Indonesian Journal of Electrical Engineering and Computer Science
Vol. 32, No. 3, December 2023, pp. 1580~1588
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v32.i3.pp1580-1588

Cybersecurity awareness among university students in Mogadishu: a comparative study

Adnan Abdukadir Ahmed[1], Abdikadir Hussein Elmi[2], Abdijalil Abdullahi[1], Abdullahi Yahye Ahmed[3]
[1]Faculty of Computing, SIMAD University, Mogadishu, Somalia
[2]Faculty of Computer Science and IT, Mogadishu University, Mogadishu, Somalia
[3]Faculty of Engineering, SIMAD University, Mogadishu, Somalia

Article Info

Article history:

Received May 8, 2023
Revised Jul 27, 2023
Accepted Sep 7, 2023

Keywords:

Awareness
Cyber security
Cybercrime
Personal privacy
University students

ABSTRACT

This study aimed to assess the level of cyber security awareness among graduate and undergraduate students in five universities in Mogadishu. The study used a one-way analysis of variance (ANOVA) to examine the difference in cyber security awareness levels between graduate and undergraduate students across five reputable universities. The questionnaire method was used to collect data from 250 graduate and undergraduate students from SIMAD, SIU, UNISO, Jamhuriya, and Mogadishu universities. The cross-tabulation result showed that there was a significant difference in cyber security awareness levels between the universities. Specifically, the results showed that students from SIMAD and Jamhuriya universities suffered from virus attacks, while SIU students struggled with password strength and social network misuse. Mogadishu students faced phishing and virus attacks, and UNISO students dealt with both virus attacks and password strength issues. The study recommended that universities educate their students and parents on safe internet usage and cybersecurity and monitor and secure their internet and computer services. Additionally, the authors recommended the development of cybersecurity software to help students use their data confidently and securely.

Corresponding Author:

Abdikadir Hussein Elmi
Faculty of Computer Science and IT, Mogadishu University
Mogadishu, Somalia
Email: xayeeysi77@gmail.com

1. INTRODUCTION

Nowadays, many internet users send different types of information in the system of complex networks, but did they ever think about the challenges of integrity and security of the data transmitted to the other person safely without any leakage of information? [1]. The rise of cybersecurity threats has posed a major challenge for organizations and individuals, given the growing reliance on online activities and decreased face-to-face interaction. Consequently, the internet has revolutionized how people acquire knowledge, learn, and engage with others. This new trend has also facilitated communication and social interactions. Khalid [2] and Khalid *et al.* [3] although the birth of the internet is widely considered one of the most valuable innovations globally, its extensive usage has negative consequences resulting from its misuse by users [4]. The use of the internet exposes users to cyber risks such as addiction [5], personal information exposure [6], and online fraud. Consequently, organizations that grant access to their internal network are exposed to numerous attacks [7]–[9]. As a result, adequate cybersecurity measures are essential to mitigate the risks associated with internet usage.

Students are the primary users of the internet, which is the fastest-growing infrastructure. However, they are also most likely to engage in cyber crimes and information leakage due to curiosity and access to emerging technologies. The study aims to investigate the factors contributing to this trend and provide insights into student motivations for cybercrime and information leakage. The research highlights the importance of educating students about cybersecurity risks and implementing strict measures to protect sensitive information from unauthorized access. The incidence of cybercrime is a growing concern, particularly among university students who are often targeted by cybercriminals [10].

Many universities have reported high rates of cyber-attacks, with the information systems of these institutions being particularly vulnerable. Cyber attacks can lead to the exposure of sensitive information, including social media and banking information, as well as intellectual property like patents belonging to both faculty and students. Additionally, personal information of staff, students, and faculty members can also be at risk. Given the high frequency of cyber-attacks on higher education institutions, promoting cyber awareness has become increasingly paramount [11].

Today, the widespread use of the internet in daily life has led to increased connectivity and reliance on technology for various purposes, such as socializing, conducting business, and accessing healthcare and education services. However, this continuous connectivity also poses increased risks, as cyber threats can jeopardize critical infrastructure and the economy. Cybersecurity risks can result in financial, identity, and privacy concerns for individuals [12].

To address these risks, it is necessary to implement cyber security awareness programs for university students in higher education institutions. A research study can be carried out to evaluate the degree of cybersecurity knowledge and awareness among college students in Mogadishu, given that computers and the internet have become essential tools for daily academic and work activities. This emphasizes the importance of educating students about the risks and challenges of cyberspace. The study aims to raise awareness about potential dangers and provide insights into measures that can mitigate these risks [13].

Adeyami [14] the majority of African organizations spend less than $10,000 on cybersecurity, with Nigeria having the highest number of such organizations. Additionally, a significant number of these organizations lack proper cybersecurity management 83% and skills to combat cyber-attacks 97%. Alarmingly, 64% of these organizations do not offer cybersecurity training to their employees. These findings indicate a lack of cybersecurity awareness across the country. In higher institutions, students heavily rely on the internet for information and social interaction [15]. However, prolonged internet usage exposes students to various online threats and vulnerabilities.

