What is Cyber Kidnapping?

Last Updated : 23 Jul, 2025

Cyber Kidnapping: Cyber Kidnapping is a kind of crime where the criminals trick their victims into hiding. Later, they get in touch with the victim's family and ask for money. To make it seem real, the victim is made to take pictures that make it look like they are being held against their will, often showing themselves tied up or with their mouths covered. These misleading pictures are sent to the family, making it seem like there's a danger. The victim and their family are made to think that not doing what the kidnappers want could put their loved ones in danger.

Cyber Kidnapping

Table of Content

What Is Cyber Kidnapping?

Cyber Kidnapping is when criminals use the internet to **trick victims into isolating themselves**, setting up a situation to demand money from their families. The victim is also forced to send pictures that make it seem like they're being held captive, showing them tied up or with their mouths covered. These pictures are then sent to the family. Both the victim and their family think their loved ones might be harmed if they don't do what the kidnappers want.

- In this crime, attackers trick victims online, making their families think they've been kidnapped and are being held against their will. The scammers then ask for money to let them go.
- In these "cyber kidnapping" situations, the scammers tell victims to be alone and might even force them to make it look like they're being held captive—sometimes using **webcams or sending voice recordings** to the families.

Cyber Kidnapping Meaning

Cyber Kidnapping refers to a form of cybercrime where malicious people use digital means to seize control of information, data, or systems with the intent of extortion. It often involves threats to disclose or manipulate data unless a ransom is paid. This can manifest in various forms, such as ransomware attacks, virtual kidnapping schemes, or the unauthorized seizure of sensitive information.

Cyber Kidnapping UPSC

Cyber kidnapping is a rising concern worldwide, and it's becoming more important for competitive exams like the UPSC. To look at this problem for the UPSC, you need to know how it could be used and what it could mean.

Check-Out: Types of Cyber Attacks

The Tactics Of Deception

Human mistakes are a widely recognized weak point in cybersecurity, and they greatly benefit cyber criminals involved in various types of online criminal activities. Deception seeks to alter human perception by taking advantage of psychological weaknesses. **Social Engineering** depends on manipulating psychology, a highly effective technique used by threat actors to obtain confidential information.

These are the following tactics often used by scammers:

1. **Social Engineering -** Cyber kidnappers exploit trust and vulnerabilities, manipulating emotional triggers like fear and anxiety to control victims and their families.
2. **Phishing and Malware -** They may infiltrate online accounts or devices through fraudulent emails or malware, gaining access to personal information and potentially monitoring communications.
3. **Exploiting Technological Naivety -** Victims unfamiliar with digital safety often prove more susceptible to falling for elaborate deception.

Types Of Cyber Kidnapping

Various types of malicious activities used to seize control of information, data, or systems, often with the intent of extortion or harm. Here are several types of cyber kidnapping:

1. **Ransomware Attacks:** In ransomware attacks, cybercriminals encrypt the victim's data or systems and demand a ransom for its release. This type of cyber kidnapping is prevalent and can affect individuals, businesses, and even government entities.
2. **Virtual Kidnapping:** Virtual kidnapping involves manipulating individuals into believing that a family member or loved one has been kidnapped. While no physical abduction occurs, the goal is to extort money from the victim through fear and deception.
3. **Data Kidnapping (Data Hostage Situations):** Data kidnapping involves the unauthorized seizure of sensitive information or intellectual property. Cybercriminals threaten to disclose or manipulate the data unless a ransom is paid.
4. **Credential Kidnapping:** In credential kidnapping, attackers steal or compromise login credentials, gaining unauthorized access to accounts, systems, or networks. This type of cyber kidnapping often leads to identity theft, financial fraud, or unauthorized data access.
5. **Device Kidnapping (Hijacking):** Device kidnapping occurs when cybercriminals take control of a user's device, such as a computer or smartphone. They may lock the device, manipulate its functions, or demand a ransom for its release.
6. **Cloud Kidnapping:** Cloud kidnapping involves compromising cloud-based services or data repositories. Cybercriminals may encrypt or manipulate cloud-stored data, demanding a ransom for its restoration.
7. **Social Media Kidnapping:** In social media kidnapping, attackers compromise or hijack social media accounts. They may use this control for various malicious activities, including spreading misinformation, conducting scams, or demanding ransoms.
8. **IoT Kidnapping:** Internet of Things (IoT) kidnapping involves exploiting vulnerabilities in connected devices. Cybercriminals may take control of IoT devices, disrupting their functionality, and demand a ransom for their release or normal operation.

Check-Out: Cybercrime Causes And Measures To Prevent It

How To Protect Yourself From Cyber Kidnapping?

