Issues in Information Systems
Volume 15, Issue I, pp. 81-87, 2014

SECURITY REQUIREMENTS IN SOCIAL NETWORKS

Mehdi Sagheb-Tehrani (PhD), Columbus State University, tehrani_mehdi@columbusstate.edu
Arbi Ghazarian (PhD), Arizona State University, Arbi.Ghazarian@asu.edu

ABSTRACT

Social networks are among the most popular web sites on the Internet. Nowadays, social networks (SN) are among the easiest forms of communication. SN can replicate the social image of a person. Facebook currently has about over one billion users, while YouTube videos receive over four billion views daily. Because social networking has become so integrated with our day-to-day lives, there is an expectation that these websites provide adequate security to protect their users' data. A survey was conducted to collect data from 50 students at a state university. This paper reports on a survey study that aimed to investigate users' perceptions, expectations, and concerns about the security of social networking websites.

Keywords: Social Networks (SN), Security Requirements, Cybercrime, Information System Hacking.

INTRODUCTION

Social networking web sites are the single largest, easiest, and perhaps convenient way to communicate with other users over the Internet. Facebook currently has over one billion users, while YouTube videos receive over four billion views daily. Nowadays, online social network usage has increased suddenly as these networks become linked into people's everyday lives as places to communicate and meet with other people [2]. Twitter is a widespread social medium. Generally, data from Twitter are often utilized in order to find out why some users of definite communities distinct from other users of the same communities [4, 12]. According to the survey report on USA Today, about thirty five percent of adults on the Internet have a social networking profile on at least one social networking site, and about fifty one percentage of the total population has profiles in more than one social networking websites, three quarters of which are aged between 18 and 24. According to Pew Research Center, 89% of these users use the site to keep up with their friends, 57% make their plans with their friends using these sites, and 49% of the users use these sites to make new friends.

According to a research study posted by Pew Internet posted on Aug 26, 2011, about 65% of adults use Internet also use social networking sites. This includes 60% of male and 69% of female users. With further analysis of the information about the users demographics, provided in the Table 1 below, it can be observed that 83% of the users lie between the ages of 18-29, 70% of them are in the age group of 30-49, 51% between 50-64, and finally 33% are adults who are of age 65 and above [9].

Table 1: Social Networking Sites

Who uses social networking sites?

% of internet users within each group who use social networking sites

All internet users	65%
Gender	
Men	60
Women	69*
Age	
18-29	83***
30-49	70**
50-64	51*
65+	33
Race/Ethnicity	
White, non-Hispanic	63
Black, non-Hispanic	69
Hispanic (English- and Spanish-speaking)	66
Household Income	
Less than $30,000	68
$30,000-$49,999	70
$50,000-$74,999	63
$75,000+	68
Education level	
Less than high school	68
High school grad	61
Some college	65
College+	67
Geographic location	
Urban	67
Suburban	65
Rural	61

Note: * indicates statistically significant difference between rows.

Source: The Pew Research Center's Internet & American Life Project, April 26 – May 22, 2011 Spring Tracking Survey. n=2,277 adult internet users ages 18 and older, including 755 cell phone interviews. Interviews were conducted in English and Spanish.

Social networking websites have their advantages as well as disadvantages [10]. It is not necessary that only the people users intend to be socially involved with, such as friends or people with a common interest, browse their profiles, but it can be a stalker, a hacker, spammers, third party application developer, market analyst, advertisement analyst, or even criminals, who would also be very interested in finding information about users from these websites. This gives rise to security and privacy concerns for social networking users. According to precisely Pew Research Center's Internet & American Life Project, 35% of the people try to avoid social networking sites. Some

reasons can be as following: First and foremost People have concerns about their privacy. Whatever information a user gives to the social networking sites or post in the walls and blogs are and may not be as private as people might think. For instance, on Facebook, a popular social networking website, whatever information a user posts in other user's wall space for them to see, is also publicly available to all other users, unless they send private messages, such as e-mails. Also, there is the possibility that personal information, such as year's birth date, place of birth, user name, real full name, etc. can be sold to third parties for marketing purposes.

