SECURITY ISSUES FOR SOCIAL NETWORK

[1]OMAR FAROOQ AHMEDDALO, [2]COSKUN BAYRAK

[1]Department of Software Engineering, Firat University, Elazig, Turkey
[2]Department of Computer Science and information Systems, Youngstown State University, Youngstown, OH 44555, USA
E-mail: [1]omer.faroq1993@gmail.com, [2]cbayrak@ysu.edu

Abstract - Social network is one of the common and new technology that people used to connect with each other and see others activities. The paper focuses on some important security issues in social network which users might face because many of them are not aware of the risks. All security issues will be discussed like phishing, malware, data privacy and fake accounts. At the same time the paper include some suggested solutions for the mentioned security issues which should be adopted by users and developers of the website.

Keywords - Social network, Security issue, Security awareness, Privacy.

I. INTRODUCTION

Social Networking is one of the primary reasons that many people have become avid Internet users and it is one of the greatest patterns on the Web, with a huge number of individuals partaking. It also represents an interaction network of individuals that are often connected to each other by a relationship [1]. It can be used for business purposes because the big companies can advertise their goods for people, which can be seen by huge number of users. In each social network there are some issues that users might face such as security and privacy. Social Network is one of the new technologies that make people to connect with each other by providing some services for users that help them to use it easily.Social networks explain the patterns in the structures by supplying a set of methods for analyzing the structure of social entities and the theories. At the same time, they provide a powerful reflection of the structure and dynamics of the society of the 21st century and the interaction of the Internet generation with both technology and other people [2,3]. Social communication and group association on the Web isn't new; the scale at which people are forming explicitly social connections in public forums is unique to social networks in the last couple of years [4]. The main approaches used in social networks enable to know social interaction being visualized first and investigated with the help of properties of relations between the units and not the unit's properties itself. Social networks are interconnected records typically represented by a graph where nodes are data points and edges represent relationships [5].
In the research, we concentrated on some important security issues such as phishing, malware and data privacythat are the most important for the social network services in which social system risks can be harmful to society's financial performance [6].

II. LITERATURE REVIEW

The usage of online social network is increasing day by day. Online Social Network enables different users to use the service with a security of using this message on the user's wall. The social community point of view gives an arrangement of strategies to investigating the structure of social elements and the speculations consequently clarifying the examples in the structure these structures use social networks analysis and identify local and global patterns, locate influential entities and examine network dynamics [5].
The active participation in social networking sites have changed the way people build their online personal network for computer-mediated communication. Social network has lot issues to discuss in the network environment. In [6], authors concentrate the unsolved issue like security and privacy. This investigationalso describes the social network model and security. The study shows that the security issues directly affect the systems and improving the stronger security and increased privacy is possible by security environment efficient access control mechanism helps to achieve high performance.
The most common way to capture information on social interactions is a network represented by a node in it, and there is an edge between two nodes. Depending on the source of data, asocial interactions cloud be a verbal or written communication, scientific collaboration, sexual contact, or physical or virtual proximity. Edges are commonly weighted by frequency of interaction. Although the network model of social interactions has been very successfully, the disadvantage of this model is basically static in that all data about the time that social interaction take place is discarded [3]

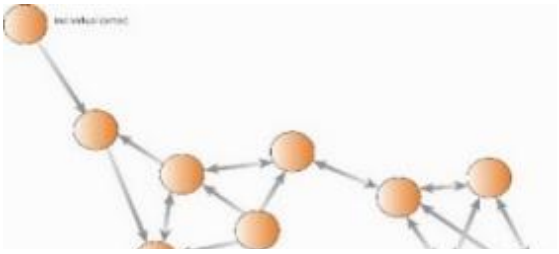


Figure 1: Simple Social Network.

III. SOCIAL NETWORK SITES

There are many social networking sites in our daily life and each of them provide some features and tools. In this study we focus on the common social networks which have many users such as Facebook, Instagram, Twitter, LinkedIn and many other sites [7].Wedefine each of the mentioned social networks shortly:

- **Facebook:** Is one of the most popular social sites which created in 2004 by Mark Zuckerberg. Facebook is used by people to connect with each other over the world and it provides many features for users with free account registration. It also provides some security tools to secure users account like two factor authentication but at the same time it can be vulnerable for users.
- **YouTube:** Is one of the good social network which is used for sharing different types of videos. Many users use YouTube for learning purpose and no need registration to see those learning videos.
- **Instagram:** Is another sites of social network which number of users increasing day by day. It is also a platform for pictures and video quality.
- **Twitter:** Is one of the social networking site which is used by people. It is a micro blogging site and used to type short message about you or friend situation.
- **LinkedIn:** Is different from user social networks because it focuses on professional identity of the users and allow them to control online instead of focusing on friends or family relationships.

