Gurukul International Multidisciplinary Research Journal (GIMRJ)*with* International Impact Factor 8.357
Peer Reviewed Journal
DOI link - https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0039

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

# Cyber Crime and Intervention of Professional Social Worker

**Saurabh Thulkar**
Assistant Professor, Dr.Ambedkar Institute of Social Work, Nagpur
Email: saurabhthulkar.daisw@gmail.com
Mobile: 8888947786

**Abstract:**
With the emergence of Internet and Globalisation, there is a huge increase in the usage of online activities in terms of networking, shopping, browing, banking etc. And this online availability of personal information and accounting details leads to increase in the online theft and robbery which we term as Cyber Crime.
Social work intervention refers to the ways social workers help people who are facing problems in their lives. It's about providing support and guidance to individuals, families, or communities to improve their well-being. Social workers use different methods, strategies, and services to address a variety of issues such as mental health problems, poverty, family struggles, or legal concerns This paper explore the complex intersection of technology, criminal activity and social welfare, highlighting how professional social work can play a crucial role in addressing these issues.
This paper is showcasing the growing of Cyber Crime and its impact on Individuals and Communities and how professional social worker has uniquely positioned to intervene and support victims.

**Introduction**
The rapid progress of technology has changed how we live, communicate and interact. Unfortunately, with these benefits, the rise of technology has also increased Cyber Crime - Criminal Activities in the digital world. These crimes can be as harmful as traditional crimes and affect individuals, communities and organizations. CYBER CRIME AND INTERVENTION OF PROFESSIONAL SOCIAL WORKER SAURABH THULKAR
Cyber Crime includes a wide range-ranging from identity theft to cyberbullying to online fraud. While law enforcement agencies work to catch criminals, social workers play an important role in supporting victims and preventing future crimes. This letter examines complex relations between Cyber Crime and Social Work, which highlights the role of Social Workers in addressing the results of online criminal activity and preventing it in the future. What is cybercrime? Cybercrime refers to any illegal activity that is performed through the internet or includes digital techniques, including computer systems, devices and networks.
In general cybercrime may be defined as "Any unlawful act where computer or communication device or computer network is used to commit or facilitate the commission of crime".
Below is a list for some of the Cyber Crimes along with their indicative explanation. This is to facilitate better reporting of complaints.CYBER CRIME AND INTERVENTION OF PROFESSIONAL SOCIAL WORKER SAURABH THULKAR

**1. Child Pornography / Child Sexually Abusive Material (CSAM)**
Child Sexually Abusive Material (CSAM) refers to material containing sexual image in any form, of a child who is abused or sexually exploited. Section 67 (B) of IT Act states that "it is

punishable for publishing or transmitting of material depicting children in sexually explicit act, in electronic form.

**2. Cyber Bullying**

A form of harassment or bullying inflicted through the use of electronic or communication devices such as computer, mobile phone, laptop, etc.

**3. Cyber Stalking**

Cyber stalking is the use of electronic communication by a person to follow a person, or attempts to contact a person to foster personal interaction repeatedly despite a clear indication of disinterest by such person; or monitors the internet, email or any other form of electronic communication commits the offence of Cyber Stalking.

**Cyber Grooming**

Cyber Grooming is when a person builds an online relationship with a young person and tricks or pressures him/ her into doing sexual act.

**Online Job Fraud**

Online Job Fraud is an attempt to defraud people who are in need of employment by giving them a false hope/ promise of employment or of better employment with higher wages.

**Online Sextortion**

Online Sextortion occurs when someone threatens to distribute private and sensitive material using an electronic medium if he/ she doesn't provide images of a sexual nature, sexual favours, or money.

**Vishing**

Vishing (a combination of "voice" and "phishing") is a type of cybercrime where scammers use phone calls to trick people into revealing sensitive information such as bank details, credit card numbers, passwords, or personal data such as Customer ID, Net Banking password, ATM PIN, OTP, Card expiry date, CVV etc. These fraudsters often impersonate CYBER CRIME AND INTERVENTION OF PROFESSIONAL SOCIAL WORKER SAURABH THULKAR legitimate organizations like banks, government agencies, or tech support to gain the victim's trust.

**SMS Phishing**

SMS Phishing is a type of fraud that uses mobile phone text messages to lure victims into calling back on a fraudulent phone number, visiting fraudulent websites or downloading malicious content via phone or web

**SIM Swap Scam**

SIM Swap Scam occurs when fraudsters manage to get a new SIM card issued against a registered mobile number fraudulently through the mobile service provider. With the help of this new SIM card, they get One Time Password (OTP) and alerts, required for making financial transactions through victim's bank account. Getting a new SIM card against a registered mobile number fraudulently is known as SIM Swap.

**Debit/Credit Card Fraud**

Credit card (or debit card) fraud involves an unauthorized use of another's credit or debit card information for the purpose of purchases or withdrawing funds from it

**Data Breach**

A data breach is an incident in which information is accessed without authorization.

