المجلة العلمية لكلية التربية – المجلد الرابع– العدد الاول – يناير 2025

Volume 4 Issue1 – January 2025 – Faculty of Education journal

الموقع الالكتروني للمجلة: http://journal.su.edu.ly/index.php/edujournalj/index

DOI: https://doi.org/ 10.37375/foej.v4i1.3152

Cybersecurity Awareness among College Students in Libyan Universities

Rabia Masoud[1], Maher Alghali[2], Taher Brideh[3], Alsanossi Ahmed[4]

[1] Electrical and Electronic Eng. Dept., Engg, Faculty, Wadi Alshatti University, Brack, Libya

r.masoud@wau.edu.ly

[2] Network Dept, Information Technology Faculty, Sebha University, Sebha, Libya

ma.alghali@sebhau.edu.ly

[3]Department of management, Faculty of Economics and Accounting Sciences Fezzan University, Libya

Taher1010@gmail.com

[4]Computer Science Dept., Faculty of Sciences Wadi Alshatti University, Brack, Libya

als.ahmed@wau.edu.ly

الملخص

ينصب التركيز في الآونة الأخيرة على الأمن السيبراني الذي يشكل مصدراً متزايداً للقلق في جميع أنحاء العالم نتيجة للتطور في الثورة الرقمية التي حولت الإنترنت إلى أرض خصبة لمجرمي الإنترنت. حيث يؤكد العدد المتزايد من الجرائم الإلكترونية على أهمية رفع مستوى الوعي وتوفير التعليم حول الأمن السيبراني للأفراد والشركات. تستكشف هذه الدراسة تأثير المعرفة بالأمن السيبراني، أمان كلمة المرور والإدراك الذاتي للمهارة على الوعي بالأمن السيبراني بين الطلبة في الجامعات الليبية. تم تجميع عينة من 480 طالبًا جامعيًا من أربع جامعات ليبية عامة. تم إجراء التحليل الكمي للبيانات باستخدام Smart PLS-SEM 3.3.9، اظهرت النتائج وجود ارتباط إيجابي بين المعرفة بالأمن السيبراني، أمان كلمة المرور والإدراك الذاتي للمهارة والوعي بالأمن السيبراني. يوصي هذا البحث أنه يجب زيادة التركيز على تثقيف عامة الناس، وخاصة فئة الطلبة حول الأمن السيبراني وممارسات الإنترنت الأخلاقية. علاوة على ذلك، فإن التركيز الأساسي لهذا البحث هو تسليط الضوء على أهمية الزيادة في تعليم الأمن السيبراني لفئة الطلبة.

الكلمات المفتاحية: الوعي بالأمن السيبراني، الجامعات الليبية، الجرائم الالكترونية، امن المعلومات.

Abstract

Cybersecurity threat continues to be a growing concern worldwide in recent times. This could be related to the digital revolution that has turned the internet into a breeding ground for cybercriminals. The growing number of cybercrimes emphasizes the importance of raising awareness and providing education on cybersecurity for individuals and businesses. This study explores the influence of password security, cybersecurity knowledge, and self- perception of skill on awareness of cybersecurity among university students in Libya. Questionnaire collected from 480 college students. Smart PLS-SEM 3.3.9 used to analyze the data collected. The findings indicated a positive and significant association of password security, cybersecurity knowledge, and self-perception of skill on awareness of cybersecurity. This research suggests that there should be increased focus on educating the general public, particularly students, about ethical internet practices and cybersecurity. Moreover, the primary focus of the research highlighted the importance of increasing cybersecurity education for the students.

Keywords: Cybersecurity Awareness, Libyan university, Cybercrime, information security.

1. Introduction

Due to the fast evolution of information technology and the wide use of network systems, people have become more reliant on the Internet. It has become an integral part of daily life, impacting education, public services, payments, social interactions, and entertainment. By January 2024, Libya had over 6.93 million Internet users, representing 88.4% of the total population at the beginning of the year (usaid, 2024). Even though the Internet has greatly increased convenience and transformed lifestyles, it also has the potential to bring negative consequences if not used properly (Annansingh, Veli, & education, 2016). The risks to individuals and organizations from the instability and insecurity in cyberspace are considerable (Li et al., 2020).

