IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, December 2025
Impact Factor: 7.67

Cyber Crime and Social Media

Asst. Prof. Savita B. Chavhan
Matoshri Anjanabai Mundafale College of Social Work, Narkhed Dist.Nagpur
chavhansb15@gmail.com

Abstract: *The internet in India is growing rapidly. It has given rise to new opportunities in the field of entertainment, business, sports, education, and many more. With the advent and increasing use of the internet, businesses have crossed the barriers of local markets and are reaching out to customers located in every part of the world. Computers are widely used in enterprises not only as a tool for processing information, but also for gaining strategic and competitive advantage.*

Keywords: *Internet*

I. INTRODUCTION

The internet in India is growing rapidly. It has given rise to new opportunities in the field of entertainment, business, sports, education, and many more. With the advent and increasing use of the internet, businesses have crossed the barriers of local markets and are reaching out to customers located in every part of the world. Computers are widely used in enterprises not only as a tool for processing information, but also for gaining strategic and competitive advantage. Computers can be used both for constructive and destructive reasons.Cybercrime on social media is a broad range of illegal activities that take place on social media. These crimes can include identity theft, harassment, and online fraud.

At the beginning we have to know the meaning of Cyber Security. Cyber security is the practice of protecting systems, networks and programs from digital attacks. It involves the use of technology, policies and procedures to protect against cyber safety and security.

Then we have to know the threats in this sector. What types of cyber threats such as Malware, Phishing Ransomware, Social Engineering, and D Dos attacks. Now we discuss in detail about threats in cyber security.

Malware:- It is found in computers with malicious software that can include viruses, worms, trojans, spyware and ransomware. Malware can be introduced by linking an email to an unstracted website or unwanted software downloaded.

Phishing:- Social Engineering attack that tricks people into sharing sensitive information. Phishing can occur through emails, fake websites or instant messages.Advanced phishing technique involves spear phishing and whaling.

Ransomware:- A type of malware that encrypts files on an infected device

The attacker demands a ransom from the victim in exchange for the encryption key.

Identity theft:- Stealing personal information from social media to commit fraud.

Cyberbullying:-Targeting people with hurtful or threatening messages, photos, or videos.

Impersonation:-Pretending to be a trusted person or brand to steal information.

Objectives:-

- To Aware people about Cyber Crime.
- To Protect them from Cyber Crime.
- To reduce Cyber Crime.

Hypothesis:-

- Awareness is Increased.
- Organise Awareness Campaign.
- Cyber Crime affects society.

DOI: 10.48175/IJARSCT-30450

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, December 2025 Impact Factor: 7.67

How to protect yourself :-

- Don't share personal information without security or privacy.
- Don't click suspicious links.
- Don't accept friend requests from strangers.
- Log out of social media after each session.
- Keep your social media profile's privacy settings restricted.

Steps to Cyber Security:-

Protect your data. Strong passwords and additional account security measures are an effective way.

Prevent Malware. Malicious software (malware) can cause untold damage to computers, devices and Avoid Phishing Attacks.

Backup your data.

Keep your devices safe.

Cybercrime is a significant issue on social media platforms, encompassing various illegal activities facilitated by online platforms. These activities range from online harassment and threats to fraud, identity theft, and the spread of malicious software. Social media's role as a communication and interaction medium also makes it a fertile ground for cybercriminals to target individuals and organizations.

Types of Cybercrimes on Social Media:-

1. Cyberbullying and Cyberstalking:-

Online harassment, threats, and stalking through social media are common, causing significant distress to victims.

2. Hacking and Fraud:-

Gaining unauthorized access to social media accounts, creating fake profiles, and impersonating others for malicious purposes are also prevalent.

3. Phishing and Malware:-

Social media platforms are used to distribute malicious links and emails, tricking users into revealing sensitive information or downloading malware.

4. Buying Illegal Items:-

Social media can be used to facilitate the sale of illegal goods or services, connecting buyers and sellers in the digital world.

