Academia Journal of Educational Research 5(9): 000-000, September 2017
DOI: 10.15413/ajer.2017.0243
ISSN 2315-7704

Academia Publishing

Research Paper

The impact of social networking sites on students' electronic privacy in Saudi Arabia society

Accepted 6th September, 2017

ABSTRACT

The rapid development of information technology has made it possible for many groups in the society, especially students to access the existence of diversity and easy ways of information exchange. There has been a high turnout among students using social networking sites, which have spread rapidly in recent times. However, there has been no progress in the necessary measures taken to ensure proper use of these sites, which has led to several problems of security breach and extortion. In this study, a survey was conducted on different groups of students in Saudi Arabia in order to identify the main problems that lead to security breach, and as a result, provide recommendations for safe usage of this technology with the aim of having a safe society. It has become imperative to qualify Students and inform them about the effects of unsafe use of this technology on the preservation of their electronic privacy. This study aims to provide recommendations to reach a secure e-community. The focus of this study is on students, as this group represents a basis for correcting the performance of societies. Moreover, there is an urgent need to get to a safe electronic community through enlightenment of students on how to use the new communication technology in a safe way, and not ignoring the importance of secure usage.

Key words: Security awareness, students, social networking sites.

Nabih T. Abdelmajeed

College of Computer and Information Security, Naïf Arab University for Security Sciences, Riyadh, KSA.

E-mail: n.arar@nauss.edu.sa

INTRODUCTION

Recent studies have shown that most people are vulnerable to cybercrime attacks due to lack of effective and safe way of using modern communication technologies (Tolnai and Solms, 2009). Also, several studies have demonstrated that IT penetration depends on manipulation of the users with what is known as social engineering (Aloul, 2010; Kruger et al., 2011; Solic et al., 2012; Talib et al., 2010). It has been observed that IT penetration problems are so common in school due to the ease of manipulation of this category (Mohammed and Apeh, 2016). Many scientific studies have confirmed that hackers are seeking to trade with students (Bidgoli et al., 2016). Traffic in this category of students is very dangerous; attacker use porn sites with the aim of subverting the morality, change intellectual believes and sabotage safe communities.

Usually, specialist transforms and develops communities starting with schools' students. This group is the most influential in changing the future of communities. Therefore, in this study, this category was considered to provide the necessary recommendations for improving the sense of electronic security in order to attain a secure electronic society.

In this study, students in middle and secondary school in the Kingdom of Saudi Arabia were targeted in order to detect the effect of negative use of social networking sites on the students' e-privacy.

This study has addressed the fundamental axes and multiple questions in order to reach the recommendations that would reduce IT penetration resulting from erroneous usage of social networking sites. These questions are about

the level of interest in the use of social networking sites, the students' goals of using these sites, the degree of exposure to security breaches and extortion attempts and finally, the level of knowledge on how to deal with social networking site.

LITERATURE REVIEW

The level of users' knowledge in the field of computer security and intelligent communication is a major cause of the electronic penetration phenomenon (Kruger et al., 2011; Boujettif et al., 2010). Thus, educating users on the use of new communication technology in a safe way is a must due to positive impact of improving the protection level of their electronic privacy (Marks and Rezgui, 2009; Talib et al., 2010). An important study indicated that trained users have a high level of security, while the untrained category remained at a low security level (Talib et al., 2010).

Oksanen and Keipi (2013) concluded that the age groups of 15-24 year-olds are vulnerable to attack than older age. In addition, in a study by Aldossary and Zeki, (2013), it was concluded that students who offer security courses can prevent many security problems. Another study demonstrated that training users is a must to enable them protect their privacy (Bidgoli et al., 2016). Markham (2009) pointed out that all levels of students need to be educated on how to use modern electronic communication in a safe way (North et al., 2007). In a study by Gross and Rosson. (2007), it was shown that students cannot differentiate between security problems and hardware problems and as such, it is necessary to improve the awareness level of electronic security among students to help them protect their electronic privacy.

Some studies have shown that the security education level of Saudi society is not acceptable due to the educational system (Alarifi et al., 2012). Moreover, Alarifi et al. (2012) observed that culture reduces important security awareness projects.

PROBLEM DEFINITION

Many communities are not familiar with the use of modern communication techniques. The sudden development of these techniques in a short period of time and its fast spread with great ease of use, as they are available to various groups of society, has led to the high demand and use of these modern technologies. This sudden and unanticipated turnaround has led to many technical problems caused by lack of pre-qualification of users before engaging in this unknown technology. One of the most striking results of this unconscious turnout is the many misguided security practices that have made societies ineligible to avoid the risk of hackers. Thus the recent successes of these hackers in penetrating users' privacy and extortion have increased in recent times, and this has led to misleading and tampering of ideas and beliefs of users, which has posed great danger to communities at different levels.