This study aims to determine how password strength, phishing, virus attacks, and misuse of social networks are related to cyber security. This study compares the awareness of cyber security among graduate and undergraduate students in Mogadishu. This paper is organized into several sections. The second section will review the relevant literature, while the third section will discuss the methodology employed in this study. The fourth section will present the research findings and discuss them in detail. Finally, the paper will conclude with a summary of the main points discussed in the previous sections.

The relevant review is the widespread use of the internet has revolutionized the way organizations conduct their operations by providing a convenient platform for communication and collaboration among stakeholders, including clients and managers. However, the internet has also resulted in various negative effects in the form of frequent cybersecurity threats. To minimize the impact of cyber attacks, cybersecurity awareness and training are essential, as these can make people aware of the dangers and help prevent attacks. Criminals often use phishing emails, network traffic, and user profiling to launch attacks, primarily targeting the most vulnerable or inexperienced people. Moallem [16], cyber attacks are usually targeted towards individuals who are vulnerable or lack experience in dealing with such threats. Reyns *et al.* [17] a small percentage of students, specifically 4.9%, have been subject to cyberstalking. It is evident that students are more susceptible to cyber-attacks, and this emphasizes the importance of promoting greater cybersecurity awareness among them. While the use of online sources can be beneficial for educational purposes, it also poses potential threats to students and educators alike [18]. Therefore, it is important for individuals to have a clear understanding of what information they should access and how to access it safely.

A research study conducted by Knapp *et al.* [19] there exists a correlation between the implementation of preventative measures and information security, which leads to an enhancement in individual security performance. In addition, Kruger *et al.* [20] suggested that the behavior and knowledge of an individual have a substantial relationship in terms of cybersecurity threat mitigation, indicating that individuals must possess adequate knowledge and good behavior for achieving cybersecurity. It is essential to include security policies in the development of a cybersecurity program to guarantee that organizations attain their intended outcome [21]. In order to address the increasing cybersecurity threats, researchers have developed various programs. A research study carried out by Kim [22] aimed to determine the perspective of students from the business department at New England regarding their awareness of information security. The results of the survey indicated the need for an effective awareness training program to increase the knowledge of cybersecurity among students.

A research study conducted by Aloul [23] investigated the level of security awareness among academic individuals in the Arab region. The survey included both students and professionals, but the methodology and effectiveness of the program were not well explained. Nonetheless, the study highlighted the importance of continuous cybersecurity awareness programs. Universities are frequently targeted by cybercriminals, making it crucial to include cybersecurity programs in organizational security management plans. To improve cybersecurity levels, a researcher has developed simulation tools for students, staff, and other personnel [24].

Cone *et al.* [25], simulation tools such as the CyberCIEGE game have a positive effect on increasing cybersecurity awareness levels among students. This study found that game-based learning tools designed for this purpose can be effective in improving students' knowledge of cybersecurity. The research suggested that such tools can be used to enhance the cybersecurity training of students who are addicted to online games. Similarly, another researcher designed simulation tools to provide or enhance the cybersecurity level of students, staff, and other personnel, and the results showed a significant impact on increasing cybersecurity awareness levels [23]. Therefore, it is crucial to incorporate such tools in the cybersecurity training programs of educational institutions to improve cybersecurity knowledge and reduce cyber threats.

A survey conducted at California State University by [26] found that the main challenge related to cybersecurity is not the absence of basic knowledge, but rather the way students utilize that knowledge in practical situations. The research also discovered that students' adherence to information security regulations is lower than their comprehension of them. Similarly, in another survey conducted in Tamil Nadu, India, 500 students were questioned to assess their knowledge about various security threats. The survey showed that 70% of the participants were aware of basic virus attacks and used antivirus software, while 11% used outdated antivirus software. Additionally, Yang *et al.* [27] more than 97% used free antivirus software available online, indicating that students often use unoriginal software that can lead to malware intrusions on their system.

A study was carried out in Malaysia by [28] to investigate how aware students were of the risks related to social networking sites. In the research study, 295 students were surveyed to investigate their awareness of risks associated with social networking sites. The results indicated that one-third of the participants had experienced scams on social networking sites. This indicated a lack of awareness among students regarding the risks of cyber threats. Likewise, in the US, a survey was conducted among college students in Pacific Northwest to determine their level of cybersecurity awareness. The results showed that students were not able to define terms such as malware, trojan horse, phishing, and worms [29]. On the other hand, a cybersecurity research study was conducted in Bangladesh by [30], and the survey results showed that there was an inconsistency in the level of cybersecurity awareness, with the overall result being at a satisfactory level.