In the below figure show number of active users in each social network which is updated on August 2, 2018 [8]:

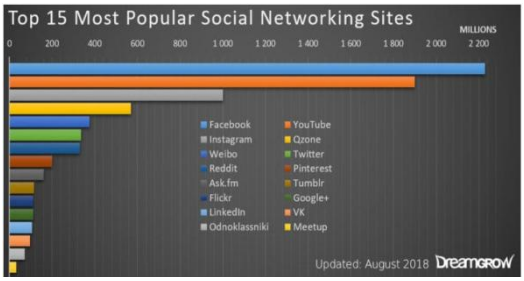


Figure 2: most popular social media sites.

IV. SECURITY ISSUES

Security is one of the important things for each social network and users should think twice before using them if it's not secured. Here we discuss common security issues of social network which are [9-18]:

- **Phishing:** Is one of the technique which attacker used to steal user's password and sensitive information by creating fake page similar to the original page and ask users to enter their credential once they entered then they will be in trouble.
- **Malware:** Is comprises of Trojans, worms and viruses which is used by attacker for stealing personal information, encrypt and delete data. It can be installed on user's computer without permission of the users and can send the activities of them to attacker. Attackers use some different techniques like post or send message that contain malicious link in social network which redirect users to malicious website then sends malicious code to computer users to steal information. The most popular malware which detected in social network are Koobface and Twitter worms.Koobface is a worm which move through messages in social network. The message might be in a form like image or video. When the users click on the link it will redirect them to another website, popup window appears which ask users updating flash player required to display a video.Once clicked on accepted button then the user's computer will be affected by worms. The second one is Twitter worm which consists of many worms like Profile Spy and create fake link worms which direct users to malicious attachments.
- **Data Privacy:** The privacy on social network is one of the important things that users should take care about it. We discuss two common privacy issues which are:
- **User's Anonymity:** Many of social network users use their real name when creating an account, so their identity exposed publicly and can be found by the search engine easily. The risk of this type is realizedwhen attacker know the name of victims and they will search for them to find the profile of them.
- **User's Profile and Personal Information:** In each social network the user's profile contains some real and sensitive information such as full name, phone number, relationships status and birthday.

The attackeruses this techniquetocollect personal information from user's profile.

Table.1Most information which users share on social network

Shared information	Percentage
Birthday	63%
Schools	61%
Familymembers	51%
Hometown	48%
Favorite TV shows	44%
Favorite Musicians	38%

Favorite books	33%
Vacation plan	26%
Pets names	23%

- **SQL Injection:** This is a technique which is used by attackers to attack the databases. The hackers try to run different malicious queries on database to show all database data and steal user's information in social network. This type of attack is closer to developer side instead of user's side. It will cause on the fields which allow users to run data directly to database such as search box.
- **Spam:** Is one of the issuewhich use an electronic messaging system to send messages in bulk. The most common types of spam in social network are email spam attacks and HTTP hijacking which make spam more successful.
- **Fake Accounts:** Creating fake accounts on social network is one of real problem of stealing user's information and sharing malicious link over social media.
- **Third Party Application:** many of social networks allow users to add some application if does not contain malicious code but it might access personal information of users without permission and use the accessed information for some reason like advertisement, access user contacts and many other things.
- **Profile Cloning:** Is one of the type of identity theft which affect user's which set the privacy option in their profile to public that means can see by all users. The attacker steals your profile information and used to create new account called false identity. There are two different type of profile cloning which are Existing Profile Cloning andCross-Site Profile Cloning. In existing profile cloning the attacker create a new profile by using all your information such as profile picture, birthday and working place then it will send requests to the user friends. The second type of cloning profile is cross-site profile cloning in this type the attacker copies all personal information of user and use it to create new account in different social network that users not registered yet.
- **Steganography** is one of the good technique which can hide secret data inside some types of files like pictures and video but at the same time this technique is also used by malware developer to obscure the transmission malicious code inside files and it runs in the background when the user clicks on the file.

