INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

CYBER KIDNAPPING IN INDIA PROTECTING AGAINST THREATS

AUTHORED BY: - RAINY KANWAR
BBA.LLB 3rd YEAR, SEMESTER6 DIV-C62
Cyber Law Assignment
Bharati Vidyapeeth (Deemed To Be University) New Law College, Pune

ABSTRACT

In the digital age, cyber kidnapping has emerged as a significant threads, criminals leverage information and organizations a like. this form of extortion involves the unauthorized access and control of sensitives digital assets often accompanied by demands for ransom. Virtual kidnapping, put simply, is a cybercrime facilitated by false claims that a significant other, child, or other relative has been abducted, and the perpetrators threaten to kill or seriously harm the victim unless they get a ransom. In general, not much is known about the traits of the individuals and organizations that engage in this cyber-enabled crime, including virtual kidnappings. This article undertakes a thorough, virtual case study analysis of kidnappings, based on a systematic investigation of over 7000 news reports, official records, and court papers between January 2000 and March 2022, in order to discover these features. The article has two objectives. To contextualize virtual kidnapping within the larger body of kidnapping literature, the paper first highlights the point at which technology and kidnapping cross. A sense of urgency and terror in the victim, perpetrators use phone calls, social media, or other contact channels. To make their statements seem genuine, they could pose as government employees, law enforcement officers, or family members. The perpetrators frequently fabricate stories about having kidnapped the victim or a loved one and then demand money or private information to be released. In abstract cyber kidnapping, technology is a key component. Spoofing techniques can be employed by criminals to modify caller IDs or fabricate false internet personas in order to trick their intended victims.

KEYWORDS

Cyber Kidnapping, Ransomware, Cyber Crimes, Phishing.

ISSN: 2582-6433

INTRODUCTION

Cyber kidnapping is also known as virtual kidnapping. Cyber kidnappers contact a victim. Cyber kidnapping is a form of crime where victims are targeted by online Sattacker and coerced into isolating themselves to demand ransom from their families. Here's what you need to know about cyber kidnapping and how to protect yourself. Cyber kidnapping are a new criminal trends in which scammers extort vulnerable victims remotely. It involves criminals calling or messaging of victims to trick them into thinking a loved one has been kidnapped through the person is actually safe. The digital age has given rise to a number of new crimes, including phishing and internet scams, including cyber kidnapping. In order to get a ransom from their family, victims are tricked into withdrawing from society. After then, the victims are watched over by cyber kidnappers via videochats.

This article aims to fill the gap in the academic and gray literature by conducting a comprehensive systematic review of news articles, government reports and briefings, and criminal cases involving virtual kidnappings. This article is based on a review of more than 7,000 articles, reports and court documents and a detailed analysis of 75 cases. The first goal is to situate the understudied topic of virtual abduction within the broader abduction literature and encourage future research on the topic. Second, the goal is to develop a comprehensive typology that identifies the different characteristics of virtual kidnapping. The questions motivating this analysis are: Who are the perpetrators and targets of virtual kidnapping cases? What are the main characteristics of the parties involved in this crime? Was the crime committed alone, with another actor, or as part of a group?

WHAT IS CYBER KIDNAPPING?

Cyber abduction, also known as ransomware assaults, is a type of malicious software designed to obstruct access to a computer system or data until a ransom is paid. Typically, the victim of this kind of cyber-extortion is locked out of their own system or has their files encrypted, with the promise that access would be restored after the ransom is paid. Virtual abduction, or cyber kidnapping, is a form of extortion in which the perpetrators utilize psychological blackmail and deceit to force victims to pay a ransom. Usually, the perpetrators of this crime get in touch with the victim and their family, say the other person is in danger, and demand a ransom to get them out of danger. Before the victim learns that their loved one is not in danger, the offenders take advantage of their fear and desperation to extract a speedy ransom payment. If you find yourself in a scenario

ISSN: 2582-6433

like this, it's critical to be alert and contact police enforcement right away.

Here, ransomware is used by hackers to encrypt and render the victim's data unreadable. After that, in order to have their data back, the victim must pay a ransom. By adopting an online persona, cybercriminals might obtain personal data about a victim. They can then manipulate the victim or people close to them by using this information to demand money.[2]

HOW CYBER KIDNAPPING WORKS?

