An Analysis of the Privacy and Security Issues Affecting the Usage of Social Media

Musa Ahmed Zayyad
Department of Information Technology & Systems, School of Mathematics and Computing, Kampala International University Uganda

DOI: https://dx.doi.org/10.47772/IJRISS.2023.7603

Received: 10 May 2023; Revised: 10 May 2023; Accepted: 24 May 2023; Published: 24 June 2023

ABSTRACT

Social media have become extremely popular in recent years, and their widespread adoption has led to the presence of huge volumes of users' personal information on the Internet. The ever-increasing number of social media users on one hand and the massive amount of information being shared daily on the other hand have encouraged attackers to develop and use different techniques to collect and analyze such information for a number of malicious purposes, including spamming, attacking through viruses, phishing, spear-phishing attacks and identity theft among others. Clearly, this trend represents a significant challenge affecting both users and administrators, and likewise create a privacy and security issues for social media users. In this paper, common security and privacy issues were examined along with recommendations to social media users to protect themselves from these issues whenever they use social media.

Keywords: Attacks, Privacy, Security, social media, Technology.

INTRODUCTION

The popularity of online Social Media Networks (SMN) is vastly growing in today's world. The online communities developed by the SMNs are growing environments on the web to support modern interaction among the people around the globe. Social Media Networks are very beneficial for the people for keeping in touch with friends, family members and other acquaintances, for research collaboration, data sharing, social campaigning and other constructive purposes. There are various social networks which are put to different purposes according to their usability. Some are used for professional and business collaborations like LinkedIn and XING, whereas there are other SMNs like Facebook, Twitter, MySpace and telegram, snap charts Instagram etc. which are primarily used for informal friendly interactions, photo and video sharing and entertainment [1].

The massive acceptance of SMNs by the users provides opportunity to the attackers to create and launch new exploit and attacks every day. The growing popularity of Facebook in turn, makes it a popular website vulnerable to reverse engineering attacks and identity thefts and may turn a social media network into an anti-social media network. Anti-social media network is the platform for the execution of malicious threats as well as it provides unauthorized accesses like Denial of Service (DOS) attack, propagation of malware etc. A very large distributed database is used for SMNs and this acts as an advantage to make exploitation ideal because SMNs include community of users that share the same interests in the form of applications. These users share the same applications with the help of platform openness. This openness results in a user installing the application which is malicious and infected. These above characteristics give attackers the chance to manipulate that user to act as antisocial against all the internet users which are connected to the victim user [2].

With the emergence of social media and the growing popularity of online communication using SMNs, more sensitive information about individuals is available online. Though much of the data that are shared through SMNs are not sensitive, some users publish their personal information. Thus, the availability of publicly accessible sensitive data can lead to the disclosure of user privacy. The privacy of users is at more risk when publicly available data can be traced, and their activities can be connected with these data for mining and extracting sensitive information from it. Privacy has different meanings in different situations, and the intensity of privacy depends upon the context of shared contents.

The ultimate value of the data be protected in order to safeguard the contextual integrity of the online shared data. Information gathered from social media for analysis purposes is generally unintended and often irrelevant. However, it may be related to the private activities of a person, for example, religion or political affiliations [3].

The power of social media networking is such that the number of worldwide users is expected to reach 3.02 billion monthly active social media users by 2021 which is about one third of the world's entire population. The total active users on different popular social media networks are presented in fig. 1. Most famous social network sites worldwide as of April 2019, ranked by number of active users (in millions).

