Improving Awareness of Social Engineering Threats among Zulfi Technical College Students

Abdulrahman N. Alseqyani

Lecturer at Zulfi College of Technology, TVTC, Saudi Arabia
analse@tvtc.gov.sa

Abstract

There are many approaches that malicious individuals or hackers apply in the attempt to violate the information security protection of a corporation or an institution. Social engineering also termed as the human method is one of them. Social engineering is explicated as the art of using human characters to breach information security without the victim or participant knowledge that they have been manipulated. A huge number of staffs, faculties, and students make use of computer devices to store, manage and share a broad range of data and information. A personal computer contains information that is confidential and distinct personal information; then, it is of great essence to comprehend information security in order to protect information stored in computers. That being said, this paper focuses on improving awareness of social engineering threats among technical college students. A research study was carried out at Riyadh Region, Saudi Arabia in Zulfi Technical College. Questionnaires were drafted and distributed to students in this technical college. A descriptive approach of analysis was adopted to analyze the collected data. This paper in indispensable to college institutions in pursuits of improving awareness of social engineering threats among technical colleges students.

Keywords: security, TVTC, computer, social.

1 Introduction

In the modern world, one of the profound substantial security risks that corporation and institutions encounter is not with applications or system but with employees and other stakeholders such as students. Hadnagy (2014) argues that malicious or negligent staff and other insiders are the ones who mainly contributes to institutions information breach. Human factors have been the primary contributory aspects. Historically, organizations and businesses have basically laid their emphasis on minimizing risk related to technical resolutions (Jakobsson, 2016). Nevertheless, little, if any, resources and efforts have been assigned to enhancing the weak security situation of personnel's. According to Gardner &Thomas (2014), a critical and significant venture to mitigate the rapidly growing risk is improving social awareness of social engineering threats among the parties involved. Several programs comprise of training of employees and students in institutions concerning security principles, required and approved standards of managing sensitive information, procedures of reporting a security breach, emails appropriates practices and security general policies that if adhered to will assist to safeguard institutions and individuals (Jakobsson, 2016). Similar to the significance of tracking and measuring the strong suit of system defenses, it is equally significant to evaluate the efficiency of an awareness program and the applicability of employees and students defenses in an institution.

2 Background

Conheady (2014) asserts that social engineering depends on methods such as persuasion and influence to deceive or persuade victims into breaching security defenses and submitting their personal information. A successful social engineer is considered a profound adept at encouraging individuals that she/he is a person who she/he is not Hadnagy, 2011). Through this approach of influence, unauthorized or illegal entities can have access to the secured system or sensitive information that by all means they are not supposed to gain the access. Therefore, a social engineer is an exceedingly dangerous enemy who is frequently in a position to take advantage of individuals to gain access to information without necessary application of technology.

Jakobsson (2016) indicate that over the past few years, the SANS Institute has reported a disturbing data within the field of social engineering. Results from some surveys show that these methods at bypassing security defense are on the rise. In various high profile or larger institution within the globe, more advanced security measures are being adopted to safeguard the perimeter of their systems (EC-Council Press., 2017). As a result, social engineers have limited access to confidential information via the use of traditional technical attacks. These systems successfully cease authorized access to company information through traditional methods. However, the hacking community is adopting and attempting to advance their techniques to cope with the current technology. Therefore, according to Jakobsson (2016), social engineering seems like a developing method of choice for the present-day hacker.

Hadnagy (2014) argues that lack of or insufficient knowledge among end users has been one of the major causes that have led to the success of social engineering attacks. Hadnagy (2011) asserts that institutions provide essential details and personal information when persuasive gifts are presented to them. Prevalently, these staffs are required to have and depict high security standards. The question is; if the kinds of people we expect to demonstrate high security principles are easily lured, what about general and home computers users who lack technical know-how, and capability to recognize and defend themselves from rapidly growing internet-based threats (Janczewski & Colarik, 2008).

According to Decker (2000), Several security consultants have branded security engineering as a disease due to its flexibility. It is like a disease which can disguise and morph itself into new forms each time is exposed. From this point of view, it seems quite challenging to defend against social engineering threats despite having the knowledge as an end user of the probable threats.

