IS SOCIAL MEDIA DRIVING THE RISE OF CYBER CRIME? EXPLORING THE INTERSECTION BETWEEN SOCIAL MEDIA USE AND CYBERCRIME VICTIMIZATION

Agrim Tandon*

ABSTRACT

Today, the internet has ingrained itself into our daily lives to the point where it is difficult to picture existence without it. Our lives have become increasingly dependent on online media as a result of advancing technology, which offers venues for simple connections with people all over the world. This vast increment in the usage of social networking sites has a significant and substantial influence on the evolution of cybercrime in today's era. In addition to that, social media also facilitates, directly or indirectly, cybercriminals with all the necessary information which is required by them for the commission of cyber crimes. This paper is therefore written with the objective of analyzing the link between social networking websites and cyber crimes. First and foremost, the paper would explain what cybercrime is and its types. Thereafter, the paper would establish the influence of social media on the evolution of cyber crimes, wherein the paper would talk about the abetment provided by social media to cybercriminals. Lastly, the paper would discuss the current position of India's cyber security infrastructure and would also suggest certain countermeasures which could help combat cybercrimes.

Keywords: Social Media, Cyber Crime, Information Technology Act, Hacking, Phishing, Stalking, Bullying

INTRODUCTION

The term *'Cyber Crime'* is per se not defined anywhere but, in a general sense, it can be defined as crimes or illegal activities which are committed through the use of the internet and digital technologies such as computers, mobile phones, etc. "According to the Organization for Economic Cooperation and Development (OCED), *Computer crime is any illegal, unethical or unauthorized behavior involving automatic processing and/or transmission of data."*[1]

*BCOM LLB, FOURTH YEAR, INSTITUTE OF LAW, NIRMA UNIVERSITY.

[1] Dr. Mrs. K Sita Manikyam "Cyber Crimes Law & Policy Perspectives" Page no. 44, Edn (2009)

Cybercriminals take the help of technology to attack computer systems and networks to steal confidential data, interfere with services, demand money, or do other forms of harm. The prevalence of digital technology and the growth of the Internet have increased the threat that cybercrime poses to people, companies, and governments all over the world.

Cyber Crimes can be committed to committing financial, personal, and reputational harm to a person, an organization/establishment, or a government agency, and it is usually difficult to detect and prosecute a Cyber Crime due to its anonymity and cyber jurisdiction.

TYPES OF CYBER CRIMES

Cyber Crime can be of several kinds. Some of the most common forms of Cyber Crimes are:

Identity Theft: The terms "identity theft" and "identity fraud" are used to describe online crimes in which a perpetrator fraudulently obtains and utilizes the personal information of another person to benefit financially. Information like the social security number, bank account number, or credit card number may be utilized for personal gain at the expense of others.

Phishing: Phishing has been a serious concern in India. Phishing is a cybercrime in which the cybercriminal tricks another person to provide him with personal or financial data about that person.

Cyber Stalking: Cyberstalking in a simple sense means online stalking. Cyberstalking typically affects women who are pursued or harassed by men, or children who are pursued by pedophilic or predatory adults. Internet, email, and other forms of electronic communication are used by cyberstalkers to track their targets.

Cyber defamation: The act of creating false claims or disseminating misleading information about a person or organization via electronic communication channels such as social media, websites, or other online platforms is known as cyber defamation, also known as online defamation. The false information may be presented as text, pictures, videos, or audio files.

Cyber Bullying: Bullying is a form of harassment where someone is coerced into doing something they do not want to. Teenagers and young adults regularly go through it. This has become incredibly commonplace. It includes, among other things, creating bogus websites about individuals, writing comments, using insulting language when referring to individuals, disseminating meaningless photographs or videos of individuals, and much more.

Hacking: Hacking means gaining unauthorized access to information systems to cause disruption, alteration, extraction, or destruction of information. It also includes the introduction of malicious software into that system.

Malware: These malicious software developers cover up harmful links, attachments, or chats, which is a typical feature of social networking websites. When these links or attachments are clicked, the virus sneakily infects the machine.

Pornography: Section 67 of the IT Act that obscenity is an offense when it is published or caused to be published in any electronic form. Therefore, if any pornographic material is published or transmitted, then it would constitute a cybercrime.

Skimming: Every credit card contains a magnetic strip at its back that carries information about that specific card. Many criminals may use a skimming machine to create a clone of that card, and then this clone/fake card is used to make unauthorized purchases.

