Roshni Kothanur
Wrexham University
Critical Research for Postgraduate Study

“ The Emerging Cyber Threats on Social Media ”

Abstract

Social networks have become an integral part of modern life, enabling millions of users to connect with friends and family and share personal updates. However, these platforms also pose significant risks, as sensitive information shared online can unintentionally get leaked and rapidly go viral, often attracting global attention and discussion. This paper delves into the various threats and risks associated within sharing multimedia content on social networking platforms. It further analyzes the latest defense mechanisms aimed at protecting users from these cyber threats, offering insights into safeguarding personal information in the digital age.

Introduction

Over the past ten years, the number of users on social media platforms such as Facebook, Instagram, Twitter and Youtube have increased dramatically. This is due to the fact that it is being actively used, particularly with smartphones, as a means of communication, knowledge sharing, and thought sharing, as well as sharing photos and videos, forming networks, and so many other aspects that draw in millions of users globally.

It is important to note that social media platforms can affect users in both positive as well as negative ways. Social networking, which connects individuals and communities, is actually one of the core positive problems. Knowledge sharing is the other most significant positive issue. It may be seen as one of the beneficial means of learning and improving people's cultures, so long as users are looking at and focusing on the appropriate material. It is also important to note social effect because it offers a simple and nearly constant method of accessing websites that helps people avoid despair and improve their psychological stability.

Moreover, social media greatly enhances learning and teaching methods at Duhok Polytechnic University and other as well as other colleges and institutions around the world, providing a significant example of this beneficial effect. These platforms help students and teachers do better academically by facilitating

efficient communication and teamwork. In order to promote smooth communication between students and faculty, social networks also help colleges create individualised communication groups, like program and project teams as well as management teams. They are also crucial resources for creating online learning platforms that enhance the educational process, including learning management systems like Moodle. These apps show how social media has a revolutionary effect on improving higher education.

Besides these practical challenges, social networking platforms are becoming more and more popular, which attracts cybercriminals and therefore leads to criminality. Numerous potential risks and security concerns are there for social media users, or perhaps the victims are even organizations. Specifically, those without an Internet usage culture are particularly prone to attacks and threats. Thus, this indicates that practically every social media platform carries security threats.

Social networking sites will eventually become a source for hackers, as their purpose is to allow users to exchange personal information with each other. These hackers or criminals are attacking user accounts by utilising connections and shared information. Through such attacks, they exploit user profiles and sensitive, private information in several ways that are detrimental

to the users. They gain from both user-friendly social media apps as well as unaware and not-so-experienced users. These dangers have the potential of harming a person or causing issues for an organisation by compromising it for stealing important data. Governments may also be impacted by the threats in terms of their economy and national security.

For this reason, everyone should be informed of the dangers, protections, and illegitimate usage of the Internet. It entails utilising Internet applications effectively and avoiding misuse. Everyone who uses the Internet should be aware that every device has an IP address, which is what hackers use to access and create data. Social media is one of the primary means that people use the Internet the most. This may be applied by identifying the security threats and risks the company faces. Furthermore, understanding the rules and regulations that have been signed with the account creation is crucial to knowing how to utilise these sites as a potential user in an efficient way. In order to caution people about these issues and create effective and best practices that can be standardised and updated as apps, this has to be shared throughout communities, companies, and institutions by knowledgeable users.

Literature Review

It is crucial to further examine the current studies on social media's vulnerabilities and the cyberthreats it attracts, further elaborating on the introduction's acknowledgement of the platform's advantages and concerns. Due to their extensive user bases and the abundance of personal data they disclose, social media platforms are often the focus of cybercriminals efforts, which can range from identity theft and phishing to massive data breaches. Research has indicated that social media networks' design, which prioritises user involvement, unintentionally increases security concerns. For example, algorithms that promote communication and information exchange frequently include weak security features for confirming user identities or protecting private information. Furthermore, there are several ways for cybercriminals to compromise both individual accounts and organisational systems due to the pervasive use of social media for both personal and professional reasons.

In the following sections, this study will be looking at different types of cyberthreats that are common on social media and will be evaluating case studies that show how these risks affect people in the real world and assess how well-working current existing prevention methods are. In order to offer a comprehensive knowledge of the relationship between social media and

cybersecurity, this literature review will be objectively assessing these fields.

Online social networks are becoming more and more popular, yet many users are unaware of the serious privacy and security threats they offer. These risks can roughly be divided into four groups. Classic risks fall under the first category. These include privacy and security issues that affect people outside of OSNs as well as OSN users. Using the network's structure to jeopardise user security and privacy in new ways, the second category consists of modern risks that are exclusive to the online social network system.

Classic Threats

Classic threats have been an issue since the Internet became widely used. Frequently known as spam, malware, phishing, or cross-site scripting assaults, they remain a persistent problem. While these threats have been handled before, because of the structure and nature of OSNs, they have grown more widespread and have the ability to propagate swiftly across network users. Classic threats can exploit a user's personal information that is posted on social network to target

not just the user but also their friends by changing the threat to fit the user's details.

An attacker for instance, may include a dangerous code inside a visually appealing spam message that uses a user's Facebook profile information. In this case, its likely that an unaware user would open this well-constructed mail and catch the virus because of its personal character. These attacks frequently target ordinary and necessary user resources, such as account passwords, credit card details, processing power, and even computer bandwidth. Unfortunately these attacks can also utilise the credentials that have been obtained from the compromised user to publish messages on the user's behalf or even alter the user's personal data.

1. Malware

Malware is harmful software designed to interfere with a computer's normal operation in order to get a user's login credentials and access their personal data. The OSN structure is used by malware in social networks to spread among users and their network friends. In certain instances, the virus may utilise the credentials it has acquired to send hazardous messages to the user's online acquaintances while posing at the user.

