INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (IJSREM)
VOLUME: 07 ISSUE: 08 | AUGUST - 2023 SJIF RATING: 8.176 ISSN: 2582-3930

CYBER THREATS IMPLICATIONS ON SOCIAL NETWORKING SITES

Madhushree
Master of Computer Applications
Dayananda Sagar College of Engineering
Banglore
madhushree2429@gmail.com

Prof.Pavithra .B
Master of Computer Applications
Dayananda Sagar College of Engineering
Banglore
pavithra-mcavtu@dayanandasagar.edu

***Abstract*—Social networkingservices have revolutionized how individuals connect, communicate, and exchange information online since their introduction and popular use. However, this digital revolution has also opened the door to an array of cyber threats that pose significant challenges to the security and privacy of users and platforms alike. The goal of this study is to investigate the complex effects that cyber attacks have on social networking sites. The research delves into various types of cyber threats, including but not limited to malware, phishing, social engineering, data breaches, and identity theft, that target social networking platforms and their users. By analyzing real-world case studies and relevant statistics, the paper identifies the most prevalent cyber threats affecting these platforms and their consequences for individuals, businesses, and the overall online community.**

Keywords— cyber threats, social networking sites, cybersecurity, privacy, data breaches, online community

I. INTRODUCTION

The advent of social networking sites has fundamentally changed how people connect, communicate, and share information in the digital era. Platforms such as Facebook, Twitter, Instagram, and LinkedIn have connected billions of individuals worldwide, fostering a global community that transcends geographical boundaries.

However, this unprecedented connectivity and the vast amount of personal data shared online have attracted the attention of malicious actors seeking to exploit vulnerabilities for their nefarious purposes. The result is a growing landscape of cyber threats that pose significant risks to the security and privacy of both social networking platforms and their users.

This research aims to delve into the social networking sites' complex cyber threat landscape and examination of available tools employed by malicious actors, the vulnerabilities that make these platforms susceptible, and the ramifications of successful attacks. By understanding the scope and scale of these threats, we can gain insights into the pressing need for robust cybersecurity measures and proactive strategies to safeguard user privacy and data.

II. LITERATURE SURVEY

This seminal paper provides a comprehensive overview of various cyber threats that target social networking sites, including malware, phishing, and social engineering. The authors analyze real-world incidents and their consequences on user privacy, data integrity, and platform reputation. The study highlights the need for robust security measures and user awareness to combat cyber threats effectively.

The above literature survey provides a diverse range of studies that address cyber threats effects on social networking platforms. These research papers contribute valuable insights into understanding the challenges posed by cyber threats, the consequences on user privacy and data security, and the importance of adopting effective countermeasures to safeguard the digital ecosystem.

III. SOCIAL MEDIA NETWORKING

The number of social networking websites has significantly increased in recent years, accompanied by a diverse range of objectives and features they offer. Additionally, the ever-increasing user base has added further complexity to the social media landscape. Social networking sites can now be classified into various categories based on their specific purposes, as outlined below.

*A. **Contact Sites***:

The primary objectives of this website are centered on facilitating the exchange of information and promoting communication among friends. Additionally, it aims to broaden user communities with common interests. LinkedIn serves as a the best illustration of a social networking site that links friends and classmates and allows users to create a network that helps them advance their professional lives. **Social Networking Sites***:*

The primary aim of these websites is to help users find and connect with friends while engaging in their online activities. Notable instances include Twitter, Facebook, and WhatsApp.

*B. **Visual Information Sharing Sites***:

On these websites, users have the ability to share both personal photos and videos, including movies and television shows. Among these platforms, YouTube stands out as the most prominent one. Siri and Alexa to understand spoken requests, provide the user with pertinent information, and carry out activities on their behalf.

*C. **Virtual Realty Site***:

These websites aim to replicate reality, providing users with immersive virtual 3D experiences. In the ever-changing and intricate online business landscape, Facebook, LinkedIn,

Instagram, MySpace, Snapchat, Twitter, YouTube, and other social media platforms have emerged as modern communication channels that engage individual users and various businesses alike.

