Gurukul International Multidisciplinary Research Journal (GIMRJ)*with* International Impact Factor 8.357
Peer Reviewed Journal
DOI link - https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0024

e-ISSN No. 2394-8426
Special Issue on Cyber Crime and Social Media
Issue–III(II), Volume–XIII

IMPACT OF CYBERCRIME IN YOUTH AND SOCIAL WORK INTERVENTION

Dr. Vaishali Malwar-Duke
Assistant Professor
Purushottam Thote College of Social work, Narsala Road, Nagpur.
Mb.No.7507507290
vaishaliduke@gmail.com

Abstract:
Cybercrimes have increased as a result of the introduction of digital technology, especially targeting the younger generation. This paper examines the several types of cybercrimes that target young generation. It effects on their mental health and social lives. A social workers played a vital role in preventing cybercrime. The increased independence on Internet has raised growing concerns that cyber security is becoming difficult to maintain. Not only do businesses depend on the internet for all types of electronic transactions, but home usersalso increasing. People also experience the immense benefit of the internet. Cyber security awareness and education are essential to any attempt to secure cyber space. In the education system, youth must be made aware of the possible attacks and types of intruders. The rapid growth in the use of cyber space is not matched by the necessary skills.

Key Words: cybercrime, legal provisions, impact, social worker.

Introduction

The younger generation has become more susceptible to cybercrimes due to the rapid growth of technology and the extensive use of the internet. Cybercrime refers to illegal activities that involve computers, networks, or digital devices. It includes a wide range of offenses, such as hacking, identity theft, online fraud, cyberbullying, ransomware attacks, and data breaches. Cybercriminals exploit technology to commit crimes for financial gain, personal revenge, political motives, or simply to cause disruption. Cybercriminals utilise computers to commit crimes for monetary gain, revenge against others, political ends, or just plain distraction. **Cybercrime has a wide-ranging impact, affecting individuals, businesses, and society, leading to financial losses, identity theft, reputational damage, operational disruptions, and even posing risks to national security.**

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Most cybercrime is committed by cybercriminals or hackers who want to make money. However, occasionally cybercrime aims to damage computers or networks for reasons other than profit. From a sociological perspective, cybercrime examines the digital criminal activities, their impact on society, and the interplay between technology, crime, and social structures. It involves illegal activities committed through digital media and technologies like the internet, networks, and computers, encompassing a wide range of criminal activities.

In a recent World Cybercrime Index, India ranks 10th, with scams involving advance fee payments being the most common type of cybercrime

Over 60,000 cybercrime related complaints registered in last four years in Karnataka. Shedding light on growing cybercrimes, Alok Mohan, Director General and Inspector General of Police noted that in some divisions of Bengaluru, over 40 per cent of registered crimes are related to cyber security.

Cybercrimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery (copy), defamation (insult) and mischief...etc. Cybercrime refers to illegal activities that involve computers, networks, or digital devices. It includes a wide range of offenses, such as hacking, identity theft, online fraud, cyberbullying, ransomware attacks, and data breaches. Cybercriminals exploit technology to commit crimes

Cybercrime targeting youngsters includes cyberbullying, sexting, phishing scams, identity theft, and exposure to harmful content, all of which pose risks to their safety and well-being. Cyberbullying:This involves using electronic communication to harass, intimidate, or threaten someone.

EconomicCauses:

Financial gain is one of the most common causes of cybercrime. Gone are the days when one had to go to a lonely street and wait for the sunset to steal, loot or cheat. Now access to a bank account is 24x7 Causes of Cyber Crime:x365. Financial gain is a major reason for motivation to commit cybercrimes.

EasyAccesstoMobile:

A mobile device has become less expensive and more powerful due to the high competition in this segment. Cheaper data packs and a faster network have made mobile devices faster and now able to handle almost all activities that used to be done by computers. Mobile devices have become a powerful weapon in the hands of cyber-criminal to commit cyber-crime.

Lack of Technology Awareness:Lack of basic technological knowledge is one of the key drivers of cybercrime growth. Even educated people ignore the technology empowerment that results in becoming a victim of cybercrime. Negligence of cybersecurity measures can be fatal and cause monetary losses. For example, in phishing crimes, victims themselves provide critical financial details that are used negatively by Cyber Criminals to commit cybercrime.