It is one of many crimes that have emerged in the digital era, such as online scams and phishing. Experts recommend being extra careful with calls from unknown numbers though **Cyber Criminals** can also make it appear like they are calling from a loved one's number. Scammers can use data you have shared on social media to make their calls more convincing, so be careful of what you share about yourself.

- Cyber criminals can also make it appear like they are calling from a loved one's number.
- Scammers can use data you have shared on social media to make their calls more convincing.
- It's important to be careful of what you share about yourself and your children online, especially names, specific locations, and pictures of your home, neighborhood, or children's school.
- Experts also recommend checking up on your loved ones before making payments and approaching the police.
- There are other measures as well to keep oneself safe i.e., Turn on multi-factor authentication, Think before you click, Use strong passwords, Social media privacy, etc.

Why Cyber Kidnapping Is In News?

Recently, a Chinese student, who fell victim to 'cyber kidnapping', was discovered safe in rural Utah. Kai Zhuang, aged 17, was reported missing on December 28. When police located him, his parents in China had already paid a ransom of $80,000. Zhuang's parents notified his host school in Riverdale, Utah, about the apparent kidnapping. The school then alerted the police. He was found in a tent approximately 40 kilometers north of Brigham City, where it appears he had chosen to isolate himself. In the Utah boy's case , his parents were sent a picture indicating he had been kidnapped. The police believe the kidnappers have manipulated him since December 20. He was traced by analysing call data and bank records.

- According to the FBI's website, Although virtual kidnapping takes on many forms, it is always an extortion scheme—one that tricks victims into paying a ransom to free a loved one they believe is being threatened with violence or death.
- Unlike traditional abductions, virtual kidnappers have not actually kidnapped anyone.
- Instead, through deceptions and threats, they coerce victims to pay a quick ransom before the scheme falls apart.
- Experts believe that with the rise of **Artificial Intelligence (AI)**, such crimes can rise, as scammers can send people voice notes that sound exactly like a loved one in distress.
- Last year, an Arizona woman testified in the US Senate about receiving just such a call. When Jennifer DeStefano picked up a call from an unknown number, "her 15-year-old daughter", crying, told her some "bad men" had her. A man then threatened her and demanded ransom. After she cut the call, she called up her daughter, and realised she was safe.
- While there is no clear data yet on how many such case are there.

Check-Out: Cyber Crime Against Women

The Information Technology Act, 2000

A legislation established to legally recognize transactions conducted through electronic data interchange and other forms of electronic communication, often known as "Electronic Commerce". which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies.

- To manage activities that infringe upon the rights of internet users, the Indian government has implemented the Information Technology Act, 2000.
- This act includes various sections designed to empower users of the internet and strive to protect the online environment.
- This act aims to replace traditional paper-based methods with electronic alternatives for communication and information storage.
- This legislation aims to streamline the process of electronically submitting documents to government agencies.
- Furthermore, it suggests revisions to the Indian Penal Code, the Indian Evidence Act of 1872, the Banker's Books Evidence Act of 1891, and the Reserve Bank of India Act of 1934, addressing associated and supplementary issues.

Cyber Laws Of India

Cyber Law also called IT Law is the law regarding Information-technology including computers and the internet. It is related to legal informatics and supervises the digital circulation of information, software, information security, and e-commerce. India's cyber laws are governed by two main legislations: the Information Technology Act of 2000 and the **Indian Penal Code**. The Bharatiya Nyay Sanhita (BNS) is the replacement of the IPC.

IPC Sections

Here we have mentioned the IPC sections related to cyber crimes:

> ***Section 65*** *– Tampering with computer Source Documents.*
>
> ***Section 66*** *- Using password of another person.*
>
> ***Section 66D*** *- Cheating Using computer resource.*
>
> ***Section 66E*** *- Publishing private Images of Others.*
>
> ***Section 69*** *- Govt.'s Power to block websites.*
>
> ***Section 43A*** *- Data protection at Corporate level.*

Bharatiya Nyay Sanhita (BNS) Sections

The Bharatiya Nyay Sanhita (BNS) has been introduced as a replacement for the IPC. This new code predominantly maintains the IPC's provisions, while also introducing new offences, eliminating those nullified by courts, and enhancing penalties for various crimes. It classifies cyber crimes and financial scams as "organized crime". The BNS also includes new offenses such as: Cyber-bullying, Cyber-stalking, Cyber-harassment, Cyber-terrorism, etc.

Check-Out: White Collar Crimes - Cyber Security

Data About Online Fraud

Online fraud became the biggest problem in this digital era. Here are some facts related about this cyber crime as mentioned below:

- Financial frauds accounted for 75% of cyber crimes in India from Jan 2020 to June 2023, according to a study by an IIT Kanpur-incubated start-up.
- Nearly 50 % fraud cases happened related to UPI and internet banking.
- In 2022, Europeans were defrauded of $8.8 billion through scams, out of which $2.6 billion was attributed to imposter scams.

