Privacy Risks and Security Threats in Online Social Networks

Marija Bukalevska
Faculty of AITMIR
University of Information Science and Technology
St. Paul the Apostle
Ohrid, North Macedonia
marija.bukalevska@mir.uist.edu.mk

Aleksandar Karadimce
Faculty of ICS
University of Information Science and Technology
St. Paul the Apostle
Ohrid, North Macedonia
aleksandar.karadimce@uist.edu.mk

***Abstract*—Online social networks (OSN) have served as a catalyst in increasing social interaction in the 21st century. Because of their nature, social networks attract many people where they can share information such as text and multimedia content using sites such as Facebook, Twitter, Instagram and more. While OSNs provide a simple and fun way to share information about one's self, these networks also give rise to new and serious privacy and security issues that could potentially harm users in serious manners. Phishing attacks, the spread of malware, internet fraud, online stalking are a few examples of the vast landscape of possible security dangers that target OSNs. This paper is intended to reach the general audience and will focus on the privacy concerns and classic security threats in OSNs.**

***Index Terms*—Online Social Networks, Privacy, Security, Risks, Threats, Issues**

I. Introduction

As a result of living in today's digital world and having access to Internet technology, various online social networks have emerged, allowing people to stay connected. While social networks attract a large number of users due to the variety of interesting features and services they provide, their huge number of active users is exactly what makes them more prone and vulnerable to security and privacy risks. Cyber-attackers target websites and social networking platforms that have a large number of users to gain access to user's data and use it for their own personal gain. This data can include: personal information, emails, passwords, credit card credentials and more. There are various ways to illegally obtain information of users, such as phishing attacks, malware, cross-site scripting attacks (XSS), cyber fraud and more. The paper is organized as follows. Section II. lays out the related work. Section III. defines OSNs and their popularity. Section IV. gives a brief discussion of security concerns and privacy issues. Section V. describes classic threats and provides a table of security threats found in OSN platforms using the Internet as a research tool. Section VI. provides the conclusion and future work.

II. Related Work

Fire, Goldschmidt and Elovici [8] provided a comprehensive review by presenting a taxonomy of various security threats that endanger the well-being of OSN users and children, offer an overview of existing solutions that improve OSN user protection, security, and privacy. The authors [7] discuss various security and privacy challenges and threats to OSNs. Furthermore, they present the findings of a survey in which participants were asked how they handled various types of privacy-related inquiries; the results revealed that the responses were unsatisfactory, as many users did not use the existing privacy settings provided by service providers. Ali, Kamran, Ahmed, Raza, Ilyas [6] explored security and privacy issues of OSNs, presented a taxonomy of OSNs threats by categorizing threats into several categories, and provided privacy recommendations for OSN users. The study [9] examines many security issues and challenges in Social Networking Sites, as well as a classification and explanation of various security risks and threats in Social Networking Sites. Jain, Sahoo, Kaubiyal [10] go through several security and privacy issues, as well as existing defensive solutions that can keep users safe. The popularity, benefits, drawbacks of OSN, as well as key challenges and appropriate security standards for protecting account information, are all examined in this study.

III. Defining OSNs and understanding their popularity

A. Defining Online Social Networks

A growing number of different kinds of services are now accessible via a computer network. These services have created a new type of virtual society known as online social networks. Web-based social networks, computer-assisted social networks, and virtual communities are all terms that have been used to describe them [2]. Boyd and Ellison [3] have defined social network sites as web-based services where individuals can create a public or semi-public profile within a limited system, aggregate a list of other users with whom they share a connection and view that list of connections.

B. The popularity of OSNs

Online social networks being the most widely used, easy to access and low-cost communication and information mediums have reached a remarkable increase in popularity in recent years. People's lives have become increasingly reliant on social networks due to their variety of features. Through social media, people can interact, communicate with their family and friends more easily, meet people with whom they share similar interests and hobbies and as well participate in discussion groups and forums. People can easily access news, information, as well as share, create, and access various types of content such as text, multimedia content, music and more by using social networks. Over the last few years, the popularity of OSNs has greatly increased and they have become a global technology phenomenon, with billions of users accessing them around the world. According to recent statistics there are 4.48 billion social media users around the world in July 2021, equating to almost 57 percent of the total

global population [11]. Table I shows the most popular social networks and their population.