**Virus, Worms & Trojans**

Computer Virus is a program written to enter to your computer and damage/alter your files/data and replicate themselves.

Worms are malicious programs that make copies of themselves again and again on the local drive, network shares, etc.

A Trojan horse is not a virus. It is a destructive program that looks as a genuine application.

Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive.

Trojans open a backdoor entry to your computer which gives malicious users/programs access to your system, allowing confidential and personal information to be theft CYBER CRIME AND INTERVENTION OF PROFESSIONAL SOCIAL WORKER SAURABH THULKAR

**Other Common Examples of Cyber Crime include:**

**Identity Theft:** Unauthorized use of someone else's personal data to fraud or steal, such as social security numbers, bank account information, or credit card details.

**Cyberbullying:** To disturb, threaten or humiliate someone through digital platforms such as social media, text messages, or email. Its victims can have severe emotional consequences.

**Hacking:** Getting unauthorized access to computer or network to theft or manipulate data, disrupt the system or engage in criminal activity.

**Professional Social Work Intervention**

Cybercrime is a growing problem due to the global access and oblivion given by the Internet.

Criminals can work from anywhere in the world, making it difficult for the authorities to track them. The victims often experience significant emotional, psychological and financial damage.

Hence when it is difficult to address technologically, Social Workers are the main players in helping the victims fix, understanding the root causes of Cyber Crime and creating preventive measures.

**Role of social workers in addressing cyber Crime**

Social Workers have a versatile role while talking about Cyber Crime, focusing on prevention, victim support, policy rehabilitation and policy advocacy.

**1. Supporting Cyber Crime Victims**

Cyber Crime victims often experience a series of emotional and psychological effects. These may include feelings of shame, anxiety, depression and trauma, especially in cases such as theft or cyberbullying. Social Workers play an important role in providing emotional support and mental health care for the victims. CYBER CRIME AND INTERVENTION OF PROFESSIONAL SOCIAL WORKER SAURABH THULKAR

Their responsibilities include:

□□Consultation and Emotional Support: Social workers help the victims deal with the trauma of their experiences. For example, cyberbullying victims may feel isolated and depressed, and social workers can provide medical help, support groups and other services to help them fix.

□□Referral for Legal and Financial Services: In cases like identity theft or financial fraud, Social Workers can guide the victims for Legal and Financial Support Services.

This may include helping them navigate the legal process or help them connect them to the victim advocacy groups.

□□Long-Term Recovery: Many victims of Cyber Crime require Long-Term Care for reconstruction of their lives. Social Workers can help find housing, employment and educational opportunities, while individuals can help recover emotionally and psychologically with the effects of crime.

**2. Prevent Cyber Crime through Education**

Stopping cybercrime begins with educating individuals and communities to save themselves online. Social workers may have an important role in providing resources to raise awareness and teach digital safety. It also includes:

□□Digital Literacy Program: Social Workers can develop and implement programs that teach people, especially weak population such as children, seniors and low technical literacy, to safely navigate the Internet. These programs may include teaching people how to identify fishing efforts, make a strong password, and how to protect their personal data.

□□School and Community Program: Social Workers can collaborate with schools to raise awareness about cyberbullying, online harassment and other risks related to digital places. They can provide workshops to safely use social media and protect someone's privacy.

□□Promoting safe online behaviour: Social Workers can help individuals understand the moral and legal implications of online tasks. They can campaign to educate people at the risks of illegal activities such as downloading pirated materials or engaging in harmful online behaviour such as harassment or exploitation. CYBER CRIME AND INTERVENTION OF PROFESSIONAL SOCIAL WORKER SAURABH THULKAR

**3. Working with Criminals**

Addressing Cyber Crime also means working with those who are engaged in illegal online activities. Many individuals who commit Cyber Crime may have underlying issues such as mental health problems, drug abuse or history of trauma. Social Workers play an important role in rehabilitating criminals and preventing them from committing future crimes.

□□Psychological Support: Social Workers can assess mental health and emotional welfare of Cyber Criminal. Many criminals cannot fully understand the impact of their functions on victims. Social Workers can help them find healthy ways to develop sympathy, work through their underlying issues and to connect with technology.

□□Rehabilitation: For criminals, Social Workers can design rehabilitation programs that address the root causes of their behaviour and provide skills for rebellion in society. This may include medical, job training and educational programs to prevent recurrence.

**4. Policy Advocacy**

Social Workers also advocate policies that can prevent Cyber Crime and support victims.

They can work with governments, organizations and technical companies to improve digital behaviour laws and rules. This can include:

□□Advocating strong Legal Safety: Social Workers can advocate strong laws that protect people from cybercrime, especially weak groups such as children and the elderly.

□□Promoting digital morality and accountability: They can work on policies that ensure that technical companies and internet service providers take responsibility for preventing Cyber Crime and protecting users' privacy.

□□Cooperation with law enforcement: Social Workers can cooperate with law enforcement agencies to ensure that victims of Cyber Crime are treated with care and respect, and that criminals receive proper rehabilitation.

