ago
Same here 😢🥺 7 clients done block me. Did you later cash out?
Reply

@Mary-pt8jm 7 months ago
Let's relate
Reply

@ogarrt 3 months ago
I've yet to do this but it probably means ur picking the wrong ppl
Reply

The TikTok video on the left shows a sextortion criminal directing his victim to a Bitcoin ATM while requiring the victim to livestream his location; commenters eagerly ask to be taught how to conduct the scam. The comments section of TikTok and YouTube sextortion tutorials serve as a virtual trade show for cybercriminals to share tactics and scam materials.

In addition to video sharing sites like TikTok and YouTube, dozens of sextortion scripts have been shared among cybercriminals using Scribd—a document hosting site. These sextortion scripts have been viewed over 100,000 times in total.



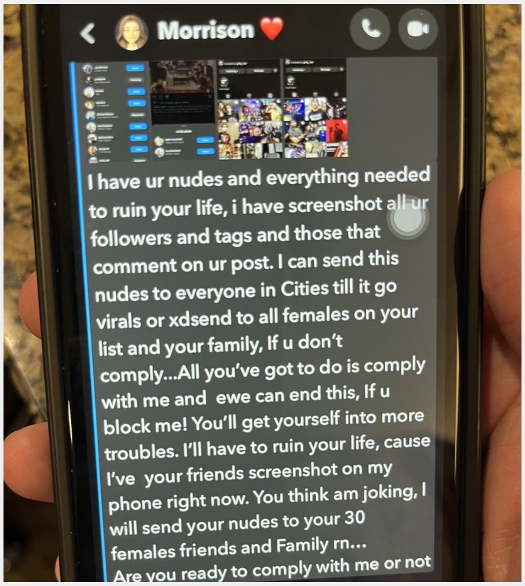
```
Black mailing

Hey
How are you doing today ?
Where are you from ?
Massachusetts(where am from )
Just wanna be friends with you
How old are you?(am 19)
What do you like to do for fun ?
I love tennis and sexy games (my response)
You in for a sexy game 😏💦?
Pic exchange but with conditions
No ss and anything we do here stays between us ...cool?
Tits for dick first 💦..cool ?
C
I wanna see you holding your dick making a cute face for me 😏💦 ..I will also do
the same rubbing my pussy😏👅💦

NOW BLACKMAIL 😏!!

Hey I have ur nudes and everything needed to ruin your life ,I have screenshot of
your followers and tags and those that commented on your posts .I can send it to
your friends and make it go viral😭 all you have to do is cooperate with me and
I'll delete your shit 😭if you try to block me I got your friends already and am
gonna ruin your life ..send me $2000and I'll delete your shit 😭😭


See now I want you to send me $1300 right back now or else am gonna post your nude
picture to all your friends and post it on Snap story and I got a couple of your
friends😭..am gonna make sure to humiliate you ..send me the money now and I'll
delete your shit off my phone 😭😭😭

IG FORMAT⚡⚡



See now I want you to send me $500 right now or else am gonna post your nude
picture to all your friends and family and post it on Instagram..am gonna make sure
to humiliate you ..send me the money now and I'll delete your shit off my phone
😭😭😭
```

Blackmail/sextortion scripts hosted on Scribd are actively being used to target minors.

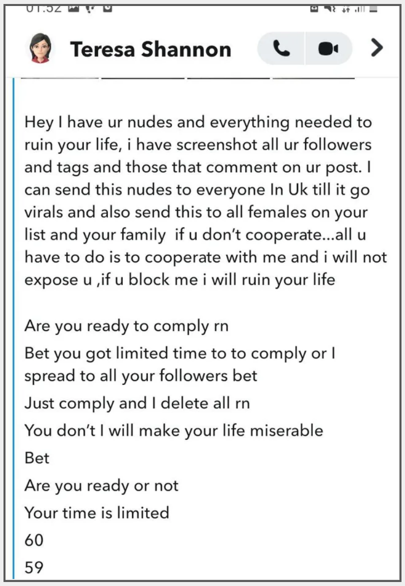
Many of the sextortion attacks happening today use the exact scripts that have been circulated in the Yahoo Boy social media networks shown above. NCRI has observed sextortion criminals actively using these scripts against minors in the United States, Canada, United Kingdom, Australia, and the Netherlands.[53] Victims frequently report receiving the same threatening messages, verbatim, in a sextortion support forum.[54]

Despite the most popular sextortion scripts being publicly accessible since 2021, their text has not yet been blacklisted by Instagram, Wizz, or Snapchat—as these scripts are actively being used today against victims. USA v. Shanu court filings show these exact materials being used against minors.[55]

[53] https://www.reddit.com/r/Sextortion/
[54] https://www.reddit.com/r/Sextortion/
[55] USA v. Shanu (2023) | Case 1:23-mj-00258-REP via PACER



I have ur nudes and everything needed to ruin your life, i have screenshot all ur followers and tags and those that comment on ur post. I can send this nudes to everyone in Cities till it go virals or xdsend to all females on your list and your family, If u don't comply...All you've got to do is comply with me and ewe can end this, If u block me! You'll get yourself into more troubles. I'll have to ruin your life, cause I've your friends screenshot on my phone right now. You think am joking, I will send your nudes to your 30 females friends and Family rn...
Are you ready to comply with me or not



Hey I have ur nudes and everything needed to ruin your life, i have screenshot all ur followers and tags and those that comment on ur post. I can send this nudes to everyone In Uk till it go virals and also send this to all females on your list and your family if u don't cooperate...all u have to do is to cooperate with me and i will not expose u ,if u block me i will ruin your life

