



Sextortion Tops Charts in Cyber Crimes

¹Dr. Neeta Gupta | ²Dr. Vandana Gaur

¹Associate Professor, Dept. of Psychology, D.A.V. (PG) College, Dehradun

²Assistant Professor of Psychology, S.D.M. Govt. PG College, Doiwala, Dehradun

To Cite this Article

Dr. Neeta Gupta and Dr. Vandana Gaur. Sextortion Tops Charts in Cyber Crimes. *International Journal for Modern Trends in Science and Technology* 2021, 7 pp. 31-37. <https://doi.org/10.46501/IJMTST0712006>

Article Info

Received: 19 October 2021; Accepted: 30 November 2021; Published: 02 December 2021

ABSTRACT

'Sextortion' is extorting money or sexual favours from someone by threatening to reveal evidence of their sexual activity. This is done through means like morphed images. Sextortion, or extortion using sexual methods, tops the charts in the Thane City police's cybercrime statistics this year. According to police officials, of the 60 cases of cybercrime registered in Thane till September, 25 were of sextortion, which is over 40% of the total cases. Police officials said that despite their best efforts of raising awareness, cases of sextortion continue to rise. A recent and fast evolving kind of cybercrime, sextortion involves befriending the victims through social networking platforms, which today exist in abundance. In case of male victims, the accused connect with them posing as women. After some initial chatting, the 'girl' initiates a video call with the victim, convincing him to perform sexual acts on camera. These acts are recorded without the victim's knowledge and then used to blackmail him for as much money as he can pay.

The same crime, when aimed at women, uses profiles in the name of men. However, as women are much more careful with regard to their online activities, a sextortion scam takes longer in their case, with the accused winning their confidence over time with promises of love and even marriage.

Keywords: sextortion, cyber, crime, victim, sexual, video, blackmail

I. INTRODUCTION

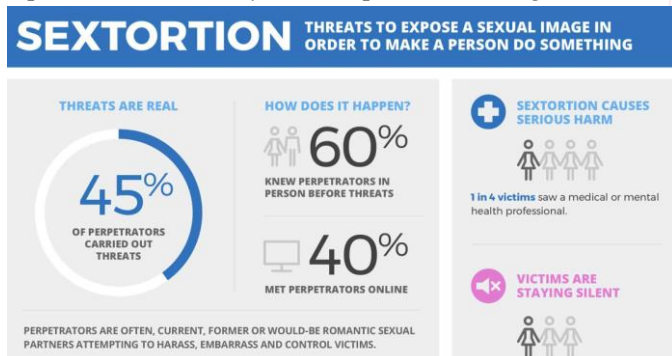
Online Sextortion occurs when a fraudster threatens to circulate your private and sensitive material online, if you do not provide images of a sexual nature, sexual favors, or money. The perpetrator may also threaten to harm your friends or relatives by using information they have obtained from electronic devices unless you comply with their demands. Sextortion is a form of online abuse, wherein the cybercriminal makes use of various channels like instant messaging apps, SMS, online dating apps, social media platforms, porn sites etc., to lure the users into intimate video/audio chats and makes them pose nude or obtains revealing pictures from them. The fraudsters later make use of

this material to harass, embarrass, threaten, exploit and blackmail the victims.[1]



"People who often get connected with strangers through social media or even gaming apps are targets of these crimes. It begins with offers of friendship but soon

leads to sharing of compromising pictures or videos that are used for blackmail. The victims of such crimes belong to all age groups. We are investigating these cases by trying to trace the Internet Protocol (IP) addresses of the accounts in question. We are also trying some additional methods of technical investigation in order to trace and apprehend the accused,” an officer with the Thane Police’s Cyber Crime Cell said. Officials said that sextortion can be damaging in more ways than one as even after the victim is bled dry for every penny that he has, there is no guarantee that the accused will not make the compromising videos public or upload them on pornographic websites. There are hundreds of porn websites on the internet where all kinds of explicit content is hugely popular. Further, there are discussion forums on the dark web that serve as marketplaces, where such videos are auctioned and sold to the highest bidder,” an officer with the Maharashtra Cyber department said. What makes this trend all the more worrying is that not a single case has been detected yet. Further, the police believe that the number of cases reported to them are just the tip of the iceberg.[2,3]