It has been observed that one of the most widespread technologies are the so-called social networking sites. Statisticians observed that there are "over 2.01 billion monthly active users of Facebook for June 2017, which is a 17% increase year over year, and 1.15 billion mobile daily active users for December 2016[1], an increase of 23% year-over-year". While, in 2016, it was reported that twitter has 328 million monthly active users. Therefore, in this study, a number of questions were raised to determine the impact using social networking sites on loss of electronic users' privacy and also, the rationale behind the loss of privacy. School students in the Kingdom of Saudi Arabia were chosen as the sample of this study due to their recent exposure to IT security breach (Bidgoli et al., 2016). The main axes were chosen to reveal the relationship between social networking sites and the penetration of the users' privacy. These axes are as follows:

i) Identify the turnout degree of using social sites;
ii) Identify the students' goals of using social sites;
iii) Identify the percentage of those who have been hacked and exposed to blackmail;
iv) Identify the level of users' knowledge of the seriousness of dealing with social networking sites.

Several questions have been raised to determine why hackers have been able to penetrate students IT security. By answering these questions, the study aims to provide recommendations that will reduce IT security breach. These questions are described as follows:

1) What is the level of interest in the use of social networking sites?
2) What are the students' goals of using social networking sites?
3) What is the degree of exposure to security breaches and extortion?
4) What is the level of knowledge regarding the seriousness of dealing with social networking sites?

The number of students, according to the official statistics at the Ministry of Education in the Kingdom of Saudi Arabia, is two millions, two hundred and fifty thousand students at the intermediate and secondary level. Based on monkey survey, the number of sample required to study 2250000 students should not be less than 385 cases, where the

[1]. https://zephoria.com/twitter-statistics-top-ten/

Table 1: Different characteristics of the survey and the ratios of each property.

Sex	Frequency	Percent (%)
Male	255	63.6
Female	146	36.4
Total	401	100.0
Educational Level	**Frequency**	**Percent**
Intermediate	88	21.9
Secondary	313	78.1
Total	401	100.0
Economy Level	**Frequency**	**Percent**
High	88	21.9
Middle	289	72.1
Poor	12	3.0
Total	389	97.0
Missing	12	3.0
Total	401	100.0

Table 2: Hour spent on social networking sites.

Hours of use	Frequency	Percent
1 to 2	80	20.0
2 to 4	91	22.7
4 to 6	89	22.2
> 6	133	33.2
Total	393	98.0
System	8	2.0
Total	401	100.0

number of implemented samples is 401. The survey was based on three different characteristics; sex, school stage, and economic level. Table 1 shows different characteristics of the survey and the ratios of each property.

The researcher consulted a group of Statistics specialist in the Department of Statistics at Naif Arab University for Security Sciences in the Kingdom of Saudi Arabia. This consultation is to test the quality level of the questions and to determine whether or not these questions have been addressed to the required study subjects.

RESULTS AND DISCUSSION

The first axis in this study was to know the extent of demand for use of social networking sites among the students. The researcher formulated nine different questions to serve this theme. One of the most important results from the selected sample is that 56% of students use social networking sites for more than 3 h and less than 6 h, while Table 2 shows that 44% of students use social networking sites between one and three hours per day.

This percentage shows the high turn-out of students that use these sites. The percentage of those who use these sites to a large extent is 62.6%, while 32.9% use it moderately. 79% of male and female students have more than one account on these sites. 87.6% of the students said that it is very difficult to stop using these sites. The standard deviation is used to determine the dispersion rate of the responses, and gives indication about homogeneity of the answers. Table 3 shows the arithmetic mean and the standard deviation level of each question.

Table 3 shows the level of standard deviation refers to the one-way agreement, which is the large turn-out of students using social networking sites. Figure 1 represents a graph of the level of standard deviation as appeared on a horizontal line to a large extent. This indicates the general consensus on these disaggregated answers.

Table 4 shows that the general level of the turn-out on the use of social networking sites in the society is 2.2821 out of 3, which is very high. The figure also shows the general average standard deviation of the first axis, which is

Table 3: Analysis of axis one.