TABLE I
SOCIAL NETWORKS POPULATION

Most Popular Social Networks	Active Users
Facebook	2.853 billion
YouTube	2.291 billion
WhatsApp	2 billion
Instagram	1.386 billion
FB Messenger	1.3 billion
WeChat	1.242 billion
TikTok	732 million
QQ	606 million
Douyin	600 million
Telegram	550 million
Sing Weibo	530 million
Snapchat	514 million
Kuaishou	481 million
Pinterest	478 million
Reddit	430 million
Twitter	397 million
Quora	300 million

* Most popular social networks of 2021 [11].

According to publicly available data up to July, 2021, at least 17 social media networks have 300 million or more monthly active users [11].

IV. Privacy and Security Issues on OSNs for Users

While, indeed, there are many benefits and positive aspects using these networks, there are also certain downsides that can cause severe challenges and problems for both individual users and for the companies that own these networks. In today's society, online social networks have exploded in popularity. People are more inclined to use several networking sites, such as Facebook, Twitter, Instagram, LinkedIn and Reddit [12]. In recent years, privacy and security in social networks has been a major concern. People who use Social Networking Sites expose themselves to a variety of risks, the most common of which being the breach of their privacy [5]. People are sharing an increasing amount of information on social networking sites in different forms, potentially providing access to personal information such as a person's name, gender, location and private images. This content is saved electronically and therefore it can easily be shared with more people than the user intended because many social networks are open to the public, given this, user's information can attract malicious people who want to harm someone [7], [10], [13]. Privacy and security risks can include various data breaches, identity theft, theft of banking information and credit card credentials for financial gain, cyber-bullying, stalking and more [12]. Phishing attacks, malware, cross-site scripting attacks (XSS), internet fraud, are a few examples of the variety of methods used to obtain information from users illegally. The lack of appropriate OSN tools and design, as well as the users' inadequate knowledge and awareness, do little to help the situation [13]. A social network's privacy component is large, with different sub-problems. User privacy, for example, comprises a number of sub-problems such as location data privacy and user personal data privacy [12]. Data in OSNs can include: personal information (derived from the user's profile), connections (such as group of friends or followers), messages (information that can be exchanged between users, but also posted publicly or privately on social media spaces), multi-media, tags, groups (a collection of users sharing information and resources), behavioral information, login credentials and location data [13]. All of these mentioned types of data can be the subject of privacy and security risks. This information could fall into the wrong hands through browsing, hacker attacks, or simple data sales [13]. There are many ways to illegally obtain information of users, such as phishing attacks, malware, cross-site scripting attacks (XSS), internet fraud and more.

V. Security threats found in Online Social Networks

According to authors threats can be classified in two main categories: classic threats and modern threats [7], while other authors add a third category, which is targeted threats and/or threats targeting children [8], [10]. The purpose of this paper is to conduct research using the Internet for content analysis to see whether users have ever been exposed and if any of the most popular social networking platforms (sec. III, Table I) have been subject to any classic security threats. Table II provides data for classic threats found on OSNs. The table is based on our findings. The data is obtained by using the Internet as a research tool to see if there have been any reported incidents of classic threats in the twelve OSN platforms given in the table. The data is obtained from references and the table II was created on that basis. [15]–[39].

User's personal information that is published on OSNs can be exploited by classic threats and compromised, but these attacks can be also tailored to target the user's friends.

- Malware - Malware is malicious software that is designed to disrupt a computer's operation in order to steal a user's credentials and access their personal information [8]. Because of the key characteristic of online social networks, which is that they connect a large number of users, malware can spread quickly among their users and infect more users [14]. There have been reported incidents of hackers targeting the popular messaging app Telegram with the ToxicEye remote access trojan. The ToxicEye malware can take over file systems, install ransomware, and leak data from victims' computers [38].
- Phishing Attacks - Phishing is a type of fraud in which an intruder obtains personal information from a user by impersonating a trustworthy third party using a fake or stolen identity [7]. There are incidents reported on Instagram where hackers have been seen targeting high-profile accounts on Instagram and getting access to accounts using phishing attacks [18].
- Spammers - Unwanted messages are known as spam. Spam appears as a wall post or a spam instant message on OSNs. Because users engage more on OSNs than they do on email, spam in OSNs is more hazardous [7]. For example, spam on Facebook and Twitter can involve sending these frauds suggesting that you're in a scandalous video. When you go to watch the video, you're directed to update a program, such as your Flash player. Instead of improving your computer, you're downloading malware that can hijack your Facebook account, collect your personal information, and even harm your computer [23], [24].

