ESP-JETA
ESP Journal of Engineering & Technology Advancements
ISSN: 2583-2646 / Volume 3 Issue 2 April 2023 / Page No: 39-45
Paper Id: JETA-V3I4P105 / Doi: 10.56472/25832646/JETA-V3I4P105

Review Article

An Analysis of the Privacy and Security Related Problem with Social Networks

Saptarshi Kumar Sarkar[1], Amitava Podder[2], Piyal Roy[3]

[1,2,3]*Assistant Professor, Department of Computer Science & Engineering, India*

Received Date: 15 April 2023 Revised Date: 22 April 2023 Accepted Date: 30 April 2023

Abstract: *Social networking is becoming more and more important as a result of the development in online communication over the last few years. Computer network operation, information flow patterns in societies, and emergent behaviour of physical and biological systems can all be studied using social network analysis. Social networks are now widely used, which has made it simpler for people to communicate with one another and share data online. However, this greater connection has additionally made it simpler for attackers and other bad actors to access user content and private data without authorization. In this paper, we will examine the various ways in which illegal access to user material and privacy breaches occur on social networks and explore the measures that can be taken to prevent them.*

Keywords: *Social Networking, OSN, Privacy, Security, Classical Threat, Modern Threat.*

I. INTRODUCTION

Today, one of the most common activities is social networking. These internet services are employed in marketing, education, and communication. There are several social networking services available nowadays. These include Facebook, Twitter and Google+, to name a few. Each service has its advantages and disadvantages; however, no network is completely infallible. Organizations must take precautions to safeguard sensitive data on social networks.

The concept of social networking emerged in the late 1990's. Initially, these services were limited to college-aged users. However, the number of users grew rapidly, prompting the invention of child-friendly versions of social networking services. Over time, these child-friendly versions became more accessible to general users. In social networks, people can connect with one another and exchange multimedia content for entertainment. Now anyone with a computer or mobile device can interact online. Users of social networks can think of them as an online community or part of a virtual communication system [1].

In addition, most social networking sites allow users to create accounts, upload and share files and messages. After creating a profile to identify himself, the user connects into one of these networks and starts looking for other people who share his interests. The mobility of data has led to an explosion in the usage of social networks. The majority of people now prefer using social networking sites like Facebook1, MySpace2, and LinkedIn3 as their primary means of communication.

There are some common features of every social networking sites [2][3]:

- Today's social networking services are all web-based and run through an Internet connection. Through a centralized access management system, contents are kept on cloud storage. With a web browser and an Internet connection, these materials are accessible from anywhere.
- Users of online social networks must construct public profiles for social networking sites in accordance with their predefined formats. This profile information is usually utilized during the social networking site's authentication process to sign in.
- The fact that the content on these sites is user-generated and that the online social networks use it for commercial purposes is an intriguing aspect of the existing online social networks.

[1] Facebook. http://www.facebook.com
[2] MySpace. http://www.myspace.com
[3] LinkedIn. http://www.linkedin.com

The rise of social networks simultaneously poses a serious threat to people. Social networking sites are a fairly simple way for attackers to obtain crucial personal information. These details, including bank account and password information, can aid attackers in a variety of network crimes, including identity theft. On social networking sites, users are encouraged to provide their name, address, gender, birthday, school, and place of birth, interests, and other personal data.

Other users will have access to this details. Attackers will then assess these data in order to discover the vital information. Attackers also receive more information if users supply more of it. Some social networking services, such as Twitter , do not provide users a lot of room to share sensitive personal information, but attackers might still exploit these tweets to their advantage by monitoring the series of posts in question.

The paper's major objective is to draw attention to privacy and security concerns associated to online social networks and to inform common users about how to safeguard their privacy and security. It is everyone's right to maintain their privacy, or at the very least, to disclose information only with those who need to know. To prevent irrelevant users from accessing private information, words like "privacy preservation" and "privacy protection" are used.

The phrase "privacy preservation" refers to circumstances in which private data are given to another party—in this case, an online social network—and that party thereafter want to publicize and give the data to any third party for research or commercial objectives. However, the online social network also wants to protect its customers' privacy.

In this situation, the online social network employs privacy preservation techniques to protect user privacy. The second term, "privacy protection," is used when a person even chooses not to share their data with an online social network server. In this situation, security measures are taken to safeguard users' privacy. The terms security and privacy are used frequently throughout the essay because privacy is our main concern, along with the security measures that are taken to safeguard user privacy.