Are you ready to comply rn

Bet you got limited time to to comply or I spread to all your followers bet

Just comply and I delete all rn

You don't I will make your life miserable

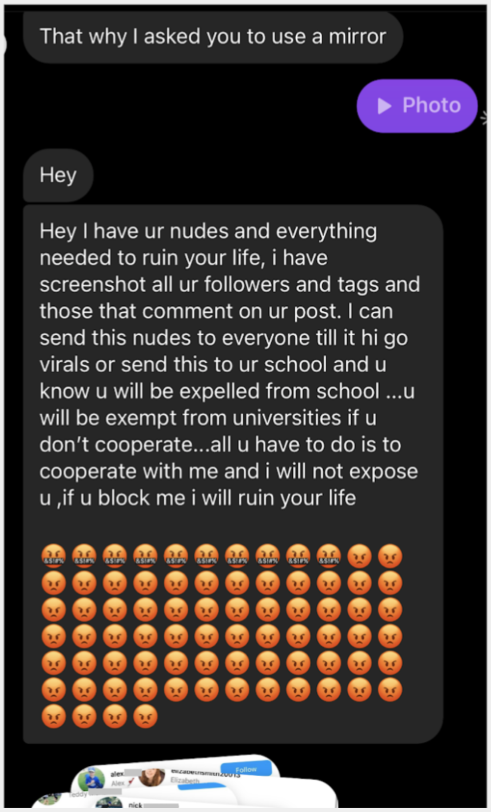
Bet

Are you ready or not

Your time is limited

60

59

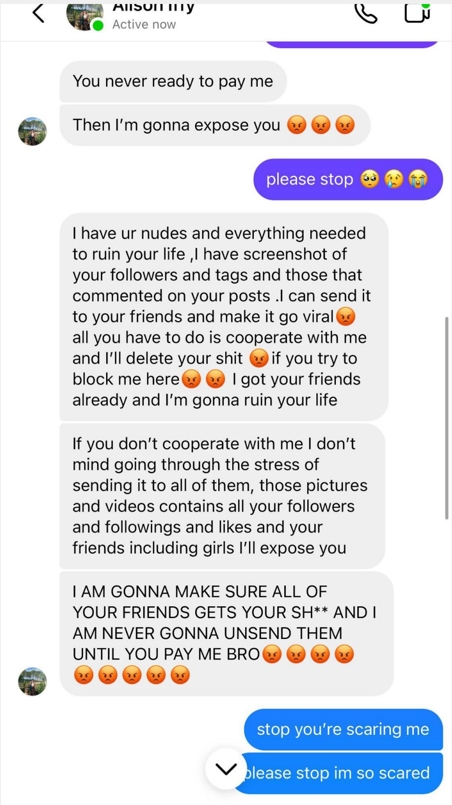


That why I asked you to use a mirror

Hey

Hey I have ur nudes and everything needed to ruin your life, i have screenshot all ur followers and tags and those that comment on ur post. I can send this nudes to everyone till it hi go virals or send this to ur school and u know u will be expelled from school ...u will be exempt from universities if u don't cooperate...all u have to do is to cooperate with me and i will not expose u ,if u block me i will ruin your life

🤬🤬🤬🤬🤬🤬🤬🤬🤬🤬😡😡
😡😡😡😡😡😡😡😡😡😡😡😡
😡😡😡😡😡😡😡😡😡😡😡😡
😡😡😡😡😡😡😡😡😡😡😡😡
😡😡😡😡😡😡😡😡😡😡😡😡
😡😡😡😡😡😡😡😡😡😡😡😡
😡😡😡😡



You never ready to pay me

Then I'm gonna expose you 😡😡😡

please stop 🥺😢😭

I have ur nudes and everything needed to ruin your life ,I have screenshot of your followers and tags and those that commented on your posts .I can send it to your friends and make it go viral😡 all you have to do is cooperate with me and I'll delete your shit 😡if you try to block me here😡 😡 I got your friends already and I'm gonna ruin your life

If you don't cooperate with me I don't mind going through the stress of sending it to all of them, those pictures and videos contains all your followers and followings and likes and your friends including girls I'll expose you