Criminals are moving faster than the development of technologies that ensure security [7]. These criminals target people (i.e. phishing, Trojan horse, social engineering) and technology (i.e. digital files, systems, hardware through malware and denial of service attacks). Today, there is no perimeter to protect, and it is difficult to know where the hacker is [13]. Firewalls have become less effective over the years. Hackers have learned how to by-pass firewalls (i.e. e-mail with malicious attachments).

Countries and businesses require information security and assurance in order to operate [5]. This is a global issue and many countries recognize the need for information security. Taiwan has a national information security policy [5, 6]. The United Arab Emirates recognized the need for security awareness in higher education [11]. A research paper from South Africa argues that education is critical for information security [3]. Romania, Qatar, and the United Kingdom see a need for education on phishing [1, 8].

The question remains how can this global issue be addressed? Because of the global scope of the issue, naturally, it requires a global solution that crosses national boundaries. New strategies, policies, regulations, and techniques need to be developed and implemented by corporations, governments, and private multi-national organizations, to provide global assurance – the confidence that the global computer systems are secure [13] However, the problem with assuring a secure Internet system is its global scope; different laws, different cultures, and different law enforcement effectiveness. The Internet does not recognize judicial boundaries.

Because social networking is so integrated in our lives, users have an expectation that the websites will have adequate security to protect the data they give out. There are many different factors that determine how well a given website may be protected. In order to understand these factors and to gain insights into users' perceptions of the security of the social networking websites, we conducted a survey study of social networking users. We hope that insights from studies like the one reported in this paper will help us to better understand users' security concerns and perceptions of the phenomenon of social networking. The rest of this paper is organized as follows: in Section 2, we will present our study survey along with participants' responses to the survey questions. In section 3, we will provide an analysis of the survey results. Conclusions and directions for future work follow in Section 4.

SURVEY DESIGN AND USERS' RESPONSES

To gain insights into the social networking users' perceptions of information security, a survey, including 10 questions with regards to users' opinions about the security on social networking sites, was designed and sent out to students at the first author's institution. The social networks security survey was designed to investigate how social networking users think about social network security. The social networks security survey is designed to reveal the standard thinking of the users. The survey was conducted anonymously as there was no need for participant identification. Fifty students from a University (the name of university is confidential) completed the survey in the fall of 2012. Please see Appendix A for the survey questions.

Responses

1. YES: 50 NO: 0

*Facebook: 34 Twitter: 5 MySpace: 1 Skype: 1 High-five:1 others: 8

2. YES: 28 NO: 22

3. YES: 5 NO: 45

4. 1~6 months: 0 7~12 months: 4 1~3 years: 8 NEVER: 38

5. Facebook: 9 Twitter: 3 MySpace:1 Others: 2 I don't know: 35

6. YES: 47 NO: 3

7. YES: 11 NO: 39

8. Some common answers included: "Report to the social network website", "I don't care", and "I don't know what to do".

9. Some answers included: "Privacy", "personal information", and "the right to feel better".

10. Some answers included: "Make users to change their password often", "Increase fine to warn hackers", and "make strong anti-virus software".

SURVEY ANALYSIS

All of the participants, without any exceptions, stated that they were using one of the social networks. This clearly shows that social networks are extremely popular (i.e., high user base) and, therefore, protecting users' information must be a high priority for these websites. Most of the participants were using Facebook, which is very popular worldwide; Twitter was the next most popular social network after Facebook. Twenty-Eight users stated that they were feeling safe when using social networks, but twenty-two had concerns, particularly with regards to the possibility of their personal information being hacked. Most social networks did not require personal information from users during sign up. Most social networks did not provide a mechanism for password expiry, which can be a protection for user's account against hackers. Participants were not sure about the safest social network, so the majority of them answered "I don't know". In response to Question six, which asked participants about receiving spam messages from hackers, 94% of the respondents stated that they had received spam messages. Furthermore, 22% of the participants stated that their accounts had been hacked in the past. Some respondents, whose accounts had been hacked, did not care about it. However, a few others reported the incident to the social network. Participants suggested that the safety of social network is related to the user rights and privacy of the account and that social networks need to improve to protect their accounts from hackers and viruses.