A study was conducted in New Zealand to determine the level of cybersecurity awareness among students of different ages regarding their use of the internet. The findings revealed that students were not familiar with cybersecurity terminologies such as phishing, indicating a lack of cybersecurity knowledge. Tirumala *et al.* [31] University students were found to be more vulnerable to cyber-attacks due to their lack of security concerns when using the internet, as well as their lack of knowledge on security threats and mitigation methods [32].

As described earlier, some researchers have been concentrating on creating cybersecurity awareness programs to enhance people's knowledge of cybersecurity, while others have been examining the effectiveness of existing cybersecurity programs [33]–[37]. In today's world, it has become essential for everyone to learn the fundamental techniques for safeguarding their personal information.

There are various forms of cyber-attacks that can harm both individuals and organizations, such as passive and active attacks, targeted attacks, clickjacking, brandjacking, botnet, phishing, spamming, and internal or external attacks. Given the range of threats and the possible negative outcomes of successful cyber-attacks, it is crucial for individuals and organizations to stay alert and take preventive measures to safeguard themselves against cyber threats [13]. The arrangements of digital security assaults appear in Figure 1.

Other previous literature reviewed shows that awareness of cyber security was conducted by different authors and researchers who were discussed differently. There were different ideas among researchers about the awareness of cyber security among graduate and undergraduate students, and some of the previous studies are as:

- Active attack: an attempt to modify or affect system resources by changing the data flow or creating false statements. Such attacks involve altering the normal operations of a system or the data it processes. Attackers may manipulate the data stream or create false statements with the goal of compromising system resources or stealing sensitive information.
- Passive attack: is aimed at acquiring or utilizing information from the system without affecting system resources. Such attacks are in the form of eavesdropping or monitoring of transmission. The attacker's goal is to obtain information being transmitted.

Amrin *et al*. [38], was conducted on the impact of cyber security the university of twenty students mostly claims the problems of the security side of phishing. Valli *et al.* [39] the author collected the small to medium enterprise for their cyber security awareness is very low because of many issues. An empirical study on cyber security perceptions, awareness, and practices, individuals and organizations often lack sufficient knowledge on the importance of cyber security, and their organizational strategy may not include measures for addressing cyber security issues. Zhang and Prichard [40] The study found that the level of cyber security awareness and perception among individuals was lower than expected. Previous studies have primarily focused on the impact of social network misuse, phishing, and password strength on cyber security awareness. In addition, this study contributes to the body of knowledge by discovering how a virus attack affects the awareness of cyber security and how Universities can be improved their students in order to avoid the effect of a virus attack by using cyber security.

