Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 10, December 2021: 6560-6565

Key Security and Privacy Issues on Online Social Networking Platform

[1]Rachana Alok Ashtekar
[1]Research Student, SKN College of Engineering, Vedgaon-Pune

[2]Dr. A. V. Deshpande
[2]Research Guide, SKN College of Engineering Vedgaon-Pune

ABSTRACT

Online social networks (OSN) have become an integral part of human life for communication, interaction and sharing the information. Due to technological advancement, everyone has access to these social networking platforms and unfortunately, many times, users are not aware of the revelation of their personal information publicly on these platforms. Leakage of a user's private information can happen in different ways. In this paper, social network and many key privacy issues associated with online social networking platform are discussed. Based on these discussions, some prevention strategies are suggested to improve a user's privacy and security on social networking platform. This study will help the readers to understand the security and privacy issues to be aware of while using the social network.

I. INTRODUCTION

Online social networks (OSN) are one of the most popular platforms for online communication and interaction nowadays. Technological advancements have facilitated people to be connected on social network wherever they go through smartphones and computers.

It has become an integral part of our social life helping us connect to friends, family, colleagues, or others. We have witnessed how the advent of social media platforms like Facebook, Twitter, and WhatsApp brought a revolutionary change in how we use the internet for personal and professional purposes. So whenever we navigate in internet, make a phone call or use different technology tools our privacy becomes vulnerable because technological developments have not only positive sides but also negative ones. These activities, effecting directly or indirectly, influence and expose privacy related aspects of the life of persons. Social networks, which are often used by

teenagers and people who do not have privacy or security on their minds, leads to a huge amount of potentially private information being placed on the Internet where others can have access to it. [2] It is very important to be careful what information we put online through OSN. The crucial problem is how secure the user data is. The OSN providers keep sensitive data in decentralized locations, where it is split among a large number of servers and is therefore controlled by the person who owns the server. Because of this, the data is susceptible to hacking and data theft. Different types of assets are prone to attacks in Online Social Networking, including private information of the individuals or organizations, digital identity, financial assets, intellectual property (IP), and corporate secrets and resources. [1]

II. ONLINE SOCIAL NETWORKS

Impact of online social networks, is becoming the major source of contemporary fascination and controversy [11, 14, 7]. A number of studies have led to different research directions like the implications of online social networks on individual connectivity, the capacity of technology to override cognitive limits in order to socialize with larger groups [4], and the challenge to maintain a balance between security, privacy, usability, and sociability on online social networks [1,16]. In this study, our main focus is on the privacy aspects of social networks, where research has primarily aimed to protect social network users with their profiles and other private information.

Social networks and content-sharing sites with social networking functionalities have become an important part of the online activities on the web and one of the most influencing media. Facebook, LinkedIn, Twitter, MySpace, Flickr, and Youtube are among the most popular online social networks. These are attracting millions of users, establishing new connections, maintaining existing relations, and using the various social networks' services. For example, Facebook reported to have one billion monthly active users that are uploading more than 250 million photos every day. On Twitter terabytes of data is generated on Twitter per day. With the large userbase and the tremendous amount of shared data, these social networks will undoubtedly shape the future of online communication. Recent studies about the use of social networks, the behaviors based on online interactions, show that there are numerous motivating factors for using social networks such as enjoyment [13], followed by the users' interest to frequently interact with their real-world life friends [12], and the users' belief that social networks improve the efficiency of their shared information to enforce existing connections and to connect with new users [10]. It was obvious from many studies that social network users are highly motivated to interact with their contacts and to share personal information [3]. And thus, social networks have become an important platform for connecting users, sharing information, and a valuable source of social network data. However, the various sources of data on social networks are not only perceived as repositories of knowledge but

availability of it becomes a form of threat as it can be exploited by attackers to disclose various sensitive information such as identities, personal details, locations etc.