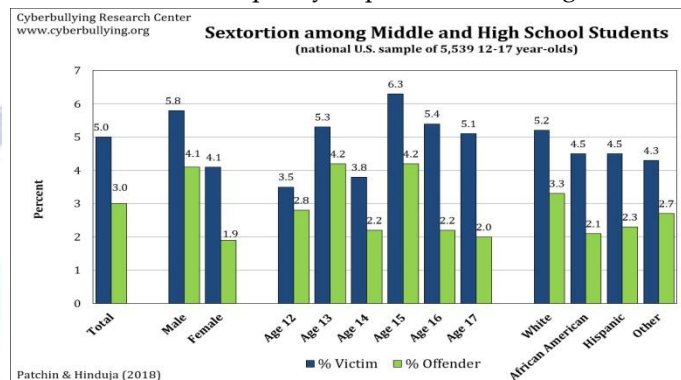


“Victims of such crimes are unwilling to come forward and report them to the police for fear of embarrassment or disrepute it might bring. However, the best and surest way of bringing such cases under control is to report them to the authorities,” Deputy Commissioner of Police Sunil Lokhande, Cyber Crime, said.

One of the cases that the Thane police is investigating is of a 19-year-old girl who stays by herself. Due to sheer loneliness during the lockdown, she turned to gaming apps and was befriended by a scamster who first offered emotional support and then convinced her to share explicit pictures of herself. Using these, the accused started blackmailing her, demanding more and more explicit pictures and videos till the victim confided in her parents and a case was

registered. Another case is of a 50-year-old man from a politically-connected family who was similarly targeted by an accused posing as a girl on social media.

Cyber expert Ritesh Bhatia said that the safest policy to follow given the rising trend of sextortion cases was to not accept any requests from strangers.



OBSERVATIONS

“If you do connect with someone you don’t know personally, never accept video calls from them. The very fact that someone who barely knows you is making a video call to you should set alarm bells ringing in your head. Further, it is advisable to make all social media profiles private. This prevents anyone from taking pictures from your social media pages and morphing your face over explicit content,” Bhatia said.

Apart from sextortion, the Thane Cyber Cell is also probing cases of phishing, website spoofing and credit and debit card frauds, officials said.[4]

Dangers

- Abuse and Exploitation
- Harassment
- Blackmail
- Threats of public humiliation
- Mental distress

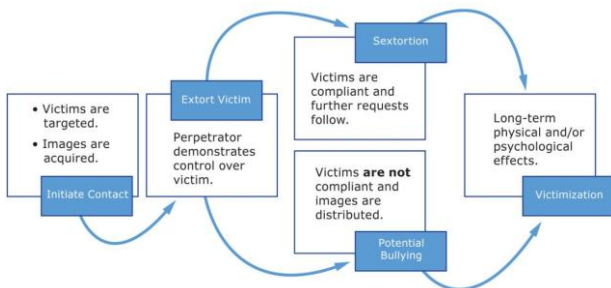
Modus Operandi

- The fraudsters try to lure the users into sharing intimate content in different ways
- posting messages for video/audio chat
- using fake accounts/profiles
- creating pages/ad campaigns

The users get victimized when they

- pay for the such services and pose nude or in compromising position in video calls

- accepts or sends friend requests to the fake account/profile and involves in intimate interaction posing nude in video chats, sends revealing pictures etc.,
- The fraudster records video/ takes screenshot/ takes pictures/makes use of revealing pictures/morphs the pictures sent
- The fraudster starts blackmailing the victim leading to sextortion.



The users of porn sites may also fall prey sextortion, when their chats/video calls on the porn sites are used for blackmailing by fraudsters.

Channels used for trapping the victims into sextortion

The fraudsters resort to sextortion following the modus operandi given above using various channels like -

- Messaging apps
- Dating apps
- Social media platforms
- Porn sites etc.,

Warning signs indicate attempts of sextortion by cyber criminals

- Repeated untoward messages/video calls from unknown number/s[5]
- Repeated friend requests from unknown person
- Repeated request for private intimate pictures, video chats, photos
- Manipulating or redirecting the conversation towards intimate topics
- Rush through the things and trying to develop intimacy

Warning signs that may indicate victimization

- Signs of fear, nervousness, anxiety, depression
- Isolating self and being very reactive & emotional
- Feeling desperate and frustrated
- Having suicidal thoughts and self harming behavior.