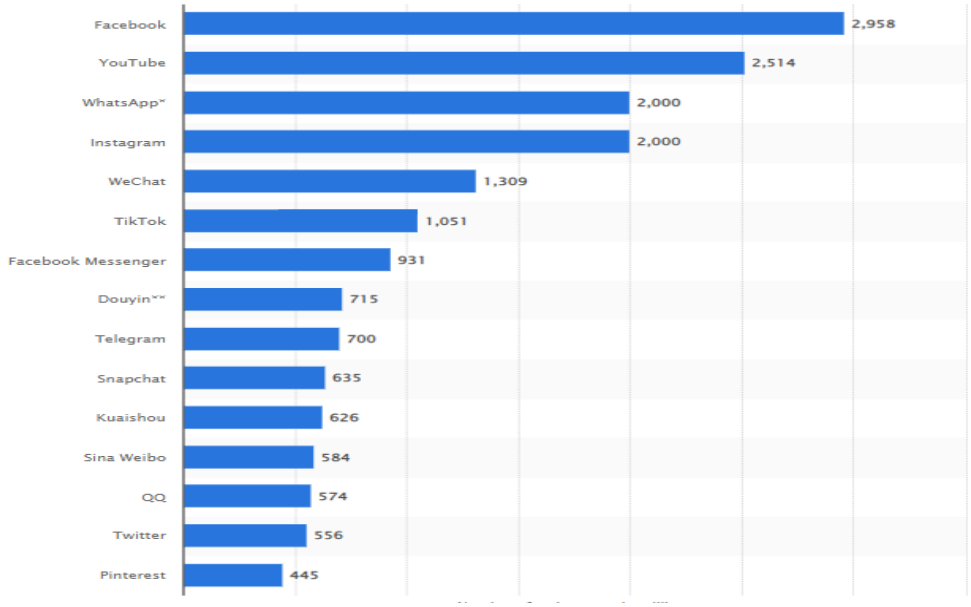

Fig. 1: Most famous Social Media Network Sites worldwide as at February, 2023 [8]

Taking into account this global number of users, privacy is one of the obvious and critical issues affecting Social Media Networks. Various privacy issues are fostered because of social media networks, such as surveillance, in which the social sphere of Networks changes to a commercial sphere and thus, service providers supervise user actions for market force access control. Standard Social Media Networks share users' personal data with third parties for advertisement purposes that may be exploited. Likewise, users leave digital imprints when they browse Online Social Network sites, and therefore are targeted as data sources for commercial uses and user profiling.

This study was aimed at investigating the issue of privacy and security affecting the usage of social media in order to suggest viable solutions for users to both improve their privacy protection, and be able to deploy the social functions expected from these types of network. The rest of the paper is organized as follows: Section II is the literature review, Section III is the methodology, Section IV is the analysis of social media attacks, and then Sections V and VI are the conclusion and recommendations respectively.

LITERATURE REVIEW

The researches on social networking sites so far are focused specifically on social network sites where some of these are connected to social media, social software, social bookmarking, educational technologies, etc. But with the development of social network sites, security protection of private information online has been a serious and important research topic. Hence the review concentrates following specific researches only on security and privacy of social network sites for investigation.

According to [13] in their research on Social network security: Issues, challenges, threats, and solutions, they analyzed the various threats faced by users of social media networks. In light of the information available and the system that protects it, they used a threat model to analyze specific privacy risks. Specifically, intruders are exploiting security holes. For each threat, they analyzed the efficacy of the current protection, and where solutions are inadequate.

Similarly, [4] in their study to understand the pattern of information revelation in Facebook developed a research model, with security and privacy concerns conceptualized as an antecedent of trust in social networking site and moderator of information sharing. The study also aimed to understand the impact of security, trust and privacy concerns on the willingness of sharing information in social networking sites.

[14] in his study on the social media see-saw: Positive and negative influences on adolescents' affective well-being commented that the majority of teens actively manage their online profiles to keep the information they believe is most sensitive 1away from the unwanted gaze of strangers, parents and other adults. While many teens post their first name and photos on their profiles, they rarely post information on public profiles they believe would help strangers actually locate them such as their full name, home phone number or cell number.

