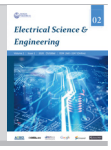
BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Electrical Science & Engineering
https://ojs.bilpublishing.com/index.php/ese



ARTICLE

Cyber Security Awareness among Students and Faculty Members in a Sudanese College

Mohammed Daffalla Elradi* **Altigani Abd alraheem Altigani** **Osman Idriss Abaker**

Communication Systems Engineering Department, University of Science and Technology, Khartoum, Sudan

ARTICLE INFO

Article history
Received: 15 October 2020
Accepted: 30 October 2020
Published Online: 30 November 2020

Keywords:
Cyber security
Awareness
Passwords
Students
Faculty members

ABSTRACT

In the last few years, cyber security has been an essential prerequisite for almost every organization to handle the massive number of emerging cyber attacks worldwide. A critical factor in reducing the possibility of being exploited is cyber security awareness. Not only having the adequate knowledge but how to utilize this knowledge to prevent cyber attacks. In this paper we conducted a survey that focuses on three vital security parameters, which are trust, passwords and defensive attitude respectively. The survey mainly aimed at assessing cyber security knowledge of 200 students and 100 faculty members in a Sudanese college and how secure these participants think they are according to their current cyber behaviour. 56% of the participants are males and 44% are females. The results revealed that all participants were having fairly-low level of security awareness and their defensive attitude is considerably weak and doesn't protect them either individually or at institutional-level. Nevertheless, faculty member showed better cyber security knowledge and skills by 8% higher than students. This study can be used to develop training approaches that bridge the security gaps depicted by the respondents of the survey questions manipulated in this study.

1. Introduction

Cyber security, or information security, has become one of the major concerns of organizations, communities, and even individuals. Cyber-crime has increased steadily as technology advanced varying from robbery, identity theft, ransom, spying, and deception. That definitely confronts us with new challenges. Hence, it is mandatory for users to fully be aware of privacy and security risks and also have the sufficient awareness to protect themselves from cyber-attacks; as users represent the weakest part of the chain [1].

Cyber-attacks have been a trend in the few past years as companies and large organizations encountered catastrophic impact from such attacks including the loss of information assets, business disruption, equipment damage and revenue loss [2]. As it is expected that the number of cyber-attacks will grow in the near future, the notion that organizations need to be cyber resilient is becoming increasingly popular [3].

On almost a daily-basis cyber-attacks and exploits are conducted, exploiting miscellaneous vulnerabilities [4]. In contrast, defensive mechanisms are also being innovated to cope up with such a rapid pace to guarantee optimum levels of Information security; which is turning out to be a

**Corresponding Author:*
Mohammed Daffalla Elradi,
Communication Systems Engineering Department, University of Science and Technology, Khartoum, Sudan;
Email: mohd_daf_elradi@hotmail.com

DOI: https://doi.org/10.30564/ese.v2i2.2477

tough task as technology keeps advancing [5].

However, developing a defensive strategy needs a comprehensive study from different points of reference [6]. Firstly and foremost, it is essential to fully understand the available approaches for designing an optimum defensive strategy, then it is also mandatory to be fully aware of and even predict the strategies been adopted by attackers. Eventually, understanding that every technological approach in one way or another can be compromised by human behaviour [7]. In the other hand, attackers exploit vulnerabilities that most probably emerge from users not aware of cyber security practices; which in return facilitate the process of systems compromise for attackers [8].

Security awareness plays a pivotal role in our daily life nowadays, as users are expected to have, at least a clue about basic security risks and privacy policies, also their attitude towards how they can protect themselves from cyber-attacks is a critical factor when it comes to maintaining a robust cyber security approach [9,10].

In African countries, college students and faculty members are expected to have more computer-related technological literacy compared to other categories of the society, which also include having the adequate cyber security awareness to govern and utilize that literacy. Hence, carrying on a thorough study to validate this assumption is one of the major aims of this paper.

