Sociological Study on Cybercrime

Dr. Pankaj Kumar
Assistant Professor
Dept. of Sociology
Asansol Girl's College,
Paschim Burdwan, (W.B.)
Email: pankajhlc@gmail.com

Abstract:

Cybercrime encompasses various illegal activities conducted through computers, networks, or the internet, including identity theft, phishing scams, malware distribution, and other digital attacks. It is a growing concern globally, prompting governments, police departments, and intelligence units to take action. In India, the police have established special cyber cells and are educating personnel to combat cyber threats. A cybercriminal is an individual or group that leverages technology expertise to commit malicious acts and illegal activities, known as cybercrimes. This paper aims to provide an overview of cybercrime in India, drawing from news media and portal reports.

Keywords:

Cybercrime, Hacking, Phishing, Vishing, Cybersquatting

Reference to this paper should be made as follows:
Received: 10.03.2025
Approved: 20.06.2025

Dr. Pankaj Kumar

Sociological Study on Cybercrime

Vol. XVI, No.1
Article No. 11,
pp. 100-108

Similarity Check: 12%

Online available at
https://anubooks.com/journal-volume/jgv-vol-xvi-no1-jan-june-2025

DOI: https://doi.org/10.31995/jgv.2025.v16i01.011

**This article has been peer-reviewed by the Review Committee of JGV.*

Introduction

In today's digital age, safeguarding personal information is increasingly challenging due to widespread internet use and public databases, making it easier for sensitive details to be accessed. Technology offers convenience and ease, but compromises personal data security, exposing users to cybercrimes and privacy risks, highlighting the need for cautious usage and robust safeguards. Technology's rapid advancement has transformed our lives but also created new opportunities for crime and exploitation. The internet has a dual nature: it offers numerous benefits, but also exposes users to cybercrime risks, underscoring the need for awareness and caution. Cybercrime refers to illegal activities committed using computers, networks, or the internet, punishable by law upon conviction. Examples include hacking, identity theft, and online fraud.

Cybercrime encompasses illegal activities conducted through computers, digital networks, or the internet, including hacking, identity theft, online fraud, and more. These crimes can range from hacking, identity theft, and online fraud to cyberbullying, data breaches, and even cyber terrorism. Essentially, cybercrime is any offense committed using technology to exploit individuals, organizations, or governments. Cybercrime involves using communication devices (like computers or phones) to commit or facilitate illegal activities, encompassing various forms of digital wrongdoing. Cybercrime involves targeting or utilizing computers/networks to cause harm, encompassing various malicious activities in the digital realm. The term "cybercrime" emerged as a response to the growing use of computers and networks, describing crimes committed in this digital landscape.

A cybercriminal utilizes technical skills to engage in malicious activities, such as hacking, phishing, or malware distribution, often for personal gain or to cause harm. Cybercriminals often operate on the Dark Web, offering illicit services and products, such as hacking tools, stolen data, and malware, anonymously and outside of mainstream oversight. Not all hackers are cybercriminals. Some, known as "white hat" hackers, use their skills to identify and fix security vulnerabilities, helping to improve cyber security. "Black hat" hackers, also known as cybercriminals, use their skills for malicious purposes, such as stealing data, spreading malware, or disrupting systems, constituting cybercrime.

Categorization of crime

Cybercrimes can be categorized into four main types:

1. Individual cybercrimes (targeting individuals, e.g., phishing, cyberstalking)
2. Organizational cybercrimes (targeting organizations, e.g., malware, DDoS attacks)

3. Property cybercrimes (targeting assets, e.g., credit card fraud, intellectual property theft)
4. Societal cybercrimes (threatening society, e.g., cyber-terrorism) These categories highlight the diverse nature of cyber threats.

Reasons of cybercrime

The increasing reliance on technology and interconnected devices (IoT) brings benefits like convenience and efficiency, but also introduces risks such as data breaches, cyber-attacks, and privacy concerns. The growing number of connected devices has led to an increase in cybercrimes, highlighting the need for robust security measures to protect against these threats. The rise in cybercrimes can be attributed to factors like:

1. Vulnerable devices due to inadequate security measures.
2. Personal motivations, such as revenge.
3. Financial motivations, where cybercriminals seek to profit from their activities.

These factors contribute to the increasing threat of cybercrime.