As technology becomes more widespread and the internet infiltrates all aspects of daily life, cybersecurity is becoming increasingly important for individuals and governments (Zwilling et al., 2022). Despite these advancements improving convenience, the rise in cyberattacks has necessitated taking precautions in this field (Kaloudi & Li, 2020). Furthermore, it is essential to note that the forms of cyberattacks, meaning the harmful exploitation of online networks,

have evolved over the past two decades. The literature now includes new "cyber" concepts and risks due to this development (Pogrebna & Skilton, 2019).

Cybersecurity breaches are now a significant hindrance to numerous companies and individuals, given that a majority of tasks are now conducted online with less physical contact. Therefore, the internet's presence has greatly altered how individuals acquire knowledge, obtain information, and build understanding (Khalid, 2017). This innovative approach has introduced a new way for individuals to communicate and participate in social activities, it has negative consequences when misused by users (Karim, Shah, Khalid, Ahmad, & Din, 2015). The internet has brought about numerous cyber-related dangers, such as cyber addiction, personal information exposure, and online fraud addiction. (Annansingh et al., 2016; Ktoridou, Eteokleous, & Zahariadou, 2012; Muniandy & Muniandy, 2012; Ratten, 2015).

The Internet and digital media have unquestionably altered how individuals acquire knowledge, access information, and build understanding (Khalid, 2017). Digital media has introduced a fresh perspective for communicating and engaging with our communities and societies. Despite being hailed as the most groundbreaking invention in the world, the Internet also has a harmful aspect that can have adverse impacts on its users, both adults and children (Karim et al., 2015). Cybersecurity involves safeguarding devices, networks, data, and electronic systems from cyberattacks that may result in unauthorized access, disruption, alteration, or exploitation, affecting various targets such as businesses and personal devices.

Network protection and application security focus on safeguarding computer networks and ensuring that hardware and software are devoid of vulnerabilities and threats (Ihmouda, Alwi, & Abdullah, 2015). Disaster recovery involves how an organization reacts to data loss and works to restore operations to keep the organization running smoothly (kaspersky, 2024). People, families, organizations, governments, schools, and companies are currently focused on internet security. (Kritzinger & von Solms, 2010) indicated that it is essential for families and parents to focus on cyber security to safeguard children and family members from online scams. Regarding financial security, safeguarding sensitive financial information that could impact an individual's financial situation is essential. Therefore, it is crucial for Internet users to know how to safeguard themselves from online fraud and identity theft. (L. Kim, 2018) determined that despite advancements in technology for protecting end-user information systems, security professionals argue that technology alone is insufficient for adequately securing these systems. Learning about online behavior and system security reduces vulnerabilities, creating a safer Internet environment. Small and medium-sized businesses

encounter multiple security challenges due to a lack of cyber security expertise and limited resources (Junior, Becker, & Johnson, 2023).

Now-a-days, protecting the reliability and privacy of data within intricate networks is a crucial and demanding task (Ihmouda & Alwi, 2014). The majority of individuals linked to these networks are students. Students may engage in cyber-crimes primarily due to curiosity and a desire for revenge. Although social networks and bank account information face increased risks, educational institutions also face the threat of losing important intellectual property and research data, including patents held by professors and students, as well as personal information of students, staff, and faculty. Due to the rise in hacking attacks targeting higher education institutions, the demand for cyber awareness has grown (Alharbi & Tassaddiq, 2021; Corallo, Lazoi, Lezzi, & Luperto, 2022).

According to (Aurigemma & Panko, 2012) the effectiveness of reducing information security risks with software and hardware security mechanisms depends on users consistently adhering to a secure policy. These researches confirm that having a strong security awareness program is crucial in enhancing cybersecurity. With society's growing reliance on technology, there is a strong need for developing safe cyber behavior practices. Implementing a security awareness program is a challenging task. (Manke & Winkler, 2013) stated that the most effective way to achieve security awareness success is by incorporating creativity in distributing materials and providing participatory experiences. According to the Security Awareness Report from (SANS, 2017) the security community should shift focus from blaming employees for security lapses to holding themselves accountable. It is our responsibility to identify the underlying reasons for not modifying human behavior and to tackle those problems. It is our belief that addressing the core issue and modifying human behavior can be achieved through fostering awareness from a young age as part of education and cultural upbringing. Ultimately, the younger generation represents the upcoming labor force, educators, and caregivers. Their security behaviors will have wide-ranging influence on both community and the work environment.