5. Vacation Robberies:-

Criminals use social media to identify when people are on vacation, making their homes vulnerable to burglary.

Impact of Social Media on Cybercrime

1. Increased Reach and Anonymity

Social media platforms provide a vast audience and anonymity, making it easier for cybercriminals to reach potential victims and evade detection.

2. Ease of Communication

The ease of communication on social media allows cybercriminals to quickly spread misinformation, scams, and malicious links.

3. Vulnerability of Users

Users' personal information and online habits are readily available on social media, making them susceptible to various

4. Cyberattacks

Legal Implications and Prevention:

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 3, December 2025 Impact Factor: 7.67

Cybercrime Laws

Many countries have laws in place to address cybercrimes, including those related to social media, but enforcement can be challenging**.**

Cybersecurity Measures:-

Individuals and organizations can take steps to protect themselves from cybercrimes, such as using strong passwords, being cautious about online interactions, and keeping security software up to date**.**

Raising Awareness

Educational campaigns and public awareness programs are crucial to educate users about cybercrime risks and safe online practices.

Relationship between Social Media and Cybersecurity:-

Social media platforms have gained popularity among users because of their distinctive communication and engagement characteristics. However, because users disclose so much private information online, these platforms have also become targets for fraudsters. This information is used by online criminals to launch a variety of assaults, such as phishing,malware, and social engineering attempts. Since social media platforms operate in a dynamic environment with continuously changing dangers and threats, social media also poses a challenge for cybersecurity specialists.

Role of Social Media Companies and Government Bodies:-

Social media firms should take precautions to shield their consumers from online threats and attacks since they have a crucial role to play in guaranteeing cyber
security. Some of the precautions social media companies can take are as follows:

In order to protect user data, social media organisations can employ encryption (Tudor,2018). This makes it more difficult for cybercriminals to access private data.

User education: According to Krumholz et al. (2017), social media firms can offer users educational materials and advice on how to safeguard themselves against online dangers and attacks.

Strong cybersecurity rules that prioritise user safety and defend against online dangers and attacks should be implemented by social media organisations, according to Panday and Chatterjee (2019).

Government entities can play a part in maintaining cybersecurity by, among other things, taking the following actions.

Regulation: Social media firms may be subject to government regulation, including requirements that they adhere to cybersecurity standards and directives (Kshetri, 2018).

Public education: According to Nurmi and Weir (2018), governments can raise the general public's knowledge of online hazards and provide information on how to defend against cyberattacks.

Collaboration: To create and execute cybersecurity measures that safeguard users and thwart online threats and assaults, governments can work with social media firms (Holt &Kilger, 2017).

II. CONCLUSION

Social media has ingrained itself deeply into our daily lives, but it has also created fresh cybersecurity challenges. Cybercriminals are launching targeted assaults and stealing sensitive data by using a large amount of personal information available on social media. People and organisations need to adopt a proactive approach to cybersecurity in order to guard against these dangers. This includes putting technical solutions into place and instructing people on the best practices for online security. By doing this, we can contribute to keeping our online activities safe and secure.

Using strong passwords, updating your software, thinking before you click on suspicious links, and turning on multi-factor authentication are the basics of what we call “cyber hygiene” and will drastically improve your online safety. These cybersecurity basics apply to both individuals and organizations.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, December 2025
Impact Factor: 7.67

REFERENCES

[1]. Cybercrime in Social Media: Theory and Solutions By Pradeep Kumar Roy, Asis Kumar Tripathy.
[2]. Cyber Crime Analysis on Social Media BSSS Publication.
[3]. A Study on Awareness of Cyber Crime and Security. By Anupreet Kaur.
[4]. SOCIAL MEDIA AND CYBER SECURITY: PROTECTING AGAINST ONLINE THREATS AND ATTACKS by Ahmed Buhari & Zayyad Isa.
[5]. Social media and policing: An overview by Holt, T. J., & Kilger.
[6]. Phishing on social media: Risks and preventative strategies byCooke,
[7]. Social media security and privacy: A systematic review. International Journal of Information Management.