Cybercriminals often target wealthy individuals or organizations, like financial institutions, to exploit sensitive information for financial gain. The challenge of catching these criminals contributes to the rise in cybercrimes globally, emphasizing the need for robust laws to protect computers and data. Computers are vulnerable due to several factors:

1. **Easy access:** Hackers can bypass security systems, steal access codes, or exploit biometric vulnerabilities.
2. **Data storage:** Computers can store large amounts of data in small spaces, making it easier for cybercriminals to steal valuable information.
3. **Complexity:** Operating systems' complex codes can have vulnerabilities that hackers exploit.
4. **Human error:** Negligence can provide cybercriminals with access to computer systems.
5. **Ephemeral evidence:** Digital evidence can be easily destroyed, hindering investigations.

These factors contribute to the challenges in securing computer systems and investigating cybercrimes.

Cybercrime can have severe consequences for individuals, including:

1. Financial losses
2. Identity theft

3. Emotional trauma
4. Reputation damage

Cybercriminals employ various tactics, such as phishing, hacking, and malware, to compromise personal data and financial information.

Cybercrime can significantly impact businesses financially, with common scams including job fraud and investment scams. Sensitive information, such as bank and personal details, can be compromised through social media platforms and banking apps, often due to:

1. Data leaks

2. Phishing links

Phishing is a common cybercrime tactic that deceives victims into clicking on fake links. These links appear as emails or websites from trusted sources but redirect users to fraudulent sites designed to steal sensitive data, such as login credentials, personal information, or financial details. Phishing can also install malware, giving cybercriminals unauthorized access to your device.

3. Social engineering tactics

Cybercrimes like honey traps, digital arrest scams, and online games can have devastating effects, including:

1. Financial loss
2. Psychological trauma
3. Mental health impacts

These scams often target vulnerable individuals, with middle-class and wealthy people being disproportionately affected. The loss of hard-earned money can be particularly traumatic.

Digital arrest:

Digital Arrest is when someone is detained or restricted through digital means (like video calls) instead of traditional physical arrest methods. This often involves scammers impersonating government officials to extort money.A digital arrest scam is an online scam that defrauds victims of their hard-earned money. Digital arrest scams involve scammers:

1. Falsely accusing victims of illegal activities
2. Intimidating and pressuring them
3. Demanding money to resolve the fictional issue

These scams exploit fear and anxiety, leading to financial loss and emotional distress for the victims.

Emotional Effects of Digital Arrest

Cyber scams manipulate people's emotions, inducing fear and anxiety that impairs rational thinking. This tactic particularly affects vulnerable groups, including the elderly and professionals concerned about reputation or legal repercussions. The resulting trauma can be severe, leading to long-term psychological distress, feelings of shame, and erosion of trust in institutions.

Government Initiatives

The Department of Telecommunications has launched the 'Financial Fraud Risk Indicator (FRI)' to deal with financial fraud. This tool will help prevent cybercrime by sharing intelligence with banks, UPI service providers and financial institutions. The FRI tool identifies a mobile number as suspicious for fraud. The FRI system boosts security by adding extra checks for digital payments from suspicious numbers and enables swift action against potential threats, leveraging advanced analysis from the Digital Intelligence Platform. The tool classifies mobile numbers as 'medium', 'high' or 'highest' risk. This classification is based on information received from the National Cyber Crime Reporting Portal, Chakshu Platform and financial institutions.FRI empowers banks, non-banking financial companies (NBFCs) and UPI service providers to implement additional security measures against high-risk numbers.The numbers involved in cyber fraud are often active for a few days only. FRI's advance risk indicator helps in taking quick action, thereby reducing the time taken for full verification. Types of Cybercrime suggested by the Ministry of Home Affairs, 2025 are-

Deepfake Cybercrime- Cybercriminals use advanced AI to create fake videos or audio clips by manipulating real footage or recordings. These fake media are then spread through social media, messaging apps, and emails, often targeting public figures, celebrities, or people in authority. The goal is to deceive viewers, manipulate opinions, or spread false information. Criminals may use social engineering techniques to make the deepfake seem real, putting individuals and organizations at risk.

Remote Access Fraud-Remote Access Fraud occurs when cybercriminals impersonate trusted entities. They trick individuals into granting unauthorized access to their devices through screen-sharing apps. Once granted access, they can steal sensitive data, take control of accounts, and carry out fraudulent transactions

Secure Browsing-Secure Browsing involves using practices and tools to protect yourself from online threats like phishing, malware, and identity theft while surfing the internet. It ensures safer interactions with websites and reduces cyber risks.