The Internet is now utilized in every aspect of people's daily lives. People engage with friends and family, conduct business and banking activities online, and utilize various services such as Virtual healthcare and education, video calls, etc. As a result, the reliance on technology for connections has grown. Nevertheless, remaining consistently linked leads to heightened vulnerabilities. Everyone is experiencing cyber threats targeting vital infrastructure and economy. As individuals, the risks of cyber security can result in threats to finances, identity,

and privacy, there is a need in higher education institutions to improve college students' understanding of cybersecurity. Presently, computers and the Internet are essential tools in daily professional and academic activities (Senthilkumar & Easwaramoorthy, 2017). This survey aims to examine the awareness of Cyber Security for students in Libya and explain them the risks they will faced in the digital world.

2. Literature Review

Efforts to enhance people's understanding the risks of cyber security and educate the people about these risks must be carefully crafted to provide individuals with a basic understanding of the subject (Al Shamsi, 2019). (Al-Janabi & Al-Shourbaji, 2016) conducted research focusing on security awareness in educational environments, specifically examining cyber security knowledge for a students, researchers, and staff. The researchers found that the participants lack a basic understanding of cyber security. (Ahmed et al., 2019) examined the awareness regarding cyber security for Bangladesh's people and utilized Pearson's chi-squared test for data analysis. These findings indicate that most individuals lack awareness of the risks related to cybercrime.

Cyber security is an expanding and significant area that encompasses a variety of research studies (Suryotrisongko & Musashi, 2019). One of the areas of focus in cyber security research is enhancing awareness of cyber security, specifically targeting the key factors crucial for achieving this goal. This part briefly discusses important research on awareness in cyber security, specifically focusing on the education field. In their study, (Kruger, Drevin, & Steyn, 2010) conducted a preliminary investigation to determine the feasibility of utilizing tests of security vocabulary to gauge levels of awareness in order to pinpoint appropriate subjects for security awareness initiatives. The vocabulary test was deemed a valuable tool for assessing awareness levels, and a strong correlation between understanding of concepts behavior and vocabulary was demonstrated. (Jeske & Van Schaik, 2017) performed a study on students' knowledge of various online risks. The subjects were given descriptions of dangers and were instructed to indicate their level of familiarity with each one, the study indicated that the more time someone spent on the Internet and the longer they had been using it, the more likely they were to be familiar with Internet threats, which in turn influenced their use of computer security measures.

(Sezer, Yilmaz, & Karaoglan Yilmaz, 2015) assessed teachers' level of knowledge to see how it impacts their everyday activities, specifically concerning personal online security and potential prevention measures. The research showed that teachers possessed a moderate level

of knowledge regarding cyberbullying. (E. B. Kim, 2014) carried out research to explore how students in a business school in New England perceive awareness of cybersecurity, the research discovered that students recognized the importance of being aware of information security, however, a majority of them did not actively engage in implementing it.

The majority of the studies indicate that students lack awareness of internet risks, highlighting the necessity for cybersecurity awareness campaigns and educational programs to equip students with the necessary knowledge and skills for safe online browsing (Kshetri, 2019; Venter, Blignaut, Renaud, & Venter, 2019). The study by (Kritzinger, Bada, & Nurse, 2017) how a play-based curriculum can assist students in improving their online safety awareness and educate them about internet-related risks. The research utilized a quantitative survey of primary school students to assess the effectiveness of a game-based curriculum in enhancing knowledge of cyber safety. The study revealed a notable statistic: 35% of students concealed their behavior of online used by the parents, while 61% of teachers and parents did not monitor their children's or students' internet activity.