The rest of this paper is organized as follows:

Section II discusses some related work to the studies conducted on students regarding their cyber security awareness. The survey questions and the methodology followed in conducting the survey is highlighted in section III. Section IV and IIV preview the results and discussion correspondingly. Eventually, recommendations and conclusion are detailed in section V.

2. Literature Review

Several studies have been carried out in recent years to assess cyber security awareness level among college students and faculty members. Most of these studies aimed at conducting surveys encompassing elementary cyber security practices that form the first line of defence from trivial to massive cyber-attacks [11].

In [12], a study was conducted to understand how students of a Malaysian university were aware of the risks imposed by social networking sites, which revealed that about 33.3% of the students had been victims to some sort of social networking scams. Another study in the realm of social networking was conducted in [13] among 377 users of Facebook, Twitter and LinkedIn, where 41% showed a concern about online privacy and 44% were lacking the mechanisms of social networking privacy policy.

Senthilkumar et al. [14] performed an online survey for 500 Tamil Nadu college students regarding miscellaneous cyber security threats. The results revealed that 70% of the participants were fully aware of security practices to prevent virus attacks and they had been using up-to-date antivirus software. In the other hand, the remaining 30% of participants were reported to using antivirus software that is obsolete and 11% of them were not even using antivirus at all.

It might be observed that most of the studies managed to highlight that most participants don't have the sufficient awareness of cyber security practices and principles, also revealing much personal information that expose their privacy to considerable security risks without having them noticing. Moreover, the issue doesn't emerge from not having enough security awareness and knowledge but from applying that knowledge when it comes to cyber-related routine; which is tremendously challenging.

3. Methods

In order to assess cyber security awareness and practical applications among students and faculty member effectively, a survey was designed in a way that proactively consider three main factors: Level of knowledge, attitude and habits. The survey questions were designed to be brief and simplified to guarantee that participants don't get confused with advanced technological terms that might be disrupting, thus reduce the expected outcome but yet effective in assessing cyber security awareness and practices. There were 8 questions as follows:

(1) Do you use an up-to-date antivirus program?

(2) Do you access links sent to you by friends of a friend or even a friend without even observing the URL i.e. the link?

(3) If you are asked by an employee from the IT department at your college to provide him with your account password for any reason, would you do it?

(4) Have you ever used your phone number, birth date or even year of birth or a combination of your first name and birthday as your password?

(5) Does your password contain a combination of Alpha-numeric (A-Z or a-z or 0-9) and special characters (@, #, $ ...etc.)?

(6) Do you use the same password for all your accounts i.e. Email, Facebook account ...etc.?

(7) Would you use password unprotected Wi-Fi networks in public?

(8) Do you always sign-out from your personal or work accounts after you finish using it, even if you are using your own device?

The previously-mentioned survey questions evolved

 DOI: https://doi.org/10.30564/ese.v2i2.2477

around three main scopes: Trust, passwords and defensive attitude. These scopes will be discussed below.

3.1 Trust

It is an undeniable fact that human-factors have been a topic of debate in Information security, as non-secure human behaviour can be easily exploited the less they lack awareness about Information security principles and practices [15]. Researches in the field of behavioural science and personality traits highlighted the matter of trust and how it exposes security breaches and they have been trying to design some methods to predict and analyse the behaviour of the attacker as well as the victim [16]. A consideration for gender psychology should also be maintained to understand how such factors affect the realm of cyber security [20]. Therefore, it was essential to consider trust as a main factor for keeping you safe or confront you to catastrophic impacts.

3.2 Passwords

In order to authenticate a user, both account identification and password are required. The process aims at indicating a specified resource to be fetched along with an authorization string associated with that identifier to guarantee an authorized access [17]. Many studies revealed that a lot of users tend to use easy-to-guess passwords, which almost incorporate part of their first name, the year of their birth or even their phone number, which is a common habit in Sudan. The issue lies in having the users using these passwords for multiple accounts, which might be disastrous if a hacker got a hand on the password [18]. Noting that account identifiers i.e. usernames didn't receive a considerable attention although they represent the first line of defence when it comes to security principles. This was essential to evaluate how our participants are ranking when it comes to passwords.