Questions	Min	Max	Mean	SD[a]
I use social networking sites permanently	1	3	2.58	0.578
I have more than one account in different sites	1	3	2.27	0.786
I actively participate in networking sites	1	3	2.11	0.703
I recommend using social networking sites	1	3	2.42	0.644
I think it's hard to do without social networking sites	1	3	2.47	0.707
I used Social Network Sides to help me in my study	1	3	2.19	0.729
I used social network side to discuss with my friends	1	3	2.54	0.624
I used social network sides spread my news	1	3	1.67	0.709

a. Standard deviation.

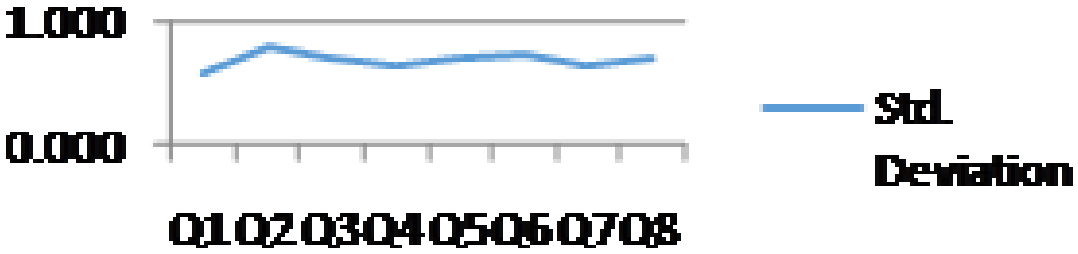

Figure 1: Standard deviation of axis one.

Table 4: General average of axis one.

Questions	Min	Max	Mean	SD
Axis1: turnout of using social networking sites	1.25	3.00	2.2821	0.37073

Table 5: Analysis of axis two.

Questions	Min	Max	Mean	SD
I used my real name in Social network sides	1	3	2.40	0.739
My personal file has right information	1	3	2.23	0.802
I build a sincere friendship through social networking sites	1	3	2.04	0.859
I build a liar friendship through social networking sites	1	3	1.49	0.732
My Parents should not read my accounts	1	3	1.91	0.834
Social network sides help me in my study	1	3	2.14	0.706
I use social network sides for entertainment	1	3	2.62	0.571
I used social network sides for marketing	1	3	1.70	0.810
I used social network sides to track my friends' news	1	3	2.30	0.705

0.37, indicating that the amount of data dispersion was very small; the turnout shown is very close to the reality.

The second axis focuses on the students' goals of using social networking sites. This axis is to determine the rationale behind the huge demand for this technology among students in the community. It was found that 15.2% of students use fake names while on these sites. In addition, 23.2% indicated that their personal information is not real. Moreover, 34.4% of students confirmed that they had established false relationships through these sites. 30.4% refused to let their parents' to see their personal accounts, while 29.7% of them reject their parents' control partially. These percentages indicate the large number of negative uses by male and female students. This negative uses may have negative effects on their privacy. Table 5 shows the mean of different responses, as well as the standard

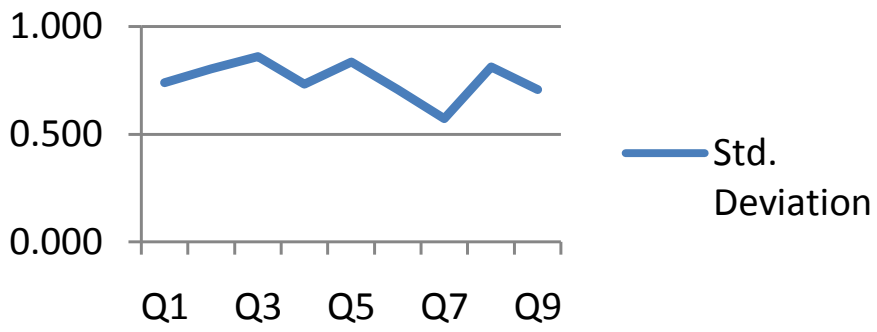

Figure 2: Standard deviation of axis 2.

Table 6: General average of axis two.

	Min	Max	Mean	SD
Axis 2: the goal of using social network sides	1.00	3.00	2.0931	0.37747

Table 7: General average of axis three.