Today, individuals who engage in cyber-attacks are increasing their distribution of harm emails, attempting to control traffic of network, and obtaining user data by taking over personal computers through the files they send to specific email addresses (Cuthbertson, 2017). To ensure safety, it is important to conduct cybersecurity education targeting students (Ismailova & Muhametjanova, 2016; Moallem, 2019), students widely use social media accounts. At times, individuals may fall victim to scams and have their personal data stolen via their social networking profiles. (Kirwan, Fullwood, & Rooney, 2018) conducted a study on this topic with the participation of Malaysian students. They examined if the students in the sample were knowledgeable about the topic and if they had experienced this form of fraud, they revealed that over 30% of students had experienced a scam on a social networking site.

(Al Shamsi, 2019) emphasized the importance of teaching children about cyber risks through cybersecurity awareness programs. (Rahim, Hamid, & Kiah, 2019) was involved in the development of a program focused on raising awareness about cyber security. In this research they found that the youth reacted positively to the program's content. They mentioned that their understanding and abilities concerning the safeguarding of personal data had evolved, as well as their execution of the intended behaviors. (Moallem, 2019) examined the awareness level of cybersecurity among Silicon Valley's students. Consequently, the dangers within the advanced technology setting were examined as well. Based on the data collected, it was found that students lack trust in the university system and are unsure about how to safeguard their personal data. (Ismailova & Muhametjanova, 2016) evaluated the students' awareness of risks related to cybercrime. The cybercrime awareness rate in Kazakhstan was impacted by the

participants' age and gender, as per the research findings. The situation in Kyrgyzstan was unaffected by any factors. The majority of research in the field has shown that the younger generation lacks knowledge about cybersecurity awareness. Some research has suggested that participants may not be fully protected from cyberattacks even if they possess knowledge.

Institutions should regularly provide students with instruction to influence their behavior and enhance their knowledge of cyber security basics and risks (Catal, Ozcan, Donmez, & Kasif, 2023). Furthermore, (Zwilling et al., 2022) indicated that although experienced users had a good grasp of cybersecurity, they seldom implemented it in practical scenarios. Preliminary research findings showed that students had a basic knowledge of cybersecurity but lacked knowledge on how to safeguard their data (Catal et al., 2023). Several researchers have demonstrated through experiments that students lacking knowledge can be easily deceived (Catal et al., 2023; Singh & Singh, 2022).

Because of the increasing amount of passcodes to remember, individuals tend to either choose simple passcodes or repeat their potentially robust passcode (Moallem, 2019; Szumski, 2018). Using the same passcodes repeatedly leads to data breaches, which are considered a significant security issue. A study in the US found that students from different ages and backgrounds have a skewed perception of safety features (Yıldırım & Mackie, 2019). The findings indicate that individuals overestimated the level of security enhancement achieved by including numbers in their passwords and underestimated the reliability of utilizing typing patterns and commonly used words. People frequently overestimated the enhanced security that came from adding digits or characters to the end of their passwords, and tended to reuse their passcodes or segments of them. Another common situation is when personal details are incorporated into passcodes chosen by users (Hartwig & Reuter, 2022). (Wang, Wang, He, & Tian, 2019) found that fewer than one-third of clients used a combination of unique fonts in their passwords, while over half of customers relied solely on numerical passcodes. The report shows that over 12% of users incorporate their phone numbers and birthdays into their password, and 11.5% use their email to create their passwords. Chinese characters were utilized in 26% of cases, either alone or alongside dates and numbers, highlighting the prevalence of English alphabets (Wang et al., 2019).

Self-perception involves our views of ourselves, our traits, and our assessments of those qualities, studies by (Herbst, 2020; Singh & Singh, 2022) regarding self-perception in relation to decision making and awareness of cybersecurity highlight the importance of this in research of information system. Nevertheless, there is limited research linking self-perception to information security. (Agarwal, Josh, & Management, 2016) investigate how awareness of cybersecurity and self-perceived impact the behavior of technology usage in Indian business

professionals. The researcher stated that there is a connection between real and awareness of cyber security. Therefore, individuals with the least cyber security knowledge are impacted by the Dunning Kruger effect, as they believe themselves to be IT professionals (Othman, Alamsyah, Rustine, Aryanto, & Setyawati, 2021).

