Suleman *et al.LGU (IJECI)* 2017

LGU (IJECI)
ISSN: 2522-3429

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol.1 issue1 Oct-Dec 2017

User Trust on Online Social Network on the basis of Security and privacy

Taseer Suleman[1], Hafiz Burhan-Ul-Haq[2], Sadia Zafar[3]
Lahore Garrison University, Lahore, Pakistan
taseersuleman@lgu.edu.pk, Burhanhashmi64@lgu.edu.pk, Zafarsadia73@gmail.com

Abstract:

Online social networks have become a popular medium of sharing information and also major source for connecting the people on a network. As we know that the threats related to online social network is affecting people to great extent, and is resulting in loss of trust among the people. The trust is basically the measure of confidence that an entity and entities will show in different manners, and privacy is basically a set of actions for controlling personal information. Our basic purpose is to improve user privacy and to build user trust on online social networks. For this purpose, we have conducted survey of users especially teenagers and have taken their views about their knowledge of maintaining privacy on social networks, whether they review privacy settings or leave it as it is, without knowing the importance of privacy. After getting survey result we concluded that most of teenagers are unaware of maintaining privacy so they did not review their privacy settings, resultantly they became a victim of different threats related to online social networks. For this purpose, the tool is designed for reviewing or checking the user's privacy settings and generating different alerts for achieving desired privacy level.

Keywords: Privacy, Online social networks, threats, Survey, response.

1. Introduction

We have seen that online social networks have become popular medium among the people during the past decade. The professor J.A Barnes was the first one to introduce the terminology of social network. By the term social network he described the association of people are brought together by family, work, hobby that is for support such as instrumental, informational, and emotional and also from low level to high level of nation. In 1979 two graduate student of Duke University Tom Truscott and Jim Ellis designed and built the first online social network called Usenet. Now, today we have many online social networks available like Facebook, twitter, Google+, and LinkedIn. As we know number of social media networks are increasing day by day, and eventually its opening doors for affecting users. In which one of major threat is

to the privacy of the user which include name, address, contact and email address, attacker steals this type of user's information and harm them in different ways.
Some of the major threats of online social networks are discussed:

Scams

Scams have been the most common threat used by criminals for centuries. In Facebook world, scam is simply a link that attracts the user. This link contains the information of winning of prizes, gift and cards which mostly attracts innocent people, when the user clicks on it, they get a form to fill their details, in this way scammers easily get their personal information like credit cards numbers etc.

Cyber bullying

This includes sending threatening text messages through online social media. Facebook users especially teenagers are mostly affected by cyber bullying.

Stalking

Cyber stalking is harassing a person with messages typically written threats, and also by adopting other ways online behavior that endangers people safety and can cause a serious problem.
Identity theft:

Due to presence of large amount of personal information on online social networks (OSNs) nowadays, it is not difficult for criminals to steal user's identities. Hackers often break into users e-mail account and then make fake online social media accounts. This happens when users are unaware to hiding their sensitive information by reviewing privacy settings.

Harassment

Harassment through online social networks is becoming common these days. If common user does not understand the way, how to protect his/her personal information this threat would continue to exist. Due to existence of these serious threats, there is an immense need to review privacy settings at the user end. There are many solutions available, in order to, minimize threat level.

However each solution can be better addressed, if we can create awareness among users. For this purpose, we have conducted an online survey. Through this survey the user's knowledge about security as well as privacy features of OSNs had been explored. Our survey was focused mainly on the teenagers because most of the users of OSNs belongs to this age group our society. Our results shows that most of the teenagers are unaware of reviewing their privacy settings and as a result their profile is exposed to the hackers. Hackers can steal their sensitive information easily. After analyzing through survey results we have developed our own feature related to OSNs privacy reviewing process, this feature will update OSN user about the exposure level to the public so that user can review his/her own privacy settings, in order to, achieve desired level of privacy. This feature will protect user from the existing threats on OSNs that we have discussed before.

The rest of the article is divided into following sections: Section III describes the

literature review, Section IV describes our methodology, and in section V we have proposed solution.