- Cross-Site Scripting (XSS) - Cross-site scripting (XSS) is a sort of attack against Web applications, including OSNs, in which the attacker involves injecting malicious script into targeted web-pages and induces the user to run it in order to steal sensitive information [14].
- Internet Fraud - Internet fraud, which is a cybercrime activity, involves using the Internet access to deceit or take advantage of people [8]. For example, fraudsters on Instagram like to impersonate well-known brands in order to trick you into purchasing counterfeit goods. They may also simply want your payment details in order to create bogus charges or empty your bank account [18], [31].

Given Table II we can note that reported incidents of phishing attacks [18]–[22], [34], [35], [37], [39], and Internet fraud [28]–[31], [33], [34], [36], [37], [39], can be found in most OSNs (in nine OSN platforms), followed by malware [15]–[17], [35], [38], [23] (in six OSN platforms) and spam attacks [23]–[27] (in five OSN platforms), whereas no reported incidents of cross-site scripting attacks (XSS) have been found.

VI. Conclusion and Future Work

OSNs have grown in popularity as a global technology phenomenon, with billions of users throughout the world accessing them. Many individuals are drawn to using them because of the various unique features they provide such as posting and sharing information and multimedia content, staying connected with friends, participating in discussion forums and more. However, while OSNs are entertaining to use, they also raise privacy concerns and security risks that could potentially cause harm to the individuals using them. From Table II we can conclude that most OSNs have been exposed to classic security threats. This is an ongoing research that will explore more content in the future and will be expanded, an extension to the security threat table will be provided where modern threats (such as clickjacking, socialbots, identity clone attacks) will be also added. A more detailed analysis of the privacy awareness of users on these networks and as well as protection recommendations and proposed solutions to better protect OSN users are also planned to be included.

Research Limitations

This paper is limited due to the following reasons:

- Research was not made for all most popular social networking sites of 2021 (sec. III, Table I). Included are those sites that have the most international and English-speaking users.
- The data was not acquired from a specific dataset, therefore the exact number of times the threats were encountered in each OSN is not known. Instead, Table II was created and the data was collected by using the Internet as a tool for content analysis to see if there have been any reported incidents of classic threats on each OSNs, respectively.
- Because the Internet was used as a research tool, data for some threats could not be found. For example, no cross-site scripting (XSS) attacks were reported on any of the platforms, but it does not mean that the platforms and users have never been exposed to such attacks.

References

[1] D. Hiatt and Y. B., "Role of Security in Social Networking," International Journal of Advanced Computer Science and Applications, vol. 7, no. 2, 2016, doi: 10.14569/ijacsa.2016.070202.

[2] K. Musiał and P. Kazienko, "Social networks on the Internet," World Wide Web, vol. 16, no. 1, pp. 31–72, Jan. 2012, doi: 10.1007/s11280-011-0155-z.

[3] D. M. Boyd and N. B. Ellison, "Social Network Sites: Definition, History, and Scholarship," Journal of Computer-Mediated Communication, vol. 13, no. 1, pp. 210–230, Oct. 2008, doi: 10.1111/j.1083-6101.2007.00393.x.

[4] S. Kumari and S. Singh, "A Critical Analysis of Privacy and Security on Social Media," 2015 Fifth International Conference on Communication Systems and Network Technologies, Apr. 2015, doi: 10.1109/csnt.2015.21.

[5] Senthil Kumar N, Saravanakumar K, and Deepa K, "On Privacy and Security in Social Media – A Comprehensive Study," Procedia Computer Science, vol. 78, pp. 114–119, 2016, doi: 10.1016/j.procs.2016.02.019.

[6] A. Ali, A. Kamran, M. Ahmed, B. Raza, and M. Ilyas, "Privacy Concerns in Online Social Networks: A Users' Perspective," International Journal of Advanced Computer Science and Applications, vol. 10, no. 7, 2019, doi: 10.14569/ijacsa.2019.0100780.

[7] [1]S. Ali, N. Islam, A. Rauf, I. Din, M. Guizani, and J. Rodrigues, "Privacy and Security Issues in Online Social Networks," Future Internet, vol. 10, no. 12, p. 114, Nov. 2018, doi: 10.3390/fi10120114.