- Deceptive Tactics: To persuade the victim that a family member has been abducted, perpetrators frequently employ manipulative and intimidating techniques.
- Isolation: In order to protect their loved one, victims are forced to isolate themselves and abide by the dictates of the cyber kidnappers.
- Virtual Scenarios: In these scenarios, the victim is frequently compelled to comply based on the information provided by the perpetrators because they are unable to independently confirm the welfare of the purported victim.
- Initial Contact: When calling a victim, perpetrators frequently pretend to have abducted a loved one or to be keeping an eye on them.
- Fear Tactics: They threaten physical damage to the purported victim if their requests are not fulfilled in order to keep the victim on the line.
- Demand for Ransom: Those who commit ransomware frequently want that the money be paid right away via wire transfers or other obscure means.[3]

CYBER KIDNAPPING TRENDS

Cybercriminals force victims to submit photos that give the impression that they are being held prisoner in order to commit cyber kidnapping. Fearing for their family members' safety, the victims cooperate, and these images are then used to demand money from the family. In most cases, nobody is in direct danger. The con games date back to the 1990s and come in a variety of shapes and sizes, much like other internet frauds such as sextortion.

In a recent instance, it was claimed that exchange student Kai Zhuang, 17, had been abducted. The attackers demanded a $80,000 ransom in exchange for Zhuang's release when they emailed his parents disturbing pictures of him. Following the kidnappers' instructions to isolate himself in a tent, Zhuang was discovered safe and undamaged. The FBI IS actively involved in

ISSN: 2582-6433

investigating.[1]

Cyber kidnapping involves the abduction of sensitive digital assets, such as confidential data, personal information, or control over critical systems, by cybercriminals. Victims find themselves in a digital hostage situation, forced to pay hefty ransoms to regain control of their data or system.

HOW TO PROTECT YOURSELF FROM CYBER KIDNAPPING?

In the current digital era, safeguarding oneself against ransomware assaults, sometimes referred to as cyber abduction, is essential. Maintain Updating Your Software Update your operating system, antivirus program, and other apps frequently to fix security holes that hackers might exploit. For your accounts, create complicated passwords that you change on a frequent basis. To create and save secure passwords, think about utilizing a reliable password manager. Refrain from opening attachments or clicking links from unidentified or dubious sources. Steer clear of phishing emails as they have the potential to spread ransomware.

Make sure you frequently backup your critical data to an external device or a cloud storage platform. In the event of a ransomware attack, you will be able to recover your files thanks to this. To shield your devices from harmful software, make use of reliable antivirus and antimalware software. To provide an additional degree of protection against unwanted access, turn on the firewall on your computer and network. Keep Up With it Stay informed about the newest dangers to cybersecurity and the safest ways to use the internet. This can assist you in identifying possible hazards and taking the necessary precautions. Whenever you can, turn on multi-factor authentication to further secure your online accounts. Provide cybersecurity best practices training to your team members if you work for a company or organization to make sure everyone is cooperating to stop cyber kidnapping. To evaluate and improve your cybersecurity procedures, think about speaking with cybersecurity experts or companies. [4]

CURRENT STATES OF CYBER KIDNAPPING

According to the material supplied, cyber abduction entails criminals tricking people into thinking their loved ones have been taken hostage while, in fact, they are safe through lies and terror. Subsequently, the crooks demand payment in ransom to free the purportedly abducted person. Language and cultural difficulties have made Chinese foreign exchange students

ISSN: 2582-6433

particularly vulnerable to scams of this kind. It is common for victims to be forced to isolate themselves and email pictures of themselves while feigning to be in captivity in order to demand money from their relatives. To stop cyber kidnapping, law enforcement and telecom firms are advised to take strong action against such calls and messages. Prior to taking any action, it's critical to confirm the veracity of kidnapping report,

A rising menace in the world of cybercrime is cyber kidnapping, also referred to as cyber extortion. Every 37 seconds, a victim of cybercrime is reported, with an average of 97 victims every hour. Comparing 2022 to 2021, there was a decrease in the number of internet users whose data was compromised every second, from 6 to 2.

METHODS EMPLOYED BY CYBERS KIDNAPPERS

Cyber kidnappers use various methods to carry out their illegal activities. Phishing emails or messages are frequently used by cyber kidnappers to deceive victims into disclosing personal information, such as banking information or login credentials. They might use ransomware to lock victims out of their devices or encrypt their contents, then demand a fee to unlock the device. This entails coercing people into disclosing private information or taking activities that jeopardize their security. Targeted spear phishing assaults are a tactic used by cyber kidnappers in which individualized messages are created to trick particular people or organizations. They may take advantage of security flaws in a system to obtain private information without authorization, which they can subsequently utilize as leverage in extortion. Cyber kidnappers may use fictitious identities to intimidate victims into agreeing with their demands. This strategy is creating the appearance of a kidnapping in order to extract a ransom from the victim, frequently with the use of threats and emotional blackmail.[5]

The sections that follow are especially relevant to cyber kidnapping

Section 43 (Damage to Computer Systems): This section considers the harm that results from illegal access to computer systems. Someone may be punished with jail time or a fine if they deliberately harm computer systems. It serves as a deterrence to hackers trying to use cyber kidnapping to obtain personal information.