3 Security Awareness Survey

A research survey is a substantial method to measure strength and effectiveness of the institution security awareness. This “Students Security Awareness Survey” has been developed to ask students how they would probably react to certain security correlated situations and questions. The results of this survey have been applied to evaluate areas of the program that need to be enhanced and determine a risk score, or the possibility of compromise or security breach involving students.

3.1 Social Engineering Threats

According to Jakobsson (2016), the current awareness levels of security among business and individuals users of computer devices are not sufficient to limit the growing threats. His notion is backed by the EC-Council Press. (2017) work whose efforts and determination illustrates user's regular inability to differentiate social engineering trial from factual communications as well as their propensity to base their decision upon unsuitable criteria. A research study carried out at the University of Sydney by Greening focused on investigating the awareness of college students to the susceptibility of social engineering conformed to the Jakobsson (2016) idea. In this scenario, 138 students out of 338 students sent a simplistic email address being spoofing replied with their correct credentials (EC-Council Press., 2017). Since 1996, practical incidences of that kind of message have become more rampant. Nevertheless, consequent studies of the same kind of nature do not encourage greater confidence in user's capabilities of identifying social engineering threats. Report from the Anti-Phishing Working Group indicated that the level of the issue continues being a major problem. The finding results indicated that approximately 25,000 distinctive phishing scams are being identified every month (EC-Council Press., 2017). Consequently, users are highly exposed to social engineering threats and high chances of falling victim if they are not properly accustomed to threats.

3.2 Enhancing Awareness of Social Engineering

Some studies have indicated that user training is a meaningless endeavor, arguing that security is a secondary factor in ending users and the most appropriate reaction to improved security depends on software developers (Balasubramanian & Merrill-Cazier, 2009). A well-designed education training program is considered to be an effective method in enhancing awareness of social engineering. In fact, contextual training, web-based training, and entrenched training have been identified to enhance user's capability to precisely recognize threats. A research study carried out by Warren (2013) employed a direct form of user education where they adopted classroom discussion. In interactive group studies, subjects that focused on the attacks of phishing and characters to consider when dealing with such risks. Then, they allowed independent questions to examine this knowledge. Findings from this survey gave favorable results that users were well equipped to handle illegal correspondence after discussing and analyzing the subject material.

Warren (2013) asserts that some of the technical, social engineering approaches revolve around similar methods of tricking the user into presenting their data. Basically, only the delivery technique that changes, instant messaging, via email, or via pop-up browser windows found on legitimate sites. These pop-up windows are often instigated by malware-infected servers. Hackers use a more persuasive approach to persuade victims into submitting their personal information or the kind of information they are interested with. Through the analysis of several established approaches of user awareness, it seems like a comprehensive training is the most appropriate and effective way to minimize users' vulnerability to social engineering threats. However, this does not imply that it will eradicate the whole problem.

4 Research Methodology

4.1 Targeted Population

The researcher formulated a survey questionnaire and adopted a descriptive method to analyze collected data. These research questionnaires were emailed and distributed strictly to Zulfi Technical College in Riyadh Region, Saudi Arabia. Out of 130 questionnaires distributed, only 110 questionnaires were returned indicating 84.6% response rate. However,

21 questionnaires were rejected representing 68.5% response rate. They were rejected because all answers were not completed.

4.2 Survey Design

The questionnaire was designed to capture and obtain information concerning social engineering threats awareness among technical college students. The survey questionnaire was divided into two sections. The first section covered information security in general. The second part covered the questions that students were supposed to answer to the best of their knowledge about social engineering. The survey questionnaire adopted YES or NO answers to make work easier for respondents. Furthermore, the questionnaire put into consideration the sequence and arrangement of the questions for the respondents to answer questions with ease and goes smoothly via the list. All these factors were considered in order to have high number complete questionnaires that could be satisfied usable and valid for the research. The table below outlines the summary of a survey questionnaire.