Ransomware is a type of malicious software that locks a victim's files, making them inaccessible. Attackers then demand a ransom payment in exchange for key to unlock the file. Ransomware can spread through phishing emails, malicious software downloads, and security flaws. It poses a severe threat to individuals and organizations, causing significant data loss and financial damage

Smart Phone- Mobile scams are on the rise, with fraudsters using fake calls, malicious apps, and SIM-related frauds to steal data and money. Scammers often disguise themselves as legitimate agencies to trick users into sharing personal details. Protect yourself by following these safety measures.

Juice Jacking- Juice Jacking is a cyber security risk associated with compromised public USB charging stations. Hackers can exploit USB ports that charge and transfer data, using them to install malware or steal sensitive information. While no confirmed cases exist, staying vigilant is essential.

Money Mules- Money Mules are individuals, knowingly or unknowingly, used to launder illegally obtained funds. Scammers persuade them to receive and transfer stolen money in exchange for commissions. These funds are moved across multiple accounts to obscure the fraudster's identity. Involvement in such activities, whether intentional or not, is illegal and carries severe legal consequences,

SIM Swapping-SIM Swapping is a cybercrime where fraudsters transfer your phone number to their SIM card. This gives them access to your calls, texts, and two-factor authentication codes, enabling identity theft, account hijacking, and financial fraud. Scammers often pose as network staff offering upgrades or benefits to trick you into revealing personal details.

Cyber slavery-Cyber Slavery involves the exploitation of individuals through digital platforms, where they are coerced or manipulated into working without fair compensation. It overlaps with human trafficking and forced labor but specifically uses the internet and digital tools for exploitation.

Mobile Application APK Scam-Cybercriminals create Fake Mobile Banking Apps that closely resemble legitimate ones, using similar logos and interfaces. These apps are distributed through unofficial channels like third-party app stores or phishing links. Once installed, they steal your banking credentials and personal data, leading to financial fraud and identity theft.

SMS, Email, and Call Scams -SMS, Email, and Call Scams are used by fraudsters to deceive victims with fake offers. They impersonate trusted NBFCs by using their logos and fake IDs, gaining credibility. Scammers may send counterfeit sanction letters or cheques, asking for upfront payments. Once the payment is made, the fraudsters disappear with the money.

Social Media Impersonation -Social Media Impersonation happens when someone sets up a fake account mimicking a real person or organization. These fraudulent accounts are used to deceive others, often leading to identity theft, financial scams, reputational damage, and the spread of false information.

Search Engine Fraud -Search Engine Fraud occurs when fraudsters manipulate search results to display fake contact information, posing as legitimate entities. Victims who unknowingly call these numbers may reveal sensitive information, such as passwords and account details, leading to financial loss, identity theft, and other severe consequences.

Quishing Scams- Quishing Scams are on the rise. The scammers lure victims with promises of deals or convenience by asking to scan QR codes but ultimately initiate unauthorized financial transactions. Malicious codes can redirect users to phishing sites, steal login credentials, or transfer money directly to the scammer's account.

Spam/Vishing Calls -Spam/Vishing Calls (voice phishing) is a deceptive form of cybercrime. Fraudsters use social engineering to trick victims into revealing sensitive information, like personal or financial data. They often impersonate legitimate entities, such as banks or government agencies, using tactics like caller ID spoofing and urgency to gain trust and steal information.

Online Gaming-Online Gaming has become a hotspot for cybercriminals, with threats ranging from virtual theft and account breaches to real-world financial fraud and identity theft. Attackers exploit platform shortcomings and target players through phishing scams, malware, and social engineering.

Investment Scam Investment Scam involves fraudulent schemes that promise high returns, often too good to be true. These scams pay earlier investors with the money of new investors instead of generating profits through legitimate economic activity. It is also known as the Ponzi scheme.

Online Shopping Fraud-Online Shopping Fraud is a cybercrime where fraudsters deceive victims into making illegitimate purchases. They create fake websites or manipulate legitimate platforms, offer deals that are too good to be true, and steal personal and financial information, leading to financial losses and mistrust in online marketplaces.

Online Job Scams -Online Job Scams trick people looking for work. Scammers post fake jobs on websites, and social media, or send emails, offering high pay and easy work. Their goal is to steal the victim's money or personal information.