I AM GONNA MAKE SURE ALL OF YOUR FRIENDS GETS YOUR SH** AND I AM NEVER GONNA UNSEND THEM UNTIL YOU PAY ME BRO😡😡😡😡😡😡😡😡😡

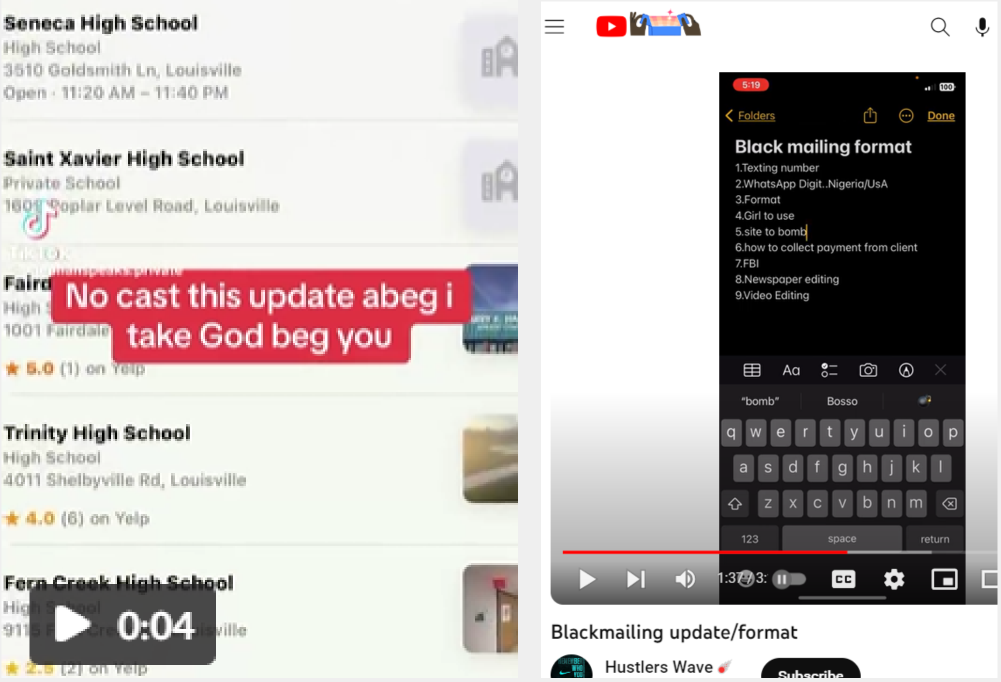
stop you're scaring me

please stop im so scared

Victims share their experiences in r/Sextortion, a community support forum. The same sextortion scripts that have been circulating in Yahoo Boy social media networks are actively being used against minors at massive scale on Instagram, Wizz, and Snapchat.

The sextortion criminals are “**bombing**” high schools, sports teams, and universities with fake accounts, using advanced **social engineering tactics** to coerce their victims into a compromising situation.

The sextortion guides on TikTok and YouTube provide step-by-step instructions to create convincing fake social media profiles and how to “**bomb**” high schools and sports teams.[56] The Yahoo Boys use this term to describe friending/following as many people in a school or target location as possible.[57] In many cases of sextortion, the victim believes the individual is potentially an unknown classmate or someone of the same age from a neighboring town. For example, the criminal who drove 15 year old Riley Basford to suicide in 2021 had fifteen mutual followers.[58]



Seneca High School
High School
3510 Goldsmith Ln, Louisville
Open · 11:20 AM – 11:40 PM

Saint Xavier High School
Private School
1609 Poplar Level Road, Louisville

Faird
High
1001 Fairdale
★ 5.0 (1) on Yelp

No cast this update abeg i take God beg you

Trinity High School
High School
4011 Shelbyville Rd, Louisville
★ 4.0 (6) on Yelp

Fern Creek High School
High School
9115 Fern Creek ... Louisville
★ 2.5 (2) on Yelp

Black mailing format
1.Texting number
2.WhatsApp Digit..Nigeria/UsA
3.Format
4.Girl to use
5.site to bomb
6.how to collect payment from client
7.FBI
8.Newspaper editing
9.Video Editing

Blackmailing update/format

Sextortion “formats” are detailed how-to guides that are shared among Yahoo Boy cybercriminals on TikTok and YouTube. They provide step-by-step instructions on how to create fake accounts, obtain a texting number, how to target victims with the scam, and cash out. They show how criminals should target high schools and also provide instruction on threats to use against the victims.

[56] https://sports.yahoo.com/rugby-players-among-athletes-becoming-201540323.html
[57] https://journalasap.org/index.php/asap/article/view/26/28
[58] https://www.insideedition.com/15-year-old-takes-his-own-life-after-falling-victim-to-internet-blackmailing-ploy-family-says-66294

Tactics, Techniques & Procedures

The numerous sextortion how-to guides on TikTok, YouTube, and Scribd direct the criminals through the steps to conduct a successful financial sextortion operation.

The criminals exploit the **platform design** and **features** of three major applications where they have unfettered access to youth. When their accounts are banned, they buy or create new accounts with impunity and/or factory reset their phones to evade app bans.

Instagram

- The criminals “bomb” high schools, sports teams, and other youth groups with follow requests in order to appear to have many mutual friends with their targets.
- The moment an Instagram user accepts the follow request of a scam account, their follower/following list is compromised. This gives criminals easy access to the target’s followers and following lists to use as blackmail, threatening to send the compromising photos to all these acquaintances. With Instagram’s current configuration, users have no way to protect themselves against their followers and following lists being copied the instant they accept a follow request.

Snapchat

- Sextortion criminals often exploit Snapchat to send pre-recorded videos of attractive females as “live” snaps (purple/red icons). Generally, pre-recorded videos and photos are shared with a blue icon. This feature exploitation gives victims a false sense of security that the Snaps they are receiving are real-time images.
- Criminals are also able to bypass the Snapchat feature that notifies users when a screenshot has been taken of their Snaps. In the absence of this notification, victims believe their images have not been screen-recorded or screenshotted.
- Additionally, Snap Scores are perceived by victims as an indicator of authentic account activity. The higher the Snap Score, the more history the account has on the platform. Criminals are inflating Snap Scores on their accounts using bot activity, automated scripts[59], and using hacked accounts with preexisting Snap Scores in order to appear as an authentic profile.[60]

Wizz

- Victims have reported being targeted nearly immediately upon account creation (in some cases within ten minutes),[61] suggesting the platform is saturated by sextortion activity.

[59] https://github.com/useragents/Snapchat-Snapscore-Botter

[60] https://content.c3p.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf

[61] https://www.reddit.com/r/Sextortion/comments/18679it/help/

- In order to reach as wide an audience as possible, cybercriminals are using two methods to “match” with thousands of potential targets. First, Wizz users can boost their profile for a small fee. Second, criminals employ the use of VPNs to spoof their location to numerous target regions.

Social Engineering

These criminals and their catfish accounts are extremely manipulative and convincing. According to Snapchat’s internal data, approximately one third of the youth who engage with a sextortion criminal end up sending a compromising photo, resulting in a blackmail incident.[62]

In order to wield extremely convincing catfish accounts, the criminals are often using stolen and hacked Instagram accounts, which give the appearance of an authentic profile, also known as “aged” accounts. They have a history of authentic activity, posts, followers, and other characteristics that make detecting the catfish profile much more difficult. Aged accounts also bypass a number of moderation and safety controls, while newly created accounts appear more likely to be taken down when reported.