2. Related Work

2.1 Implicit trust:

Researchers [1] have defined the trust as one's belief towards the ability of others providing valuable rating. They also defined the properties of trust such as Asymmetry, Dynamicity, and Transitivity. At last they represent trust in two ways.

1. Trust representation
2. Trust matrices.

2.2 Privacy-Related Threats:

In this paper [2] the author describes, user requirements regarding privacy issues, user always like that their data must be kept private, but when the data is posted online on social network their data is not secure, ,and as a result they are exposed to threats like spamming, phishing and malicious attacks which causes harm to the users. The spammers send a link or message to victim and capture their personal data. These attacks are specially carried out by cyber criminals through social engineering. Author divided threats into two types in the paper i.e. Privacy related threats and Traditional Networks Threats. Privacy related threats includes user private profile information i.e. birthday, address, contact no, etc.

Author has also discussed the solution to these problems like creating awareness about the information disclosure, Encouraging awareness through educational campaigns, updating the existing legislation, and empowering the authentication.

2.3 Information Attacks on Online Social Networks

In this research [3] the researcher provides many solutions that can be used to increase security as well as privacy regarding use of OSNs. While the best long-term solution to the security problems is increasing the user's awareness, this may be unpractical because of the huge amount of user using OSNs and their perception is that they are in a safe environment, and they believe that there are many solutions and software available which can be used to improve the overall security.

2.4 Measuring Privacy Risk in Online Social Networks

The problem discussed by author in this research [4] highlight the difficulties in quantifying the amount of information revealed unintentionally and also discuss the privacy issue of online social networks. In order to, overcome this problem a tool has been developed namely as a Privaware to detect the unintentional loss of information. The goal of this tool is to recommend user information that should and also to report the loss of information to mitigate privacy threats.

2.5 Online Social Networks: Privacy Threats and Defenses:

The researchers in [5] explain the four causes that may lead to privacy leaks in OSNs. These causes are design or limitation flaws, clash of interest, implicit flow of information,

and user limitations. The user should have control on these flaws and protect themselves from threats. The information given by the user on online social network describes the users and it will be interesting for the hacker.

2.6 Privacy in Online Social Networks:

In this study [6] the researchers have discussed different problem related to OSNs privacy. Researchers have discussed that the risk of privacy is often ignored or underestimated due to lack of experience and awareness among users. The poorly designed tool made by the OSN and also the centralized nature of OSN make the User dependent on the services provided by the social media network, which at times is not as appropriate as required. The solution of this problem is also provided by researchers is that, the user should actually reveals minimum information which is required for basic functionality of OSNs, but at the same time he/she should keep in mind the consequences that might occur because of revealing personal information .So person must be careful while using these functionalities. The writer also discuss that many laws, including the Data Protection Act 1998 UK, focus on data controllers

2.7 Threats of Online Social Networks:

In this study [7] the researchers discussed that the sharing of the personal information is the one of major issue for users. They have also measured the privacy altitude and have criticized the current privacy setting in Online Social Network. Basically the privacy setting is incomplete without knowing that what the user want to share, For this purpose they have conducted an interview of different user of OSNs in order to know what type of, or what features in the privacy settings that user want. At last they concluded that the information must be categorized as it was categorized previously, but more advancement in this feature is needed.

2.8 Trust Management in Online Social Networks:

The problem discussed in this research [8] is the limited trust of users in Online Social Networks. Mostly the people leave the Social networks because of privacy concerns. Another reason of limited trust on online social networks is that, there is increase in privacy or security threats on online social networks like scamming phishing etc. A solution was suggested to control security threats or to develop user trust. He describes that the only way to find trust is the controlling access in which users grouped together into different categories and access all or limited to specify these groups.

3. Methodology

A step-by-step process was needed to address the privacy threat problem faced by end user of OSNs. It started with a survey that was used to gather information about the privacy related feature and its effects on users especially teenagers. Based on the result of the survey, an additional feature of OSNs privacy is developed which would be help to reduce privacy concerns of the OSNs users.

3.1 Survey results and Analysis:

Our first question was about selection of occupation. The responses had shown that most

of the person using online social networks are students as shown in Fig.01.