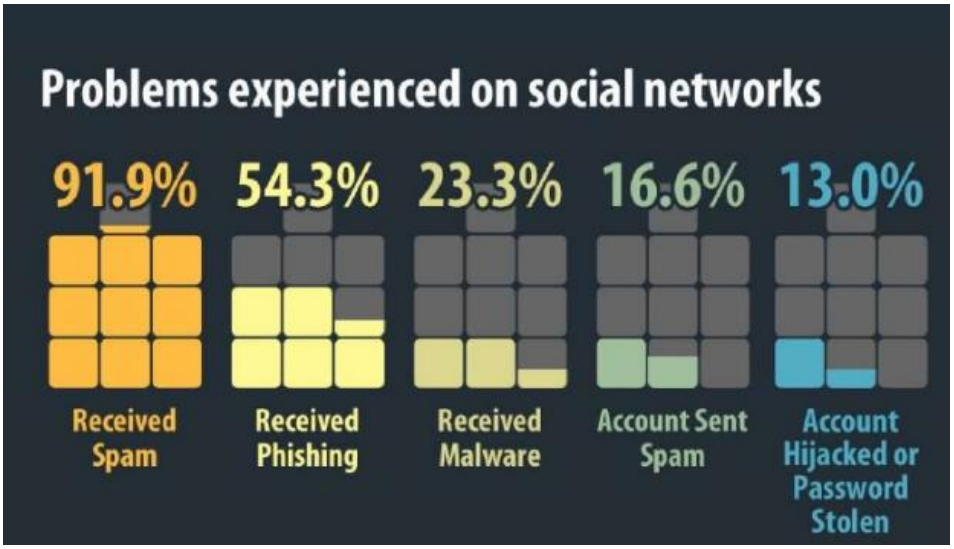


Figure 3: Problems in Social Network.

V. RECOMMENDATIONS

There are some recommendations for users and Developer Company to know how to secure their information from hackers [11, 20]:

- To prevent stealing user password by using phishing technique, the company should provide some filters to detect phishing page directly and block them, at the same time the users should take care and check the URL of page if it's legitimate or not before entering any credential.
- To prevent SQL Injection Developer Company should use some techniques to stop executing malicious queries on database by using prepared statements to run query and setting filter to check the query before running on database.Also the database user which is used to connect web application to database should have simple permissions like select, update, insert and delete, instead of dropping or creating permission.
- Two-Factor Authentication is one of the good feature which is provided by many social

networks to secure users account. The users of social network should enable this feature for their accounts which prevent unauthorized users from login to your social account if they have your password.

- To keep safe from malwares the company should use such techniques which provide good antivirus and scan any attachments before uploadingit, block some types of file such as .exe, .bat and .dll to be send or post which might contain malware, create algorithm to check all shared link daily and compare them if it's in the blacklist and whitelist website.
- The cryptography technique should be used by the company to secure user's information in social network by encrypting transferring data between user's browser and server. It also encrypts messages between sender and receiver users. This technique make attacker face some difficulties to get user's information or messages.
- For privacy issue users should use those social network which include some tools to make personal information secure by allowing user to switch from public to private status. At the same time the users should not share any important information on social network such as location address, phone number and many other sensitive information that make account vulnerable.
- Users should use good browsers that has ability to block popups window and phishing sites. Also they make sure the browser is up to date and auto update activated.
- Developer Company should provide authentication in every level to prevent attackers from accessing personal information of users.
- Company should make some good identification algorithm to detect fake accounts and delete them,this technique can reduce number of fake accounts.
- To protect user's account from Steganography technique which might attacker bind malicious code inside files and run in the background on user's click, Users should not open any attached file from unknown users. At the same time, company should provide some security tools to check the sent attachments for malicious code.
- Users should not accept friend request from unknown people to reduce risk of social networks and protect them from fake accounts.
- To secure users social network account from third party application users should not give access to any application to access their information

CONCLUSION

Social Network is one of the common technology which is used widely by the people to connect with each other. In this research, we discussed important security issues in social network and weakness of developers which can make user's information vulnerable. The main goal of this paper is to make user'sbe aware and more concerned about main security settings of social networks while using them. At the same time, some good recommendations are discussed. It also focuses on privacy issue which is important. By reading this paper, the usersget an idea about the risks of using social network and what are the main security issues that may face. They learn some ways which help them how to protect their account from attackers.

REFERENCES

[1] Golbeck, J. "The dynamics of Web–based social networks: Membership, relationships, and change", Vol. 12, No. 11, November 2007. Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/2023/1889 (Accessed: 2 Feb 2018).

[2] Hunter, D., Goodreau, S., & Handcock, M. (2008). Goodness of Fit of Social Network Model. Journal of the American Statistical Association, 103(481), 248-258. Retrieved from http://www.jstor.org/stable/27640035 (Accessed: 4 Feb 2018).

[3] Berger-Wolf, T.Y. & Saia, J. "A Framework for Analysis of Dynamic Social Networks", August 2006. Retrieved from https://www.cs.unm.edu/~saia/papers/kdd.pdf (Accessed: 5 March 2018).

[4] Skyrms, B., &Pemantle, R. (2000). A Dynamic Model of Social Network Formation. Proceedings of the National Academy of Sciences of the United States of America, 97(16), 9340-9346. Retrieved from http://www.jstor.org/stable/123177 (Accessed: 7 Feb 2019).

[5] Nema, R. and Pandey, A. (2016) A Review on Online Social Network: Issues & Challenges. Social Networking, 5, 57-61. Retrieved from http://www.scirp.org/Journal/PaperInformation.aspx?PaperID=65536 (Accessed: 10 Feb 2019).