[9] in their study on online social networks security and privacy: comprehensive review and analysis conducted a thorough review of different security and privacy threats and existing solutions that can provide security to social network users. They also discussed OSN attacks on various OSN web applications by citing some statistics reports. In addition to that, they also discussed numerous defensive approaches to OSN security. The study similarly discusses open issues, challenges, and relevant security guidelines to achieve trustworthiness in online social networks.

According to [3. DeGroot, 2017] in their research on we were not prepared to tell people yet: confidentiality breaches and boundary turbulence on Facebook identified that the lack of established explicit privacy rules led to privacy violations and boundary turbulence. The findings of the study also provided insight regarding motivations of privacy violations, reactions to privacy violations, and the role of privacy rules in the violation.

METHODOLOGY

This study adopted the review methodology using a qualitative technique to identify and review articles that focuses on the privacy and security issues affecting the usage of social media networks. According to [xx] stated that the review methodology provides an important linkage between the immense and disperse assortment of articles on a particular topic. One of the main purpose of the review methodology include developing knowledge base that has a significant impact in the literature and for future researches. The study uses secondary data that was obtained from research databases such as Google Scholar, by using the search terms which include: social media, social network, security issues in social media, and privacy issues in social media. The articles that were obtained were screened based on the criteria of year of publication,

and relevancy to the topic of this paper.

TYPES OF SOCIAL MEDIA ATTACKS

Social Media Networks can be the target of several types of attacks like phishing, spamming, clickjacking, and cross-site scripting, to name a few. In this section, we discuss some common attacks on online social networks.

Based on the studies of Privacy and Security Issues in Online Social Networks by various researchers [2], [5], [6], [7], and [11] some attacks that are prevalent in SMNs include:

- Social engineering attack: The main driver behind social engineering attacks is the fact that Social Media Network users are not aware of the real value and importance of private information and, as a result, they do not pay much attention to keep it safe against attacks launched by malicious In such a situation, the attacker can deceive users into revealing confidential information employing different mechanisms.
- Reverse social engineering attacks: A reverse social engineering attack is another threat to Social Media Networks in which the malicious attacker deceives the user into contacting him using different types of Since the user initiates the connection, a higher degree of trust is then established between the attacker and the user. After this connection is established with the deceived user, the attacker begins his malicious actions, such as phishing and spamming.
- Identity theft: Identity theft is a type of attack on Social Media Networks in which the adversary attempts to collect personal information of Social Media Network users so that he can impersonate the victim of the attack in order to gain some benefits or harm the Different methods can be used to launch identity theft attacks, including phishing, accepting friend requests from unknown people, sharing account details with others, clicking links that lead the user to other websites, downloading free applications, low privacy settings, etc.
- Phishing attack: This is probably the most common method to initiate an identity theft attack. In this type of attack, the fraudulent user attempts to steal the victim's personal information like his credentials or credit card information by impersonating a legitimate user or entity such as a colleague or a
- Spamming attack: The main purpose of spammers is to send out a huge number of emails to advertise and sell their products and gain sensitive information about the users (e.g., username and password) by masquerading as a trusted party (e.g., banks or online payment processors). Such sensitive information can be gained using fake Social Media Network profiles created by malicious users. With this approach, the attacker sends random friend requests to the members of the Social Media Network target community waiting for them to accept their
- Malware issues: Malware is a type of malicious software designed to cause damage to computer systems or take control of their operation in order to obtain sensitive Malware can easily spread in Social Media Networks because of the main property of online social media networks, which is connecting a huge number of users. Being a popular communication infrastructure, social media networks create a platform for the malware to easily propagate among their users and compromise more members.
- Cross-site scripting: Cross-site scripting is a type of attack against Web applications, including Social Media Networks, in which the attacker injects malicious code into target webpages and encourages the user to run the code in order to steal his sensitive information. Cross-site scripting has become more common since HTML and AJAX were integrated. This is mainly due to the fact that the attacker does not need to deceive the user into clicking on a malicious link to exploit XSS