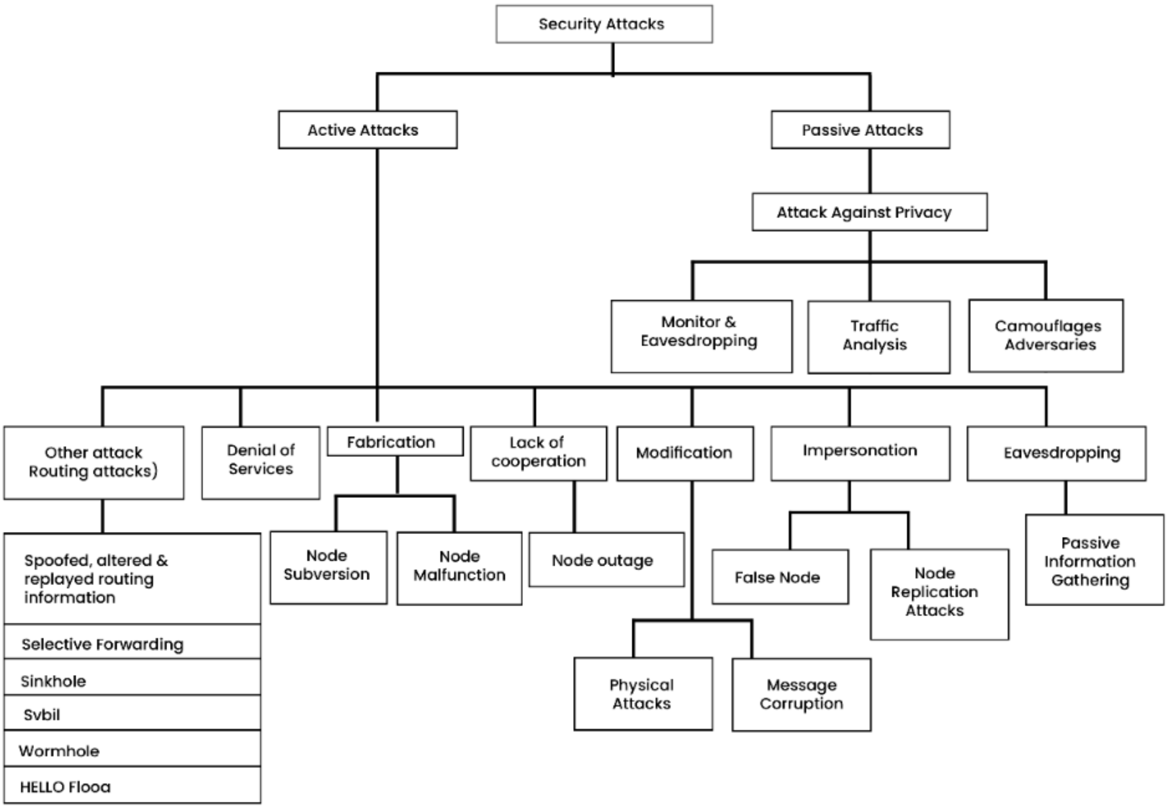

Figure 1. Padmavathi and Shanmugapriya [12] developed classifications of cyber security attacks

2. METHOD

2.1. Statistical method

The use of the analysis of variance (ANOVA) goes back to the British statistician Ronald Aylmer Fisher (1955). This methodology has become a key instrument in most science and engineering research. This research aims to use one-way ANOVA, which is a type of statistical analysis, to investigate if there is a significant difference in the level of Cyber Security Awareness between undergraduate and graduate students.

2.2. Data collection method

The research employed a survey methodology that utilized a questionnaire as a data collection instrument. The online questionnaire method was utilized to distribute a set of pre-prepared questions to a large number of university students who were selected through a purposive sampling technique. The purpose of the study was to obtain data from a representative sample of the target population.

2.3. Target population and sample

In a survey, the population refers to the complete set of entities under examination, while the sample is a smaller subset of the population that is actually studied. For our survey, we aimed to target all universities in Mogadishu as the population, and we selected a sample size of 250 students from five major universities (namely SIMAD University, Somali International University, University of Somalia, Jamhuriya University of Science and Technology, and Mogadishu University) by randomly selecting 50 students from each university.

3. RESULTS AND DISCUSSION

3.1. Demographics profile of respondents

The Table 1 provides a snapshot of the demographics of the study's respondents, including their gender, age distribution, level of education, marital status, and the universities they are affiliated with. The data shows a gender distribution with a majority of male respondents. Respondents' ages span various categories, with a notable representation in the 20-25 years range. They possess diverse educational backgrounds, including bachelor's, master's, and other forms of education. Marital status is divided into single and married, while participants come from a variety of universities, with SIMAD and Jamhuriya being the most prominently represented institutions. This demographic information provides a foundation for understanding the characteristics of the study's participants, which will be further examined in subsequent sections.

Table 1. Demographics profile of respondents

Gender	Frequency	Percent
Male	160	64.0
Female	90	36.0
Total	250	100.0
Age		
Below 20 years	40	16
20-25 years	155	62
26-30 years	40	16
Above 30 years	15	6
Total	250	100.0
Level of education		
Bachelor	110	44
Master	105	42
Other	35	14
Total	250	100.0
Marital status		
Single	205	82
Married	45	18
Total	250	100
Selected Universities		
SIMAD	50	20 20
Jamhuriya	50	20
Mogadishu	50	20
UNISO	50	20
SIU	50	100
Total	250	

Table 1 presents a breakdown of the demographic characteristics of the respondents who participated in the study, including gender, educational level, marital status, age, and university affiliation. The survey was conducted among a sample of 250 undergraduate and graduate students randomly selected from five major universities in Mogadishu: SIMAD University, Somali International University, University of Somalia, Jamhuriya Univerity of Science and Technology, and Mogadishu University in Mogadishu. In terms of the respondents' gender, the majority (64%) were male students, while the rest (36%) were female. Among the respondents' level of study, a little more than one-third (44%) were bachelor students, followed by those pursuing a master's degree (42%), while the rest (14%) fell under other categories. The majority of the respondents were single (82%), while less than a third (18%) were married. Regarding the age of the respondents, the majority (62%) were aged between 20 to 25 years old, while a small percentage (6%) were above 30 years old. In terms of the universities categories, the majority of the respondents were from Jamhuriya University of Science and Technology (20%), followed by SIMAD University (20%), Mogadishu University (20%), University of Somalia (20%), and Somali International University (20%).

3.2. Which type of attack do you meet mostly?

The Table 2 offers a snapshot of the types of cyberattacks experienced by the respondents in the study. The main finding reveals that virus attacks are the most prevalent among the reported incidents, followed by phishing attempts. Password strength issues and the misuse of social networks are also reported, but the table does not delve into the percentages. This data provides a broad overview of the cybersecurity challenges faced by the surveyed individuals, with a particular emphasis on virus and phishing attacks.

Table 2. Which type of attack do you meet mostly?