[8] M. Fire, R. Goldschmidt, and Y. Elovici, "Online Social Networks: Threats and Solutions," IEEE Communications Surveys Tutorials, vol. 16, no. 4, pp. 2019–2036, 2014, doi: 10.1109/comst.2014.2321628.

[9] S. Rathore, P. K. Sharma, V. Loia, Y.-S. Jeong, and J. H. Park, "Social network security: Issues, challenges, threats, and solutions," Information Sciences, vol. 421, pp. 43–69, Dec. 2017, doi: 10.1016/j.ins.2017.08.063.

[10] A. K. Jain, S. R. Sahoo, and J. Kaubiyal, "Online social networks security and privacy: comprehensive review and analysis," Complex Intelligent Systems, Jun. 2021, doi: 10.1007/s40747-021-00409-7.

[11] DataReportal, "GLOBAL SOCIAL MEDIA STATS," DataReportal – Global Digital Insights, Oct. 2021. https://datareportal.com/social-media-users

[12] M. Siddula, L. Li, and Y. Li, "An Empirical Study on the Privacy Preservation of Online Social Networks," IEEE Access, vol. 6, pp. 19912–19922, 2018, doi: 10.1109/access.2018.2822693.

[13] Beye, M., Jeckmans, A., Erkin, Z., Hartel, P.H., Lagendijk, R.L., Tang, Q. (2010). Literature Overview - Privacy in Online Social Networks. CTIT technical report series.

[14] S. Deliri and M. Albanese, "Security and Privacy Issues in Social Networks," Data-Centric Systems and Applications, pp. 195–209, 2015.

[15] SecureIca. (2020, May 20). Cyber-criminal targets facebook tags to spread malware. Medium. Retrieved from https://medium.com/@secureica/cyber-criminal-targets-facebook-tags-to-spread-malware-2015da5a6a6.

[16] Hautala, L. (2020, October 1). Facebook: Malware that took over accounts and placed scammy ads a growing risk. CNET. Retrieved from https://www.cnet.com/tech/services-and-software/facebook-malware-that-took-over-accounts-and-placed-scammy-ads-a-growing-risk/.

[17] Syntactics Inc., Batilong, J. (2021, September 30). Instagram virus: What you need to know and do. Syntactics Inc. Retrieved from https://www.syntacticsinc.com/news-articles-cat/beware-instagram-virus/.

[18] Instagram ransoms targeting social media influencers. (2018, October 5). Tech Monitor. Retrieved from https://techmonitor.ai/techonology/cybersecurity/instagram-ransom-attacks.

[19] Sasnauskas, M. (2021, September 28). We uncovered a Facebook phishing campaign that tricked nearly 500,000 users in two weeks. CyberNews. Retrieved from https://cybernews.com/security/we-uncovered-a-facebook-phishing-campaign-that-tricked-nearly-500000-users-in-two-weeks/

[20] Williams, R. (2018, February 20). Snapchat's phishing attack breached 50k accounts. Marketing Dive. Retrieved from https://www.marketingdive.com/news/snapchats-phishing-attack-breached-50k-accounts/517377/.

[21] Bisson, D. (n.d.). Reddit clone site uses SSL certificate to lure users into handing over login credentials. Venafi. Retrieved from https://www.venafi.com/blog/reddit-clone-site-uses-ssl-certificate-lure-users-handing-over-login-credentials.

[22] Kan, M. (2021, October 20). Hackers are phishing YouTube creators to steal their accounts, Google warns. PCMAG. Retrieved from https://www.pcmag.com/news/hackers-are-phishing-youtube-creators-to-steal-their-accounts-google-warns.