After establishing contact with a target, sextortion criminals use established techniques, operating under false pretenses and employing sophisticated emergent technologies including generative AI, to coerce victims, many of whom are underage, to share nude photos of themselves in compromising situations.

To conduct the sextortion scam, criminals tend to use files of amateur, self-produced imagery, sometimes stolen or bought from OnlyFans models, adding to the apparent authenticity of the account.

Extreme Threats & Coercion

Immediately after a victim shares an explicit photo, their extortionist uses an established script that is shared widely among Yahoo Boys on social media. This script takes advantage of a victim’s embarrassment at the threat of exposure of their explicit photo(s). Oftentimes, these scripts include extreme threats and coercion:[63]

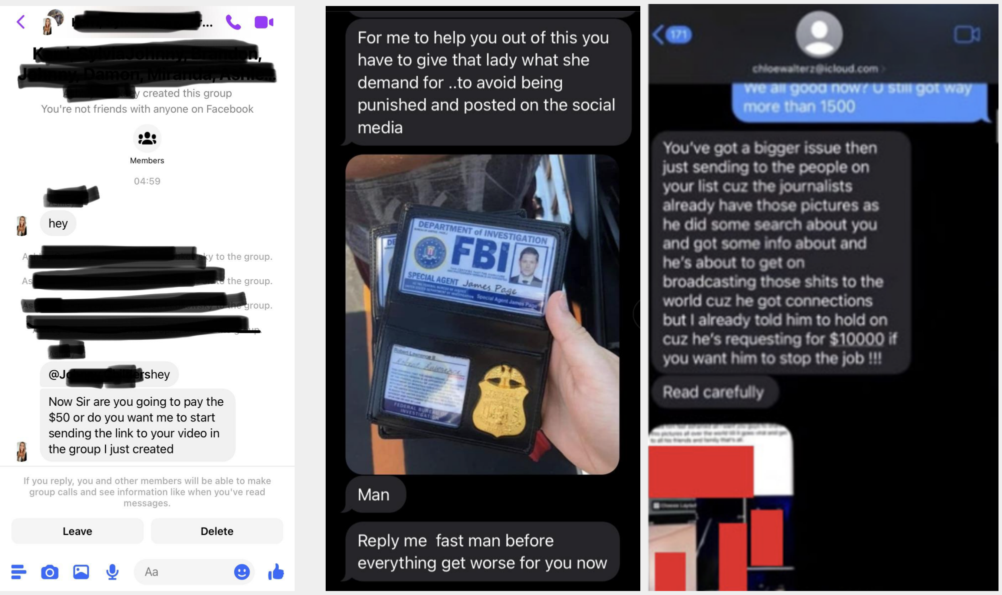
- Sharing screenshots of a victim’s Instagram followers and following lists to establish that the criminal can share the photos with all the individuals in the victim’s social network.
- Sending screenshots of draft messages to the victim’s friends or family.
- Claiming that they will frame the victim for sending nude pictures to a child.
- Creating a “wanted” posted with the victim’s nude images, name, and number.

[62] https://www.foxbusiness.com/technology/sextortion-schemes-target-two-out-every-three-teens-snap-research-shows
[63] https://content.c3p.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf

- Threatening that the photos being shared will result in the victim being expelled from school, exposed to criminal action, unable to attend college, or that their parents will be fired from their jobs.
- The criminals sometimes begin sending the photos to Instagram group chats with the victim and some of the victim's contacts. Since the victim is in this group chat, the criminal tries to persuade payment in order to un-send the photos before others see the message.

Aggressive Cyber Stalking Tactics

Sextortion criminals also employ ruthless tactics amounting to cyber stalking.[64] They use multiple accounts to continually harass victims on social media. They barrage victims with incessant texts and iMessages from many different phone numbers. On occasion, criminals will contact friends and family members, asking to be put in contact with the victim. Data aggregators and people databases are common tools of the sextortion criminals. They search these databases to find their victims' address, photos of their home, their relatives and known associates, and sometimes their phone numbers. These elements intensify the threats against victims. Sometimes the schemes involve a different phone number, pretending to be law enforcement, offering to "settle" the case with a monetary sum. In some cases, this harassment can continue for months.



[redacted]...

[redacted]

[redacted] created this group

You're not friends with anyone on Facebook

Members

04:59

[redacted]

hey

[redacted]

@J[redacted]shey

Now Sir are you going to pay the $50 or do you want me to start sending the link to your video in the group I just created

If you reply, you and other members will be able to make group calls and see information like when you've read messages.

For me to help you out of this you have to give that lady what she demand for ..to avoid being punished and posted on the social media

Man

Reply me fast man before everything get worse for you now

chloewalterz@icloud.com

We all good now? U still got way more than 1500

You've got a bigger issue then just sending to the people on your list cuz the journalists already have those pictures as he did some search about you and got some info about and he's about to get on broadcasting those shits to the world cuz he got connections but I already told him to hold on cuz he's requesting for $10000 if you want him to stop the job !!!