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS |Volume VII Issue VI June 2023

- Cyberbullying: Cyberbullying is a type of attack that takes place by sending out harmful or offensive materials, including text and images, to targeted users. Once such material spreads among a large group of Social Media Network users, it is very difficult, if possible at all, to remove them from the Cyberbullying materials are often posted anonymously; therefore, tracking their source is not always an easy task. The negative consequences of cyberbullying attacks can be devastating for the target users. They may feel annoyed, unsafe, angry, or humiliated. The negative effects of cyberbullying are usually much more serious on children and youths and typically persist through adulthood. According to a 2013 survey by the National Center for Educational Statistics (NCES), almost 30% of the students reported that they have been the victims of cyberbullying.
- Internet fraud: Due to the huge number of users, investors can use Social Media Networks as a source of information for making financial decisions. At the same time, malicious users can leverage different types of vulnerabilities and weaknesses to manipulate such information and to commit fraud aimed at gaining some kind of monetary benefits. Threats include non- delivery of merchandise, identity theft, and credit card fraud. For instance, purchase fraud is a type of Internet fraud in which a malicious user makes a purchase from a merchant and uses a counterfeit or stolen credit card to make the payment. As a result, the merchant will lose some money because of accepting the counterfeit/stolen credit card and receiving a chargeback as a
- Data mining and inference attacks: Data mining is a powerful tool in the hands of researchers to discover valuable knowledge from large volumes of data. Although information gathered from Social Media Networks (SMNs) using data mining techniques can be a useful resource to evaluate OSMNs and improve the quality of services, it can also be used by attackers to extract knowledge that may compromise users' privacy. An Inference Attack is an example of a data mining technique used by attackers to collect sensitive information from a database by analyzing relatively insignificant data. The main difference between inference attacks and other types of attacks that are mentioned above is that this is not the result of unprivileged access to the data. Indeed, it is an attempt to gather sensitive information from authorized available In other words, it is the nature of the information itself that makes it vulnerable to inference attacks. Attackers can take advantage of the information disclosed by Social Media Network users to derive additional sensitive data about them.
- Clickjacking, Likejacking, and Cursorjacking Attacks: Clickjacking: In this type of attack, a malicious user deceives SMN users into clicking on a link, which is different from what the users expect it to be by overlaying multiple frames and hiding some frames from them. In other words, the webpage that is displayed to the user is different from the page where the user's action is taking Actually, the attacker chooses the webpage and clicking on a button on the page performs a different function than the user perceives. Cursorjacking: is another type of clickjacking attack, which deceives users into clicking on a malicious link and performing unwanted actions by changing the location of the cursor from the place that the user perceives to the location that the attacker expects. In Likejacking, the attacker uses social engineering techniques in order to intrigue users to click on links that include embedded scripts or code. The embedded links will then repost the attacker's link on the user's wall automatically or make the user like a survey page from which the attacker makes profit without the permission of the affected user.

SOLUTION TO SOCIAL MEDIA ATTACKS

The Table below illustrates the clear depictions of various attacks in social media sites and given the possible solution to how to handle the attacks safely.

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS |Volume VII Issue VI June 2023

Table I: Types of Attacks and their Solution

Types of Attacks	Sub-Attacks	Solution to handle the attacks	Ref.
Malware attacks	Crimeware, Spyware, Adware,Browser hijackers, Downloader, Toolbars	Use of anti-virus. – Do not go for unknown links, friends, applications, email attachments, etc. – Disable cookies, Sessions, ActiveX if unknown or no counter-measures available.	[15]
Phishing Attacks	Deceptive phishing (emails), Malware based phishing, Key loggers, Search engine phishing	Examine the emails carefully. – Validate the source of the data. – Beware of ads with offers	[16]
Evil twin attacks	Social engineering attack	Careful about having friends and sharing information. – Authenticate the user profile and share the data. – Try to completely understand the policies of having friends in the social networking sites.	[17]
Identity theft attacks	Dumpster diving	Use complex passwords, avoid password re-usage. – Shred your email or documents properly.	[15]
Cyberbullying	Cyberbullying	Do not acknowledge the messages that are intended to hurt or threat. – Save and archive the messages as evidences. – Take all threats seriously. – Do not share personal information with all users.	[18]