Information Security Questions
1. Does your college have a security team?
2. Can you be able to tell if your computer is infected or hacked?
3. Have you ever come across a Trojan or virus in college computer or in your computer?
4. Is firewall of college computers enabled?
5. Are college computers configured to be automatically updated?
6. Do you feel secure with your computer or college computer?
7. Passwords are significant for avoiding illegal access to documents and information.
8. Does your computer have an anti-virus?
9. Is anti-virus in your computer enabled and updated?
10. Have you ever logged into college accounts using public devices such as cyber café computers or from public libraries?
11. Have you ever attended security awareness lessons at college?
12. Do you apply the same password for college accounts as you do for personal accounts such as Facebook?
13. Does the college have policies regarding which websites you visit and cannot visit?
14. All information in a hard drive is permanently lost if you format it or erase
15. How frequently do you access your email or college files remotely?
Social Engineering Questions
16. Do you understand the term “social engineering?”
17. Are you aware of social engineering threats?
18. Have you ever shared your password with someone else at college?
19. In my computer, there is nothing important that is of value to other

people.
20. How likely are you going to open an attachment to an email that is not college work related?
21. Do you understand the meaning of the word “Phishing"?
22. Have you ever received a call asking for your sensitive data?
23. Has anyone at college requested you to share your password?
24. Do you understand the procedures to follow if your computer is infected or hacked?
25. Have you ever downloaded the software and installed on a computer college?

4.3 Determine Risk Using Survey

This research survey questionnaire has 25 questions. Some of the responses to these questionnaires show good security practices and strong awareness while other reflect weak awareness, high-risk practices, and negligent activities. Based on these variances, every response or answer has been given a risk value between one and five. “One” indicates lowest risk value while “Five” represents the highest risk value. After the collection of the data, the results can be applied to evaluate the risk level of technical college or the overall risk score.

5 Results and Analysis

Evaluating the Risk Level of Technical Colleges

For all twenty-five questions, multiply the assigned risk value for every response in each question with its frequency. (Assigned response risk value * frequency = total response). Sum up the total response for the whole survey then divide the total cumulative response with the number of respondents to get an institutions’ risk score. Use the college risk value to determine “risk levels.”

Risk levels	Descriptions
low (25-39)	Respondents are informed concerning good security threats and principles, they have been well oriented, and they adhere to the college security policies and standards.
Elevated (40-60)	Respondents have been already trained to college policies and security standards. They understand security threats; however, they might not comply with good security controls and principles.
Moderate (61-81)	Respondents are well informed concerning security threats, and they understand that they are supposed to adhere to security controls and principles, but they require training about institution policies and standards. Besides, they may not know how to report or recognize a security

	threat.
Significant (82-96)	Respondents are not aware security threats or principles, and they do not adhere to college security standards and principles.
High (97-110)	Respondents are not aware of security threats nor do they understand institutional policies and standards. They indulge in activities that are exploited and attacked

The risk score of technical college is 61.7; hence, it shows they have moderate risk levels.

From the research survey carried out, 64% of respondents were computer students. According to the research, 59.6% indicated that they do not know whether their respective colleges have a security team. These type of users put colleges at risk. In the same note, 7.9% of respondents stated their college have not established a security team. This group of users poses a higher risk to the college because they are really misinformed but they seems like they are aware of security threats. A high percentage 41.6% indicated that they cannot be able to tell if a computer hacked or infected. Mostly likely, they will continue using compromised computers; thus, exposing the college to further breach.

Respondents who are not aware of computer viruses expose the college to a substantial danger and they would not understand when and how to report it. Respondents who stated that they are aware of Trojan but still have ever come across a compromised also make college network vulnerable to risk. Their actions might have contributed to the infections by visiting prohibited sites or opening some links. In this case, 34.8%% indicated that they have come across a compromised computer while 23.6% stated that they do not know what is a virus or a Trojan is. It was quite shocking to note that 65.2% of respondent indicated that they cannot be able to tell if firewall of college computers is enabled. They pose an essential risk to the college. While 14.6% responded that the college computer firewall was not enabled. This group sets a higher risk because they understand what firewall is but they do not make efforts to have it enabled.

Also, 67.4% stated that they feel secure with college and their personal computers. Perhaps they right and thus their computers set little danger to the college. Nevertheless, users are more likely to carry out risky transactions or handle sensitive information. As a result, this would raise the consequence of compromise. Only 32.6% showed that they do not feel secure with their personal and college computers. Also, they might be right, and the problem is supposed to be reported to the relevant department. These users are less likely to transact or handle sensitive data which mean that would decrease the effect of hacking. Respondents (20.2%) who indicated that anti-virus is not installed in their computers are ignorant to security. Their actions and behaviors set a huge risk to the college as they are likely to carry out risk transactions. Besides, 23.6% showed that they know what anti-virus is but they cannot be able to tell whether a computer is protected. They make college susceptible to threats. 73% of respondents suggested that they use the same password for school accounts with personal accounts such as Facebook. This high percentage is worrying because the moment personal account is hacked the rest of the accounts are much more susceptible to password guessing and attacks.