III. PRIVACY ISSUES REGARDING ONLINE SOCIAL MEDIA PLATFORM

With ever increasing use of OSNs, the associated risks are also increasing tremendously. Privacy on social network platforms is a very complex concept involving numerous challenges. Following are some of the issues which users have been facing since beginning of social networks and still struggling to overcome those.

Spam Attack: Spam is the term used for unsolicited bulk electronic messages. The communication details of users can easily be obtained from social networking platforms and can be used to target the clients to send spam messages. Most of the spams are commercial advertisements but they can also be used to collect sensitive information from users or may contain viruses, malware or scams [5] .

Identity Theft: Some of the attackers attack through the application in which they ask permission for accessing the information provided in the profile of OSN. When a user allows todo so, they get all the information and can misuse that easily without the user knowledge or permissions.

Phishing: The purpose of phishing is to harm economically that is the phishers try to retrieve the profile information to know about the banking or the financial information of the users.

Profiling Risk: Profiling risk is the risk associated with profile cloning. The attackers retrieve the personal information of the users and make a clone of the profile. They do so to make their social image bad or for other purposes like knowing about friends of victims. This is the most popular security risk associated with the OSNs as it is very easy to do without the permission of the uses. Another way of profile cloning is “cross-site profile cloning” where attacker steals information from one social networking site and uses this information to make a profile on another social networking site.

Fake Product Sale: The attacker advertise on the OSNs for selling the products offering huge discount and as the user clicks on the products advertisement their profile information is received by the attackers. Sometimes when user tries to purchase and give their account information for payment, all the account information is retrieved by the attackers and they misuse this information.

Cyber Espionage: Cyber espionage is an act that uses cyber capabilities to gather sensitive information or intellectual property with the intention of communicating it to opposing parties. These attacks are motivated by greed for monetary benefits. It might bring about a loss of competitive advantage, materials, information, foundation or death toll. A social engineer can perform social engineering assaults using social networking sites by acquiring important data like worker’s assignment, email address, and so forth utilizing social networking sites

Cyberbullying: In Cyberbullying, users' emails, chats, phone conversations, and online social networks are used to bully or harass a person. The attacker repeatedly sends intimidating messages, sexual remarks, posts rumors, and sometimes publishes embarrassing pictures or videos to harass a person. He can also publish personal or private information about the victim causing embarrassment or humiliation.

Cyberstalking: Cyberstalking is stalking a person on OSN continuously which results in fear of violence and interferes with the mental peace of that individual. It involves the invasion of a person's right to privacy. The attacker tracks the personal or confidential information of the victims and uses it to threaten them by continuous and persistent messages throughout the day. Many users share their personal information like telephone number, location-based data, and schedule in their social networking profile. An attacker can gather this data and use it for cyberstalking.

Study of all these issues indicates that the existing privacy policies and mechanisms must be improved to better address security threats and make the users feel safe on OSN.

IV. PREVENTION STRATEGIES

Online social media and network have become an integral part of everyone's life. As the usage of these platforms grows, the risks of using them is also increased. It becomes essential to secure users on these platforms. Below are some strategies for users which can keep themselves reasonably secure.

Use a strong password: For the security of accounts, users should choose a strong password which must be long enough and contain alphanumeric values with some special characters. Also avoid using the same password for other accounts asif an attacker gets to know that password, he can compromise all accounts of that user.

Avoid location sharing: Many social networking sites have the feature of geotagging which automatically tags the geographical location of the user when the user uploads any multimedia on social media. The user has to change the setting as manual so that it does not tag location automatically. Sharing location online makes a user vulnerable to real-life crimes like robbery.

Don't accept unknown friend requests: Before accepting friend requests on OSN platform, analyze the profile of the requester carefully. Sometimes attackers create fake accounts or may impersonate an account. Hence, ignore unknown friend request which could be a fake account attempting to steal sensitive information.

Be careful about posting updates: Users must not create posts which may reveal their personal information. Many organizations have strict rules and regulations for sharing information and multimedia content on OSN platforms. Sharing information unlawfully can harm an organization's reputation in the market along with its data and intellectual property also.