Physical attacks	Impersonation, Harassment through messages	Need a well-defined social networking policy. – Background security and privacy checks. – Properly make use of privacy settings options.	[15]

Table 1 above shows the different types of threats that can jeopardize SMN users' security and privacy. These threats attempt to achieve one or more of the following goals: (a) gain access to the user's resources, such as passwords and credit card numbers (b) gain access to the user's private and sensitive information, such as age, political views, and current or future whereabouts, (c) utilize the gained control over the user's SMN pro?le as a spreading platform to attack his or her trusting online friends; and (d) locate future potential victims. Some of these threats/attacks are passive; they use only the user's lack of awareness or knowledge to achieve their goals. For example, the face recognition threat introduced in the above can simply utilize the user's public pro?le photos to create a biometric database.

Other threats are active, and their goal is to try and set up the users. For example, the clickjacking threat tries to trick SMN users into clicking on something different from what they had intended to click. Alarmingly, many of the presented threats are not limited to cyberspace but have the potential to threaten the user's well-being in the real world as well. For example, it has been suggested that most burglars use SMNs such as Facebook and Twitter to target their victims. To better protect SMN users from the above mentioned threats, SMN operators, commercial security companies, and academic researchers offer SMN users a variety of security and privacy solutions which are presented above. Similar to real-world security solutions, these solutions can provide SMN users with several layers of protection against these threats.

RECOMMENDATIONS

As explained in the above, users of Social Media Networks deal with various types of privacy and security risks. The study made the following recommendations:

- Users must not share too much personal information in Social Media Networks. Sharing unnecessary private information within a large network can provide malicious users with opportunities to gather or infer personal information about Social Media Network users, putting their privacy and security at risk.
- Users must not take the risk of accepting friend requests from unknown people, since such requests are likely to come from malicious users.
- Reading the Terms of Use and Privacy Policies of the online social network is recommended to users before
- Since the default privacy settings of Social Media Networks are often inadequate, users are advised to modify their settings after joining a Social Media Network so that the information they share in their profile is not visible to unknown people. For instance**,** friends only are typically the best option among available levels of privacy settings and permits only friends of the user to gain access to the information shared in a user's
- Installing Internet security software is recommended to protect users' personal information while surfing through Social Media Another suggestion is to remove unnecessary third-party applications that can potentially gather personal information about the users.
- Social Media Network users must be cautious about location-based applications provided by social

networks since they can reveal a user's location and trace any movement. Also, it is a good practice that users do not share their contact information, like email addresses, schedules, and routines with others, which might allow malicious users to stalk

- Since children are more vulnerable to computer crimes, their parents must monitor their online activities. They must also educate their children about the inherent dangers of cybercrimes and teach them the basic rules to follow while surfing through the Internet in general and Social Media Networks in
- Users must report any concern they might have about their privacy and security, like spam, cyberbullying, or identity They should consider contacting the Social Media Network provider and local enforcement agencies or consulting knowledgeable attorneys if they think that they are the victims of cybercrime. In summary, users must be aware of the fact that once their personal information is disclosed online, there is no guarantee that this information can be removed, since it may have been collected by search engines or copied by other users.