Type of attack	Frequency	Percent
Virus attack	140	56.0
Phishing	35	14.0
Password strength	45	18.0
Misuse of social network	30	12.0
Total	250	100.0

Table 2 presents the results of the respondents’ beliefs on the most common types of cyber-attacks they encounter. The majority of the respondents, accounting for 56%, believed that virus attacks were the most common type of attack. Password strength was the next most commonly believed type of attack, with 18% of respondents, followed by phishing at 14%. Only a minority of respondents, 12%, believed that the most common type of attack was a misuse of the social network.

3.3. Cross tabulation (Universities * which type of attack do you meet mostly?)

The below Table 3 presents a cross-tabulation between different universities and the types of cyberattacks encountered most frequently by respondents in the study. Notably, SIMAD University and Mogadishu University reported virus attacks as the most common threat, while Jamhuriya University reported encountering password strength issues most frequently. Meanwhile, the University of Somalia and Somali International University indicated a higher incidence of misuse of social network-related attacks. This cross-tabulation offers a snapshot of how different universities’ communities experience and prioritize various cybersecurity challenges, which can be valuable for tailoring university-specific cybersecurity strategies and awareness programs.

Table 3. Cross tabulation (Universities * which type of attack do you meet mostly?)

Universities	Virus attack	Phishing	Pass strength	Misuse of social network	Total
SIMAD University	45	2	1	2	50
Jamhuriya University	50	0	0	0	50
Mogadishu University	40	10	0	0	50
University of Somalia	5	20	25	0	50
Somali International University	0	0	20	30	50
Total	140	32	46	32	250

Table 3 shows the results of a cross-tabulation of universities and the type of attack that the participants reported encountering mostly. The table presents the number of participants from each university who reported encountering each type of attack (virus attack, phishing, password strength, and misuse of social network). The results of the table suggest that there are differences in the types of attacks that participants from different universities reported encountering mostly. For instance, the participants from SIMAD University and Jamhuriya University reported encountering a higher number of virus attacks compared to participants from the other universities. On the other hand, participants from Mogadishu University and the University of Somalia reported encountering a higher number of misuse of social network attacks.

This information could be useful for universities to understand the types of cyber-attacks that their students are facing and develop strategies to prevent these attacks. For instance, universities with a higher number of virus attacks could focus on improving their antivirus and malware detection systems. Universities with a higher number of misuse of social network attacks could provide awareness training to their students on how to use social media safely and avoid phishing attacks. Overall, the table provides valuable information for universities to understand the cyber threats that their students are facing and take appropriate measures to protect them from these attacks.

3.4. ANOVA table of comparison of five universities

The Table 4 presents the ANOVA results for a comparison among five universities. The key statistics include the F-statistic and associated p-value, which help determine if there are significant differences between the universities in terms of the variable being studied. In this case, the F-statistic is approximately 2.27, and the p-value is approximately 0.12, providing important information for evaluating the differences among the groups. In Table 4 shows the results of an ANOVA for a dataset with 5 groups and 250 respondents. The ANOVA is used to test whether the means of the groups are equal or not, by comparing the variance between groups to the variance within groups.

The ANOVA table also shows the sum of squares (SS) and degrees of freedom (df) for each source of variation. The mean square (MS) is calculated by dividing the SS by the corresponding degrees of freedom. In the given table, the p-value for between groups is 0.120036, which is higher than the significance level of 0.05, indicating that there is no enough evidence to reject the null hypothesis of equal means. Therefore, we can conclude that there is no significant difference between the means of the five groups in this dataset.

In Table 4, the sum of squares between groups is 1627.8, the degrees of freedom between groups is 3, and the mean square between groups is 542.6. The sum of squares within groups is 3831.2, the degrees of freedom within groups is 16, and the mean square within groups is 239.45. The F statistic for the overall test is 2.266, with a corresponding p-value of 0.120.

However, it is worth noting that the choice of the threshold for statistical significance is somewhat arbitrary, and in some cases, a more or less stringent threshold may be appropriate depending on the context and the specific research question being investigated. Additionally, other factors, such as effect size and sample size, should also be considered when interpreting the results of a statistical analysis.

Table 4. ANOVA table of comparison of five universities

	Sum of squares	df	Mean square	F	P.value
Between groups	1627.8	3	542.6	2.266026	0.120036
Within groups	3831.2	16	239.45		
Total	5,459	19			