Section 66C (Identity Theft): One of the most often used strategies in cyber abduction is identity theft. This violation is expressly covered in Section 66C of the IT Act. It stipulates that jail time and a fine are the penalties for anyone who uses another person's password, electronic signature,

ISSN: 2582-6433

or any other distinctive identifying feature fraudulently for their own benefit.

Section 66D (Cheating by Impersonation Using Computer Resources): Another tactic in cyber kidnapping is impersonation. People who use computer resources to impersonate someone else are subject to penalties under Section 66D. A fine and up to three years in jail are possible penalties.

Section 66F (Cyber Terrorism): Cyberterrorism and cyber kidnapping may be related. Acts that endanger national security, create panic, or harm vital infrastructure are all targeted by Section 66F. Offenders risk a life sentence of hard labour.

NEGATIVE IMPACT OF CYBER KIDNAPPING

Cyber kidnapping, also known as ransomware attacks, can have severe and far-reaching negative impacts on individuals, businesses, and even nations. Both individuals and businesses may suffer large financial damages as a result of cyber abduction. Substantial financial damages may result from ransom payments, lost revenue from system outages, and expenses associated with cleanup and recovery. Operations of key infrastructure and businesses that are the target of cyber abduction may be severely disrupted. This may result in decreased output, service delays, and eventually harm to the company's reputation. Sensitive data may occasionally be exfiltrated by cyber kidnappers prior to encryption, which could result in data breaches. Long-term repercussions from this could include losing the trust of customers, legal troubles, and fines from the authorities.[6]

Cyber kidnapping cases can cause reputational harm to organizations involved. The long-term sustainability of the business might be impacted by news of a ransomware attack, which can undermine investor and customer confidence. Cyber kidnappers may cause serious psychological distress to those they target. Mental health may be negatively impacted for some time by the anxiety and terror that come with becoming the target of such an attack. Cyber abduction that targets government buildings or vital infrastructure can be extremely dangerous for national security. The disruption of vital services, such as electricity, transportation, and healthcare, can have far-reaching effects on the security and stability of a nation. Incidents of high-profile cyber abduction have the potential to erode public confidence in digital technologies and online services. This may prevent the uptake of cutting-edge technologies and obstruct the expansion of the economy.[7]

ISSN: 2582-6433

UNTERSTANDING OF CYBER KIDNAPPING

Cyber kidnapping is the practice of threatening to damage someone or their property using digital means in order to extract money or other concessions from people or organizations. This can manifest in a number of ways, like as phishing scams, ransomware attacks, and virtual kidnapping. Recognizing the strategies employed by offenders to take advantage of weaknesses in digital systems and human behavior in order to achieve illegal benefit is essential to understanding cyber abduction. It's critical to familiarize yourself with the tactics employed by cyber kidnappers, such as phishing, ransomware, social engineering, and impersonation frauds, in order to recognize and minimize potential threats. People and organizations need to be aware of the possible repercussions of cyber abduction, which include monetary losses, data breaches, damage to one's reputation, and psychological suffering, in order to completely appreciate the seriousness of the threat it poses. To lessen the incidence of cyber kidnapping, it is crucial to comprehend cybersecurity best practices. Establishing strong authentication protocols, updating software, alerting employees to potential threats, and regularly backing up data are some examples of these methods. Minimizing the effects of an attack requires knowledge of the proper reaction protocols in the event of a cyber kidnapping incident. These protocols include reporting the crime to authorities, obtaining professional aid for data recovery, and successfully communicating with stakeholders. [8]

CONCLUSION

Cyber kidnapping is a form of crime in which victims are targeted by online attackers and coerced into isolating themselves in order to demand ransom from their families. The victims, often foreign exchange students, are convinced to take photos of themselves that make it appear as though they've been taken captive, while the cyber kidnappers monitor them through video chat and threaten their families in order to demand compliance. Therefore, it's crucial to be cautious and take necessary steps to protect oneself from falling victim to such crime. Cyber kidnapping is a dangerous crime that targets people and their families. In a circumstance like this, it's critical to be alert and contact police enforcement right away. People can safeguard themselves and their loved ones from being victims of cyber kidnapping schemes by taking the advised precautions. Cyber-entrapment, as part of the wider spectrum of cybercrime, requires a rapid and multifaceted response. This includes not only individual vigilance and taking cyber security measures, but also coordinated international actions.

ISSN: 2582-6433

REFERENCES

1. https://www.bbc.co.uk/news/world-us-canada-67869517
2. https://www.legalserviceindia.com/legal/article-14707-cyber
3. https://www.gktoday.in/the-emerging-threat-of-cyber
4. https://pwonlyias.com/mains-answer-writing/what-is-cyber-kidnapping
5. https://www.wionews.com/trending/what-is-cyber-kidnapping
6. https://www.wionews.com/trending/what-is-cyber-kidnap
7. https://www.legalserviceindia.com/legal/article-14707
8. https://www.gktoday.in/the-emerging-threat-of-cyber