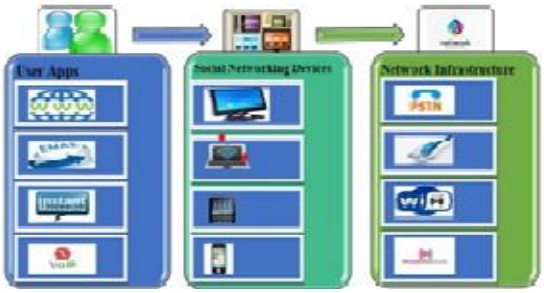

Figure 1 : Framework for Social Networking

There are three primary sections to the construction. Web browsing, email, instant messaging, voice-over-IP, and other services are all featured in the first section of user applications. Social networking devices, which include desktop PCs and non-portable mobile phones, are displayed in the second section. The public switched telephone network, networking cables, wireless network (WLAN), and cellular network are all covered in the last section's discussion of network infrastructures.

Social network users have the opportunity to connect with individuals from around the globe and interact in numerous languages. The list of the most popular global social media platforms is based on Statista company's 2018 data on active user counts.

IV. CYBER THREATS TO SOCIAL NETWORKING

The way users interact with each other on social networks significantly influences various internet trends, including those related to commerce, professionalism, and social activities. Moreover, numerous organizations, businesses, and individuals have mastered the art of engaging with colleagues and customers using well-known social networking sites like Facebook, Twitter, and LinkedIn

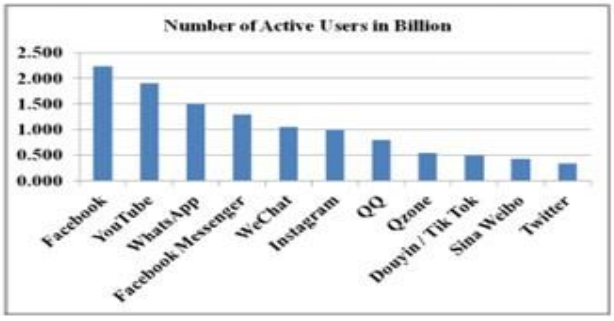

Figure 2 : Total Number of Social Media Users

Spyware, computer viruses, and other dangerous software have become more prevalent as a result of social networking sites' quick rise in popularity, posing serious concerns to the security and confidentiality of user data. Traditional dangers and modern threats are the two categories into which internet and social networking risks can be divided. Due to the infrastructure of online social networking, which might jeopardize user security and privacy, modern threats are particularly relevant to users of these networks. On the other hand, traditional hazards expose all users on a certain network to threats.

A. Traditional Threats:

Traditional hazards have existed on the Internet since its creation, and as the Internet and social networking applications have continued to spread, so have these problems.

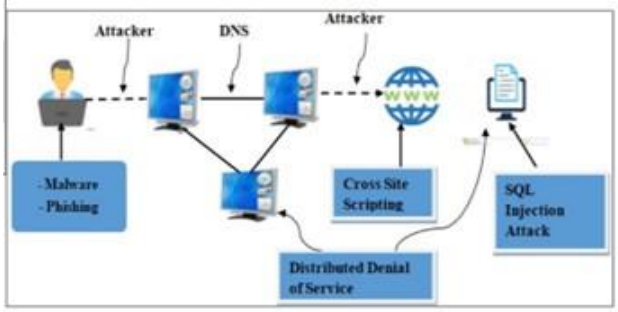

Figure 3: Different Types Of Traditional Threats

1. Malicious software, also referred to as malware, is created with the intention of obtaining unauthorized access to a user's sensitive information by frequently exploiting the way people communicate. Among the most prevalent types of malware include adware, bots, bugs, ransomware, rootkits, Trojan horses, spyware, viruses, and worms.
2. Another type of cyberattack is phishing, in which a hacker sends an email with a harmful link or attachment in order to gain sensitive personal data including login credentials, credit card numbers, and online banking information.
3. Cross-site scripting (XSS), a common attack method against web-based systems, involves injecting malicious code into online applications so that users' browsers can run it.
4. Distributed denial of service (DDoS) assaults are attempts to take down a system by flooding it with an excessive amount of network traffic, rendering the system's resources inaccessible to users. Computers, routers, and Internet of Things (IoT) devices are among the numerous resources that are the target of these attacks.