(Wang et al., 2019) stated that individuals need to differentiate between phishing emails and emails that are legitimate. General perception alone cannot accurately predict detection. Research is being conducted on the exaggerated optimism of information security managers. The study of business executives reveals a positive slant in their perception of risk. The leaders have an inaccurate view of the situation as they are oblivious to the risks, thinking their company is less vulnerable than others and more equipped to handle cyber security threats (Chandarman & Van Niekerk, 2017).

3. Research Hypotheses

Based on the aforementioned discussion, this study postulates the next hypothesis

H1: Cybersecurity knowledge positively and significantly influences cybersecurity awareness among university students.

H2: Password security has a positively impact on awareness of cybersecurity among university students.

H3: Self-perception of skills positively and significantly influences cybersecurity awareness among university students.

Additionally, this study proposed a framework which indicates that each and every variable in the framework have influences on the awareness of cybersecurity figure 1.

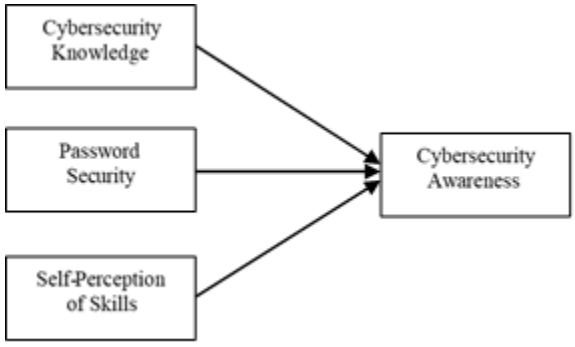

Figure 1. Study Framework

4. Research Methodology

A quantitative research approach was used, the primary instrument used for data collection was structured questionnaires, the questionnaire was designed in five –point Linkert scale, data collection was conducted from September to November 2022, which lasted for nearly two

months, a total of 480 questionnaires were administered to participants that consist of undergraduate students from four different universities in Libya (Sebha University, Tripoly University, Fezzan University, Aljafara University).

5. Finding

The collected data analyzed using PLS-SEM modeling as the chosen tool, Cronbach Alpha, convergent reliability, and discriminant validity used for assessment the measurement model (Hair Jr, Sarstedt, Hopkins, & Kuppelwieser, 2014). Experts suggest that an item is deemed dependable if the factor loading is above 0.70. The factor loading is above 0.70 for all items, indicating the reliability of each item, as presented in Table 1 and Figure 2.

Table 1: Factor Loading

	CSA	CK	PS	SP
CSA1	0.863			
CSA2	0.779			
CSA3	0.815			
CSA4	0.866			
CSA5	0.857			
CSA6	0.821			
CK1		0.871		
CK2		0.702		
CK3		0.793		
CK4		0.695		
PS1			0.827	
PS2			0.893	
PS3			0.814	
PS4			0.876	
SP1				0.796
SP2				0.809
SP3				0.802
SP4				0.789

Note: CK= cybersecurity knowledge; PS= password security; SP= self-perception skills; CSA= Cybersecurity Awareness.

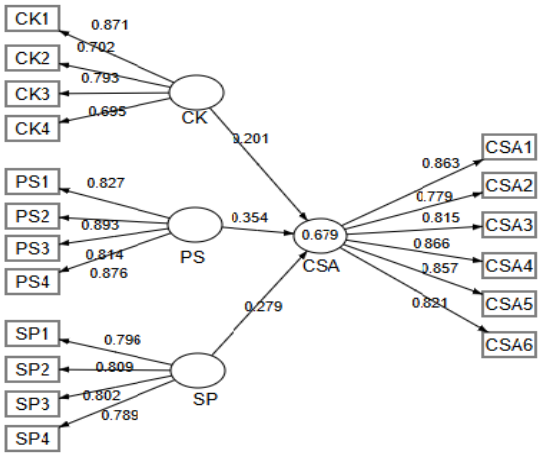

Figure 2: Measurement Model

Cronbach's Alpha and CR used to assess internal consistency reliability, when Cronbach's Alpha and CR above 0.70 is deemed satisfactory (Bagozzi & Yi, 1988). As shown in table 2, the CR and Cronbach's Alpha values are well above the 0.791, indicating that internal consistency has been achieved. Afterwards, to evaluate convergent validity the AVE was used. (Chin, 1998) suggests that the AVE value should be 0.50 or more. As shown in Table 2 the AVE values between (0.699 – 0.863) which indicate that the threshold has been met, validating the convergent validity.