Safety tips to protect yourself against online sextortion

- Never share any compromising images, posts, videos of yourself to anyone, no matter who they are
- Remember that the internet never forgets or forgives. If you have shared something once, it will remain present on the Net forever, in one form or the other.
- Never accept or request for friendship from unknown people on social media platforms.
- Enable privacy and security features on your social media accounts and instant messaging apps.



- Use "Report User" option over social media platforms to report any such[6]
- Do not share your personal/private pictures publicly.
- Turn off your electronic devices and web cameras when you are not using them.
- Use two factor authentication with strong passwords and different passwords for different your social media accounts.
- During an online interaction or chat, if the person on the other side is trying to rush through the things and develop intimacy, then it is cause of alarm.
- Never allow anyone, however close to capture any private part or intimate activity with any device. Such a data can be misused at a later stage.
- Do not accept video calls or open attachments from people you do not know.
- Save the evidence and the screen shots for referring to the incident later.
- Do not suffer in silence, know that you are not alone, reach out and seek help from trusted family and friends.
- File a complaint against sextortion online or at your nearest cyber crime cell.Remember that you can also anonymously file an online complaint against such

offence on the national cyber crime reporting portal cybercrime.gov.in.

- Avoid clicking intimate/nude/semi-nude photos/videos on your phone, which if leaked could cause embarrassment. There are several rogue mobile apps that could access your gallery/storage and can be used to blackmail you.
- Don't hesitate in filing a complaint or contacting police due to shame, embarrassment and self-blame.

DISCUSSION

These types of frauds can take place both against male and female victims (although majority of the victims are primarily females) and the perpetrator can be both an unknown person or a known one. In such crimes, the culprit usually entices and induces the victim to share their private and nude photographs or videos over phone, which are then stored and saved by the former for future extortion (sextortion). In a lot of cases, people come in contact with unknown persons through dating apps or even matrimonial websites/apps. [7]



The profiles that they connect with, are mostly fake. The person behind the profile is actually a criminal whose main motive is to extort money from the victim. These fake profiles are deliberately made to look very attractive so that people fall prey to this scam easily. The persons who operate these fake profiles first talk to the victims normally for a few days and then induces them to share their intimate/nude pictures and videos with them. Once the criminal has access to these private pictures and/or videos, he starts extorting the sender for money, sometimes up to several lakhs claiming that in case the victim does not pay up, he will upload their pictures/videos on the internet or share those with his/her relatives, family and friends.

In a new variant of this Modus Operandi, a lot of people (mostly men) are being contacted on Instagram recently by women with attractive profiles, who immediately ask them for a sex chat or a nude video call. When the person agrees to it, they record the entire episode and start blackmailing/extorting the victim for money threatening to share the video with his relatives and friends. This crime can also be committed by someone known to the victim and with whom the victim has had an intimate relationship. Sometimes, such people get access to or clandestinely obtain private pictures/videos of the victim and then, when the relationship ends, they use it to extort money from the victim.[8]



Sextortion gang arrested by Ghaziabad police

RESULTS

1. Please remember – the internet never forgets or forgives. If you have shared something once, it will remain present on the Net forever, in one form or the other.

2. Secondly, the reach and speed of the internet is enormous. In a short span of time, the offensive content can spread to millions of people. Therefore, it is very important that under no circumstances, nothing that could, if leaked into the public domain, cause harm or embarrassment at a later stage, should be posted, shared, transmitted, recorded, etc.

3. During an online interaction or chat, if the person on the other side is trying to rush through the things and develop intimacy, then it is cause of alarm.


4. Never allow anyone, howsoever close that person may be, to capture any private part or intimate activity with any device. Such a data can be misused at a later stage causing serious harm or damage to reputation to the victim.