A. *Modern Threats*:

Surveillance	• Social, Environment, e-Commerce, and political governance
User Profile	• Activities and Behavioral characteristics
Inference Attack	• Prediction Sensitive, Religious, Political, and Educational Information.
Cyberstalking	• Harassment and Intimidation
Clickjacking	• Press Link or Like button, Moving cursor, Using Microphone and Camera
Location Privacy	• Geotagging
Identity Profile Cloning	• Creating a Fake Profile
Information Leakage	• Health , Operational, Infrastructure, and Intellectual Property Information
Fake Profile Attacks	• User Information
De-Anonymization	• Health Services, Social Media, and e-Commerce Trades

Figure 4 : Modern Threats and Information

These risks are often associated with online social networking, where attackers not only seek to obtain personal information from users but also from their friends. Hackers specifically target users' privacy settings on social networking platforms like Facebook, recognizing the significance of these settings in safeguarding user data.

1. User data for individuals, groups, organizations, and enterprises is tracked and collected as part of the listing and measuring process used to monitor social networking sites.
2. Information privacy leakage occurs when sensitive and private data is made available to unauthorized people. Users frequently communicate and exchange information with their friends and other people on social media platforms during online social networking.
3. False profile attacks involve attackers creating deceptive profiles on social networks, using fake names, interests, social security numbers, and other fabricated information to send messages to targeted individuals. The main goal of these false profiles is to gather user data. Apart from consuming network bandwidth, such fraudulent profiles also tarnish the overall reputation of the network.
4. A de-anonymisation attack uses data mining to try to identify a specific person. or a group by linking anonymous data with other publicly available sources, thereby revealing the source of previously unidentifiable data.

V. ENHANCING THE SECURITY OF ONLINE SOCIAL NETWORKING PLATFORMS

The surge in social networking sites and their user base has led to a significant increase in piracy on these platforms. Splash Data reported the top ten worst passwords used predominantly between 2015 and 2018, in North America and Western Europe, following an online analysis of over five million compromised credentials. Despite the dangers, users of computers persist in employing predictable and easily guessable passwords.

1. Users often opt for easily memorable and straightforward passwords for their convenience.
2. They tend to use the same password across multiple networking sites without changing it, making it easier for unauthorized access.
3. Users frequently select passwords based on personal information, which makes them vulnerable to hacking by anyone familiar with that data.

The practice of establishing and using several passwords is the biggest security risk that social networking sites face. To address this issue, the following list of guidelines is provided to mitigate these risks:

1. It is recommended to utilize complex passwords instead of simple ones, as they are more challenging to crack.
2. As a breach on one website could potentially result in breaches on other websites as well, it is imperative to avoid using the same password across different websites.
3. To efficiently store and manage passwords, consider utilizing applications like ZOHO, Keeper, and Dash lane.

VI. PREVENTING RISK AND ADDRESSING VULNERABILITIES ASSOCIATED WITH THREATS

Risk refers to the likelihood that potential harm may exploit a vulnerability to compromise, expose, or harm users' information or devices.

Figure 5 : Risks,Threats and Vulnerabilities

As risks on social networking sites continue to expand globally, impacting user information privacy to a great extent, it is imperative to implement the following measures to combat the challenges faced by users on these platforms.

1. Assess the level of privacy expected from the social media platform based on the frequency of usage and the extent of user engagement

2. Exercise caution and conduct thorough reviews before accepting or engaging with users on the platform.

3. Regularly suspend and gradually reintroduce site features to enhance security and privacy measures.

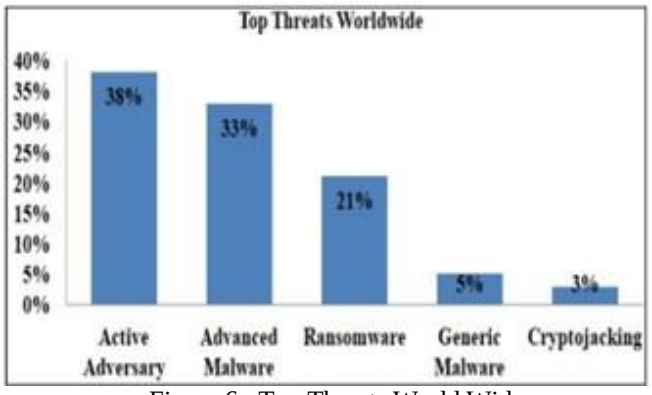

Figure 6 : Top Threats World Wide

Several studies have emphasized the importance of the impact of threats, especially for institutions that heavily depend on social networking sites to manage interactions with customers, suppliers, and employees in critical operational, economic, and production-related activities.