Read carefully

[redacted]

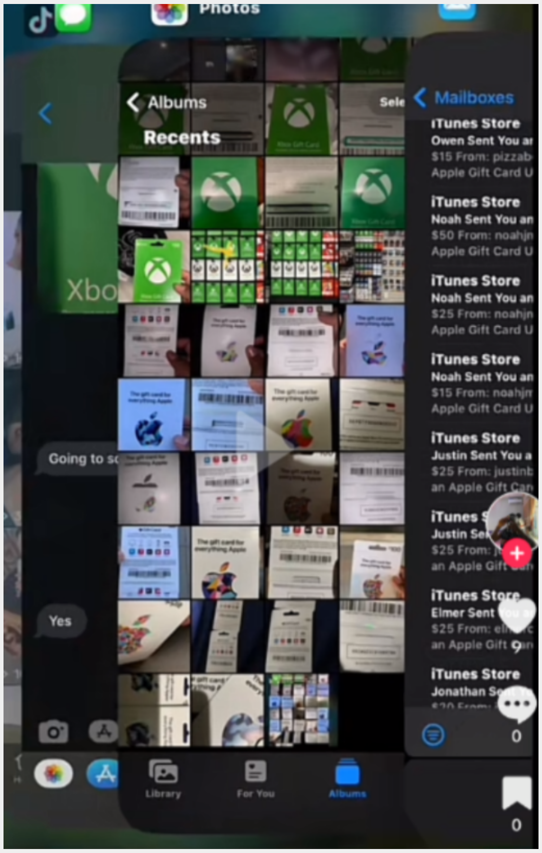
Sextortion criminals threaten to expose illicit photos in group chats made with victims' family members or friends. They also operate under false pretenses, sometimes posing as law enforcement agents or journalists.

[64] USA v. Shanu (2023) | Case 1:23-mj-00258-REP via PACER

Payments in Perpetuity

Sextortion criminals often start with a single demand: "pay me now and the photos will be deleted." However, if the victim pays, the photos aren't deleted and the criminals continue to demand multiple payments over an extended period. This is why the prevailing guidance from law enforcement is to immediately block the criminal and do not pay.

If the victim pays, it's common for victims to be put on scheduled payment plans with a ransom payment due weekly or monthly.[65]



iTunes Store
Owen Sent You ar
$15 From: pizzab
Apple Gift Card U

iTunes Store
Noah Sent You an
$50 From: noahjn
Apple Gift Card U

iTunes Store
Noah Sent You an
$25 From: noahjn
Apple Gift Card U

iTunes Store
Noah Sent You an
$15 From: noahjn
Apple Gift Card U

iTunes Store
Justin Sent You a
$25 From: justinb
an Apple Gift Car

iTunes S
Justin Se
$25 From:
an Apple Gift

iTunes Store
Elmer Sent
$25 From: el
an Apple Gift

iTunes Store
Jonathan S

Sextortion criminals often ask victims to purchase gift cards or make payments via Cashapp, Venmo, iTunes, Steam, or gift cards.[66]

[65] USA v. Shanu (2023) | Case 1:23-mj-00258-REP via PACER
[66] https://protectchildren.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf

Victims as Forced Accomplices, Money Mules & Account Creators

If victims cannot afford payments, the criminals often request victims to hand over their social media accounts or create new accounts for the criminal to use in the furtherance of the scam.

The NCRI has also observed that sextortion criminals sometimes demand that victims create fraudulent accounts on websites like Login.gov and IRS.gov, in the furtherance of other fraudulent activity.

U.S. citizens are used as intermediaries, or 'money mules', to transfer funds to sextortion criminals.[67] Victims have been coerced into acting as money mules facilitating layered transactions, receiving funds from victims and then passing them on to other members of the criminal network. The schemes extensively use peer-to-peer (P2P) payment apps like Venmo and Cashapp, along with gift cards, for initial fund transfers. Cryptocurrency is also often used.[68]

> Artificial Intelligence and deepfake nude apps are already being used to target minors in widespread financial sextortion-at-scale operations.

Generative artificial intelligence ("AI") software is already being used to conduct a growing number of the financial sextortion-at-scale attacks against minors, and the likelihood of abuse will become considerably greater in coming months as generative AI technologies become more realistic and convincing.[69]

There are two distinct methods by which AI is being used in sextortion operations:

1. To generate artificial nude photos of someone, through which to extort payment
2. To create more convincing "catfish" profiles than ever before

AI Generated Nude Photos of Non-Consenting Victims for Sextortion

In this newest variant of the sextortion scam, the cybercriminals don't need to coerce the victim to share a compromising photo. All the criminal needs is a fully clothed photograph from Instagram and a clothes-removing AI app to initiate their extortion attack.[70] The

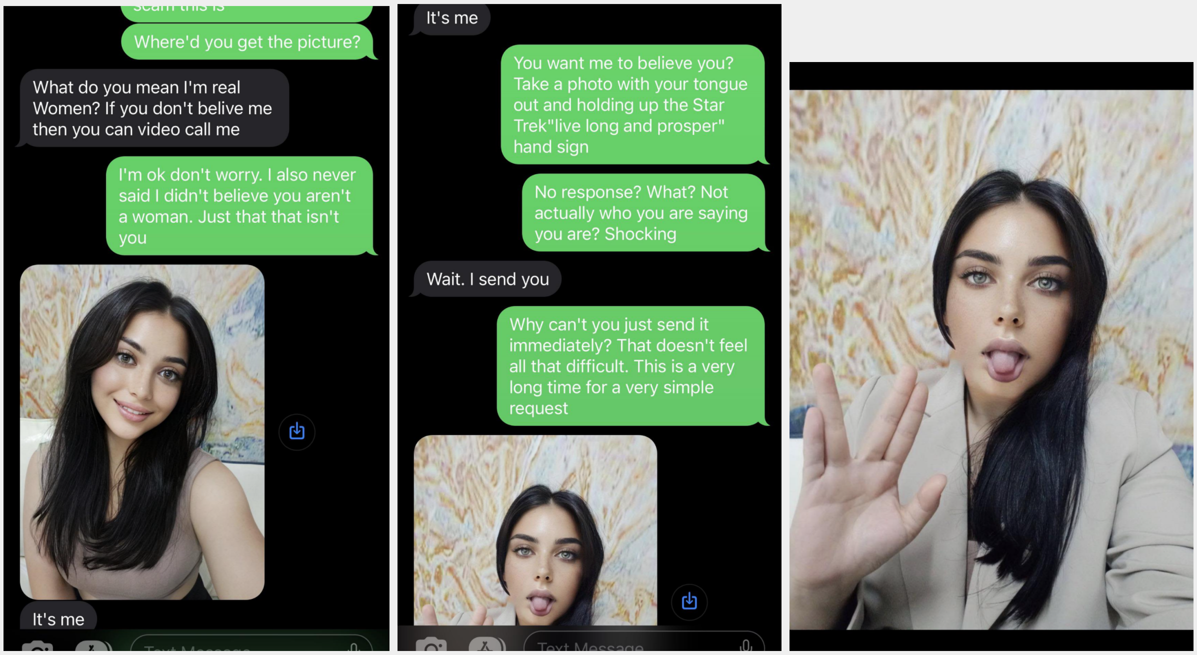
[67] USA v. Shanu (2023) | Case 1:23-mj-00258-REP via PACER
[68] USA v. Shanu (2023) | Case 1:23-cr-00296-BLW via PACER
[69] https://www.ic3.gov/Media/Y2023/PSA230605
[70] https://www.iwf.org.uk/media/q4zll2ya/iwf-ai-csam-report_public-oct23v1.pdf