CONCLUSION

Many people use webcams for flirting and cybersex - but sometimes people you meet online aren't who they say they are. Criminals might befriend victims online by using a fake identity and then persuade them to perform sexual acts in front of their webcam, often by using an attractive woman to entice the victim to participate. These women may have been coerced into these actions using financial incentives or threats.[9]

AN EXPENSIVE DATE

CHARACTERS
Shalini | A software engineer, jobless since lockdown last year
Aryan Dixit | MBA graduate, dealt in garments
Rajkeshore Singh | Computer engineer turned spa owner in Gurgaon



MODUS OPERANDI
➤ Find wealthy businessmen on dating app Tinder
➤ Initiate a chat after swiping right, fix a meeting at a hotel after a few days
➤ Record the target in objectionable positions using a spy cam fitted in handbag

➤ Contact the target after a few days through social media, share his nude pictures/videos
➤ Demand between ₹10 lakh and ₹1 crore in lieu of not making them public or sending them to the target's family

SYNDICATE BUSTED
➤ Crime Branch files FIR after a victim, asked to pay ₹1 crore, files complaint
➤ Tracks IP addresses of devices of suspected social media accounts, nabs trio. Equipment seized

These webcam videos are recorded by the criminals who then threaten to share the images with the victims' friends and family. This can make the victims feel extremely ashamed and embarrassed and, tragically, here in the UK at least four young men have taken their own lives after being targeted in this way. Both men and women can be victims of this crime, either by being blackmailed or by being coerced into carrying out sexual acts.

The best way to stop yourself from becoming a victim is to be very careful about who you befriend with online, especially if you're considering sharing anything intimate with them. Don't Panic: The first big step is to recognise you are the 'victim' in this and that you may require support to help you through what has happened.

Don't pay: The choice to pay is yours but experience shows where victims have paid then there is

no guarantee that offenders will not still post the recording

and are in fact more likely to come back with further demands. Don't keep communicating: By replying to these threats it indicates to the criminals that you are someone who may be persuaded to pay their ransom. Do consider getting support: You can contact your local Police force (101) to report what has happened to you. This is particularly important if you are struggling to cope with the issue. If you are under 18 consider speaking to a trusted adult and additional support is also available via Child Exploitation Online Protection. (CEOP)[10]

WHAT THE CHARGESHEET SAYS

➤ The gang is using money extorted from bookies, property dealers and businessmen to buy benami properties	fees – from proceeds of crime
➤ The extortion money is often on per-month (₹ 50,000) basis, increased periodically	➤ Members of this gang have been procuring sophisticated arms and ammunition from contacts outside Delhi
➤ The gang members support families – even pay school fees	➤ The gang is in possession of high end SUVs by committing car-jackings or extortion



Jitender Gogi

We have evidence that organised crime groups – mostly based overseas - are behind this crime. For them it's a low risk way to make money and they can reach many victims easily online. Victims are often worried about reporting these offences to the police because they are embarrassed.

Various cases

- Anthony Standel of Wisconsin, then 18, received 15 years in prison in February 2010 after he posed as a girl on Facebook to trick male high school classmates into sending him nude cell phone photos, which he then used to extort them for homosexual sex.
- Jonathan Vance of Auburn, Alabama, was sentenced to 18 years in prison in April 2010 after sending threatening e-mails on Facebook and MySpace extorting nude photos from more than 50 women in three states.
- Luis Mijangos was sentenced to six years in prison in September 2011 for hacking into dozens of computers, stealing personal information and

demanding naked images from female victims in exchange for not releasing the stolen information. Forty-four of the victims were under age 18.



- Isaac Baichu, a federal immigration officer in New York, was sentenced to 1+½ to 4+½ years in prison in July 2010 after demanding sex from a 22-year-old Colombian woman in exchange for a green card.
- Steve Ellis, an immigration adjudicator in Toronto, was sentenced to 18 months in jail in July 2010 after telling a South Korean woman he would approve her refugee claim in exchange for sex.
- Michael Ngilangwa, a secondary school teacher in Tanzania, was sentenced to pay a fine or serve one year in prison in June 2011 after demanding sexual favors from his student in exchange for favorable exam results.
- Christopher Patrick Gunn, 31, of Montgomery, Alabama was indicted for using fake Facebook profiles to extort nude photos and videos from underage girls in numerous states. He got 35 years in federal prison after being convicted.
- In May 2010, the police of the Basque Country in Spain arrested a 24-year-old man accused of blackmailing a woman he met on an online chatroom and threatening to distribute nude photographs of her from her webcam. [11]
- A video of the Chinese Communist Party official Lei Zhengfu having sex with a woman was a part of a sextortion plot by a criminal gang. [12]
- In 2013, Daniel Perry committed suicide hours after falling victim to webcam blackmail