CONCLUSION

SMNs have become part of our everyday life and, on average, most internet users spend more time on social networks than in any other online activity. We enjoy using SMNs to interact with other people through the sharing of experiences, pictures, and videos. Nevertheless, social networks have a dark side ripe with hackers, fraudsters, and online predators, all of whom are capable of using SMNs as a platform for procuring their future victims. In this paper, we have presented scenarios which threaten SMN users and can jeopardize their identities, privacy, and well-being in both the virtual world as well as the real world. Furthermore, we have provided examples of many of the presented threats in order to demonstrate that these threats are real and can endanger every user. We have also emphasized certain threats which challenge the safety of young children and teenagers across the SMN cyberspace. There are remedies to these threats, and we have offered a range of solutions which help protect an SMN user's privacy and security. However, the presented solutions are not magical antidotes that will provide full protection to a user's privacy and security. In order to be well protected against the various online threats, users must stay attentive to the information they post online, and they must employ more than one solution. In many cases, the users should seek the SMN operator's assistance in providing tools both to better protect their privacy and to identify potential threats.

REFERENCES

1. Ali, S., Islam, N., Rauf, A., Din, I. U., Guizani, M. & Rodrigues, J. J. P. C. (2018). Privacy and Security Issues in Online Social Networks. Future Internet. 10(12):114. https://doi.org/10.3390/fi10120114
2. Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of social engineering attacks on social networks. Procedia Computer Science, 198, 656-661.
3. DeGroot, J. M., & Vik, T. A. (2017). "We were not prepared to tell people yet": confidentiality breaches and boundary turbulence on Facebook. Computers in Human Behavior, 70, 351-359.
4. Dhami, A., Agarwal, N., Chakraborty, T. K., Singh, B. P., & Minj, J. (2013, February). Impact of trust, security and privacy concerns in social networking: An exploratory study to understand the pattern of information revelation in Facebook. In 2013 3rd IEEE International Advance Computing Conference (IACC)(pp. 465-469). IEEE.
5. Giumetti, G. W., & Kowalski, R. M. (2022). Cyberbullying via social media and well-being. Current Opinion in Psychology, 101314.
6. Gupta, S., Singhal, A., & Kapoor, A. (2016). A literature survey on social engineering attacks: Phishing attack. In 2016 international conference on computing, communication and automation (ICCCA)(pp. 537-540). IEEE.

7. Hajli, N., & Lin, X. (2016). Exploring the security of information sharing on social networking sites: The role of perceived control of information. Journal of Business Ethics, 133, 111-123. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/
8. Jain, A. K., Sahoo, S. R. & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. Complex Intell. Syst. 7, 2157–2177. https://doi.org/10.1007/s40747-021-00409-7
9. Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973-993.
10. Jyotiyana, P., & Maheshwari, S. (2018). Techniques to detect click jacking vulnerability in web pages. In Optical and Wireless Technologies: Proceedings of OWT 2017(pp. 615-624). Springer Singapore.
11. Pulido, C. M., Redondo-Sama, G., Sordé-Martí, T., & Flecha, R. (2018). Social impact in social media: A new method to evaluate the social impact of research. PloS one, 13(8), e0203117.
12. Rathore, S., Sharma, P. K., Loia, V., Jeong, Y. S., & Park, J. H. (2017). Social network security: Issues, challenges, threats, and solutions. Information sciences, 421, 43-69.
13. Weinstein, E. (2018). The social media see-saw: Positive and negative influences on adolescents' affective well-being. New Media & Society, 20(10), 3597-3623.
14. Etuh, E., & Bakpo, F. S. (2022). Social Media Networks Attacks and their Preventive Mechanisms: A Review. arXiv preprint arXiv:2201.03330.
15. Kumar Birthriya, S., & Jain, A. K. (2022). A Comprehensive Survey of Phishing Email Detection and Protection Techniques. Information Security Journal: A Global Perspective, 31(4), 411-440.
16. Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of social engineering attacks on social networks. Procedia Computer Science, 198, 656-661.
17. Ademiluyi, A., Li, C., & Park, A. (2022). Implications and preventions of cyberbullying and social exclusion in social media: systematic review. JMIR formative research, 6(1), e30286.