2. Phishing Attacks

Phishing attacks are a type of social engineering in which a reliable third party is impersonated in order to get private and sensitive information about the victim. The sociable and trusting aspect of social networking sites makes users more susceptible to phishing frauds, according to recent research. Furthermore, there has been a significant rise in phishing efforts within OSNs in recent years.

3. Spammers

Users that send unwanted communications, such as ads, to other users via electronic messaging networks are known as spammers. False profiles are created by OSN spammers, who utilise the social networking site to send messages with advertisements to other users. The OSN platform also gives spammers the ability to leave comments on pages that are frequently visited by network members. The ubiquity of network spamming is demonstrated by Twitter, which has experienced a significant increase in spam. In August 2009, spam accounted for 11% of all tweets. But by the

start of 2010, Twitter has managed to reduce the amount of spam by 1%.

4. Cross-Site Scripting

An attack on a web application is known as an XSS attack. By using XSS, the attacker takes advantage of the web client's faith in the web application and makes the web client execute malicious code that can gather private data. Applications such as OSNs are susceptible to XSS attacks. Moreover, attackers can develop an XSS worm that can be transmitted among social network members by combining an XSS vulnerability with the OSN infrastructure. An XSS virus known as Mikeyy attacked several users in April 2009, including celebrities like Oprah Winfrey by quickly spreading automated tweets over Twitter. The Mikeyy worm spread via Twitter user accounts by taking advantage of an XSS vulnerability and the network architecture of Twitter.

Modern Threats

Modern threats are specific to OSN settings. These attacks often particularly target user's personal information as well as their friends' personal information. For instance, an attacker attempting to obtain a Facebook user's high school name, which is only visible to the person's Facebook friends, can make a fradulent profile with relevant information and send the targeted individual a friend request. The user's information will be made public to the attacker if they accept the friend request. As an alternative, the attacker might gather information from the user's Faacebook friends and perform an inference attack to deduce the name of high school from the information gathered.

1. Clickjacking

Clickjacking is a malicious technique that tricks users into clicking on unwanted components, giving attackers the ability to control operations like spam posting, "lifejacking," or even accessing webcams and microphones. One famous instance was the "Dont Click" assault on Twitter in 2009, in which people clicked on a false link and unwittingly shafted the message widely across their accounts.

2. Face Recognition

Every day, millions of images are submitted to Facebook, and many of these profile pictures are available for public viewing amnd download. Concerns about privacy are raised by websites such as Faces of Facebook, which display the profile photos of more than 1.2 billion members. The creation of biometric databases using these publicly accessible images would allow for user identification without permission. This emphasises are necessity of more stricter privacy regulations to safeguard users' information and identities.

Discussion

This section covers strategies, software solutions and techniques currently available to asist online social network (OSN) users in enhancing their protection against privacy and security threats. Buy leveraging these tools, users can mitigate risks such as information leakage, clickjacking and unauthorised access to personal data. Additionally, the effectiveness of existing technologies and best practices in addressing these challenges is examined to promote a safer OSN environment.

By implementing safety features like user authentication and privacy settings, OSN operators attempt to keep their consumers secure while using their services. Here is a detailed description of a few of these methods.

1. User Verification Methods

OSN systems employ features like CAPTCHA, multi-factor authentication, and friend photo identification and even government ID verification to make sure users are real and not socialbots or hacked accounts. For instance, to prevent unwanted access, Twitter's two-factor authentication needs a mobile verification code in addition to a password. Events like the 2013 Associated Press Twitter account hack, which disseminated misleading information and sparked market panic, are prevented in part by such actions.

2. Privacy and Security Settings

To assist users in managing who has access to their personal information, OSNs include customisable privacy options. For example, Google+ employs "circles" for selective sharing, whereas Facebook allows users to control who may see their

postings. Users of both platforms may also activate extra security features like secure browsing and login warnings, as well as control app permissions. Many people still utilise the default settings in spite of these alternatives, which exposes their data.

Recommendations

It is recommended that users frequently examine their accounts and eliminate any unnecessary personal information about themselves, their relatives, and friends. It is advised to hide the friends list, refrain from using complete names, and use non-identifiable profile photographs in order to reduce privacy concerns and prevent facial recognition. To limit data exposure and make sure that only those they can trust receive it, users should also modify their privacy settings. To further improve security, enable secure browsing and authentication capabilities, such as two-factor authentication on Twitter and other services.

Conclusion

With the ability to interact and exchange experiences, OSNs have become an essential element of everyday life. However, they also present serious security and privacy hazards, with dangers ranging from online predators to hackers. Although there are methods to safeguard users, no one step provides complete protection. Users need to utilise a variety of protective techniques, be on guard, and reduce the amount of personal information they divulge. Future studies should concentrate on enhancing privacy and security protocols to make OSNs safer for all users.

REFERENCES

1. **(PDF) Social Media Networks Security Threats, risks and recommendation: A case study in the Kurdistan Region,** https://www.researchgate.net/publication/348930053_Social_Media_Networks_Security_Threats_Risks_and_Recommendation_A_Case_Study_in_the_Kurdistan_Region **(Accessed Dec. 9, 2024)**

2. “Online social networks: Threats and solutions,” IEEE Journals & Magazine | IEEE Xplore, Jan. 01, 2014. https://ieeexplore.ieee.org/abstract/document/6809839 (Accessed Dec. 9, 2024)

3. Author links open overlay panelShailendra Rathore et al., “Social Network Security: Issues, challenges, threats, and solutions,” Information Sciences, https://www.sciencedirect.com/science/article/abs/pii/S0020025517309106 (Accessed Dec. 9, 2024).