KYC Scam-KYC Fraud involves cybercriminals exploiting identity verification processes to steal personal information, commit identity theft, or access

financial accounts illegally. This can lead to significant financial losses and reputational damage for individuals, businesses, and financial institutions. Common tactics include tricking people, forging documents, and creating fake identities(Cybercrime Handbook-2025).

National Cyber Crime Reporting Portal (NCRP) of the Home Ministry and Indian Cyber Crime Coordination Center (I4C) has revealed new hideouts of cyber thugs' are- active networks of cyber thugs were found in Jharkhand's Deoghar, Jamtara, Dumka, Dhanbad, Giridih, Ranchi and Hazaribagh. Apart from this, gangs of cyber criminals have also been found in Nuh in Haryana and Deeng district of Rajasthan, adjacent to NCR. Out of these places Nuh in Haryana is in the first place, Deeng in Rajasthan is at the second place, Deoghar in Jharkhand is at the third place, Alwar in Rajasthan is in the fourth place and Nalanda in Bihar is at the fifth place. Jamtara which has been the most notorious for cyber fraud so far.

According to NCRB (National Crime Records Bureau), there was a 24.4 percent increase in cybercrime cases in 2022.In the year 2023, 7.9 crore cases of cyber fraud were reported across the country, while in May 2024, I4C had said that 7,000 complaints of cybercrime were reported daily. Right now the fear of digital arrest is high, but with the increase in digital payments in the country, cases of UPI fraud have also increased rapidly. In 2024 November , the government told the Parliament that there was an 85 percent increase in UPI fraud cases in the financial year 2024. Obviously, while these figures show the need to take strict measures against cybercrime.

Recent Case

Godda: A shocking incident of cyber fraud has come to light from the district. Fraudsters called a young man posing as a bank employees and stole Rs 93,600 from the victim's account. The incident took place in Badhauna village of Nagar police station area. The victim youth Suraj Raut received a call from an unknown number. The caller introduced himself as an employee of IndusInd Bank and said that Suraj had recently taken a loan from the bank, regarding which some important information is needed. While talking about the loan, the fraud asked Sooraj for his bank account details. Thinking that he was a bank employee, Sooraj shared his personal information. But when he checked his account after some time, he was shocked. Rs 93,600 had disappeared from his account. Suraj Raut said that the caller was talking in such a professional manner that he did not have any doubt. He had no idea that this could be a fraud(Nanda,2025).

Conclusion

Cybercrime and traditional crime often stem from similar motivations, including financial gain, materialism, and illicit desires. However, cybercrime's

unique characteristics, such as anonymity and remote operation, set it apart from traditional crime. Cybercrimes are diverse and can be difficult to track down due to the anonymity and distance provided by the online environment. This makes it easier for offenders to bully and harass others without being held accountable. Police officials have appealed to the public not to trust unknown calls, suspicious links or messages and to immediately report any suspicious activity to the cybercrime portal or local police. Avoid clicking on any suspicious link or unknown message; be cautious before sharing your personal information on social media or other digital platforms, if any kind of cyber fraud happens, immediately lodge a complaint on the National Cyber Crime Reporting Portal. Vigilance is very important to avoid cyber crimes. Advising to be cautious in online banking, do not share your OTP, ATM PIN number, net banking password or other confidential information with anyone. No bank, insurance company, telecom department or government agency asks for passwords through phone calls or messages. If such a call or message is received, ignore it and do not fall into any greed or fear.

We can use the Internet to increase knowledge and stay updated with the digital world. Need for cyber awareness in society In view of the increasing cases of cybercrime in today's era, it is very important to spread information about its prevention and measures to avoid it to every section of the society. Need for cyber awareness in society In view of the increasing cases of cybercrime in today's era, it is very important to spread information about its prevention and measures to avoid it to every section of the society.

References

1. Ministry of Home Affairs, 2025.Cyber Crime Prevention Handbook.
2. Ministry of Home Affairs, 2024.Cyber Cyber Digest.
3. National Crime Records Bureau 2022
4. Nanda, Aditya. 2025. Hello Talking from Bank, News18 https://hindi.news18.com/news/jharkhand/godda-cyber-fraud-fraudsters-called-a-man-posing-as-bank-employees-and-withdrew-rs seen on 24.05.2025.