IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cyber Security Risks In Social Media

Pooja Ankush Bhoite[1], Sanika Ravindra Desai[1], Ms. Shitole A.N[2]

[1] Department of Computer Science, Annasaheb Magar Mahavidyalaya, Hadapsar, Maharashtra, India.

[2]Assistant Professor, Department of Computer Science, Annasaheb Magar Mahavidyalaya, Hadapsar, Maharashtra, India.

ABSTRACT

Social media has become an important part of everyday life, allowing people to communicate, share information, and connect globally. Along with its advantages, it has also created new opportunities for cybercriminals to exploit users through various online threats. Social media platforms are increasingly being used for cyberattacks, making cybersecurity a major concern for individuals, organizations, and governments.This paper focuses on different cybersecurity threats found on social media platforms, including phishing attacks, identity theft, malware attacks, social engineering, and data privacy issues. The research is based on the review of existing literature related to cybersecurity risks and social media security.

Platforms such as Facebook, Twitter, and Instagram are considered highly vulnerable because they store large amounts of personal information and involve continuous user interaction. These platforms are widely used for communication and information sharing, but they can also be misused for spreading misinformation, conducting cyberattacks, and stealing sensitive data.The paper highlights important cybersecurity concerns associated with social media and discusses practical preventive measures that can help users protect their personal information and maintain online safety.

KEYWORDS

Cybersecurity risk, Cyber threats, mitigation techniques, Identity Theft, Risks Prevention in Social Media sites, Social Engineering

INTRODUCTION

In today's digital world, social media has become a major part of our everyday lives. People use it to stay connected with friends and family, share ideas, and communicate across the globe. Over time, it has grown from simple tools like email and early online forums into powerful platforms such as Facebook, Twitter, and MySpace, where users can interact instantly and share content on a large scale[3]. The rise of smartphones and easy internet access has made these platforms even more popular and widely used[4].

Although social media offers many benefits—like better communication, quick access to information, business opportunities, and increased awareness—it also comes with serious cybersecurity risks[6]. Many users share personal details, including their location and daily activities, without realizing how this information can be misused[1]. This makes them easy targets for cybercriminals[2].

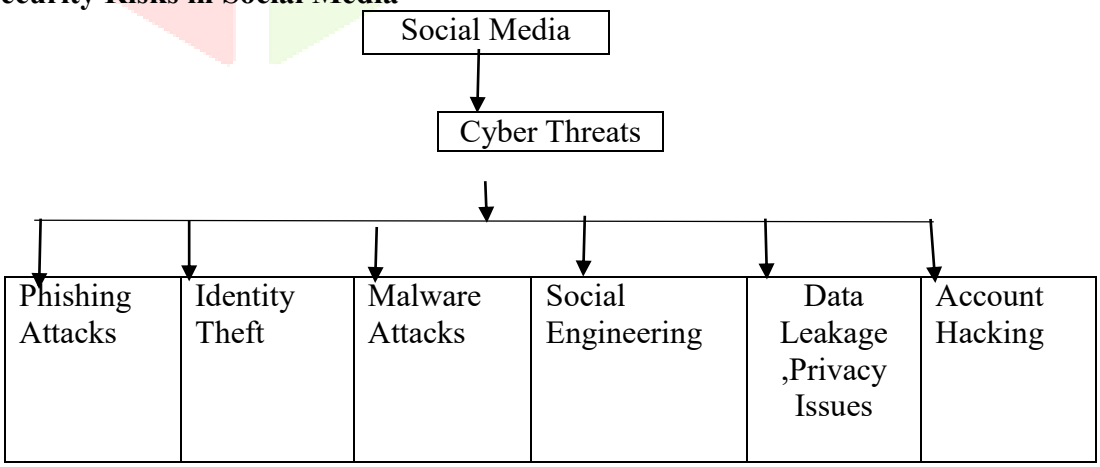
The problem is often made worse by a lack of awareness about online safety. People commonly use weak passwords, accept friend requests from strangers, or click on unknown links, which can lead to hacking or data theft [6][11]. Even organizations are at risk when employees accidentally share sensitive information online, which raises security and privacy issues for businesses and institutions [7][12].Because of these issues, it is very important to understand the different types of cybersecurity

threats on social media, why they happen, and how they affect users [8]. Taking proper precautions and following safe practices can help ensure a more secure and responsible use of social media [9][10].