4. CONCLUSION

The primary aim of the present scientific investigation was to evaluate the extent to which university students in Mogadishu possess cyber security awareness while emphasizing various internet-based security threats. This study employed-way ANOVA to test whether there is a difference among awareness of cyber security among graduate and undergraduate students or not of five well-known universities (i.e., SIMAD, SIU, UNISA, Jamhuriya, and Mogadishu). The study also adopted the questionnaire method as data collection technique and collects 250 graduate and undergraduate students from five well-known universities (i.e., SIMAD, SIU, UNISO, Jamhuriya, and Mogadishu). This study found, the result shows that the cross-tabulation (universities * which type of attack you meet mostly), in which the SIMAD and Jamhuriya students suffers virus attack. At the same time, they have no problem phishing, password strength, and password strength furthermore, in SIMAD every ten students 9 of them suffer virus attack, while in Jamhuriya, 11 students, 11 of them suffer virus attacks. In regard to SIU students, both password strength and misuse of the social network whereas they are free from others. In contrast, the Mogadishu students suffer both virus attacks and phishing while free from others. Finally, the UNISO virus attack and password strength while free from others, the result of the ANOVA Table of comparison of five universities indicates a statistically significant difference in cyber security of the five universities since the P.value is less than 5%. F (245, 4) =11.185, p.value =0.0000. This result confirmed the result of the cross-tabulation. So, we reject the null hypothesis that there is no difference between the cyber security of the five universities and conclude that there is a statistically significant difference in cyber security.

REFERENCES

[1] A. Abdullahi, S. Manickam, S. Karuppayah, and M. A. Al-Shareeda, “Proposed enhanced link failure rerouting mechanism for software-defined exchange point,” *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 31, no. 1, pp. 259–270, Jul. 2023, doi: 10.11591/ijeecs.v31.i1.pp259-270.

[2] F. Khalid, “Understanding university students‘ use of Facebook for collaborative learning,” *International Journal of Information and Education Technology*, vol. 7, no. 8, pp. 595–600, 2017, doi: 10.18178/ijiet.2017.7.8.938.

[3] F. Khalid, Y. Daud, and M. N. M. Nasir, “"Cross-cultural education for sustainable regional development & quot; Bandung the relationship between talent management and self-efficacy from the perspective of secondary school administrators and teachers,” *International Conference on Education and Regional Development*, vol. 2016, no. November, 2016.

[4] A. A. Karim, P. M. Shah, F. Khalid, M. Ahmad, and R. Din, “The role of personal learning orientations and goals in students’ application of information skills in Malaysia,” *Creative Education*, vol. 06, no. 18, pp. 2002–2012, 2015, doi: 10.4236/ce.2015.618205.

[5] F. Annansingh and T. Veli, “An investigation into risks awareness and e-safety needs of children on the internet: a study of Devon, UK,” *Interactive Technology and Smart Education*, vol. 13, no. 2, pp. 147–165, Jun. 2016, doi: 10.1108/ITSE-09-2015-0029.

[6] L. Muniandy and B. Muniandy, “State of cyber security and the factors governing its protection in Malaysia,” *International Journal of Applied Science and Technology*, vol. 2, no. 4, pp. 106–112, 2012.

[7] G. Anderson, D. Ktoridou, N. Eteokleous, and A. Zahariadou, "Exploring parents' and children's awareness on internet threats in relation to internet safety," *Campus-Wide Information Systems*, vol. 29, no. 3, pp. 133–143, 2012, doi: 10.1108/10650741211243157.

[8] L. Mosalanejad, A. Dehghani, and K. Abdolahifard, "The students' experiences of ethics in online systems: a phenomenological study," *Turkish Online Journal of Distance Education*, vol. 15, no. 4, pp. 205–216, Dec. 2014, doi: 10.17718/tojde.02251.

[9] V. Ratten, "A cross-cultural comparison of online behavioural advertising knowledge, online privacy concerns and social networking using the technology acceptance model and social cognitive theory," *Journal of Science and Technology Policy Management*, vol. 6, no. 1, pp. 25–36, Mar. 2015, doi: 10.1108/JSTPM-06-2014-0029.

[10] A. A. Gabra, M. B. Sirat, S. Hajar, and I. B. Dauda, "Cyber security awareness among university students: a case study," *Journal of Critical Reviews*, vol. 7, no. 16, pp. 825–833, 2020, doi: 10.31838/jcr.07.16.108.

[11] H. Aldawood and G. Skinner, "Educating and raising awareness on cyber security social engineering: a literature review," *Proceedings of 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering, TALE 2018*, pp. 62–68, 2019, doi: 10.1109/TALE.2018.8615162.

[12] D. G. Padmavathi and M. D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," *arXiv preprints*, 2009, [Online]. Available: http://arxiv.org/abs/0909.0576.

[13] A. Moallem, "Cyber security awareness among college students," *Advances in Intelligent Systems and Computing*, vol. 782, pp. 79–87, 2019, doi: 10.1007/978-3-319-94782-2_8.

[14] Adeyemi, "Nigeria: financial losses to cybercrimes," allAfrica, 2019, [Online]. Available: https://allafrica.com/stories/201806070110.html.

[15] M. Y. Daud and F. Khalid, "Nurturing the 21st century skills among undergraduate students through the application and development of weblog," *International Education Studies*, vol. 7, no. 13, pp. 123–129, 2014, doi: 10.5539/ies.v7n13p123.