CONCLUSIONS

Security of social networking is an important aspect in counteracting cybercrime. Cyber victimization is a severe problem faced by Internet users at any age. There is a need to properly understand the factors related to security of social networking so as to develop appropriate policies as well as security and privacy measures. Studies, such as the one reported in this paper, provide a systematic approach to gaining such an understanding. In future work, we plan to put forward a conceptual model of security in social networking. A limitation of our study was that we only had 50 participants, all of which were university students. It will be interesting to replicate the survey with a more diverse and larger population of Internet users. The survey can also be extended with more sample size and further questions to get a deeper understanding of users' thinking about social networks and their security.

REFERENCES

1. Al-Hamar, M. & Dawson, R. & Al-Hamar, J. (2011). The need for education on phishing: a survey comparison of the UK and Qatar. Campus-Wide Information Systems, 28(5), 308-319.
2. Fire, Michael, Roy Goldschmidt, and Yuval Elovici (2013). Online Social Networks: Threats and Solutions Survey., arXiv preprint arXiv:1303.3764.
3. Futcher, L. & Schroder, C. & Rossouw S. (2010). Information security education in South Africa. Information Management & Computer Security, 18(5), 366-374.
4. Gritzalis, Dimitris, M. Kandias, V. Stavrou, and L. Mitrou (2014). "History of Information: The case of Privacy and Security in Social Media." In Proc. of the History of Information Conference.

5. Ku, C.Y. & Chang, Y.W. & Yen, D. D, (2009). National Information Security Policy and its Implementation: A case study in Taiwan. Telecommunications Policy, 33(7), 371.
6. Kumar, Abhishek, Subham Kumar Gupta, Animesh Kumar Rai, and Sapna Sinha. (2013), Social Networking Sites and Their Security Issues?. International Journal of Scientific and Research Publications 3, no. 4 (2013): 3.
7. Luo, X. & Liao, Q. (2007). Awareness Education as the key to Ransomware Prevention. Information Security Journal, 16(4), 195-202.
8. Lungu, L & Tabusca, A. (2010) Optimizing Anti-Phishing Solutions Based on User Awareness, Education, and the Use of the Latest Web Security Solutions, Informatica Economică vol. 14, no. 2, p.27-36.
9. Madden, M., & Zickuhr, K. (2011). *Pew internet*. Retrieved from http://www.pewinternet.org/Reports/2011/Social-Networking-Sites/Report.aspx?view=all.
10. Magklaras, G., Furnell, S., Brooke, P.: Towards an insider threat prediction specification language. (2006) In: Information Management & Computer Security, vol. 14, no. 4, pp. 361--381.
11. Rezui, Y. & Marks, A. (2008). Information security awareness in higher education: An exploratory study. Computers & Security, 27(7/8), 241.
12. Theoharidou, M., Papanikolaou, N., Pearson, S., Gritzalis, D (2013).: Privacy risks, security and accountability in the Cloud. In: 5th IEEE Conference on Cloud Computing Technology and Science, pp.177--184, United Kingdom. IEEE Press.
13. White, G. (2010). "The Evolution and Implementation of Global Assurance." Issues in Information Systems, 11(1), 35-40. (Also appears in PROCEEDINGS of the International Association for Computer Information Systems, Las Vegas, NV, October 6-9, 2010)

APPENDIX A

1. Are you using one of the social networks such as Facebook, Twitter and MySpace?

- YES
- NO

*What is your favorite social network?

2. If you answered YES, do you feel safe on using social networks such as Facebook, Twitter and MySpace?

- YES
- NO

3. Do you need to provide your personal information like address and phone number to access social networks?

- YES
- NO

4. How often does it require changing your password?

- 1~6 months
- 7~12 months
- 1~3 years
- NEVER

5. What do you think the safest social network is?

- Facebook
- Twitter
- MySpace
- Others
- I don't know

6. Have you ever received spam messages from social networks?

- YES
- NO

7. Has your social network account ever been hacked before?

- YES
- NO

8. If you answered YES, what did you do about it?

9. Why are safe social networks important to you?

10. What things do social networks need to improve for their security?