Cyber Kidnapping Cases

1. The Mirai Botnet Attack

Plot: In 2016, cybercriminals hijacked **IoT devices** like webcams and routers to launch a massive DDoS attack, essentially "kidnapping" the functionality of these devices and holding them hostage for ransom.

Focus: This case highlights the risks of unsecured connected devices and the potential for large-scale disruption through cyber kidnappings.

2. The Ashley Madison Data Breach

Plot: In 2015, the dating website Ashley Madison suffered a data breach exposing millions of user records, including personally identifiable information and intimate communication. The hackers threatened to release this information unless ransom demands were met.

Focus: This case showcases the dangers of online privacy breaches and the potential for blackmail through cyber kidnapping tactics.

3. The Cambridge Analytica Scandal

Plot: In 2016, the political consulting firm Cambridge Analytica harvested millions of Facebook user profiles without consent, using the data for targeted political advertising campaigns. While not a classic cyber kidnapping scenario, it demonstrates the manipulation of online identities and the potential for controlling narratives through digital means.

4. The Ransomware Epidemic

Plot: The rise of ransomware attacks targeting individuals and organizations alike shows how cybercriminals can "kidnap" digital assets and information, holding them hostage for financial gain.

Focus: This case emphasizes the importance of data security and backup systems to mitigate the impact of cyber kidnappings.

Check-Out: Cyber Crimes Against Children

Government Initiatives To Protect Cyber Frauds And Crimes

With the growth of the internet, cyber crimes are also on the increase. The Government is aware of cyber crimes incidents including phishing originating in some parts of India including Jharkhand. 'Police' and 'Public Order' are State subjects as per the Seventh Schedule of the **Constitution of India**. States/UTs are primarily responsible for the prevention, detection, investigation and prosecution of crimes including cyber crime through their Law Enforcement Agencies (LEAs). Here are some initiatives taken by government -

- The Central Government supplements the initiatives of the State Governments through advisories and financial assistance under various schemes for their capacity building.
- The Ministry of Home Affairs has provided financial assistance to all the States & UTs under Cyber Crime Prevention against Women & Children (CCPWC) scheme.
- Cyber forensic-cum-training laboratories have been commissioned in 28 States.
- The Central Government has taken steps for spreading awareness about cyber crimes, issuance of alerts/ advisories, capacity building/ training of law enforcement personnel/ prosecutors/ judicial officers, improving cyber forensic facilities etc.
- The Government has launched the National Cyber Crime Reporting Portal (www.cybercrime.gov.in).

Cyber Kidnapping - Future Challenges

Anticipating the future challenges of cyber kidnapping requires a practical approach to address the ever-evolving threat landscape. Here are seven challenges that may emerge:

- **AI Impact** - As cyber kidnappers use artificial intelligence (AI), it could make their attacks smarter and harder to catch.
- **Ransomware Services** - More criminals might use Ransomware-as-a-Service, making it easier for anyone to launch cyber kidnapping attacks.
- **Tricky Social Tricks** - Future kidnappers might get better at tricking people through social engineering, using advanced methods and even deepfake technology.
- **Critical Systems Targeting** - Cyber kidnappers may start targeting important systems like power and healthcare, causing big problems. Protecting these critical systems will be a major challenge.
- **New Tech Exploitation** - As new technologies like quantum computing and 5G become common, cyber kidnappers might find ways to use them for attacks. Securing these technologies will be crucial.
- **Changing Cryptocurrency Use** - Cyber Criminals might switch to different cryptocurrencies, making it harder to track ransom payments.
- **Global Rules Issue** - The lack of consistent international rules on cybercrime could make it difficult to tackle cyber kidnapping globally. Cooperation and clear rules will be essential to fight these threats effectively.

Check-Out: Cyber Crime - Mobile Security Threats

Conclusion

In Conclusion, cyber kidnapping is a serious threat that needs a good understanding. We talked about different kinds of cyber kidnapping, like ransomware attacks and taking control of virtual and data. These create challenges for people and groups. Cyber kidnapping doesn't just cause money problems; it also affects people's emotions and has legal consequences. Looking at real cases shows that cyber kidnappers keep changing their methods, so we urgently need better ways to protect against them.

To sum up the main ideas, preventing and dealing with cyber kidnapping needs a full approach. This includes using good cybersecurity habits, using technology to protect, and working together between industries and governments. Everyone—individuals, businesses, and policymakers—needs to focus on learning about cybersecurity, using advanced technologies, and cooperating globally. Only by working together we can make our digital world stronger and avoid the harmful effects of cyber kidnapping in the future.

Related Resources:

- Cyber Crime
- Cyber Crime - Identity Theft
- Cyber Security and Cyber Crimes
- Cyber Stalking