[16] A. Moallem, *Cybersecurity awareness among students and faculty*. Boca Raton, FL : CRC Press/Taylor & Francis Group, 2019.: CRC Press, 2019.

[17] B. W. Reyns, B. Henson, and B. S. Fisher, "Stalking in the twilight zone: extent of cyberstalking victimization and offending among college students," *Deviant Behavior*, vol. 33, no. 1, pp. 1–25, Jan. 2012, doi: 10.1080/01639625.2010.538364.

[18] S. Al-Janabi and I. Al-Shourbaji, "A study of cyber security awareness in educational environment in the middle east," *Journal of Information and Knowledge Management*, vol. 15, no. 1, p. 1650007, Mar. 2016, doi: 10.1142/S0219649216500076.

[19] K. J. Knapp, T. E. Marshall, R. K. Rainer, and F. N. Ford, "Information security: management's effect on culture and policy," *Information Management and Computer Security*, vol. 14, no. 1, pp. 24–36, Jan. 2006, doi: 10.1108/09685220610648355.

[20] H. Kruger, L. Drevin, and T. Steyn, "A vocabulary test to assess information security awareness," *Information Management & Computer Security*, vol. 18, no. 5, pp. 316–327, Nov. 2010, doi: 10.1108/09685221011095236.

[21] E. A. Mcdaniel, "Securing the information and communications technology global supply chain from exploitation: developing a strategy for education, training, and awareness," *Issues in Informing Science and Information Technology*, vol. 10, no. 2012, pp. 313–324, 2013.

[22] E. B. Kim, "Recommendations for information security awareness training for college students," *Information Management and Computer Security*, vol. 22, no. 1, pp. 115–126, 2014, doi: 10.1108/IMCS-01-2013-0005.

[23] F. Aloul, "The need for effective information security awareness," *International Journal of Intelligent Computing Research*, vol. 2, no. 1, pp. 116–123, Mar. 2011, doi: 10.20533/ijicr.2042.4655.2011.0014.

[24] V. Pastor, G. Diaz, and M. Castro, "State-of-the-art simulation systems for information security education, training and awareness," in *IEEE EDUCON 2010 Conference*, Apr. 2010, pp. 1907–1916, doi: 10.1109/EDUCON.2010.5492435.

[25] B. D. Cone, C. E. Irvine, M. F. Thompson, and T. D. Nguyen, "A video game for cyber security training and awareness," *Computers and Security*, vol. 26, no. 1, pp. 63–72, Feb. 2007, doi: 10.1016/j.cose.2006.10.005.

[26] L. Slusky and P. Partow-Navid, "Students information security practices and awareness," *Journal of Information Privacy and Security*, vol. 8, no. 4, pp. 3–26, Oct. 2012, doi: 10.1080/15536548.2012.10845664.

[27] Y. Yang, L. Zhou, Z. Peng, N. Spread, S. Deng, and H. Huang, "A survey on cyber security awareness among college students in Tamil Nadu a Survey on cyber security awareness among college students in Tamil Nadu," in *IOP Conference Series Materials Science and Engineering*, 2017, p. 263.

[28] G. H. Kirwan, C. Fullwood, and B. Rooney, "Risk factors for social networking site scam victimization among Malaysian students," *Cyberpsychology, Behavior, and Social Networking*, vol. 21, no. 2, pp. 123–128, Feb. 2018, doi: 10.1089/cyber.2016.0714.

[29] D. Sarathchandra, K. Haltinner, and N. Lichtenberg, "College students' cybersecurity risk perceptions, awareness, and practices," in *2016 Cybersecurity Symposium (CYBERSEC)*, Apr. 2016, pp. 68–73, doi: 10.1109/CYBERSEC.2016.018.

[30] N. Ahmed, U. Kulsum, I. Bin Azad, A. S. Z. Momtaz, M. E. Haque, and M. S. Rahman, "Cybersecurity awareness survey: an analysis from Bangladesh perspective," in *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*, Dec. 2017, vol. 2018-Janua, pp. 788–791, doi: 10.1109/R10-HTC.2017.8289074.

[31] S. S. Tirumala, A. Sarrafzadeh, and P. Pang, "A survey on internet usage and cybersecurity awareness in students," in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, Dec. 2016, pp. 223–228, doi: 10.1109/PST.2016.7906931.

[32] D. Pramod and R. Raman, "A study on the user perception and awareness of smartphone security," *International Journal of Applied Engineering Research*, vol. 9, no. 23, pp. 19133–19144, 2014.

[33] H. Chan and S. Mubarak, "Significance of Information security awareness in the higher education sector," *International Journal of Computer Applications*, vol. 60, no. 10, pp. 23–31, Dec. 2012, doi: 10.5120/9729-4202.