	Min	Max	Mean	SD
The amount of exposure to penetration	1.00	3.00	1.4759	0.48973

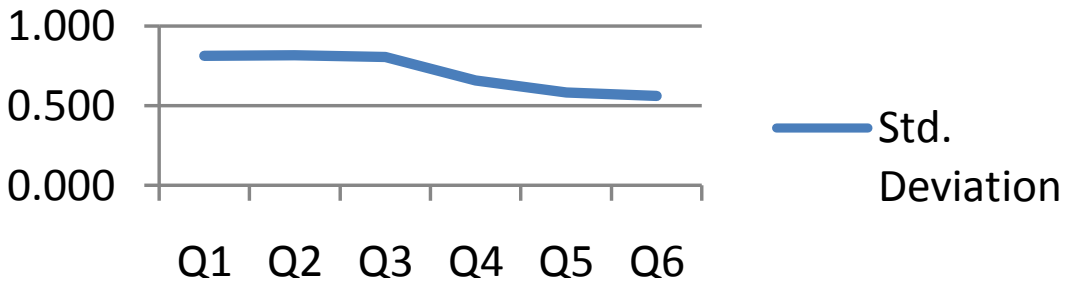

Figure 3: Standard deviation of axis 3.

deviation level of these responses.

The level of standard deviation shown in Table 5 indicates a good degree of consensus among the respondents. The standard deviation in Figure 2 shows this compatibility.

Figure 2 shows the general standard deviation of the axis 2, which is only 0.377 as shown in Table 6.

The third axis is about exposure of students to infiltrations and electronic extortion. The results were remarkable; 22.2% of the students reported that they had been exposed to penetration during their use of these sites. In addition, 34.7% of their passwords have been stolen. Moreover, 15.2% of the students have stolen their files and their own pictures. With regard to extortion, 15.5% indicated that they are being subjected to extortion continuously. These results have been a great surprise, which necessitated this study to determine how to stop this problem in order to reach a secure society. Tables 6 and 7 and Figure 3 illustrate the quality of the answers using mean and standard deviation.

For the last axis, which reveals the level of students' knowledge about the danger of unsafe use of social networking sites, the study pointed to the urgent need to improve awareness among this category. It is obvious that the students do not follow any guidelines or instructions during the use of these sites to keep their files secured. 58.8% of students expressed their acceptance of any friendship requests through these sites and 38.9% believe all the information presented through these sites. In addition, 65.6% of the students believe that social networking sites are safe and trustworthy. Moreover, 64.6% have been using the same password for a long time

Table 8: Analysis of axis three.

Questions	Max	Min	Mean	SD
I have been hacked by social network sides	1	3	1.33	0.656
One of my friends have been attacked by social network sides	1	3	2.00	0.809
My password has been stolen	1	3	1.55	0.814
My account in social network side has been stolen	1	3	1.52	0.803
I have lost my data by social network sides	1	3	1.23	0.582
I get blackmail messages permanently	1	3	1.22	0.561

Table 9: General analysis for axis four

	Min	Max	Mean	SD
Axis 4: Level of knowledge	1.00	3.00	1.9923	0.35875

Table 10: Analysis of axis four.

Questions	Min	Max	Mean	SD
I accept any of a friend request	1	3	1.78	0.741
I believe everything in social network sides	1	3	1.46	0.632
I believe that social network sides is secured	1	3	1.81	0.684
I know what is the electronic penetration	1	3	2.43	0.722
I am well educated how to deal with the social network sides	1	3	2.34	0.728
I know that there are many hackers are targeting users of social network sides to steal their information	1	3	2.54	0.677
I used to check the strength od my password	1	3	2.23	0.798
I used to change my password	1	3	1.78	0.814
I don't mind to give my password to my friend	1	3	1.88	0.841
I think that hackers are targeting the famous people only	1	3	1.93	0.808
I am using antivirus	1	3	2.06	0.833
I am updating the antivirus every time	1	3	2.07	0.831
I do accept all files receipt from social network sides	1	3	1.59	0.750

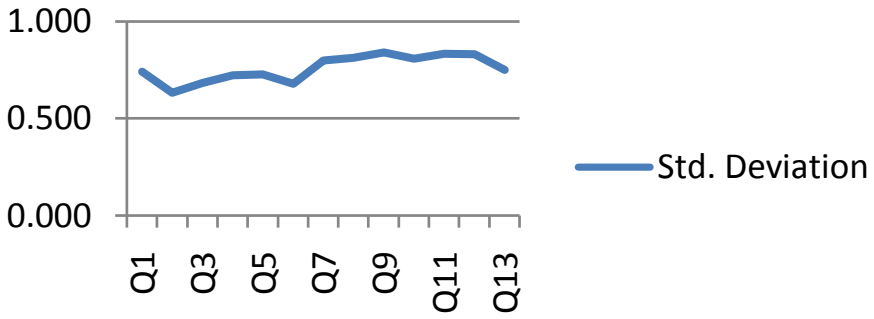

Figure 4: General average of axis three.

and never change it, and more than 57% do not mind telling their friends their passwords. The study indicated that more than 30% do not use any of the protection programs, and 31.2% are using a protection programs but unfortunately, they do not update them at all. These and many other practices indicate that the students are not aware of the seriousness of these sites and may lead to the collapse of society in the future. Tables 8, 9 and 10 and Figure 4 show how accurate these results are.