II. MOTIVATION

The purpose of this work is to provide a quick overview of the privacy and security concerns that have arisen as a result of the use of online social networks. This is a fact that makes using a technical facility for easy and quick communication essential for everyone. Social media one type of these communication channels that might affect people negatively or positively. Sharing information online is easier and quicker than in-person contact because of social networks. They enable globalisation and give their users a platform for self-expression.

International partnerships, whether they be for business or social engagements, can now be forged through online social networks. People can easily communicate with one another through online social networks at any time and from any location. Those are the advantages of social networks. But there are some disadvantages also in social networks among them is the concern over security and privacy. This essay discusses the problems that online social network users may encounter and offers advice on how to keep their personal information private while browsing these networks.

In this paper we focus on social network hazards and mitigation strategies. The rest of the article is structured as follows. A summary of the privacy and security related risks in online social networks is provided in Section 3. The results and discussions are presented as question answer season in Section 4. Section 5 offers suggestions for preventing illegal access to user material and privacy. Section 6 brings the paper to a close.

III. PRIVACY AND SECURITY RELATED RISKS IN ONLINE SOCIAL NETWORK

On social media, user-generated content may include users' experiences, opinions, and knowledge. Additionally, it could contain confidential information like name, gender, location, and private images [4]. Information shared online is permanently, easily retrievable, and shareable because it is electronically preserved. Social media is widely used today. As of April 2022, there were more than five billion internet users worldwide, that is 63.1 percent of the global population. Of this total, Social media was used by 4.7 billion people, or 59 percent of the world's population. The total number of users of internet and social media are present in Table 1.

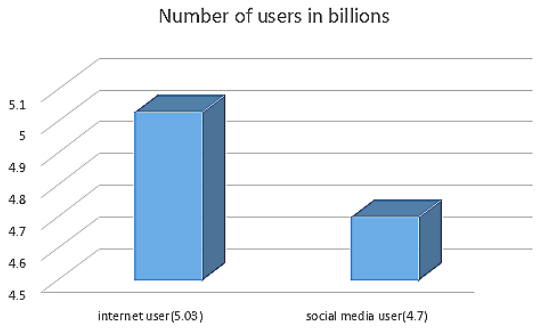

Figure 1: Number of Internet and Social Media Users Worldwide as of July 2022 (in billions)

As of 2023, Facebook is the world's largest social media platform, with 2.91 billion Monthly Active Users (MAUs). The top three are Youtube (2.56 billion MAUs) and Whatsapp (2 billion MAUs) . Because this data is more dependable for determining actual use and geographic penetration, the majority of social networks provide growth data in terms of the number of monthly active users rather than the number of registered profiles.

Table 1: Popular Online Social Media Platform and their total Monthly Active Users in millions.

Social Media Platform	Number of Users
Facebook	2910 million
Youtube	2560 million
Whatsapp	2000 million
Instagram	1470 billion
WeChat	1260 million
Tik Tok	1000 million
Facebook Messenger	988 million
Douyin	600 million
QQ	574 million
Sina Weibo	573 million
Kuaishou	573 million
Snapchat	557 million
Telegram	550 million
Pinterest	444 million
Twitter	436 million

Since there are so many members worldwide, privacy is one of the most important and evident problems with online social networks. Because of Online Social Networks, a number of privacy concerns are raised, including surveillance, in which the social environment of Online Social Networks transforms into a commercial realm and Online Social Network service providers monitor user behavior for market-force access control. Standard Online Social Networks distribute users' personal information to outside parties for potentially exploitative advertising objectives. Similar to this, Online Social Network users leave digital traces when they access Online Social Network websites, making them prime targets for data collection for marketing purposes and user profiling.

Social networks are important for both our personal and professional life, but they also pose substantial privacy and security issues. Social Networks have become the most popular target for attackers in recent years due to the hundreds of thousands of people who regularly utilize them. Social media's widespread use has exposed online users to privacy and security risks. There are different type of threats and these threats can be categorized classic threats and modern threats.

