WISDOM Vol 1 Issue 1 Pp. 13 - 20 October - December, 2025
ISSN (Print) : XXXX-XXXX

Sextortion: A continuing mode of cyber crime

Author- Neha Das[1]

Abstract:
Sextortion, a form of cybercrime obvious by the exploitation of intimate pictures or videos for fiscal, sexual, or psychological advantage, has become an rising global threat in the digital age. This crime includes forcing victims into compliance—often by bullying to openly release flexible content if specific demands are not met. As wrongdoers exploit the suppression and reach provided by digital platforms, sextortion cases progressively target vulnerable individuals, including juveniles and young adults. The emotional influence on sufferers is thoughtful, ranging from apprehension and depression to extreme cases of suicide, underlining the urgent need for robust legal, technical, and edifying measures.

These abstract goals to discuss the skeletons of sextortion as a contemporary cybercrime, investigating into its psychological, legal, and technical dimensions. Furthermore, it highpoints the urgent need for a multi-disciplinary method that involves lawmakers, cybersecurity specialists, educators, and numerical platform providers to implement preventive measures and effective response campaigns. In hypothesis, sextortion underscores the obligation for a resilient framework to shield individuals from mistreatment in an increasingly digitalized the world.

[1] 9th Semester BA LLB University of Calcutta

Keywords: Digital coercion, Sexual extortion, Digital safety, Preventive measures, Social media risks, Vulnerability

Introduction

Sextortion, a term derived from "sex" and "extortion," refers to a troubling cybercrime that exploits the secrecy and dignity of individuals through intimidations of releasing sexually overt images or videos unless certain demands are met. These demands may range from fiscal payments to additional explicit factual or even coercing victims into unwanted sexual acts. As a fast growing form of online abuse, sextortion influences the ease and anonymity of digital communication to target individuals of all ages and backgrounds, with young people, particularly adolescents and young adults, amongst the most vulnerable. The pervasive nature of digital campaigns and social media platforms has further strengthened the risk, enabling perpetrators to manipulate victims from effectively anywhere in the world.

This introduction examines sextortion as an budding cybercrime with extensive implications for individual wellbeing, public policy, and digital ethics. By considerate its mechanisms and consequences, backers can work toward emerging preventive measures, improving legal frameworks, and supporting victims to generate a safer digital environment for all.

Modus Operandi

Sextortion outlines stereotypically follow a systematic outline that manipulates trust, anonymity, and digital accessibility to exploit victims. The modus operandi can contrast based on the strategies and expertise used by wrongdoers, but most sextortion crimes disclose through a series of mutual steps. The stages which illustrate how wrongdoers expand control over victims, exploit private information, and ultimately force them into compliance.

1. Early Interaction and Training: Wrongdoers often initiate interaction with potential victims on social media, dating apps, or other online daises under the guise of friendship, idealistic interest, or professional networking. They

stereotypically make bogus profiles to appear credible, sometimes copying familiar figures or fabricating entire facades. Through conversation and trust-building, the wrongdoer gains entrée to personal information, which is often used as influence later in the system.

2. Gathering of Penetrating Substantial: Once faith is recognized, the wrongdoer may persuade the victim to share intimate photos or videos, from time to time framing it as a mutual exchange. In other cases, they might hack into devices, or online accounts to gain private images without the victim's acquaintance. Some aggressors also use webcam hacking or malware to record private videotape without consensus.
3. Intimidations and Bullying: Through penetrating material in hand, the wrongdoer initiates the extortion stage, threatening to publication the images or videos publicly or share them with the victim's networks, household, or workplace unless exact demands are met. These difficulties may include cash transfers, further overt content, or other forms of obedience. Wrongdoers often intensify their threats to increase psychological load on victims, leveraging their fear of social humiliation.
4. Separation and Operation: Wrongdoers recurrently use terrorization strategies to separate victims, making them feel abandoned or blameworthy. This sensitive manipulation may include continuous threats or declarations that the demands will stop if the victim fulfils. Numerous victims, especially undeveloped people, experience intense guilt, which discourages them from seeking aid, further detaching them and making them more vulnerable to constant exploitation.

Through considerate the steps in this modus operandi, establishments, digital platforms, and educational organizations can work near creating pre-emptive measures, permitting potential

victims, and emerging strategies to dislocate the typical sextortion cycle. Additionally, alertness programs that teach the public on these strategies can stimulate potential victims to diagnose initial signs of sextortion, pursue timely help, and alleviate harm.

Soft Target

In the background of sextortion, "soft targets" refer to individuals who are mainly vulnerable to this form of cybercrime due to explicit personal, social, or psychological factors. Thoughtful who these soft targets are and why they are inclined is essential in developing effective prevention strategies and support systems.

1. **Adolescents and Young Adults**: Adolescents and young adults are communal bull's eye for sextortion due to their high levels of online activity and frequently partial awareness of secrecy risks.
2. **Individuals Seeking Companionship**: Those who are isolated and actively watching for relationships or companionship online are also recurrent soft targets.
3. **Marginalized Communities**: Individuals from sidelined societies, counting LGBTQ+ individuals or those in conventional social circles, can be defenseless to sextortion due to the risk of social or family refusal. In the world or communities with robust social dishonors around sexuality, victims may be more effortlessly coerced because the consequences of exposure could be plain, potentially leading to snubbing or worse.