**Challenges faced by social workers in cybercrime intervention**

While Social Workers are important in addressing Cyber Crime, they have to face many challenges:

□□Lack of special training: Many Social Workers do not have specific knowledge or training required to deal with unique issues around Cyber Crime. This includes understanding online behaviour, digital equipment and legal aspects of Cyber Crime.CYBER CRIME AND INTERVENTION OF PROFESSIONAL SOCIAL WORKER SAURABH THULKAR

□□Rapid changing technology: Cyber Crime develops quickly with regular emerging new methods, equipment and strategy. Social Workers should live with technical changes to effectively educate communities and intervene in cases of online damage.

□□Privacy and moral concerns: Digital world often presents moral dilemmas to social activists, especially when balanced the concerns of privacy with the need to protect individuals from loss. These moral issues should be carefully navigated while providing assistance to social workers.

**Recommendations:**

□□Training for Social Workers: Specialized training on digital safety, cybercrime prevention, and online behaviour should be extended to social workers to enhance their ability to address cyber-related challenges effectively.

□□Awareness Campaign: A comprehensive community education campaign should be initiated to raise awareness about the risks of cybercrime and the necessary measures for online protection.

□□Collaboration with technical companies: Social workers should work with technical companies so that they can make equipment that help users protect them from cyber criminals and support victims.

□□Strengthen the legal framework: Advocate strong laws and policies that protect children, especially children from online exploitation.

The paper has underlined the versatile role of social workers in addressing Cyber Crime and emphasized the need for continuous education, cooperation and policy advocacy to create a positive impact.

**Conclusion:** Cybercrime is a growing concern that affects individuals, families and entire communities. While law enforcement agencies focus on catching criminals, Social Workers play an important role in supporting victims, preventing future crimes and rehabilitating criminals. By addressing the emotional and social effects of Cyber Crime, Social Workers help individuals to heal and move forward. However, to be effective, social workers require proper training, resources and cooperation with other stakeholders such as law enforcement and technical companies. A comprehensive approach is required to address the challenges of Cyber Crime that

involves prevention, intervention and rehabilitation. Through these efforts, social workers contribute to the creation of a safe and more supportive online world.CYBER CRIME AND INTERVENTION OF PROFESSIONAL SOCIAL WORKER SAURABH THULKAR

**References**

1. Cyber Crime in India: A Comparative Study M. Dasgupta, 2009
2. Phishing, Pharming and Identity Theft
By Brody, Richard G.; Mulig, Elizabeth; Kimball, Valerie Academy of Accounting and Financial Studies Journal, Vol. 11, No. 3, September 2007
3. Jaishankar, K. (Ed.). (2016). Cyber Criminology: Exploring Internet Crimes and Criminal Behavior. CRC Press.
4. National Institute of Standards and Technology
- http://www.nist.gov/cyberframework/upload/cybersecurity-021214-final.pdf. February 12, 2014
5. Vijayalakshmi, Y. (2017). Cyber Crimes in Kerala. UGC Approved Journal , 1159.
6. Panda, B., & Rout, J. K. (2020). Cyber Crime Prevention in India: A
Critical Analysis of the Information Technology Act, 2000. International Journal of Information Science and Communication Technology, 9(1), 1-8.
7. Indian Computer Emergency Response Team (CERT-In). (2021). Annual Report 2020. Ministry of Electronics and Information Technology, Government of India.
8. Shetty, P., & Bhatt, V. (2019). Cybersecurity Challenges in India: A
Comprehensive Study. International Journal of Computer Applications, 182(6), 11-17.
9. Sharma, A., & Choudhary, A. (2021). Cyberbullying in India: Challenges and Preventive Measures. Journal of Cybersecurity and Privacy, 2(1), 45-59.
10. Tiwari, M., & Garg, V. (2020). A Study on the Prevalence and Impact of Online Grooming in India. International Journal of Cybercrime and Digital Forensics, 12(2), 76-89.
11. Patil, A., & Kapoor, S. (2019). Trends in Cyber Crime: A Case Study of Online Identity Theft in India. Journal of Information Technology and Management, 10(4), 112-125.
12. Ministry of Home Affairs, Government of India. (2021). Cyber Crime Prevention Initiatives: A
Status Report.
13. National Crime Records Bureau. (2021). Crime in India 2020. Ministry of Home Affairs, Government of India.
14. Vatuk, S. (2021). Cyber Crime and the Legal Challenges in India. Journal of Cybersecurity and
Data Privacy, 3(2), 87-101.
15. Kapoor, R., & Singh, S. (2019). Cybersecurity Preparedness in India: An Assessment of Government Initiatives. Journal of Cybersecurity Policy and Strategy, 7(3), 213-228.
16. National Commission for Protection of Child Rights (NCPCR). (2021). Guidelines on Safeguarding Children from Cyber Crime.
17. Jain, A., & Mehra, A. (2022). A Roadmap to Strengthen Cyber Laws in India: Addressing Emerging Challenges. International Journal of Cyber Law and Ethics, 9(2), 189-20.