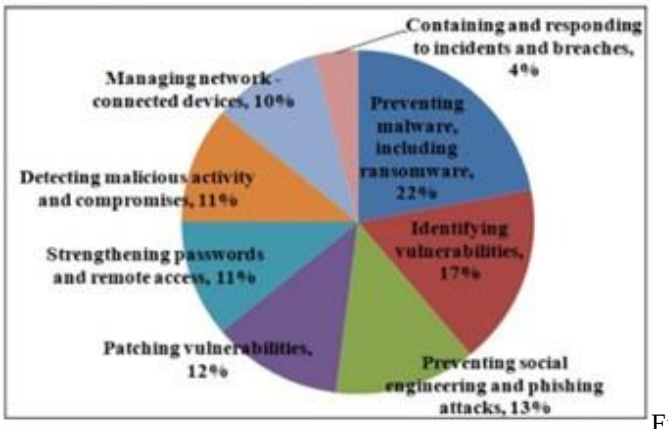

Figure 7 : Most Pressing Cyber Security Issues

The level of effort needed to attain the most effective risk mitigation for data preservation, as indicated in the SOPHOS[48] research on managing risk to data and IT assets.

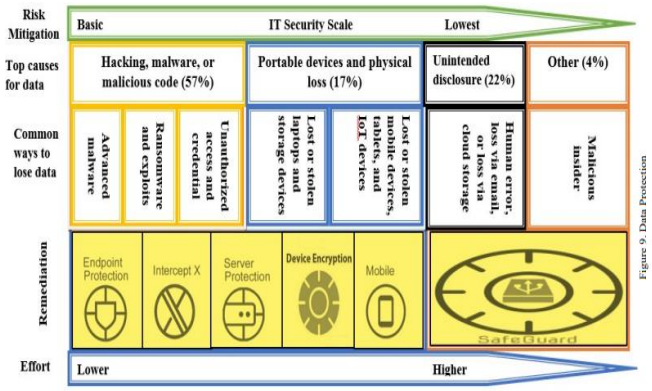

Figure 8 : Data Protection

To address the dynamic advancements in online networking applications and ensure data security and confidentiality at both institutional and individual levels, the essential recommendations mentioned the aforementioned considerably benefit consumers of online social media.

By implementing key recommendations on social networking platforms, the adoption of "Web0.2" technology can be encouraged, which aids in data protection and the mitigation of various threats, as part of the broader efforts to tackle these risks.

1. Businesses need to effectively control and manage the usage of applications on the Internet to prevent the utilization of harmful programs that do not comply with accepted protocols.
2. Discover the browsers in use and examine their data security mechanisms, which employ advanced features to protect user information.
3. In order to counteract malicious software, spyware, and other threats effectively, anti-threat software should be regularly updated to stay ahead of the rapidly evolving dangers.

VII. CONCLUSION

In the early twenty-first century, the internet and social media applications have experienced amazing growth and advancement. Consequently, the widespread adoption of various web applications has led to increased user engagement on social media platforms. However, this expansion has brought forth various risks that threaten the security and confidentiality of user data. The intrusion of unauthorized users, service providers, and others who utilize data from online social networking sites for their purposes is considered a significant concern in the context of using online social networking. This study's primary goal is to inform users and increase awareness of the potential risks linked with social media. of online social networking platforms on how to protect their personal information and themselves from these risks.

VIII. REFERENCES

[1] Hathi, S. (2009). How Social Networking Increases Collaboration at IBM. Strategic Communication Management.
[2] Kim, H. J. (2012). Evaluating the Security Risks of Online Social Media Networking. International Journal of Security and Its Applications, 6(3).
[3]Statista.(n.d.). Retrieved from www.statista.com/statistics.
[4] Davison, H. K., Maraist, C. C., Hamilton, R., Bing, M. N. To Screen or Not to Screen? Using the Internet for [6] Murphy, K. (2010Internet images that expose personal information, such as your location. The New York Times, AUG11.Retrievedfrom https://www.nytimes.com/2010/08/12/technology/personaltech /12basics.html.
[5] A severe SQL injection vulnerability has been discovered in the Next GEN Gallery Word press plugin. Retrieved from http://news.softpedia.com/news/critical-sql-injection-vulnerability-found-in-nextgen-gallery-wordpress-plugin-513375.shtml.
[6] Phys.org. (2018). People Fall for Fake Profiles Online. Retrieved from https://phys.org/news/2018-09-people-fall-fake-profiles-online.html.