LITERATURE REVIEW

Social networking sites have become a popular way for people to create an online presence and stay connected with family, friends, and even strangers. These platforms let users easily share their activities, interests, and personal experiences. However, the large amount of information shared online has also given hackers and cybercriminals chances to steal personal data and misuse it [1]. This study focuses on the main privacy and security challenges found online and discusses the different types of threats that users face. It also suggests practical ways to improve digital safety and awareness [6]. While social media platforms may seem secure and easy to use, they can still expose individuals to hidden risks, harmful content, and cyberattacks [2]. The study explains the key features of Social Networking Sites (SNSs) and provides a clear understanding of their concept and how they have developed over time. It highlights how these platforms have changed and become an important part of modern communication. The research also reviews previous studies related to SNSs for a better understanding of existing findings and to identify future research opportunities in this area [3].Social media has made communication and content sharing faster and easier. However, these platforms collect a lot of user data and create detailed user profiles using new technologies. This raises serious privacy concerns and increases the risk of misuse of personal information. The study discusses legal and technical measures that can help protect users and improve privacy on social networking platforms [4]. Researchers also note that privacy and security issues are affected by both technology and institutional policies, making user awareness and proper regulations very important [7]. Social networking platforms support communication, information exchange, and business growth, but they also bring many cybersecurity threats. These threats continue to evolve and include phishing attacks, malware, identity theft, and unauthorized access to personal information [5]. Studies on mobile social media security further highlight the growing risks associated with smartphones and portable devices, where cybercriminals often target users through malicious links and applications [8]. To reduce online risks, organizations and individuals should follow cybersecurity policies and adopt safe online practices. Research shows that awareness programs, penalties, and user motivation play a key role in encouraging secure behaviour and improving compliance with security policies [9][10]. Training programs, including techniques that focus on phishing awareness, have also been effective in reducing the success of cyberattacks [11]. With the rapid growth of Web 2.0 technologies and enterprise social networking, concerns about online security have increased significantly [12]. Recent research has explored how social media platforms can be used for cybersecurity intelligence and cyberattack detection through crowdsourcing and data analysis techniques [13].

Cyber Security Risks in Social Media



Social media platforms expose users to a wide range of cybersecurity threats due to the large volume of personal information shared and the high level of user interaction. These risks can affect both individuals and organisations, leading to financial loss, privacy breaches, and reputational damage. The major cybersecurity risks associated with social media are discussed below:

Phishing Attacks

Phishing is one of the most common cyber threats on social media platforms. Cybercriminals send deceptive messages, links, or emails that appear to originate from legitimate sources. These messages are designed to trick users into revealing sensitive information such as login credentials, banking details, or personal data. Once obtained, this information can be used for unauthorised access or financial fraud.

Identity Theft

Identity theft occurs when attackers collect personal information from user profiles, such as names, photos, contact details, and other private data. This information is then used to impersonate the victim, commit fraud, or gain access to secure systems. Social media makes it easier for attackers to gather such data due to oversharing by users.

Malware Attacks

Malware attacks involve the distribution of malicious software through infected links, advertisements, or downloadable content on social media platforms. When users click on such links, their devices may become infected, allowing attackers to steal data, monitor activities, or damage the system.

Social Engineering

Social engineering exploits human psychology rather than technical vulnerabilities. Attackers manipulate users into revealing confidential information by gaining their trust. This may involve fake profiles, impersonation, or emotional manipulation to trick users into sharing sensitive details.

Data Leakage and Privacy Issues

Many users unknowingly share personal information such as location, daily activities, and contact details on social media. This oversharing increases the risk of data leakage, where sensitive information becomes accessible to unauthorized individuals and can be misused for cybercrimes.