In this study, it was found that there is a high demand,

among students in Saudi society, for the use of social networking sites. However, there is an urgent need to raise the level of awareness for safe use of these sites. Teaching students has become very necessary, ignoring this may affects families and communities.

CONCLUSION AND FUTURE WORK

This study examined the effects of using social networks sites by students in Kingdom of Saudi Arabia. Three basic criteria were chosen: the gender of the student, the school stage, and economic level. A specialized questionnaire was prepared to verify the level of students' knowledge and study the impact of this level on penetration of the students' privacy during the use of social media. In the first axis, the researcher found that the level of turnout on the use of social networking sites has reached more than 76%. In response to the second question, the percentage of those with not noble targets of using these sites reached more than 69%. The third axes showed that the probability of penetration into Saudi student community is close to 50%. The level of students' knowledge is only 33% and more than 66% suffer from poor electronic awareness. Thus, the researcher discovers that the students in Saudi society suffer from poor awareness on how to use modern communication technology in a safe manner, although the turnout of using these sites is very high. This may pose huge problem at multiple levels, including moral and ideological, as well as intellectual and sexual extortion. Therefore, it is necessary to work to reach an electronic secure society, by working to qualify students on how to use this technology in a safe manner.

Therefore, in order to raise the students' knowledge of e-security, it is necessary to adopt an electronic awareness project for students in the intermediate and secondary stages. Such project on the safe use of social media, can be achieved through a training course. This program must be based on the implementation of many practical simulated scenarios in order to raise the readiness of students to the challenges of this electronic world.

REFERENCES

Tolnai A, Solms SV (2009). Solving security issues using Information Security Awareness Portal. Paper presented at the International Conference for Internet Technology and Secured Transactions.

Aloul FA (2010). Information Security Awareness in UAE: A Survey Paper. Paper presented at the Internet Technology and Secured Transactions (ICITST).

Kruger H, Flowerday S, Drevin L, Steyn T (2011). An assessment of the role of cultural factors in information security awareness., Paper presented at the Information Security South Africa (ISSA).

Solic K, Tovjanin B, Ilakovac V (2012). Assessment Methodology for the Categorization of ICT System Users Security Awareness, Paper presented at the MIPRO.

Talib S, Clarke NL, Furnell SM (2010). An Analysis of Information Security Awareness within Home and Work Environments. Paper presented at the International Conference on Availability, Reliability and Security.

Mohammed S, Apeh E (2016). A model for social engineering awareness program for schools, *2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA)*, Chengdu 2016. pp. 392-397.

Bidgoli M, Knijnenburg BP, Grossklags J (2016). When cybercrimes strike undergraduates," *2016 APWG Symposium on Electronic Crime Research (eCrime)*, Toronto, ON, 2016. pp. 1-10.

Boujettif M, Wang Y (2010). Constructivist Approach To Information Security Awareness In The Middle East. Paper presented at the 2010 International Conference on Broadband, Wireless Computing, Communication and Applications.

Marks A, Rezgui Y (2009). A comparative study of informatioin security awarness in higher education based on the concept of design theorizing, Paper presented at the International Conference on Management and Service Science.

Oksanen A, Keipi T (2013). Young people as victims of crime on the internet: A population-based study in Finland, Vulnerable Child. Youth Stud. 8(4): 298–309.

Aldossary AA, Zeki AM (2013). The Influence of Students' Knowledge on Security towards Their Behavior with Security Risks within the Context of Saudi Arabia, *2013 International Conference on Advanced Computer Science Applications and Technologies*, Kuching. pp. 1-4.

Markham SA (2009). Expanding Security Awareness in Introductory Computer Science Courses. Paper presented at the InfoSecCD '09, Kennesaw, GA, USA.

North MM, George R, North SM (2007). A Brief Study of Information Security and Ethics Awareness as an Imperative Component of Management Information Systems. Paper presented at the ACMSE 2007, Winston-Salem, N. Carolina, USA.

Gross JB, Rosson MB (2007). End User Concern about Security and Privacy Threats. Paper presented at the Symposium On Usable Privacy and Security (SOUPS), Pittsburgh, PA, USA.

Alarifi A, Tootell H and Hyland P (2012). A Study of Information Security Awareness and Practices in Saudi Arabia. Paper presented at the The 2nd International Conference on Communications and Information Technology (ICCIT): Digital Information Management, Hammamet.