[6] Rajam, S. T. R & Kumar, S. B. R. "Security & Privacy issues in Social Network Services: An Overview", IJOIRIE, Vol. 2, Issue 1, January 2014. Retrieved from https://pdfs.semanticscholar.org/ef90/22e0494f0a2e15467b48c16919dcd96a8a00.pdf (Accessed: 11 Feb 2019).

[7] Kallas, P. Retrieved from https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/ (Accessed: 2 Feb 2019).

[8] Edosomwan, S., Prakasan, S. K., Kouame, D., Watson, J., Seymour, T. (2011). The History of Social Media and its Impact on Business. The Journal of Applied Management and Entrepreneurship, 2011, Vol. 16, No.3 Retrieved from (Accessed: 15 March 2019).

[9] Bossetta, M. (2018). THE WEAPONIZATION OF SOCIAL MEDIA: SPEAR PHISHING AND CYBERATTACKS ON DEMOCRACY. Journal of International Affairs, 71(1.5), 97-106. Retrieved from https://www.jstor.org/stable/26508123 (Accessed: 10 May 2019).

[10] Rys, V. (2010). A brief history of the sociology of social security. In Reinventing social security worldwide: Back to essentials (pp. 63-72). Bristol, UK; Portland, OR, USA: Bristol University Press. Retrieved from http://www.jstor.org/stable/j.ctt9qgmmj.9 (Accessed: 18 May 2019).

[11] Toptchiyska, D. (2016). Protecting privacy in social media. In Guadarrama Rico L. (Ed.), Controversial Matters on Media Ethics(pp. 113-126). Madrid: Dykinson, S.L. Retrieved from http://www.jstor.org/stable/j.ctt1k8576r.9 (Accessed: 2June 2019).

[12] Kupiainen, R., Suoninen, A., &Nikunen, K. (2012). Between public and private: Privacy in social networking sites. In Livingstone S., Haddon L., &Görzig A. (Eds.), Children, risk and safety on the internet: Research and policy challenges in comparative perspective (pp. 99-112). Bristol: Bristol

University Press. Retrieved from http://www.jstor.org/stable/j.ctt9qgt5z.13 (Accessed: 5 June 2019).

[13] DAY, G. (2017). SOCIAL NETWORKING SECURITY. In Security in the Digital World (pp. 177-185). Ely, Cambridgeshire, United Kingdom: IT Governance Publishing. Retrieved from http://www.jstor.org/stable/j.ctt1x07wx5.19 (Accessed: 2 June 2019).

[14] Sood, A. K &Enbody, R. J. (2011). Online social networks: Malware launch pads. Retrieved from https://www.helpnetsecurity.com/2011/11/01/online-social-networks-malware-launch-pads/ (Accessed: 9 June 2019).

[15] Huber, M., Mulazzani, M., Kitzler, G., Goluch, S. &Weippl, E. (2011). Friend-in-the-middle Attacks: Exploiting Social Networking Sites for Spam. Retrieved from https://www.sba-research.org/wp-content/uploads/publications/FITM_InternetComputing_preprint.pdf (Accessed: 12 June 2019).

[16] Zhou, B. & Pei, J. (2008). Preserving Privacy in Social Networks Against Neighborhood Attacks. Retrieved from https://www2.cs.sfu.ca/~jpei/publications/NeighborhoodAnonymization-ICDE08.pdf. (Accessed: 14 June 2019).

[17] Luo, W., Lui, J. & Fan, C. (2009). An Analysis of Security in Social Networks. International Conference on Dependable, Autonomic and Secure Computing. Retrieved from https://www.researchgate.net/publication/220716432_An_Analysis_of_Security_in_Social_Networks (Accessed: 15 June 2019).

[18] Kumar, A., Gupta, S. K., Rai, A. K.& Sinha, S. (2013). Social Networking Sites and Their Security Issues. International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013 1 ISSN 2250-3153 Retrieved from http://www.ijsrp.org/research-paper-0413/ijsrp-p1666.pdf (Accessed: 15 June 2019).

[19] Hiatt, D. & Choi, Y. B. (2016). Role of Security in Social Networking. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 2, 2016 Retrieved from https://thesai.org/Downloads/Volume7No2/Paper_2-Role_of_Security_in_Social_Networking.pdf (Accessed: 16 June 2019).

[20] Jabee, R. &Alam, M. A. (2016). Issues and Challenges of Cyber Security for Social Networking Sites (Facebook). International Journal of Computer Applications (0975 – 8887) Volume 144 – No.3, June 2016. Retrieved from https://pdfs.semanticscholar.org/b501/886f966f8cd7e47115d390afbbda017506e1.pdf(Accessed: 15 June 2019).

★★★