From the research survey, 32.6% indicated that they do not comprehend the meaning of the term social engineering while 31.5% stated that they are not aware of social engineering threats. This category of students set a high risk to the college as they cannot be able recognizes malicious practices of adversaries. It was quite shocking to note that 49.4% of students do not know which procedures to follow when a computer is hacked. They pose a higher risk to the institution and are more likely to continue using compromised devices. Besides, 70.8% of respondent stated that they have ever downloaded and installed software on college computers. They also pose a high risk because they are likely to download malicious software and affect a computer. There is a worrying trend of password sharing among technical college students where 58.4% showed they had been requested to share their passwords. The last but not the least, 47.2% do not know the meaning of the word "phishing."

6 CONCLUSION

Having arrived at risk score value of 61.7 which indicate a moderate risk level, there is need to come up with methods that can improve awareness of social engineering threats. These college students set a high risk to the institution. Greatest security concern in technical colleges is students who threat security system via information leak. Insufficient knowledge among end users has been one of the major causes that have led to the success of social engineering attacks. Hackers exploit multiple institutional, human and demographic aspects to deceive users into unknowing actions and behaviors that advance or support social engineering threats.

7 RECOMMENDATION

From the literature review and analysis of our findings, we suggest the following approaches improve awareness of social engineering threats among technical colleges' students. Technical colleges should develop and adopt effective awareness and training focused on enlightening students concerning social engineering threats. These programs should be objective to assist students to recognize deceiving practices, identify patterns of doubtful patterns of social engineering threats. Training should also focus on teaching how to deal with malicious activities and incident management practices. These are ways to overcome personal susceptibilities and limitations together with proper responses to social engineering threats. Students should be in a position to whether the devices they are using are well secured. That is, anti-virus is installed and updated, the firewall is enabled, and computers are configured to be automatically updated.

Both technical colleges and students may highly benefit from avoiding unsecured websites, avoid downloading and installing software, and limit data that malicious people or hackers might exploit. It is of great importance for technical colleges to maintain and enable enhanced tools for network and computer defense to catch up with sophisticated approaches are being used by adversaries. Technology is rapidly changing leading to more sophisticated social engineering threats. In some instances, social engineering threats might be well developed in such a way that it can bypass institution finest countermeasures. Hackers achieve their goals even if only one student is vulnerable to deceiving practices. Therefore, technical college strategies to counter attack social engineering threats much be comprehensive and take in security practices, advanced cyber security tools, and training programs.

ACKNOWLEDGEMENT

The researcher thanks TVTC for its support and thanks all Zulfi Technical College staff for assistance and comments that help improving the topic.

REFERENCES

Balasubramanian, S., & Merrill-Cazier Library. (2009). Strides towards better application security. Logan, Utah: Utah State University Merrill-Cazier Library.

Conheady, S. (2014). Social engineering in IT security: Tools, tactics, and techniques. New York: McGraw-Hill Education.

EC-Council Press. (2017). Ethical hacking and countermeasures: Book 2. Boston, MA: Cengage Learning.

Gardner, B., & Thomas, V. (2014). Building an information security awareness program: Defending against social engineering and technical threats.

Decker, L. G. (2000). Factors affecting the security awareness of end-users: A survey analysis within institutions of higher learning. Minneapolis: Capella University.

Hadnagy, C. (2011). Social engineering: The art of human hacking.

Hadnagy, C. (2014). Social Engineering and Nonverbal Behavior set. Hoboken: Wiley.

Jakobsson, M. (2016). Understanding Social Engineering Based Scams. New York, NY: Springer New York.

Janczewski, L., & Colarik, A. M. (2008). Cyber warfare and cyber terrorism. Hershey: Information Science Security. (1986). Newton, MA: Cahners Pub. Co..

Warren, M. . (2013). Case studies in information warfare and security: For researchers, teachers and students. Academic Conferences and Publishing International Limited: United Kingdom.