A. Classic Threats

Since the introduction of the Internet, classic threats have become a problem. Online dangers known as "classic threats" put other users of the internet at risk in addition to Social Network users. Spam, Phishing, Spread malware, Data theft and website compromise are some common type of classic threat. By adapting the threat to correlate to users' private features,

traditional threats are utilized to separate the personal information of users that are shared over a social network in order to attack not just the target users but also their peers.

a) Spam

Spam is any unwanted, uninvited digital message that is distributed in large quantities. Spam is frequently transmitted by emails, but it may also be sent through social media, text messages, and phone calls. Social network spam is more harmful than spam sent via traditional email since consumers spend more time there. Spam communications frequently include spam links or adverts that might take users into phishing or malware sites. Spam typically originates from dishonest profiles or spam programmers. A false profile is typically distributed from one made in the name of a well-known individual. Normally, spam messages come from hacked accounts and spam bots [5]. But most spam comes from accounts that have been compromised [6] [7]. Before a message is delivered to the target system, spam-filtering techniques are employed to identify any harmful content or URLs [8].

b) Phishing

Another fraudulent attack method is phishing, in which a hacker assumes the role of a reliable third party using a stolen or fictitious identity to obtain the user's personal information. An attacker might impersonate the sender of an email message using social media data collection to entice recipients to click on links or provide the attacker their personal information. An email sent from a high-ranking employee may contain a message telling the receiver to give money, click a harmful link, or reply with sensitive information. For instance, key U.K. and U.S. military officials were duped into becoming Facebook "friends" with someone posing as U.S. Navy Admiral James Stavridis during an attack that the Chinese government claimed was the result of intelligence. Similar to this, phishers using false identities frequently used social media [9][10][11].

c) Spread Malware

Malicious software is referred to as malware. It is a collective word for intrusive software. It was created with the goal of gaining access to a person's computer and sensitive information. In comparison to other online businesses, social networks are more vulnerable to virus attacks because of their user interactions and organization structures. Similar to brand impersonation, an attacker could build domains and websites that pretend to be the real company in order to fool consumers into downloading malware or giving personal information. For example, OSNs like MySpace, Facebook, and Twitter were used to distribute the Koobface malware. It was used to gather login information and incorporate the compromised computer into a botnet [12].

d) Data theft and website compromise

It is among the most prevalent and critical security issues that seriously harm web applications. With enough social media information, a hacker may create software that specifically targets a company or launch an assault that would grant access to the internal network, allowing the attacker to part of a shared data.

B. Modern Threat

These dangers frequently include online social networks. Modern threats typically aim to get sensitive data from users and their acquaintances. For instance, an attacker would want to find out a user's current employer. Users' Facebook accounts can be easily observed if their privacy settings are set to public. If they have a specific privacy option, however, only their friends can see it. A Facebook profile might be made by the attacker in this scenario, and friend requests could be sent to the persons they are after. Details are sent to the attacker once the friendship request is accepted. This is categorized into different types like Fake Profiles, Identity Clone Attacks, Clickjacking, Information Leakage, Surveillance, Location Leakage etc.

a) Fake Profiles

A fake-profile attack is a common type of attack on most social networks. In this type of attack, a hacker creates a social network account using fictitious information and mails authentic users. It delivers spam to users after getting friend requests from them. The purpose of the false profile is to gather sensitive user data from Online Social Network that is only visible to friends in order to spread it as spam. Additionally, it can be widely used for a variety of things, such advertisements.

b) Identity Clone Attacks

An attacker can copy a profile by using credentials from a stolen account to create a new false profile while using the stolen personal data. Identity clone assaults are what these are known as (ICAs). The compromised credentials may be used on

various networks or on the same network. The attacker can gather information from peers or engage in various forms of online fraud by taking advantage of the cloned user's confidence.

c) Click Jacking

When a malicious technique is used to fool users of the internet into clicking on anything apart from what they intended to, this is known as click-jacking, sometimes known as a user-interface repair attack. In clickjacking assaults, an attacker can trick OSN users into publishing spam on their timelines and secretly requesting "likes" on links. Attackers may even use user computer hardware, such as a camera and microphone, to record the activities of users through the use of a clickjacking assault.

d) Information Leakage

Sharing information with friends in an open way on social media is the whole point. Some users voluntarily divulge their private information, including health-related information. Unfortunately, some of them divulge a little bit too much private information about goods, projects, businesses, or other types of private information. Users of online social networks may experience negative consequences from disclosing such private and delicate information.

e) Surveillance

A new kind of monitoring that is distinct from traditional monitoring methods like those used in politics, the economy, and civil society is social media surveillance. By utilizing their profiles and connections with others, it turns into a procedure for keeping tabs on the varied behaviors of their users in various social roles. Technology-based surveillance known as "social media surveillance" keeps track of people's online activity.

f) Location Leakage

Data leakage is a form of hazard that includes location leaking. A social network is increasingly being accessed by different individuals via mobile devices. Apps are typically used to connect a mobile device to an online source. The new privacy risk of location leakage is introduced by the use of portable devices for online access. Users are more likely to divulge their location while using portable devices for web access [13]. As a result, attackers may utilize the disclosure of geographic information on social networking sites to hurt victims.