INFLUENCE OF SOCIAL MEDIA ON CYBER CRIMES

As long as the internet has existed, cybercrimes have existed. But the prevalence and seriousness of cybercrimes have significantly increased since the advent of social media. The usage of social media has given cybercriminals new ways to perpetrate crimes. Any digital technology that enables users to instantly generate and share material with the public is referred to as social media. Facebook, WhatsApp, Twitter, Instagram, and LinkedIn are among well-known social networking platforms. Any internet-connected device, whether a computer, smartphone, iPad, or other mobile device, can access it.

Due to its extensive reach, online media has an impact on young people. Social media offers a platform that connects people to the rest of the world via the internet, voice, and video conversations, chat rooms, and a host of other features. Any social media network can be joined with a very simple method that is also suitable for young people to use. A person must register with their personal information to join any social media platform. Once logged in, they can view the platform's material and share data, images, or information with other users of that social media platform.

Social networking is a fantastic tool for meeting new people, forming connections, exchanging ideas, and growing businesses. Without relying on conventional media outlets, social media gives people a platform to easily share information and thoughts with a huge section of the

public. “Social media has been playing a significant influence in influencing people's thoughts and beliefs. Social networking site data is a useful source of information for analyzing the flow of ideas, viewpoints, and opinions, among other things. Knowing how often information is shared, who is sharing it, and what the information is about is incredibly useful”.[2]

Social media will have both beneficial and harmful effects on today's youngsters. “Despite several wonderful advantages, these social networking platforms are also responsible for the dissemination of pornographic material on a large scale among teenagers. There have been instances where teens have discussed raping a minor on a social networking platform”.[3] Additionally, while social media on the one hand disseminates information, it also facilitates the propagation of false information. The main platform for spreading fake information is WhatsApp and the fact that some people still believe it is worrisome. Spreading of such rumors and fake news often becomes the reason for conflict and hostility among distinct groups

Apart from that, these social networking sites are also a haven for cybercriminals looking for unwary victims. Social media, for instance, has given a platform for identity theft, online abuse, and cyberbullying. Social media has also been used by cybercriminals to propagate malware, launch phishing attacks, and steal financial and personal data.

In the current digital era, social networking websites are widely used, which has drawn online scammers who want to boost their chances of obtaining victims to create many social media accounts and join various social media platforms. Cybercriminals are preferring social media websites for the commission of cyber crimes due to the following advantages which are offered to them by these social networking websites:

Wide Audience: Studies demonstrate how popular social media is in India. Social media sites have a big user base, which allows cybercriminals to spread malware, conduct phishing schemes, and otherwise target more people. Additionally, social media makes it simpler for fraudsters to locate potential victims. A cybercriminal might, for instance, utilize social media to find people who are on vacation and hence more open to phishing attacks.

[2] Zhang, X., Huang, L., Cheng, T. and Wu, W. "Exploring the effects of social media on consumers' brand attitude: The roles of message content, message sender, and message receiver" (2021) 130 Journal of Business Research 454-462.
[3] Rastogi, R. and Rastogi, M. "Study of the Impact of Social Networking on Today's Youth" (2017) 7(5) International Journal of Advanced Research in Computer Science and Software Engineering 973-977.

The large pool of data: Due to the enormous amount of data provided by users, social media has had a huge impact on the development of cyber crimes. Social networking sites gather a ton of information on their users, such as personal data, internet activity, and social connections. For cybercriminals, this information is a gold mine that they may exploit to execute specialized assaults and con games. Anybody can hack into that person's information, and other people may misuse it. Anybody can create a new profile using your name and details, and anyone with access to your photos can use them for whatever purpose they choose.

Easy access: The ease of information access is another way social media has influenced the development of cybercrimes. Instant information sharing is made possible by social media platforms, which can be both a blessing and a curse. While this has made it simpler for people to communicate with one another and for organizations to do business, it has also made it simpler for hackers to obtain private data. A cybercriminal, for instance, might utilize social media to obtain data on a company's staff, clients, and partners for use in a phishing attack.

Anonymity: social media has made it simpler for cyber criminals to maintain their anonymity. This is because the users of social media platforms are not required to disclose their true identities or other forms of identification. The difficulty in locating cybercriminals due to their anonymity has contributed to the surge in cybercrime.

Trust: Users of social media may be more vulnerable to fraud or phishing efforts because they tend to believe the content that they encounter on these sites.

Easy transmission: Social media has also made it simpler for hackers to transmit malware. A sort of software called malware is intended to harm or interfere with computer systems. Malicious links are sent to their targets by online criminals who utilize social media to propagate malware. When the user clicks on these links, their machine is infected with malware even though they seem to be legal.

To commit cyber crimes over social media, cybercriminals use certain forms of social engineering techniques to convince people to reveal confidential information or take activities that could jeopardize their security. Some of the most popular social engineering techniques are:

Bating: Cybercriminals might, for instance, set up phony social network accounts that offer gift cards, vouchers, or other incentives to individuals who click on a link. Users unknowingly

download malware onto their devices when they click on the link, which can be used to steal their private information or give thieves access to their devices.