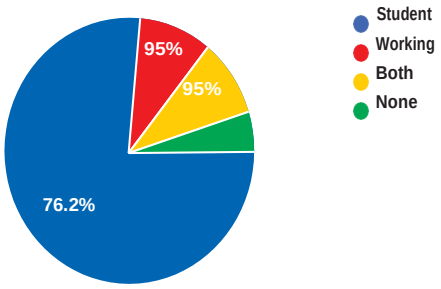

Fig.01. Survey result Question.01

In our next question of the survey, we have asked participants about the social media network that they use? We got to know that more than 70% of them have joined Facebook as their online social network as shown in Fig.02.

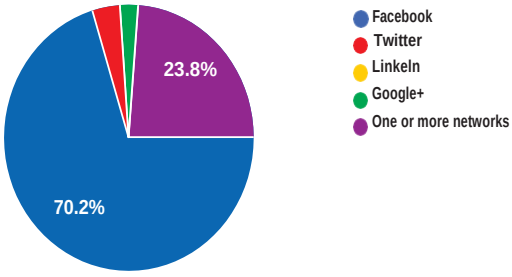

Fig.02. Survey result Question.02

In our proceeding question we had asked about what kind of information they want to include on social sites? Users share all of their vital information on OSNs as shown in Fig.03.

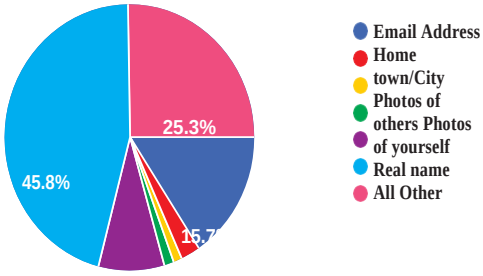

Fig.03. Survey result Question.03

In another question we had ask user about their familiarity about privacy concerns regarding third party applications. Their response was very strange as shown in Fig.04. Most of them had no concern of their privacy while using third party applications in any OSN.

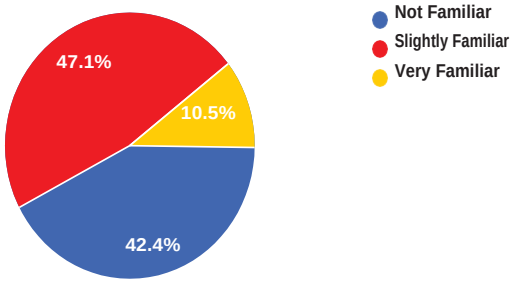

Fig.04. Survey result Question.04

In another question we have asked whether they had ever been victim to a cybercrime. Most of them said “No”. Our analysis is either they had very little knowledge about the effects of cybercrime or they had actually made themselves save from such attacks. The result shows in Fig.05.

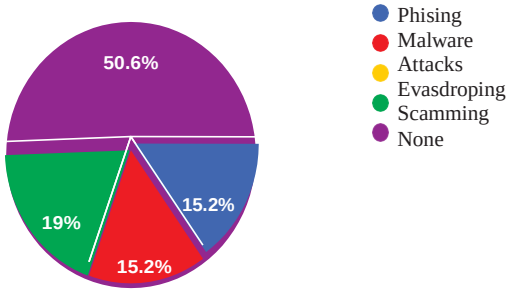

Fig.05. Survey result Question.05

These results show that users have very less knowledge about privacy. They are careless in reviewing their privacy settings, and ultimately they become victim to cyber-attack by hackers. Even OSNs does not provide such mechanism for generating alerts, in order to,

review user privacy settings, we have developed a new feature in which user will be informed about his current privacy settings, and if his/her privacy setting does not comply to the standards of privacy settings, he or she will be notified through our developed mechanism.

3.2 Privacy-alert Mechanism:

We have developed a feature to overcome these problems and to make the OSNs user data more secure, which is the novel idea in online social network. This is dummy tool or feature because online social networks like Facebook do not give the permission to integrate any tool. By using this tool or feature, teenagers set their password strong which is only for their safety purposes as shown in Fig.06.