IV. RESULTS AND DISCUSSION

The purpose of the study was to learn how consumers reacted to various privacy-related options and if they were aware of or concerned about them. Students at the bachelor's level subsequently asked some queries. Students at the bachelor's level who participated in the survey were chosen at random from various classrooms. Some of the following questions were asked of the participants:

Question 1: Do you share your personal information on Social Network?

42% of individuals said that they share their personal details on social networks, which is a YES. Further inquiries into the participants' content restriction and friend-only sharing revealed that many of them were not even utilizing the service providers' provision for restricted data-sharing. As an illustration, the social network offered the option to limit sharing to friends, friends of friends or custom sharing.

Question 2: Do you accept friendship requests from the same user more than once?

To find out if users are susceptible to clone assaults, this question was posed. Participants gave a 29% affirmative response when asked if they accept friend requests from people who have already accepted their friend requests. Although this does not imply that each of these request are clone assaults, it does demonstrate that all these users are susceptible to them.

Question 3: Do you use your true name on your online profiles?

52% of users in this situation choose their true names for their profile names.

Question 4: Do you check the privacy statement or terms of use?

When questioned about their online social network's privacy statement, users were polled, and 54% of them admitted to not even trying to read the terms of service.

Question 5: How often do you update your passwords?

To prevent unwanted access to the user account, the password must be changed. As a result, each user must frequently update their password. In our survey, 45% of participants said they didn't consistently change their passwords.

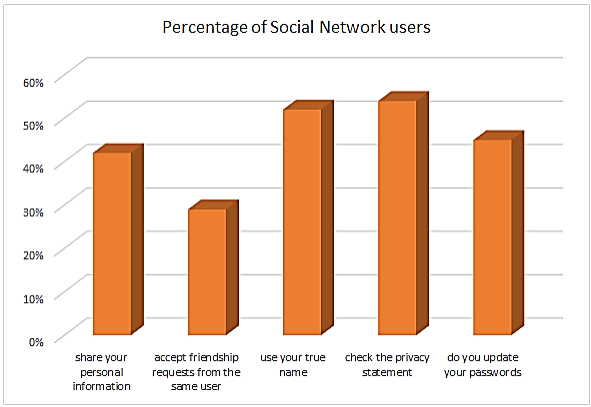

Figure 2: Percentage of users who either do not know or care about their privacy while using Social Network.

A. Preventing illegal access to user material and privacy

As the use of social media rises, so do the threats on it. Users' carelessness causes security and privacy problems, which an attacker exploits. Users of social networks run the risk of having their friends' shared content end up in the wrong hands, whether it's in the same format or not. Similar to this, shared content can be combined with other public datasets using re-identification algorithms, potentially revealing even more private information. The privacy options managed by Social Network serve as the first line of protection against such privacy attacks. There are some prevention methods to secure your privacy and illegal access of user materials. They are as follows:

- One of the most effective ways to prevent illegal access to user material and privacy breaches on social networks is to implement strong security measures. This can include implementing strong password policies, encouraging the use of two-factor authentication, and regularly monitoring activity on the network for suspicious behavior. Additionally, encryption can be used to protect user data both in transit and at rest.
- Unfortunately, 80% of users don't check their OSNs or know about the privacy of their profiles, regardless of whether they've been given default privacy settings or sufficient privacy that fulfils the desired level [14]. Although OSNs provide data owners with a certain amount of access control through customised settings to protect contents from unwanted access, practically all OSNs have limited privacy due to their default privacy settings. Users are also recommended to regularly review their privacy settings because many OSNs alter them with each update. Regularly reviewing and updating the network's security policies and procedures is also crucial in preventing illegal access to user material and privacy breaches. This includes compliance with data protection laws and regulations such as GDPR and CCPA. Having a robust security incident response plan in place to quickly detect, respond to, and recover from security breaches is also important.
- Another important aspect of preventing illegal access to user material and privacy breaches on social networks is educating users about the importance of privacy and security and providing them with the tools and resources they need to protect their information. This can include providing training on how to identify and avoid phishing scams, as well as providing information on the different privacy settings and controls available on social networks.
- Several mobile applications gather user location data. Online Social Network can exploit this location data and disseminate it to third parties, usually for financial gain, which compromises privacy. Attackers may abuse this location data if they are aware of your present location. Users are advised to refrain from sharing their location data over Online Social Network in order to protect themselves from these possible threats.
- Since their code is stored somewhere other than the Social Media network and under the user's control, third-party apps generate a variety of security and privacy issues. Users have little control over how their content is used or distributed because the data has been transported outside of the social network. Thus, to strengthen privacy protection, it is highly advised to delete third-party applications.