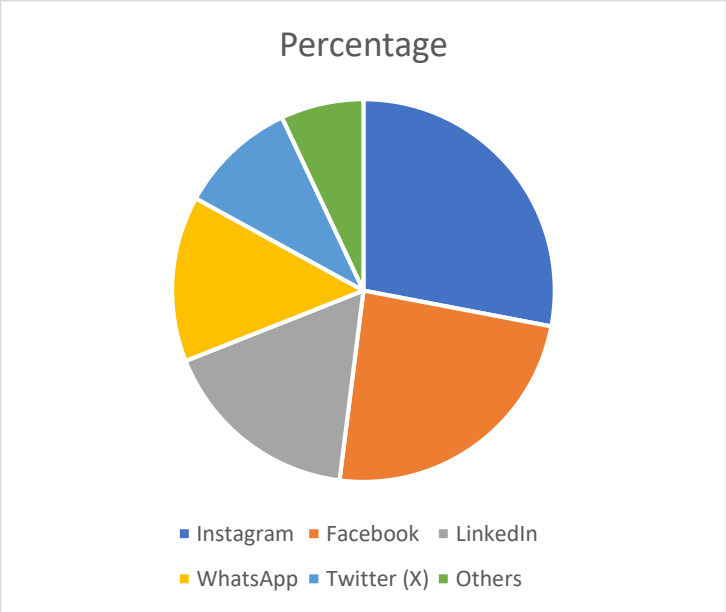
Account Hacking

Account hacking occurs when attackers gain unauthorized access to user accounts. This is often due to weak passwords, reuse of credentials across multiple platforms, or the use of unsecured networks. Once compromised, accounts can be used to spread spam, scams, or malicious content.

Tables

1. SOCIAL NETWORKING SITES

Platform	Percentage
Instagram	28
Facebook	24
LinkedIn	17
WhatsApp	14
Twitter (X)	10
Others	7



Instagram

Instagram is a popular platform for sharing photos, videos, and reels, widely used for communication, entertainment, and business promotion. Users interact through likes, comments, and messages.

However, its high user engagement and personal content sharing make it vulnerable to cyber threats like fake accounts, phishing, and identity theft. It accounts for about **28%** of social media threats due to its large user base and frequent sharing of personal information.

Facebook

Facebook is a widely used platform where users create profiles, share updates, join groups, and connect globally. It is also popular for business promotion and events.

However, the large amount of personal data and high user interaction make it vulnerable to cyber threats like phishing, malware links, and data leakage. It accounts for about **24%** of social media threats, making it a common target for such attacks.

LinkedIn

A professional networking platform used for jobs, career growth, and business connections. Users share resumes, skills, and company details. Due to sensitive professional information, it is targeted by fake recruiters, job scams, and phishing attacks. LinkedIn contributes **17%** of cyber threats, as it contains professional and sensitive information, making it vulnerable to job scams and phishing attempts.

WhatsApp

A messaging application used for sending texts, media, and calls. It is widely used for personal and business communication. However, it is vulnerable to OTP scams, fake messages, and account hacking due to user trust and message forwarding. WhatsApp accounts for **14%**, where threats mainly occur through fraudulent messages, OTP scams, and account hijacking.

Twitter

A platform used for sharing short messages (tweets), news, and trending topics. It is widely used by individuals and organizations for real-time communication and promotion. Due to its public and fast nature, it is exposed to fake accounts, phishing links, misinformation, and hacking. Information spreads quickly, increasing risk.

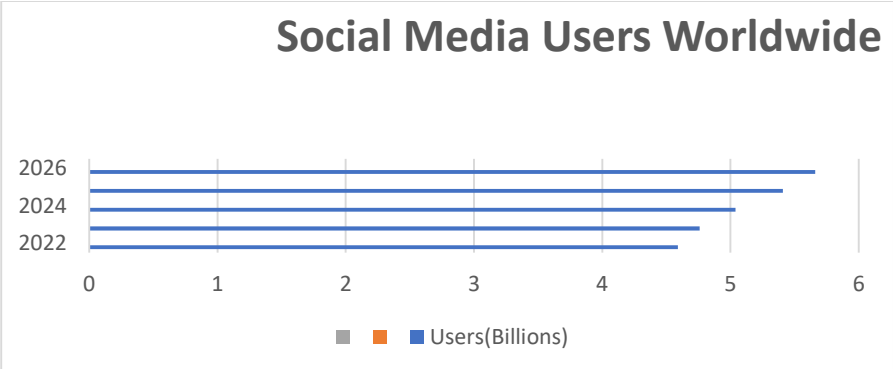
Twitter (X) represents **10%** of threats due to its open and public nature, which allows the spread of fake accounts, phishing links, and misinformation.