Privacy:The concept of privacy is a personal choice and varies from one individual to another. Exposing too much information on social media platforms can be fatal. The lack of awareness of the privacy option available on social media is a concern as it may be exploited by cybercriminals.

Sexting:The term sexting stands for a combination of sex and texting. Sexting is the act of sending sexual text messages. It often also involves sending nude, semi-nude, or suggestive photos. Sometimes, the messages also include sexual or explicit videos.This refers to the sending or sharing of sexually explicit images or videos, often without consent, which can lead to serious consequences for the victim.

Phishing Scams:Phishing is a type of cybercrime where attackers, using emails, text messages, or social media, trick victims into revealing sensitive information or clicking malicious links, often posing as a trusted entitycybercriminals use deceptive emails or websites to trick individuals into revealing personal information, such as usernames, passwords, or financial details.

Identity Theft: Criminals steal personal information, like Social Security numbers to open accounts or make purchases in the victim's name.

Exposure to Harmful Content: Youngsters can be exposed to inappropriate or illegal content online, including pornography, hate speech, or violent material.

Grooming or Tutoring:

Predators can exploit children's vulnerabilities online by building relationships with them to gain their trust and then potentially abuse them.

Doxing and Stalking:This involves disclosing personal information online, which can lead to harassment and stalking.

Online Job Fraud: Cybercriminals create fake job postings to scam individuals out of money or personal information.

Online Matrimonial Fraud: Scammers pose as legitimate individuals on online dating or matrimonial sites to trick people into giving them money or personal information.

Hacking: Unauthorized access to computer systems or networks can lead to data breaches and other cybercrimes.

Ransomware Attacks: Cybercriminals encrypt a victim's data and demand a ransom for its release.

To Protect Against Cybercrime, use strong passwords and enable two-factor authentication.Avoid clicking on suspicious links or downloading unknown attachments.Keep software and antivirus programs updated.Be cautious when sharing personal information online.Regularly monitor bank statements and online accounts for fraud.

Impact of Cybercrime on Youngsters:

Cybercrime has become a major concern in the digital age, with young people being particularly vulnerable. As technology becomes more integrated into daily life, the risks associated with cyber threats also increase. The following are some key impacts of cybercrime on youngsters:

Psychological and Emotional Effects: Identity Theft: Personal data can be stolen and misused for fraud.Scams and Phishing are now commonly experienced. Youths may fall prey to online scams, losing money or sensitive information.

Laws Against Cybercrime & Their Special Features

Cybercrime laws differ across countries but generally focus on preventing, investigating, and prosecuting online offenses. Below are some special features commonly found in cybercrime laws:Data Protection & Privacy which Protects personal data from unauthorized access, theft, or misuse.Laws like GDPR (Europe), CCPA (California), and IT Act (India) focus on securing user data.Social media& Fake News RegulationsLaws against cyberbullying, hate speech, and misinformation.Cyber Forensics & Investigation PowersAllows law enforcement to investigate digital crimes with proper warrants. Several countries have dedicated cyber police and digital forensic units.Penalties & PunishmentsImposes fines, imprisonment, and sometimes cyber-rehabilitation programs for offenders.The severity of punishment depends on the crime type and jurisdiction.The Information Technology (IT) Act, 2000, and appropriate provisions of the Indian Penal Code (IPC) are the main laws that govern cybercrimes in India. The kind and seriousness of theoffence determine the punishment.

Typical Cybercrimes in India and Their Penalties Hacking (Section 66, IT Act)

The Indian Penal Code (IPC) and the Information Technology Act provide a healthy framework to address a wide range of cybercrimes in India. Under the IPC, Section 292 targets the sale of obscene materials, prescribing punishments that deteriorate with repeated offenses. Section 354C addresses voyeurism, penalizing the unauthorized capture or dissemination of private images of women. Similarly, Section 354D tackles stalking, whether physical or cyber, aiming to protect individuals from repeated unwanted contact or monitoring. Sections 379 and 411 deal with theft and receiving stolen property, respectively, while Sections 419 and 420 cover fraud-related offenses such as phishing and cheating. Forgery and document tampering are addressed under Sections 465, 468, and 469, with varying degrees of imprisonment and fines. Defamation via electronic means falls under Section 500, while Sections 504 and 506 address offenses like intentional insult and criminal intimidation through electronic communication. Section 509 specifically protects the modesty of women from insults or invasion via electronic means.