Don't click unknown links and download third-party applications: Attackers can get access to someone's account and get sensitive information by sharing a malicious link. Clicking on such links may allow attacker to gather the personal and confidential information of a user which may breach the privacy of that user. Additionally, hackers may take advantage of vulnerabilities present in a third-party application such as games that are integrated with many popular social networks asking user's public information to consume their services. This information may be sold to outsiders without users' consent.

Install and regularly update internet security tools or antivirus software: Install good antivirus software or make use of internet security tools which can detect many threats like cyber grooming, cyberbullying to some extent. Also update this antivirus software regularly as many viruses are created by hackers on a daily basis.

V. CONCLUSIONS

In this paper we have discussed various privacy and security issues in social networking platforms which needed attention on priority. Also presented some strategies which can be adopted by the users to be safe from privacy and security glitches on online social networking platform.

From this study, it is noticeable that one must be aware of how much and what kind of information they are disclosing on such platforms. At the same time, one must be educated about the precautions to be taken for keeping the private and sensitive information secured on social networks.

Every user on OSN should take appropriate measures to be cyber-crime safe and shall protect their personal information to avoid any misuse. Cybercrimes have increased significantly due to easy availability of sensitive information on networking sites and hence there is a need for comprehensive worldwide collaboration to work together and fight these social network security and social media cyber-attacks, which is a continuously growing threat.

REFERENCES

1. A. Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and B. Bhattacharjee, "Measurement and analysis of online social networks," in Proceedings of the 5th ACM/USENIX Internet Measurement Conference (IMC'07), (2007).
2. Barnes, S. A privacy paradox: Social networking in the United States. First Monday, 11(9). doi:10.5210/fm.v11i9.1394, (2006)
3. Correa, T., Hinsley, A., de Z´uniga, H.: Who interacts on the web? The intersection of users' ˜personality and social media use. Comput. Hum. Behav. 26(2), 247–253 (2010).

4. Dunbar, R.I.M.: Social cognition on the internet: testing constraints on social network size. Phil. Trans. Roy. Soc. B Biol. Sci. 367(1599), 2192–2201 (2012).
5. Faris H et al: An intelligent system for spam detection and identification of the most relevant features based on evolutionary random weight networks. Inf Fusion 48:67–83 (2019).
6. Gupta BB, Sahoo SR: Online social networks security: principles, algorithm, applications, and perspectives. CRC Press (2021)
7. Heidemann, J., Klier, M., Probst, F.: Online social networks: A survey of a global phenomenon. Comput. Network 56(18), 3866–3878 (2012).
8. https://www.statista.com/statistics/263303/proportion-of-the-most-common-causes-for-possible-identity-theft/
9. https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/.
10. Kwon, O., Wen, Y.: An empirical study of the factors affecting social network service use. Comput. Hum. Behav. 26(2), 254–263 (2010)
11. Musial, K., Kazienko, P.: Social networks on the internet. World Wide Web 16(1), 31–72 (2013)
12. Pempek, T., Yermolayeva, Y., Calvert, S.: College students' social networking experiences on facebook. J. Appl. Dev. Psychol. 30(3), 227–238 (2009).
13. Sledgianowski, D., Kulviwat, S.: Using social network sites: The effects of playfulness, critical mass and trust in a hedonic context. J. Comput. Inform. Syst. 49(4), 74–83 (2009).
14. Steinfield, C., Ellison, N., Lampe, C.: Social capital, self-esteem, and use of online social network sites: A longitudinal analysis. J. Appl. Dev. Psychol. 29(6), 434–445 (2008).
15. Zhang, C., Sun, J., Zhu, X., Fang, Y.: Privacy and security for online social networks: challenges and opportunities. IEEE Netw. 24(4), 13–18 (2010).
16. Zheleva, E., Terzi, E., Getoor, L.: Privacy in social networks. Synth. Lect. Data Min. Knowl. Discov. 3(1), 1–85 (2012).