- [1] De la Cerna, Madrilena (April 15, 2012). "Sextortion". Cebu Daily News. Retrieved 2012-10-05.
- [2] "How to curb sextortion, violence against women – Amaechi". Punch. Nigeria. July 2, 2012. Archived from the original on August 6, 2012. Retrieved 2012-10-05. 'Sextortion is the currency of corruption and eats the fabric of society and it is in all sectors of the society,' [Justice Binta Nyako] said
- [3] "CSW Wraps up Second Week of Work". School Sisters of Notre Dame. March 9, 2012. Retrieved 2012-10-05.
- [4] "11th Biennial World Conference of the IAWJ, London 2012, Keeping Safe – Keeping Well" (PDF). Provincial Judges' Journal. The Canadian Association of Provincial Court Judges. 35 (1): 58. Summer 2012. Retrieved 2012-10-05. Sextortion is a form of sexual exploitation and corruption that occurs when people in positions of authority – whether government officials, judges, educators, law enforcement personnel, or employers – seek to extort sexual favours in exchange for something within their power to grant or withhold.
- [5] Mayol, Ador Vincent; Matus, Carmel Loise (March 4, 2011). "Lady judges: 'End sextortion'". Cebu Daily News. Archived from the original on May 12, 2012. Retrieved 2012-10-05. When a boss asks an employee to have sex with him in exchange for a job promotion, that's 'sextortion,' a female magistrate said yesterday. So is a teacher seeking sexual favors from a student seeking better grades.
- [6] Soyingbe, Anthonia (July 4, 2012). "Sextortion: Checkmating this new alias for bribe in Nigeria". Daily Independent. Nigeria. Archived from the original on December 24, 2012. Retrieved 2012-10-05. Sextortion ... is basically about an element of abuse of power by somebody entrusted with authority and somebody who is seeking either an advantage or justice from that person who holds the clout. And sadly, it is in all spheres of life – the judiciary, executive, legislator, media, police, army and indeed, every sector of the Nigerian life.
- [7] Jundu, Hon. Fakihi A.R. (December 2, 2010). "ILO – Speech by Hon. Fakihi A. R. Jundu, Principal Judge". Judiciary.go.tz. Retrieved 2012-10-05. Another global plight ... is the one dubbed 'Sextortion' ... [t]hese harassers insist on sexual favours in exchange for benefits they can dispense because of their positions in hierarchies including getting or keeping a job, favourable grades, recommendations, credentials, projects, promotion, orders, and other types of opportunities.
- [8] Ozler, Berk (February 16, 2012). "When it comes to female education, have we gotten it all backwards?". Blogs.worldbank.com. Archived from the original on February 10, 2013. Retrieved 2012-10-05. Mary Hallward-Driemeier ... quantifie[d] the stories we all heard working in Africa: running a small business as a woman is also treacherous business. Many say they had to exchange sex with a person of authority (person in charge of a permit, border police, etc.) or a supplier in order to be able to go about their business.
- [9] "2012 State of the Field in Youth Economic Opportunities – A Guide for Programming, Policymaking, and Partnership Building" (PDF). Making Cents International. 2012. p. 84. 'Sextortion,' researched by Mary Hallward Driemeier, Lead Economist for Financial and Private Sector Development at the World Bank Group, is where sexual favors are traded instead of money for routine business dealings.

REFERENCES

- [10] Fatoorehchi, Cléo (February 27, 2011). "Time to Drag Sextortion into the Light". Inter Press Service. Retrieved 2012-10-05. In their 2010 book 'Half the Sky', Pulitzer Prize-winners Nicholas Kristof and Sheryl WuDunn write about a disturbing but not uncommon problem in Southern Africa – male teachers who trade good grades for sex with students. ... There's a word for this – 'sextortion'.
- [11] Kujenya, Joke (June 28, 2012). "How randy judge killed five women, wife, by Justice Nyako". The Nation. Nigeria. Retrieved 2012-10-05. It is no longer a hidden complaint how students complain about lecturers demanding for sex for them to get good grades. So, if these instances are something that have been with us, then sextortion is also an age-long problem within our society ...
- [12] Raftree, Linda (September 13, 2011). "Barriers to girls' economic opportunities". The Ethnos Project. Retrieved 2012-10-05. 'Sextortion' ... refers to the sexual harassment that girls and women often face when trying to get a job, e.g., 'I'll give you a job but you must provide sexual favors if you want it'.