Impact Of Cyber Crime:

EconomicImpact:

Financial losses due to cybercrime are enormous. According to a report published in 2019, Rs 1.25 lakh crore was lost due to cybercrimes. Every year, thousands of people and businesses fall victim to cybercrimes like phishing and ransomware. According to one report, more than 78% of enterprises have been affected by ransomware attacks.

Impact of Cybercrime on India's Economy: Cybercrime significantly impacts India's economy, particularly due to its rapidly expanding digital economy. It causes financial losses, reputational harm and operational disruptions for both large and Cybercrime has negative impacts on individuals, resulting in financial losses, identity theft, emotional trauma, and reputation damage. Cybercriminals use multiple approaches like phishing, hacking, and malware to access financial information, steal personal data, and post damaging content online mall enterprises.

EmotionalLoss:

A cybercriminal uses various techniques to commit cybercrime and one the common method is texting or chatting and luring into an emotional relationship which latter converts into blackmailing and harassment. The victim may suffer from depression and, in some instances, has even committed suicide. The physiological loss of cybercrime requires focus and study.

DiversityVictimProfile:

A cybercrime victim may be a minor, young or elderly person. There are different types of cybercrime, which is why victims of cybercrime have different age groups. Young children are more likely to be victims of cybercrime because they are unaware of it. For instance, the Blue Whale Challenge game where the players have to complete different task including self-harm andsuicide.

Cybercrimes And the Role of The Social Worker

PreventiveRole:

A social worker can play an important role in preventing cybercrime, especially among students, especially school children. There are certain signs or behavioural changes that a social worker

can recognize and conduct counselling. A social worker can discuss things like cyberbullying and how it affects an individual. Through Counselling cybercrime may possible tocontrol. Cybercrime causes huge physiological problems in certain cases, especially when the victim was emotionally attached to the cyberattacked. In cases of extortion where the victim has shared personal photos or videos the victim may suffer from guilt and fear. In such cases, counselling is very important as the victim lives in constant fear or guilt.

Conclusion:

The law related to cyberspace is contained in the Information Technology Act, 2000, which was amended in 2008. The Information Technology Act has introduced and covered new areas of application, such as electronic records, digital signatures, cybercrime, etc. The technological world has changed the way we live, learn and communicate. Now we share pictures, stories, thoughts on the digital platform. We see, comment, agree and disagree on digital platform. We purchase online and sometimes sell online and so do contracts.

The new advantage brought by the technology brought its vulnerability in the form of cybercrime. Prevention is better than healing is rightly said for cybercrime, because most cybercrimes are preventable if proper education and counselling are conducted. Most of children and youngster are becoming a victim of cybercrime and has a social worker plays a vital role in prevention and as well as a counsellor. Unfortunately, the role of social workerhas been ignored in the case of cybercrime and the victim suffers in silence.

Social workers can play a crucial role in addressing cybercrime, especially among young people, by educating them about online safety, promoting digital literacy, and providing support to victims, as well as collaborating with other stakeholders to prevent cybercrimes.

A social worker can play an important role in preventing cybercrime, especially among students, especially school children. There are certain signs or behavioural changes that a social worker can recognize and conduct counselling.

References:

- "Cyber Crime analysis on Social Media" Swati Sharma and Vikash kumar Sharma, BSSS Journal of Computer: ISSN (Print)-0975-7228,E-ISSN - 2582-4880, Vol. XI, Issue-I (2020), pp1
- "A Survey on Cybercrime Using Social Media"Zainab KhyioonJune 2023, Iraquo Journal for computers and Informatics 49(1):52-65.
- Proliferation of Cyber Crime via social media Und International Journal of NovalResearch and Development *(IJNRD*) an international open Access Peer Reviewed, Refereed Journal.
- Cybercrime and Role of social Worker written by **Savita Kale kolekar** Views: 17607