3.3 Defensive Attitude

The term attitude stands for (what you think) [19]. In cyber security, adopting a defensive attitude isn't always efficient because you might think you are safe and satisfied with the security practices that you follow; not knowing that you are putting yourself at the verge of being exploited as hackers are developing their strategies much rapidly than you can ever expect, which makes cyber security a major concern nowadays. Hence, it was essential to estimate how secure our participants think they are.

Taking into consideration the previously mentioned scopes, an overall of 300 participants were segmented into two categories; students and faculty members respectively. The two categories have been further categorized according to gender as shown in figure 1 below. Another factor that had been considered in this study is the average age of participants in the two categories, which was 22 years for students and 37.5 years for the faculty members.

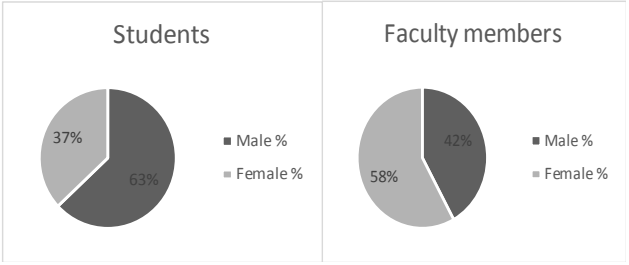


Figure 1. Pie charts that illustrate the percentage of participants from the two categories according to gender

The results of the survey will be discussed thoroughly in the next section.

4. Result

This section describes the results revealed from the survey conducted in this study, where the questions aimed at assessing the cyber security awareness among students and faculty members from specific perspectives, like how they might unconsciously forget to apply cyber security principles they know as being affected by their level of trust, how they manage their passwords and how secure they think.

Numerical Results

The response to the first question whether our participants use an antivirus program or not showed that a majority of 77.75% consent to use an up-to-date antivirus program while 22.25% didn't use or even know if they have an antivirus program installed on their devices or not. 78.5% of the students answered "Yes". On the other hand, 21.5% answered "No". Similarly, 77% of faculty members answered "Yes". While 23% answered "No", the majority were females 69.6% and a minority of 30.4% females.

The second question proactively measures the degree of trust in friends or acquaintance, where an overall of 74.75% answered "No". In contrast to 25.25% who answered "Yes" among both students and faculty members evenly. Again, the third question was intended to measure the level of trust in IT employees for both categories of participants. The results were as follows: 86% of students and 95% of faculty members agreed to provide IT employees with their personal identifier i.e. password. It was noticed that most of the responders who disagreed were hesitant at first and it was also obvious that they didn't answer confidently and took longer time than they did to

DOI: https://doi.org/10.30564/ese.v2i2.2477

answer other questions.

Then the questions ranging from four to six adopted the scope of how our participants manage to think regarding passwords, we were actually expecting them to use easy-to-remember yet easy-to-guess passwords that might expose their entire cyber experience to hazardous risks. Typically, as our fourth question highlighted, 97% of overall participants have used their phone number, birth date, year of birth or a combination of first name and birthday as their password, which makes it an easy task for hackers to guess their victim's credentials. However, three quarters of them managed to use a combination of Uppercase, lowercase, figures and special characters sometimes.

The most terrifying fact actually emerged from the response to question six, which indicated that 85% of our participants use the same password for multiple accounts. This "as a personal opinion" clearly depicts that the participants put their personal privacy in cyber security at risk as well as in a critical situation.

Question seven also retained a considerable agreement among both categories by 86% who might use an open public Wi-Fi. The rest 14% who disagreed were further asked about "why not?" and their answers were not related for security concerns as we expected but most of them reflected that they were satisfied with the cellular data connection either in their laptops via modems or via their phones.