Prominent Instances

State of West Bengal v. Animesh Boxi, 2018 in this case, the naked videos that were sent to multiple persons were recorded by the girl herself on her phone. The accused had the footage and decided to share it in a fit of rage. The offender was punished by five years imprisonment and a fine of Rs. 9000 in this case. Hon'ble Judges was made decisions based on justice and fairness. This case was regarded to be India's first "revenge porn" conviction.

Caution to Be Taken

Averting sextortion requires watchfulness, accountable online behaviour, and proactive steps to shield personal privacy. These restraints apply to anyone who interrelates online, especially those who may be weaker to cyber manipulation. Here are some vital actions for preservation oneself against sextortion:

1. Perimeter Sharing of Private and Intimate Content: Evade sharing overt images or videos, even with people you trust.
2. Validate Online Influences: Exercise caution when cooperating with new contacts online, especially on social media, dating app platforms. Verify individualities when conceivable, and be sceptical of profiles with little info, few influences, or new accounts—communal red flags for fake or malevolent profiles.
3. Toughen Privacy Settings: Appraisal and adjust secrecy settings on all social media accounts, ensuring that private information is available only to reliable individuals. Boundary what outsiders or new acquaintances can see to decrease the risk of exposure to probable offenders.
4. Be aware of Suspicious Links and Messages: Duck ticking on unknown links, particularly those sent through unswerving messages or emails, as these could contain malware designed to entree your device's camera, files, or personal information. Be careful of messages that appear too forward or ask for private information early on.
5. Refuge Your Webcam When Not in Use: Some wrongdoers may use spyware to increase entree to a victim's webcam. To avert illegal recording, retain your webcam enclosed when not in use, or restrict it through your device's settings.
6. Instruct Yourself on Cybersecurity Practices: Straightforward cybersecurity practices, such as diagnosing phishing efforts, using trustworthy security

software program, and evading unsecured Wi-Fi networks, can go a extended way in stopping unauthorized access to strategies and accounts.

7. Tale Suspicious Behaviour: If somebody begins to burden you for explicit gratified or money under threats, report the individual to the podium and block them immediately. Most social media and communication platforms have instruments for reporting unmannerly behaviour and will take action to prevent supplementary exploitation.
8. Pursue Support and Report to Authorities: If targeted, recall that support is available. Victims should sensation sanctioned to report sextortion efforts to local authorities or cybercrime units without fear of judgment or retaliation. Many formations offer private counselling and care services specifically for cybercrime victims.

Captivating these defences can deliberately reduce the jeopardy of becoming a sextortion target.

Prompt steps to be taken

Lodge A Complaint Against Sextortion

It is necessary to file a complaint against sextortion. It is easy to make complaint. There are such steps –

Offline mode

1. File a formal report with the nearest cybercrime cell.
2. Share your personal details when you filed a complaint such as you name, phone number and address.
3. If you are unable to make a complaint with the cyber cell, you may register an FIR with any police station. If they refuse your complaint, may appeal to the commissioner or judicial magistrate.

   Under section 154 of the CrPC it is mandatory to record the complaint.

Online mode

Go to the website Ministry of Home Affairs' National Cyber Crime Reporting Portal

1. Click on the “File a Complaint”.
2. Click the “Accept”.
3. Click the option “Report cybercrime involving women/child” if your complaint is about a cybercrime involving a women or child.
4. Then click “Report”.
5. If your report is not related to this then click another option “Report other cybercrimes”.

Provisions Related To Sextortion And Punishment For Sextortion In India

In India there is no explicit law that expressly deals with sextortion. But in Indian laws there are some provisions recognize one or the other aspects of sextortion.

1. Section. 354 of Indian Penal Code,1860 deals with assault or criminal force to a women with intent to outrage her modesty.
2. Section. 354 A of Indian Penal Code, 1860 deals with sexual harassment and punishment for sexual harassment.
3. Section. 375 of Indian Penal Code, 1860 deals with rape, done in different capacities, one of which is rape due to the abuse of authority and **Section. 376** deals with punishment for rape.
4. Section. 383 of Indian Penal Code, 1860 which deals with law against extortion.
5. Section. 384 of Indian Penal Code, 1860 deals with punishment for extortion.
6. Information Technology Act, 2000 deals with certain sexual offences, though it also does not cover the changing aspects of cyber sexual crime.
7. The Shield of Children from Sexual Offences Act, 2012 deals with child sexual abuse.

Conclusion

Sextortion is becoming a common phenomenon in India. Sextortion is a serious and dangerous crime. Sextortion also involves blackmail in which the victim is threatened to share sexual photographs in order to extort money or sexual pleasure by

sextortionists. The most prevalent form of sextortion is blackmail through social media. If anyone has been a victim of sextortion, he/she must report it immediately in nearly police station.

Citation

[i] *State of West Bengal v. Animesh Boxi,* (2018)

[ii] *United States v. Rodger,* (2020) 981 F.3d 1001 (9th Cir)

Bibliography

i. K D Gaur, *INDIAN PENAL CODE* (Universal LexisNexis, 7th edn., 2020).

ii. Sneha Mahawar, 'How to take legal action against Sextortion' 5 June 2021, *available at* <https://blog.ipleaders.in/take-legal-action-sextortion/> (4 November, 2024)

iii. 'How to file a cyber complaint against online sextortion' 8 February 202, *available at* <https://www.onlinelegalindia.com/blogs/file-cyber-crime-compliant-online-in-india-against-online-sextortion> (4 November, 2024)

iv. 'Sextortion: An emerging crime into the gray area of law', *available at* <https://legalserviceindia.com/legal/article-6707-sextortion-an-emerging-crime-into-the-gray-area-of-law.html> (November, 2024)