tactics remain the same: the criminal threatens to share the photo with the victim's friends and family, often with an embarrassing accusation, to entice payment.

In June 2023, the FBI published a warning that sextortion criminals manipulate benign photographs or videos to target victims using synthetic images (deepfakes) to extort payment.[71] In the month of October 2022, Crime Stoppers Houston received at least eight reports from Houston-area moms with teenage boys who were targeted with AI generated nude photos of themselves.[72]

There are numerous AI apps, websites, and services that 'nudify' images, generating explicit interpretations of clothed individuals and these apps and services are proliferating across criminal networks.[73] With the growing accessibility of these apps paired with the lack of meaningful safeguards from non-consensual imagery, they are an effective tool for cybercriminals to exploit victims without ever needing to receive a compromising photograph.[74]

AI-Enhanced Catfish Profiles



scam this is

Where'd you get the picture?

What do you mean I'm real Women? If you don't belive me then you can video call me

I'm ok don't worry. I also never said I didn't believe you aren't a woman. Just that that isn't you

It's me

It's me

You want me to believe you? Take a photo with your tongue out and holding up the Star Trek"live long and prosper" hand sign

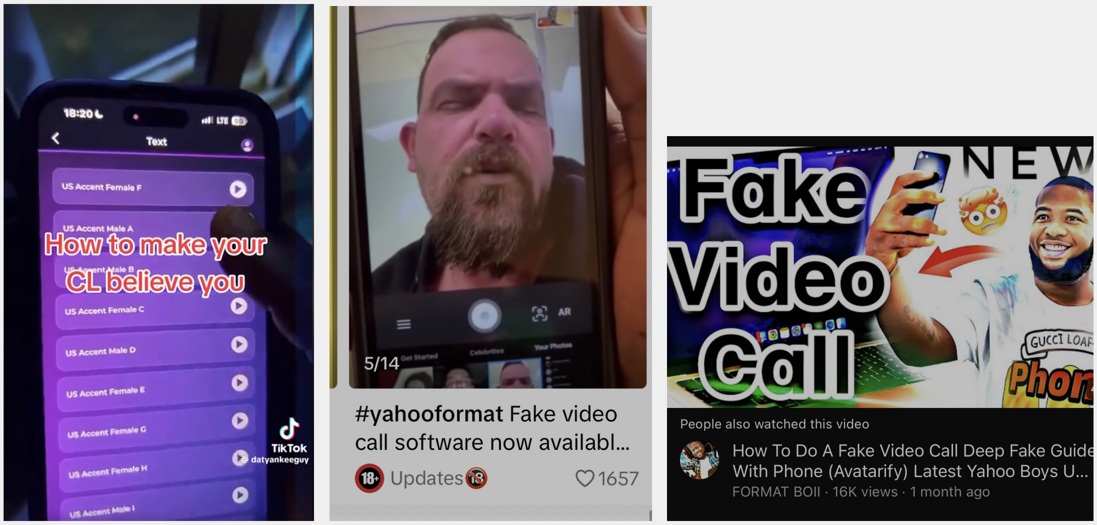
No response? What? Not actually who you are saying you are? Shocking

Wait. I send you

Why can't you just send it immediately? That doesn't feel all that difficult. This is a very long time for a very simple request

This conversation between a cybercriminal and a potential victim shows how criminals are effectively using generative AI tools to manipulate photographs to falsely show “proof of life”, resulting in a convincing catfish.

[71] https://www.ic3.gov/Media/Y2023/PSA230605
[72] https://www.khou.com/article/news/local/houston-kids-online-sextortion-photos/285-3f18171a-3a2d-47c3-a86f-d34d47416425
[73] https://www.iwf.org.uk/media/q4zll2ya/iwf-ai-csam-report_public-oct23v1.pdf
[74] https://www.graphika.com/reports/a-revealing-picture


US Accent Female F
US Accent Male A
How to make your CL believe you
US Accent Male B
US Accent Female C
US Accent Male D
US Accent Female E
US Accent Female G
US Accent Female H
US Accent Male I
TikTok
datyankeeguy
5/14
#yahooformat Fake video call software now availabl...
Updates
1657
Fake Video Call
NEW
People also watched this video
How To Do A Fake Video Call Deep Fake Guide With Phone (Avatarify) Latest Yahoo Boys U...
FORMAT BOII · 16K views · 1 month ago

Numerous videos posted to Yahoo Boy networks on TikTok and YouTube provide instruction about how to exploit AI tools to conduct sextortion and other scams, specifically how to use real-time face swapping software, voice-changers, and using pre-recorded video calls to communicate with their victims.