Lastly, answers to question eight disclosed that a majority of 73.5% of students don't sign-out of their accounts but just close the page or window. Contradictorily, 81% of faculty members ensured that they got accustomed to sign-out of their accounts according to their work routine. Figure 2 below illustrates the level of security awareness among students and faculty members by evaluating the parameters discussed earlier in the preceding section.

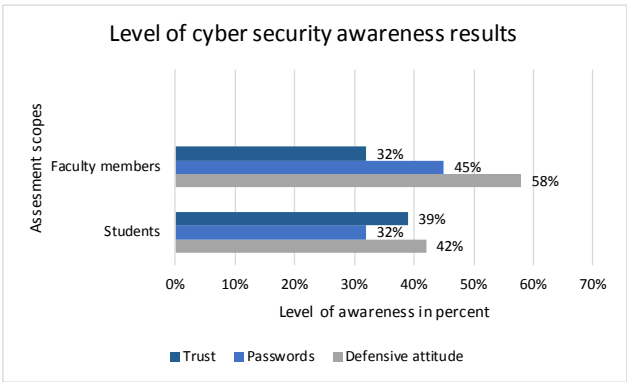


Figure 2. A bar chart that represents the level of cyber security awareness revealed by students and faculty members

5. Discussion

The levels of cyber security awareness for both categories of our study indicate that the mechanism of defensive attitude maintained by our participants is significantly unsecure and exposes them to cyber security risks. Most of the participants were aware of the importance of keeping themselves secure when it comes to information security but they were tremendously lacking the sufficient knowledge to keep them complying with the basic principles of such a challenging aspect. By considering figure 2, it is obvious that the average of cyber security awareness level is quite low. Yet faculty members exhibited better skill set and knowledge compared to students by 54% and 46% respectively as represented in figure 3 below.

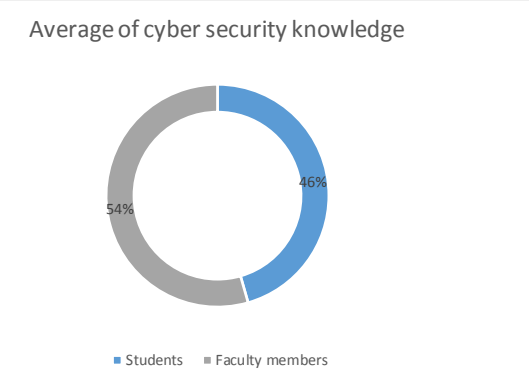


Figure 3. Average cyber security knowledge for students and faculty members

6. Conclusion

In this paper, a thorough study was conducted, aiming to assess the cyber security awareness among students and faculty members in a Sudanese college. As the technology is advancing rapidly, threats also increase; confronting organizations and educational facilities to miscellaneous attacks if cyber security knowledge and practices haven't been well considered. The results of the survey conducted were highlighting a severe lack of awareness when it comes to Information security. This might be reasonable because most of the participants are related to the medical field, which is "far away" from the realm of computer or information technology as they indicated but that's not reasonable if we consider that cyber security is turning out to be as serious as personal or even national security. Nevertheless, it is mandatory to amend our behaviour to cope up with such a high priority line of defence.

It is highly recommended to educate users i.e. students and faculty members about how to securely use their devices (including PCs, laptops, PDAs and mobile phones) safely from anywhere. One way to do this is by creating

DOI: https://doi.org/10.30564/ese.v2i2.2477

policies and regulations that govern the usage of information and devices in a simple way that can be easily understood. Another way is to include basic cyber security knowledge in the first year of the college or for early education levels such as primary or secondary school. It should also be extensible to include security at home, such as securing home Wi-Fi to securing IoT (Internet of Things) items; which are getting popular nowadays.

It is also essential to train users by implementing real-life scenarios to guarantee the effective practicing of the knowledge attained when confronted to a situation that might put their cyber security at the edge of exploitation. This paper can be considered to mainly focus on the points of weaknesses indicated by the individuals who had been questioned and designing an effective cyber security curriculum or at least, training sessions that fit all ages and consider the difference in students' specializations.