[34] N. Hayani, A.Rahim, S. H. M. L. M. Kiah, S. Shamshirband, and S. Furnell, "A systematic review of approaches to assessing cybersecurity awareness," *Kybernetes*, vol. 44, no. 4, pp. 606–622, 2015, [Online]. Available: http://dx.doi.org/10.1108/K-12-2014-0283%5Cnhttp://dx.doi.org/10.1108/K-12-2014-0283.

[35] K. Rantos, K. Fysarakis, and C. Manifavas, "How effective is your security awareness program? An evaluation methodology," *Information Security Journal*, vol. 21, no. 6, pp. 328–345, 2012, doi: 10.1080/19393555.2012.747234.

[36] A. Tsohou, S. Kokolakis, M. Karyda, and E. Kiountouzis, "Investigating information security awareness: research and practice gaps," *Information Security Journal: A Global Perspective*, vol. 17, no. 5–6, pp. 207–227, Dec. 2008, doi: 10.1080/19393550802492487.

[37] R. Willison and M. Warkentin, "Beyond deterrence: an expanded view of employee computer abuse," *MIS Quarterly: Management Information Systems*, vol. 37, no. 1, pp. 1–20, 2013, doi: 10.25300/MISQ/2013/37.1.01.

[38] N. Amrin, P. Hartel, M. Junger, and A. Leijtens, "The impact of cyber security on SMEs," *University of Twente*, pp. 1–77, 2014, [Online]. Available: http://eprints.eemcs.utwente.nl/24978/.

[39] M. Valli *et al.*, "Osteogenesis imprefecta and type-I collagen mutations: a lethal variant caused by a Gly910→Ala substitution in the α1(I) chain," *European Journal of Biochemistry*, vol. 211, no. 3, pp. 415–419, 1993, doi: 10.1111/j.1432-1033.1993.tb17565.x.

[40] C. Zhang and J. J. Prichard, "An empirical study of cyber security perceptions, awareness and practice," *Issues In Information Systems*, 2009, doi: 10.48009/2_iis_2009_242-248.

BIOGRAPHIES OF AUTHORS

Adnan Abdukadir Ahmed holds a B.Sc. degree in Information Technology from SIMAD University in Somalia. He is currently pursuing a Master of Data Science at the same university, where he is also employed as a Lecturer with the Faculty of Computing. He is known for his engaging teaching style and ability to inspire students to excel in their academic pursuits. In addition to his academic role, he serves as the Multimedia and Design Administrator at SIMAD University. Apart from his academic and administrative responsibilities, Adnan is an avid researcher with a keen interest in exploring the latest advancements in data science, artificial intelligence, cybersecurity, and emerging technologies. He constantly seeks opportunities to contribute to the field through publications and presentations at relevant conferences and workshops. Adnan's dedication to staying updated with the latest industry trends and his commitment to lifelong learning make him a valuable asset to the academic community. He can be contacted at email: maazin284@simad.edu.so.

Abdikadir Hussein Elmi is a highly skilled IT and Computer Science professional with a wealth of experience in various data-related roles. Over the past several years, he has successfully transitioned towards Data Science and Machine Learning, honing his expertise in these cutting-edge fields. Abdikadir holds a Master of Science in Data Science and Analytics from the prestigious University Science Malaysia (USM), where he gained a strong foundation in advanced data analytics and machine learning techniques. Currently, Abdikadir serves as a Lecturer at Mogadishu University, where he passionately shares his knowledge and expertise with aspiring data scientists. Known for his dynamic and engaging teaching style, Abdikadir inspires his students to excel in their academic pursuits and prepares them for the challenges of the data-driven world. Abdikadir’s research interests revolve around machine learning, artificial intelligence, natural language processing, and neural networks. He is constantly exploring new methodologies and techniques in these areas to develop innovative solutions that can have a real-world impact. He is known for his strong work ethic, analytical mindset, and keen attention to detail, which enable him to excel in complex data-driven projects. For any inquiries, collaborations, or opportunities related to data science, machine learning, or artificial intelligence. He can be contacted at email: xayeeysi77@gmail.com.

Abdijalil Abdullahi received a B.Sc. degree in information technology and an M.Sc. degree in networking and data communication from SIMAD University, Mogadishu, Somalia, in 2014 and 2018, respectively, where he is currently pursuing the PhD degree with the National Advanced IPv6 Center (NAv6), Universiti Sains Malaysia (USM). His research interests include software-defined networking, inter-domain routing, and the Internet ecosystem. He can be contacted at email: cabdijaliil22@gmail.com.

Abdullahi Yahye Ahmed earned a degree in Telecommunication Engineering from SIMAD University in 2022. Presently, he serves as an independent junior researcher and collaborator on academic university-level research projects. His research pursuits encompass a range of interests, including antennas, microwaves, IoTs, and renewable energy. He can be contacted at email: cabdullaahish.yaxye@gmail.com.