Others

Other platforms also contribute to cyber threats but at a lower level. These include smaller or less frequently used social media applications. Risks include basic phishing, malware, and data misuse. The remaining **7%** falls under other platforms, which also face cyber risks but at a lower level.

2. Social Media Users Worldwide

Year	Users (Billions)
2022	4.59
2023	4.76
2024	5.04
2025	5.41
2026	**5.66**

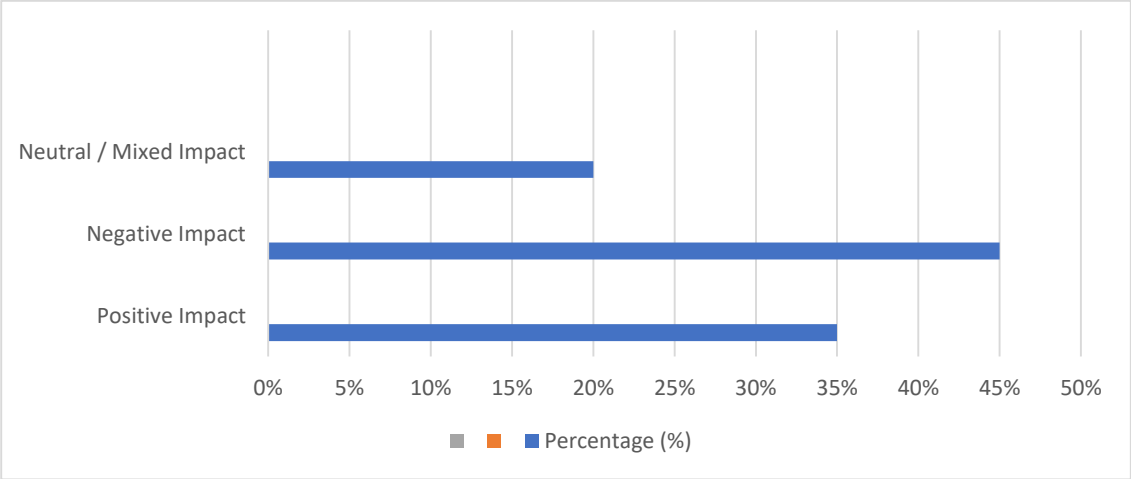


The bar graph shows the growth of social media users worldwide from 2022 to 2026. It is observed that the number of users has increased continuously each year, reaching approximately 5.66 billion users in

2026. This growth indicates the rapid adoption of social media across the globe, making it an essential part of communication, business, and daily life.

3. Impact of Social Media on Teenagers (2026)

Impact Type	Percentage (%)
Positive Impact	35%
Negative Impact	45%
Neutral / Mixed Impact	20%



The bar graph shows the impact of social media on teenagers. It indicates that 45% of teenagers experience negative effects such as addiction, anxiety, and reduced concentration. About 35% experience positive impacts like learning, communication, and creativity, while 20% have a neutral or mixed impact. This shows that although social media has benefits, its negative effects are more dominant among teenagers.

Research Methodology

1.Research Approach

This study adopts a **qualitative research approach** to analyze cybersecurity risks associated with social media platforms. The research focuses on understanding different types of cyber threats, their impact on users, and the role of social media platforms in increasing vulnerability.

2.Data Collection Method

- Research papers and journals
- Online articles and reports
- Cybersecurity statistics websites
- Case studies related to social media threats
-

3.Future Scope of the Study

- Use Artificial Intelligence (AI) and Machine Learning (ML) for threat detection
- Develop **advanced security systems** like multi-factor authentication and biometrics
- Create **awareness programs** to educate users about cybersecurity
- Improve **government policies and regulations** for cybercrime prevention
- Continuous research on **new and evolving cyber threats**

4.Challenges and Open Issues

Despite advancements in cybersecurity, several challenges still exist in securing social media platforms:

Lack of User Awareness

Many users are unaware of cyber threats and follow unsafe practices, increasing their vulnerability.

Rapidly Evolving Cyber Threats

Cyberattack techniques continuously change, making it difficult to detect and prevent new threats effectively.