Pretexting: Pretexting is a social engineering tactic where cybercriminals fabricate a story to win over their target's trust and induce them to reveal private information. For instance, to acquire personal information, fraudsters may set up phony social media accounts impersonating a customer service agent or a reliable friend. Cybercriminals may request sensitive information, such as login credentials or credit card information after they have won the user's trust.

Social Grooming: Using the social grooming strategy, hackers establish a rapport with their victims over time to acquire their trust before taking advantage of it. Cybercriminals could construct phony social media profiles, reach out to their target, and start conversations, slowly but surely establishing a relationship over time. Once they have the user's trust, they can utilize that relationship to get access to private data or trick them into doing something that might jeopardize their security.

INDIA'S CYBER SECURITY INFRASTRUCTURE

Depending on a nation's level of technological development, the size and complexity of its digital networks, and the amount of money invested in cybersecurity, different nations have different levels of cybersecurity infrastructure. "Law enforcement agencies in various countries such as the USA, the UK, and China have created specialized teams to investigate and prosecute these types of offenses, and many nations have legislation in place to handle cybercrime".[4]

The vast usage of social media and digitalization has made it crucial for India too to develop a strong cybersecurity infrastructure. Threats to cyber security are always changing, and the risks connected to them are increasing quickly. The Indian government has made several steps to strengthen its cyber security infrastructure after realizing the necessity for one.

India's cyber security infrastructure is made up of a variety of components, including laws, regulations, and technologies. The Indian legislation has implemented several regulations to govern the increasing number of crimes. The enactment of the Information Technology Act, of

[4] Bhaskar, U. and Kodackal, S. M. "Cyber Crime: A Review of the Evidence" (2011) 5(1) International Journal of Cyber Criminology 1-21.

2000 is its prime example. The IT Act of 2000 stipulates sanctions for several offenses and offers a legal framework for handling cybercrime.

Some of the relevant provisions of the Information Technology Act, of 2000 are:

Section 43[5]: This provision of the IT Act is applicable to those people who commit cyber crimes, such as harming the victim's computer without the victim's express authorization. If a computer is damaged in such a case without the owner's permission, the owner is completely entitled to a refund for the whole damage.

Section 66B[6]: As per this provision, receiving computers or other electronic equipment that has been obtained fraudulently has repercussions, including a maximum three-year prison sentence, which is described in this section. Depending on the severity, a fine of up to Rs. 1 lakh may also be levied.

Section 66C[7]: The key subjects covered in this section include digital signatures, password hacking, and various forms of identity theft. A maximum punishment of three years in prison and a fine of one lakh rupees are associated with this clause.

Section 66D[8]: The use of computer resources to impersonate someone else to cheat is covered in this section. The maximum sentence for conviction is three years in prison, and the maximum fine is Rs. 1 lakh.

Section 66E[9]: This law makes it illegal to take pictures of private spaces without the owner's permission and to publish or transmit those images. If found guilty, penalties include up to three years in prison and/or a fine of Rs.2 lakh.

Section 67[10]: This provision talks about the publishing of obscenity through electronic means. If found guilty, can be punished with imprisonment up to 5 years or a fine of up to Rs.10 lakhs

If the IT Act is not sufficient enough to cover all cybercrimes, then law enforcement agencies can also simultaneously apply the following relevant provisions of IPC:

[5] Information Technology Act 2000, s 43
[6] Information Technology Act 2000, s 66B
[7] Information Technology Act 2000, s 66C
[8] Information Technology Act 2000, s 66D
[9] Information Technology Act 2000, s 66E
[10] Information Technology Act 2000, s 67

Section 292[11]: Although the purpose of this provision was initially to prevent the selling of pornographic materials, it has now expanded to include several cyber offenses. This section also applies to the electronic dissemination of young people's sexually explicit or pornographic acts or adventures. Such violations are subject to fines of Rs. 2000 and prison sentences of up to two years. Any of the aforementioned crimes may carry a penalty of up to five years in prison and/or a fine of up to Rs. 5000 for repeat (second-time) offenders.

Section 354C[12]: This section defines cybercrime as the taking or disseminating of photos of a woman's private or intimate actions without the woman's consent. The only subject discussed in this section is voyeurism because it is impermissible to observe a woman having sex. In the absence of the elements required by this section, Sections 292 of the IPC and Section 66E of the IT Act are broad enough to cover offenses of a similar nature. The maximum jail term for first-time offenders is three years, while the maximum punishment for repeat offenders is seven years.