Fig.06. A dummy Facebook page asking for strong password

Secondly, we have given the easiest or simplest format of security and privacy settings along with important security question which we have obtained after comparison of different online social networks. These privacy settings are quite similar to any other real online social network. It may include privacy features like showing email address and contact number, Blocking messages and third party applications, friend list hiding option etc. A user can adopt any of these settings; For example he or she can show his or her friend list to the public or hide it. In case of showing friend list chances of compromising privacy is higher. This developed feature will determine whether the user profile is secure or it's at risk.

4. Results and Discussions

This feature will create a graph and show the information to the user. The developed feature categorizes the provided information of user privacy settings in to three categories.

- Extremely risky
- Risky
- Secure

In case of "Extremely risky" the user is in red portion of the graph, and has to review his or her profile privacy settings, in order to, prevent from privacy-related threats. In case of "secure" mode, the user has taken all possible measure to ensure privacy. A user with excellent privacy settings is in "Secure" mode as shown in Fig.07.

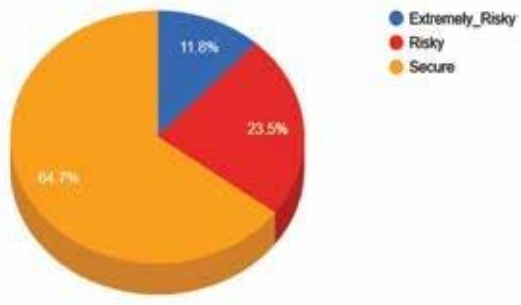

Fig.07. "Extremely risky" profile graph

A user with normal privacy settings is being warned of categorizing him/her in "Risky" mode as shown in Fig.08.

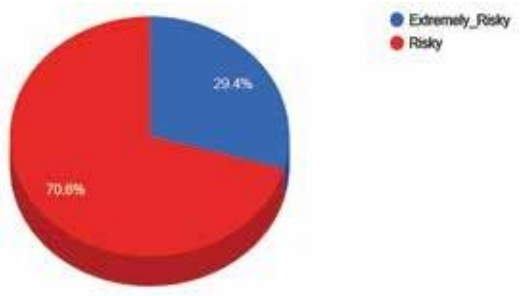

Fig.08. "Risky" profile graph

These pie charts are displayed to the user so that user can review profile privacy settings. This feature would help especially teenager, to, secure themselves form privacy-related threats. This is novel feature that is not included before in any online social network(s).

5. Conclusion and Future Work

In this paper, we have discussed privacy threats regarding OSNs privacy of users especially teenagers. Users are generally don't bother to review their privacy settings which results in the leakage of their vital information. Moreover, there is no such built-in mechanism that exists in any online social network. Which can enforce user to check and review their privacy settings. In our survey results we have also observe irregularities and unawareness at the user end regarding lose privacy settings. This would eventually lead to victimization of a cybercrime. Our proposed feature will help user to find out the level of privacy achieved by checking and reviewing privacy settings. This will help an OSN user to protect his/her profile safe from cyber-attacks.

In future, we will enhance our developed system of OSNs privacy features, and we will also work on security features of social network, that would eventually build user trust on online social networks.

6. Refrences

1 Yadav, A., Chakraverty, S., & Sibal, R. (2015, October). A survey of implicit trust on social networks. In Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on (pp. 1511-1515). IEEE.

2 Gharibi, W., & Shaabi, M. (2012). Cyber threats in social networking websites. arXiv preprint arXiv:1202.2420.

3 Franchi, E., Poggi, A., & Tomaiuolo, M. (2014). Information Attacks on Online Social Networks. Journal of Information Technology Research (JITR), 7(3), 54-71.

4 Becker, J. L. (2009). Measuring privacy risk in online social networks. University of California, Davis.

5 Mahmood, S. (2013). Online social networks: Privacy threats and defenses. In Security and Privacy Preserving in Social Networks (pp. 47-71). Springer Vienna.

6 Beye, M., Jeckmans, A. J., Erkin, Z., Hartel, P., Lagendijk, R. L., & Tang, Q. (2012). Privacy in online social networks. In Computational Social Networks(pp. 87-113). Springer London.

7 Al Hasib, A. (2009). Threats of online social networks. IJCSNS International Journal of Computer Science and Network Security, 9(11), 288-93."

8 Fu, B. (2007). Trust Management in Online Social Networks. University of Dublin, Trinity College September.