References

[1] Moallem, A. Cybersecurity Awareness Among Students and Faculty. Boca Raton, FL: CRC Press, 2019.

[2] Tareq Ahram, Waldemar Karwowski. Advances in Human Factors in Cybersecurity. Proceedings of the AHFE 2019 International Conference on Human Factors in Cybersecurity

[3] Aboul Ella Hassanien, Mohamed Elhoseny. Cybersecurity and Secure Information Systems_ Challenges and Solutions in Smart Environments, 2019.

[4] Cuthbertson A. Ransomware attacks rise 250 percent in 2017, Hitting U.S. Hardest. Newsweek, September 28, 2017.
www.newsweek.com/ransomware-attacks-rise-250-2017-us-wannacry-614034

[5] Yuri Diogenes, Erdal Ozkaya, Cybersecurity. Attack and Defense Strategies_ Infrastructure security with Red Team and Blue Team tactics, Packt Publishing, 2018.

[6] National Institute of Justice. 2018. The Fingerprint Sourcebook. NIJ.
https://www.ncjrs.gov/pdffiles1/nij/225320.pdf

[7] Adhikari, D. Exploring the differences between social and behavioral science. Behavioral Development Bulletin, 2016, 21(2): 128-135.

[8] Crossler, R.E., Bélanger, F., Ormond, D. The quest for complete security: an empirical analysis of users' multi-layered protection from security threats. Inf. Syst. Front. 2017, 1-15.

[9] Cuthbertson A. Ransomware attacks rise 250 percent in 2017, Hitting U.S. Hardest. Newsweek, September 28, 2017.
www.newsweek.com/ransomware-attacks-rise-250-2017-us-wannacry-614034

[10] Young, H., van Vliet, T., van de Ven, J., Jol, S., Broekman, C.: Understanding human factors in cyber security as a dynamic system. In: International Conference on Applied Human Factors and Ergonomics. Springer, Cham, 2018: 244-254.

[11] Farzan A. College students are not as worried as they should be about the threat of identity theft. Business Insider, 2015.
www.businessinsider.com/students-identity-theft-2015-6

[12] Grainne H. et al. Factors for social networking site scam victimization among Malaysian students. Cyberpsychology, Behavior, and Social Networking, 2017.
DOI: 10.1089/cyber.2016.0714

[13] Hossain A., Zhang W. Privacy and security concern of online social networks from user perspective. International Conference on Information Systems Security and Privacy (ICISSP), Angers, 2015: 246-253

[14] Senthilkumar K., Easwaramoorthy S. A survey on cyber security awareness among college students in Tamil Nadu. IOP Conference Series: Materials Science and Engineering, Volume 263, Computation and Information Technology, Tamil Nadu, 2017: 1-10.

[15] Wisniewska, M., Wisniewski, Z. The relationship between knowledge security and the propagation of innovation. Adv. Intell. Syst. Comput. 2019, 783: 176-184.

[16] Winston-Proctor, C. E. Toward a model for teaching and learning qualitative inquiry within a core content undergraduate psychology course: Personality psychology as a natural opportunity. Qualitative Psychology, 2018, 5(2): 243-262.

[17] Brumen, B., Taneski, V. Moore's curse on textual passwords. In: 2015 28th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2015.
https://doi.org/10.1109/MIPRO.2015.7160486

[18] Stainbrook, M., Caporusso, N.: Convenience or strength? Aiding optimal strategies in password generation. In: International Conference on Applied Human Factors and Ergonomics. Springer, Cham, 2018: 23-32.
https://doi.org/10.1007/978-3-319-94782-2_3

[19] Kruger H., Kearney W. A prototype for assessing information security awareness. Computers & Security, 2006, 25(4): 289-296

[20] Wayne Patterson, Cynthia E. Winston - Proctor - Behavioral Cybersecurity. Applications of Personality Psychology and Computer Science. Taylor & Francis. CRC, 2019.

DOI: https://doi.org/10.30564/ese.v2i2.2477