In light of the escalating use of generative AI in perpetrating financial sextortion, urgent attention and proactive measures are imperative. The documented instances of AI's application in creating deceitful profiles and manipulating multimedia for fraudulent activities are alarming. As these technologies advance, the risk of exploitation amplifies, potentially causing irreparable harm to vulnerable individuals. Mitigating this threat demands a multi-faceted approach encompassing stringent regulation, heightened cybersecurity awareness, and the collaboration of tech platforms to curb the misuse of AI tools. The responsibility falls on both policymakers and technology innovators to proactively address these challenges to safeguard individuals, especially minors, from falling victim to these increasingly sophisticated and damaging cybercrimes.

Outlook

This research has shed light on the factors contributing to the alarming rise in sextortion cases. By delving into the methods employed by criminal entities and unraveling the profound scale and impact on victims, this study has laid a foundation for effective countermeasures to disrupt this crime. The insights garnered here are pivotal in crafting effective strategies and evidence-based policies aimed at preventing and combating sextortion. Moreover, by dissecting the tactics utilized by criminals, this report underscores the importance of enhanced detection, mitigation, and adjudication of these incidents. Ultimately, this research has focused on understanding how social media features have been exploited by sextortion criminals, shedding light on safety controls and privacy issues. To mitigate this emergent threat, stakeholders in civil society and technology must strive to mitigate the vulnerabilities and misuse of these platforms, offering a pathway towards a safer online landscape.

Recommendations

Recommendations to Social Media Platforms

1. **Instagram should give users the option to set their Followers and Following lists to Private, and set all minors' Followers and Following lists to private by default.**

   One common factor in nearly all sextortion cases reviewed by the NCRI was the cybercriminals' consistent use of the victim's Instagram Followers and Following lists. Using these screenshotted lists, criminals exert immense leverage on victims, threatening to send the material to all of their friends, family, and connections.

   Unlike Meta's other social network, Facebook, Instagram users cannot make their connections private. Because Instagram users cannot make their Followers and Following lists private, extorters have easy access to other users connected to their victim, and the opportunity to craft their accounts to appear more authentic by establishing mutual connections.[75]

   Instagram can mitigate a vast majority of financial sextortion cases by hiding minors' Followers and Following lists on their platform by default,[76] and by giving all users the option to make these lists private. This setting should be decoupled from the setting to make your Instagram photos public or private.

2. **Instagram and Wizz should improve the in-app reporting process to quickly and effectively ban sextortion accounts.**

   In early 2023, Snapchat created a distinct reporting category for sextortion.[77] Instagram, Wizz, and other platforms where financial sextortion occurs should follow suit and ensure that all reports of sextortion are adjudicated by a human

[75] https://protectchildren.ca/en/resources-research/an-analysis-of-financial-sextortion-victim-posts-published-on-sextortion/
[76] https://content.c3p.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf
[77] https://www.weprotect.org/blog/two-thirds-of-gen-z-targeted-for-online-sextortion-new-snap-research/

moderator within hours. Victims have repeatedly suggested that Instagram took no action on reports made against sextortion accounts.[78]

3. **Instagram and Snapchat should proactively detect the sextortion scripts and investigate any users who attempt to use them.**

   Identical scripts are being repeatedly deployed at scale on Instagram, Snapchat, and Wizz by accounts linked to sextortion. Identification and detection of these sextortion scripts in real-time should be a high priority for content moderators.

4. **TikTok, YouTube, and Scribd must take down the sextortion how-to guides, materials, and scripts that they are hosting.**

   TikTok, YouTube, and Scribd must moderate their platforms to remove manuals and tools that are actively used to blackmail, extort, and scam victims. Each of these platforms hosts sextortion material and scripts, garnering hundreds of thousands of views. This material has been subsequently used in countless sextortion schemes against minors.[79]

5. **Instagram and Snapchat should improve their detections of Account Takeovers and Sextortion behaviors.**

   Cybercriminals are known to use account takeovers on Snapchat and Instagram to more effectively socially engineer their targets and to evade bans. These platforms should prioritize elimination of illegally acquired accounts and the creation of robust security measures to prevent further account takeovers. For example, both platforms can improve detections by tracking significant upticks in account activity after account details are altered (indicative of an account takeover). They should also detect significant upticks in account activity after a first-time login from either a VPN or an elevated-risk geographical location. Instagram, Snapchat, and other platforms should improve coordination within established organizations, such as the Tech Coalition, to share indicators of sextortion, IP addresses, usernames, and other intelligence.

6. **Wizz, and its Paris-based parent company Voodoo, must take immediate action to secure the platform from endemic sextortion.**

   Sextortion on Wizz is pervasive and dangerous. The app's design, seemingly akin to a Tinder-like interface for minors, has fostered an environment ripe for the rampant spread of sextortion.[80] The absence of robust security protocols to thwart

[78] https://content.c3p.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf
[79] USA v. Shanu (2023) | Case 1:23-mj-00258-REP via PACER
[80] https://www.reddit.com/r/Wizz_app/comments/15bt3v1/have_you_been_blackmailed_over_nudes_on_wizz/

the creation of new sextortion accounts, coupled with the platform's inability to effectively identify such schemes or adequately moderate existing sextortion-linked profiles, creates an inherently risky environment for minors.[81] The growth of Wizz presents significant challenges to controlling the propagation of sextortion schemes, necessitating urgent action to safeguard users, especially minors.[82]

7. **The App Store and Google Play Store should enforce their store policies with regards to Wizz, as it remains a pervasive child safety risk beyond sextortion.**

The App Store and Google Play Store should monitor and take action on app reviews of children being sexually exploited on Wizz and other apps. Dozens of parents and children post reviews of their experience being sextorted on Wizz in the App Store[83] and Google Play Store.[84]