Privacy and Data Misuse

The large amount of personal data shared on social media raises serious concerns about privacy and unauthorized use.

Fake Profiles and Bots

The presence of fake accounts and automated bots makes it difficult to control misinformation, scams, and malicious activities.

Third-Party Application Risks

Integration with external applications can introduce security vulnerabilities and increase the risk of data breaches.

Conclusion

Social media has become an essential part of modern life, providing a powerful platform for communication, information sharing, and business growth. However, along with these benefits, it also introduces significant cybersecurity risks that cannot be ignored. This study highlights that social media platforms such as Instagram, Facebook, LinkedIn, WhatsApp, and Twitter are increasingly targeted by cybercriminals due to the large amount of personal and professional data shared by users.

The research shows that common threats such as phishing, identity theft, malware attacks, social engineering, data leakage, and account hacking are widely present across these platforms. Among them, phishing and account-related attacks are the most common, mainly due to user negligence and lack of awareness. Instagram and Facebook account for the highest percentage of threats because of high user engagement and data sharing.

Furthermore, the increasing number of social media users worldwide, reaching approximately 5.66 billion in 2026, indicates that the risk of cyber threats will continue to grow. The study also reveals that social media has a significant impact on teenagers, with negative effects such as addiction, anxiety, and reduced concentration being more dominant than positive outcomes.

In conclusion, while social media offers numerous advantages, its safe usage depends on user awareness, responsible behavior, and proper security practices. Users must adopt measures such as strong passwords, privacy settings, and cautious interaction with unknown sources. Continuous awareness and improvements in cybersecurity technologies are essential to minimize risks and ensure a safer digital environment.

References

1. . Kumar, A., Gupta, S. K., Rai, A. K., & Sinha, S, "Social networking sites and their security issues," International Journal of Scientific and Research Publications, vol. 3, no. 4, pp. 1-5, 2013.
2. saima shoro2018 https://www.academia.edu/94157465/Social_Media_Security_Risks_and_Cyber_Threats
3. N. B. Ellison, "Social network sites: Definition, history, and scholarship," Journal of computer-mediated Communication, vol. 13, no. 1, pp. 210-230, 2007.
4. Gritzalis, D., Kandias, M., Stavrou, V., & Mitrou, L, "History of information: the case of privacy and security in social media," In Proc. of the History of Information Conference , pp. 283-310, 2014.
5. Dr. Sunil Kumar, Vikas Somani April 2018 https://www.scribd.com/document/634424038/Untitled
6. He, W. (2012). *A review of social media security risks and mitigation techniques*. Journal of Systems and Information Technology, 14(2), 171–180. DOI: https://doi.org/10.1108/13287261211232180
7. Kshetri, N. (2012). *Privacy and security aspects of social media: Institutional and technological environment*. Pacific Asia Journal of the Association for Information Systems, 4(4), 1–28. DOI: https://doi.org/10.17705/1pais.03401

8. He, W. (2013). *A survey of security risks of mobile social media through blog mining and an extensive literature search*. Information Management & Computer Security, 21(5), 381–400. DOI: https://doi.org/10.1108/IMCS-12-2012-0068

9. Herath, T., & Rao, H. R. (2009). *Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness*. Decision Support Systems, 47(2), 154–165. DOI: https://doi.org/10.1016/j.dss.2009.02.005

10. Herath, T., & Rao, H. R. (2009). *Protection motivation and deterrence: A framework for security policy compliance in organisations*. European Journal of Information Systems, 18(2), 106–125. DOI: https://doi.org/10.1057/ejis.2009.6

11. Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). *Training to mitigate phishing attacks using mindfulness techniques*. Journal of Management Information Systems, 34(2), 597–626. DOI: https://doi.org/10.1080/07421222.2017.1334499

12. Almeida, F. (2012). *Web 2.0 technologies and social networking security fears in enterprises*. DOI/Link: https://arxiv.org/abs/1204.1824

13. Khandpur, R. P., Ji, T., Jan, S., Wang, G., Lu, C. T., & Ramakrishnan, N. (2017). *Crowdsourcing cybersecurity: Cyber attack detection using social media*. DOI/Link: https://arxiv.org/abs/1702.07745