- One of the most popular platforms for inter-person communication where content transfer is simple is an OSN. Malware distribution has exploded due to the nature of content delivery through OSNs. Malware refers to any type of harmful software that interferes with user operations, collects sensitive data without authorization, accesses private information without authorization, or annoys users with intrusive pop-up advertisements. Installing antispyware and antivirus programs on desktops and mobile devices is advised for OSN users in order to protect against this malware and spyware.
- A logo or text can be added as a watermark to a documents or image file. Copyrights and marketing for digital works are provided by this procedure.
- Multiple users share ownership of this data, and each user applies their own privacy policies to that shared ownership.
- Social media sites have a lot of dangerous material available, and steganography is utilised to find this information. After the data has expired, digital oblivion is employed to stop hackers from accessing user-sensitive data.
- Without disclosing any private data to a third party, storage encryption is utilised to store and recover user data efficiently.

V. CONCLUSION

The use of social networks has made it easier for individuals to connect and share information online, but it has also made it easier for hackers and other malicious actors to gain unauthorized access to user material and personal information. To prevent these types of breaches, it is essential to implement strong security measures, educate users about the importance of privacy and security, and regularly review and update the network's security policies and procedures. Additionally, having a transparent and fair data usage policy and having a dedicated team or vendor to monitor and maintain the security of the network is important. By taking these steps, we can help to ensure that social networks remain a safe and secure platform for individuals to connect and share information online.

VI. REFERENCES

[1] X. Li, D. Zeng, W. Mao and F. Wang. Online Communities: A Social Computing Perspective. Intelligence and Security Informatics 2008 Workshops, 2008, pp. 355-365, doi:10.1007/978-3-540-69304-8.

[2] Obar, J.A.; Wildman, S. Social media definition and the governance challenge: An introduction to the special issue. Telecommun. Policy 2015, 39, 745–750.

[3] Kaplan, A.M.; Haenlein, M. Users of the world, unite! The challenges and opportunities of Social Media. Bus. Horiz. 2010, 53, 59–68.

[4] Taddicken, M. The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. J. Comput.-Mediat. Commun. 2014, 19, 248–273.

[5] Egele, M.; Stringhini, G.; Kruegel, C.; Vigna, G. Towards detecting compromised accounts on social networks. IEEE Trans. Dependable Secure Comput. 2017, 14, 447–460.

[6] Grier, C.; Thomas, K.; Paxson, V.; Zhang, M. @spam: The underground on 140 characters or less. In Proceedings of the 17th ACM conference on Computer and Communications Security, Chicago, IL, USA, 4–8 October 2010; pp. 27–37.

[7] Gao, H.; Hu, J.; Wilson, C.; Li, Z.; Chen, Y.; Zhao, B.Y. Detecting and characterizing social spam campaigns. In Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement, Melbourne, Australia, 1–3 November 2010; pp. 35–47.

[8] Thomas, K.; Grier, C.; Ma, J.; Paxson, V.; Song, D. Design and evaluation of a real-time URL spam filtering service. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, USA, 22–25 May 2011; pp. 447–462.

[9] Dvorak, J.C. LinkedIn Account Hacked. Available online: https://www.pcmag.com/article2/0,2817, 2375983,00.asp (accessed on 1 November 2018).

[10] Miller, S. Sen. Grassley's Twitter Account Hacked by SOPA Protesters. Available online: https://abcnews. go.com/blogs/politics/2012/01/sen-grassleys-twitter-account-hacked-by-sopa-protesters/ (accessed on 1 November 2018).

[11] Vishwanath, A. Getting phished on social media. Decis. Support Syst. 2017, 103, 70–81.

[12] Baltazar, J.; Costoya, J.; Flores, R. The Real Face of Koobface: The Largest Web 2.0 Botnet Explained. Trend Micro Threat Research. 2009. Available online: https://www.trendmicro.de/cloud-content/us/pdfs/ security-intelligence/white-papers/wp_the-real-face-of-koobface.pdf (accessed on 21 October 2018).

[13] Humphreys, L. Mobile social networks and social practice: A case study of Dodgeball. J. Comput.-Mediat. Commun. 2007, 13, 341–360.

[14] Zhang, W.; Al Amin, H. Privacy and security concern of online social networks from user perspective. In Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP2015), ESEO, Angers, Loire Valley, France, 9–11 February 2015; pp. 246–253.