Section 354D[13]: This clause defines and criminalizes stalking, which includes offline and internet stalking. Cyberstalking is the act of contacting or following a woman despite her lack of interest via technology, such as the Internet or email. This felony carries a potential term of 3 years in prison for a first offense and a maximum sentence of 5 years in prison and a fine for a second offense.

Section 379[14]: This IPC Section is important in part because many cybercrimes include electronic devices, data, or computers that have been stolen. The maximum punishment for theft under this provision is three years in prison as well as a fine.

Section 420[15]: The handover of property under duress and fraud is covered in this section. According to this provision, internet criminals who fabricate websites and engage in online fraud face a seven-year prison sentence in addition to a fine. This section of the IPC deals with offenses like fabricating websites or stealing passwords to make money.

Apart from laws and regulations, the cyber security infrastructure in India is heavily reliant on technology. To enhance cyber security, the government has adopted several technologies,

[11] Indian Penal Code 1860, s 292
[12] Indian Penal Code 1860, s 354C
[13] Indian Penal Code 1860, s 354D
[14] Indian Penal Code 1860, s 379
[15] Indian Penal Code 1860, s 420

including firewalls, intrusion detection systems, and antivirus software. "The National Cyber Coordination Centre (NCCC), which monitors the nation's internet traffic and aids in the identification of potential cyber threats, is just one of the efforts the government has put into place".[16]

Although the Indian government has made substantial efforts in improving India's cyber security infrastructure, India's cyber security infrastructure still has several flaws. The general public's ignorance of cyber security issues is a serious problem. "India's population is still mostly technologically illiterate, and many people are unaware of the dangers posed by cyber security attacks. This increases their susceptibility to phishing scams and online threats".[17]

PRECAUTIONARY MEASURES/COUNTERMEASURES TO PREVENT CYBER CRIMES

Cybercrime can be fought using a variety of countermeasures. Among these defenses are:

Education: Spreading knowledge or awareness is one of the best strategies to fight cybercrime. People need to be aware of the dangers of social media and how to defend themselves against online attacks. This involves educating people on how to spot phishing emails and safeguard their personal data.

Cyber security tools: Cyber security technologies including intrusion detection systems, antivirus software, and firewalls can assist defend against cyber attacks. By detecting and blocking illicit communication, these solutions help stop fraudsters from obtaining confidential data.

Strong passwords: For the protection of personal information, strong passwords are crucial. For each of their internet accounts, people should choose unique, difficult passwords that they change frequently.

Platform security measures: Social media sites must defend their members against online criminality. To prevent unauthorized access to user data, platforms should have strong security measures in place, like encryption. Additionally, they must keep an eye out for any suspicious activity, such as repeated login attempts or odd patterns of behavior, and notify users when

[16] Sharma, S. "India to set up National Cyber Coordination Centre" The Economic Times (10 January 2017)
[17] Shukla, S. "Lack of awareness makes Indians susceptible to phishing scams" (2021) The Economic Times (28 April 2021)

they believe their accounts may have been hijacked. The use of tools to report and block questionable activity, such as spam, fraudulent accounts, and phishing scams, should be available to users on social media platforms.

Two-step authentication: By forcing users to submit two different forms of identity, two-factor authentication adds an extra layer of protection. This will prevent cybercriminals from accessing personal information even after obtaining the user's password.

CONCLUSION

In summary, social media has significantly influenced the development of cybercrime. Cybercrime has increased as a result of easier access to private information, anonymity, and the capacity to reach a wider audience. These social networking websites not only serve as a platform for the commission of cybercrimes but have also been responsible for the invention of new cybercrimes or cyber frauds.

In conclusion, "cybercrime is a complicated and dynamic issue that calls for a multifaceted strategy to address it. One of the primary issues with cybercrime is the absence of an absolute law at any place in the world".[18] The problem gets worse because all internet and cyber-related rules are growing at an unbalanced rate. Even if the Information Technology Act and the IPC changes mark a great start, there are still issues and concerns related to cybercrime. Laws must be amended, but the internet literacy gap must also be closed. To defend people and organizations from cyber attacks, it is crucial to adopt countermeasures including education, cyber security tools, strong passwords, and two-factor authentication. In the era of social media, it is crucial to be cautious and take preventative measures to safeguard personal information.

Furthermore, to find and pursue cybercriminals, law enforcement organizations should collaborate closely with social networking sites. This may entail exchanging details regarding dubious actions or people and working together on investigations. Law enforcement organizations and social media companies can collaborate to fight cybercrime and safeguard users.

[18] Verma, S. and Kapoor, S. "A Comprehensive Review on Cyber Security and Cyber Crime" (2017) 8(1) International Journal of Advanced Research in Computer Science 111-116.

JLRJS
Journal of Legal Research and Juridical Sciences