TABLE II
SECURITY THREATS FOUND IN ONLINE SOCIAL NETWORKS

Threats	Facebook	YouTube	WhatsApp	Instagram	FB Messenger	TikTok	Telegram	Snapchat	Pinterest	Reddit	Twitter	Quora
Malware	✓ [15], [16]	✓ [22]	X	✓ [17]	✓ [35]	X	✓ [38]	X	X	X	✓ [23]	X
Phishing Attacks	✓ [19]	✓ [22]	✓ [34]	✓ [18]	✓ [35]	✓ [37]	✓ [39]	✓ [20]	X	✓ [21]	X	X
Spammers	✓ [24]	✓ [27]	X	✓ [25]	X	X	X	X	✓ [26]	X	✓ [23]	X
Cross-Site Scripting (XSS)	X	X	X	X	X	X	X	X	X	X	X	X
Internet Fraud	✓ [29]	✓ [30]	✓ [34]	✓ [31]	✓ [36]	✓ [37]	✓ [39]	✓ [28]	X	X	✓ [33]	X

[23] Kerr, D. (2012, September 25). Twitter users may be victims of Direct Message malware. CNET. Retrieved from https://www.cnet.com/tech/services-and-software/twitter-users-may-be-victims-of-direct-message-malware/.

[24] Varnsen, K. (2013, March 14). Types of facebook spam. Ranker. Retrieved from https://www.ranker.com/list/types-of-facebook-spam/kel-varnsen.

[25] Red. (2016, September 7). Welcome to Instagram spam. Medium. Retrieved from https://medium.com/@iamredmh/welcome-to-instagram-spam-dcbd89d692cb.

[26] Information environmentalism research: Fake accounts and MIS/disinformation on Pinterest. Digital Learning Inquiry (DLINQ). (2019, October 23). Retrieved November 30, 2021, from https://dlinq.middcreate.net/blog/2018/03/14/information-environmentalism-research-fake-accounts-and-mis-disinformation-on-pinterest/.

[27] Breadnbeyond. (2020, August 27). Easy ways to handle spam comments on YouTube. Medium. Retrieved from https://breadnbeyond.medium.com/easy-ways-to-handle-spam-comments-on-youtube-7b2ea20d8727.

[28] Snapchat Scam: This is what users need to look out for ... (2020, August 2). Retrieved from https://www.leaderlive.co.uk/news/18621697.snapchat-scam-users-need-look/.

[29] Author, L. W. (2021, November 4). Top facebook scams of 2021 and how to avoid them. VPNoverview.com. Retrieved from https://vpnoverview.com/privacy/social-media/facebook-scams/.

[30] Newman, L.H., 2021. How hackers hijacked thousands of high-profile YouTube accounts. Wired. Available at: https://www.wired.com/story/youtube-bitcoin-scam-account-hijacking-google-phishing/.

[31] Author, L. W. (2021, October 20). Top Instagram scams of 2021 and how to avoid them: Vpnoverview. VPNoverview.com. Retrieved from https://vpnoverview.com/privacy/social-media/instagram-scams/.

[32] Hall, G. E. (2019, August 12). Remove twitter virus (removal guide) - updated Aug 2019. Remove. Retrieved from https://www.2-spyware.com/remove-twitter-virus.html

[33] Bisson, D. (2016, January 7). A guide on 5 common twitter scams. The State of Security. Retrieved from https://www.tripwire.com/state-of-security/security-awareness/a-guide-on-5-common-twitter-scams/.

[34] Giordano , C. (2021, May 21). Whatsapp warning over scam that allows criminals to lock account and access messages. The Independent. Retrieved from https://www.independent.co.uk/life-style/gadgets-and-tech/whatsapp-scam-hack-warning-news-b1851552.html.

[35] Palmer, D. (2017, August 24). Facebook Messenger user? watch out for fake messages rigged with malware. ZDNet. Retrieved from https://www.zdnet.com/article/facebook-messenger-user-watch-out-for-fake-messages-rigged-with-malware/.

[36] Blanco, O. (2020, February 11). How to avoid Facebook Messenger Scams. Consumer Reports. Retrieved from https://www.consumerreports.org/scams-fraud/facebook-messenger-scams-how-to-avoid/

[37] Wong, Q. (2019, August 14). TikTok is filled with adult-dating scams and fake accounts, report says. CNET. Retrieved from https://www.cnet.com/news/privacy/tiktok-is-filled-with-adult-dating-scams-and-fake-accounts-report-says/

[38] Montalbano, E. (2021, April 22). Telegram platform abused in 'Toxiceye' malware campaigns. Threatpost English Global threatpostcom. Retrieved from https://threatpost.com/telegram-toxiceye-malware/165543/.

[39] Ricle, J. (2019, October 2). What is "scam" label next to telegram username? how to report telegram scammers? Telegram Adviser. Retrieved from https://www.telegramadviser.com/scammers-in-telegram-and-how-to-report/.