Beyond the pervasive sextortion problem on Wizz, the app appears to be egregiously non-compliant with App Store and Google Play policies. For example, Apple's App Store policy 2.5.18 states that "Ads displayed in an app must be appropriate for the app's age rating."[85] Similarly, Google Play's policy states "The ads [...] shown within your app must be appropriate for the content rating of your app."[86] Despite this, there have been scores of complaints from parents and kids that Wizz serves pornographic advertisements to minors on their platform—including "age-verified" profiles confirmed belonging to minors.[87] [88] [89] [90]

[81] https://www.bark.us/app-reviews/apps/wizz-app-review/
[82] https://www.nbcnews.com/tech/social-media/friend-finding-app-offered-safe-space-teens-sextortion-soon-followed-rcna91172
[83] https://apps.apple.com/us/app/wizz-app-chat-now/id1452906710
[84] https://play.google.com/store/apps/details?id=info.wizzapp&hl=en_US&gl=US
[85] https://developer.apple.com/app-store/review/guidelines
[86] https://support.google.com/googleplay/android-developer/answer/9857753
[87] https://www.reddit.com/r/Wizz_app/comments/14sicj3/wizz_got_the_most_insane_ads_i_ever_seen/
[88] https://www.reddit.com/r/Wizz_app/comments/18jxlvf/how_is_this_allowed_bro/
[89] https://www.reddit.com/r/Wizz_app/comments/150eshw/wizz_got_the_most_insane_ads_i_ever_seen_part_2/
[90] https://www.reddit.com/r/Wizz_app/comments/176fosx/this_not_crazy/

Recommendations to Parents & Families

Open Conversations: Have conversations about online risks with your children. Continue to counsel children to not share intimate photos with anyone, especially a stranger online. But most importantly, let your children know that when it does happen, they are safe coming to you for help.

Understand Instagram's Risks: Inform your children that on Instagram, there are criminal accounts pretending to be youth. These accounts often initiate intimate conversations in an attempt to entrap sextortion victims. Understand that the moment someone accepts an unknown person's Follow request, their entire Followers & Following lists are exposed, giving criminals the leverage they need to conduct a highly effective extortion scam.

Snapchat Misconceptions: Have informed conversations about Snapchat. Make children aware that photos can be saved and screenshotted. Combat the belief that photos sent on Snapchat disappear, which can create a false sense of security. Additionally, emphasize that pre-recorded "catfish" videos can be sent to appear as a "live photo" or "live video" from criminals, bypassing yet another product safety feature.

Wizz: Schools,[91] parent advocacy networks,[92] law enforcement,[93] and watchdog organizations[94] have strongly advised children to steer clear of the Wizz app. Parents should emphasize its dangers and make sure they understand the risks associated with using it.

Community Involvement: Raise awareness in your community, schools, sports teams, and youth groups about the dangers of sextortion and ways to prevent it. Work on destigmatizing conversations about sextortion. Encourage openness in discussing experiences and the scope of the problem, which can be a significant step towards undermining the tactics of criminals.

Educational Resources: Review publications from organizations like NCMEC and the FBI, or the equivalent organizations in your country, for detailed guidance from law enforcement.

[91] https://roughwoodprimary.org/2023/03/14/online-safety-wizz-app/
[92] https://www.commonsensemedia.org/app-reviews/wizz-make-new-friends
[93] https://www.timescall.com/2023/08/08/longmont-teen-becomes-victim-of-sextortion-case-involving-wizz-app/
[94] https://www.bark.us/app-reviews/apps/wizz-app-review/

If you become a victim of sextortion…

Block the criminal. Report the account. Do not pay. Do not continue contact. Save any evidence for law enforcement. Deactivate the accounts where criminals contact you. Speak with a parent, friend, or trusted adult; they will support you through this process.

Report the incident to authorities. In the United States, report to the FBI's cybercrime portal IC3.gov and if you're a minor, also report to NCMEC's Cypertipline at report.cybertip.org. You can also call the FBI Field Office 24/7 Tipline nearest you or the NCMEC 24/7 hotline at 800–843–5678.

Several services have been introduced in partnership with NCMEC and Meta to prevent non-consensual imagery from being shared on social media. This includes StopNCII.org (for anyone) and TakeItDown.NCMEC.org (for minors), which hash the photos and block future uploads of the blacklisted photos to social media sites.

Be aware of post-victimization recovery scams and for-profit entities taking advantage of sextortion victims. There are legitimate and illegitimate businesses targeting sextortion victims.[95]

The FBI warns victims of for-profit firms exploiting sextortion victims by charging high fees for assistance. Unlike law enforcement and non-profit agencies, these companies use deceptive tactics like threats and manipulation to coerce payments. Some services offered, such as cease and desist orders, may provide emotional relief but lack legal enforceability.[96] Additionally, these companies discourage victims from reporting sextortion to law enforcement in their advertisements targeted at victims claiming "the police can't help you."[97]

Furthermore, NCRI has observed coordinated inauthentic activity of accounts promoting illegitimate "sextortion recovery services." These accounts often portray themselves as hackers, cybersecurity experts, or reputation management firms, but are simply another scam fuelling account takeovers.[98]

The Network Contagion Research Institute (NCRI) aims to identify and forecast cyber-social threats targeting individuals, organizations, and vulnerable communities.

To learn more about this research, please contact Paul Raffile (paul_r@ncri.io), Alex Goldenberg (alex@ncri.io), or Cole McCann (cole_m@ncri.io)

[95] https://content.c3p.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf
[96] https://www.ic3.gov/Media/Y2023/PSA230407
[97] https://adstransparency.google.com/advertiser/AR00520246364907503617?origin=ata&region=US
[98] https://www.cbc.ca/news/canada/british-columbia/sextortion-recovery-scams-1.6774652