Table 2: Reliability and Validity

	Cronbach's Alpha	CR	AVE
CSA	0.898	0.905	0.863
CK	0.815	0.844	0.699
PS	0.791	0.817	0.704
SP	0.873	0.891	0.798

(Fornell & Larcker, 1981) criteria and the HTMT method used to demonstrate discriminant validity. Table 3 displays the estimates of the connections between the square roots of the AVE and the Latent Variables, which exceeds the correlations between variables and falls between 0.792 to 0.916, that indicate the satisfactory discriminant validity assessment (Fornell & Larcker, 1981).

Table 3: Fornell and larker

	CSA	CK	SP	PS
CSA	0.916			
CK	0.687	0.810		
SP	0.765	0.676	0.792	
PS	0.801	0.695	0.765	0.845

Furthermore, the HTMT criteria were employed to confirm discriminant validity. As shown in table 4 the findings of HTMT values below 0.85 which indicates that the discriminant validity of the variables has been established (Henseler et al., 2005).

Table 4: HTMT

	CSA	CK	SP	PS
CSA				
CK	0.703			
SP	0.811	0.703		
PS	0.823	0.711	0.621	

Once the measurement model was successfully validated, the proposed hypotheses were tested, the results of the hypotheses test displayed in table 6. The results indicate that cybersecurity knowledge positively influences Cybersecurity Awareness in a significant way, supporting H1. Likewise, H2, indicating a substantial positive impact of password security on Cybersecurity Awareness, is supported by the statistical findings, and H3 confirmed that the self-perception skills have positive impact on Cybersecurity Awareness.

Table 6: hypotheses Results

		Beta	Std error	T-Value	P Values	
H1	CK-> CSA	0.168	0.072	3.210	0.001	Supported
H2	PS -> CSA	0.154	0.093	2.102	0.000	Supported
H3	SP -> CSA	0.112	0.081	2.098	0.001	Supported

6. Conclusion

Cyber threats pose a serious threat to national security that everyone must address. Common individuals are at risk of having their personal information stolen when they visit infected websites, respond to phishing emails, store log data in third-party locations, or share confidential information over the phone, or on social media. Within the limited literature on cybersecurity awareness and education for college students, this research used a quantitative method and gathered data via a survey tool from four universities in Libya. The current research has proposed a framework which considers factors such as password security, cybersecurity knowledge, and self- perception of skills, along with the connections of cybersecurity awareness. Therefore, these factors are important predictors of awareness in cybersecurity.

Research is increasingly important in the shifting focus of university students from technology to preventing cyberattacks and vulnerability to cybercrime. The present research shows how different factors related to perceived security, cybersecurity knowledge, and skill

perception can influence an individual's capacity to participate in effective cybersecurity awareness. The researchers highlighted that awareness of cybersecurity about information security needs to extend further than that. To overcome this issue, it is suggested that knowledge should be pertinent, practical, and concentrated, and individuals should receive feedback to assess their performance. These methods also provide the chance to pinpoint individuals who present a greater threat to an organization because they do not follow proper cyber security protocols, providing the chance for extra training or education rather than punishment for these individuals.

While it is important to educate college students on cybersecurity, this research suggests that additional efforts are required to educate the public about cybersecurity and secure online behaviors. Since they represent the largest segment of the population and can impact the cybersecurity knowledge of the educated, it is crucial to prioritize educating those lacking higher education. There is a need from the Universities to consider offering students more training.

this research focuses on a single African nation: Libya. Hence, the findings of this study should be interpreted carefully because of the differences in population sizes across African countries. This research centers on exploring the viewpoints of college students in regards to awareness of cybersecurity. The future research can create awareness of cybersecurity and education structures for African nations.

7. References

Agarwal, P., Josh, C. J. I. J. o. M., & Management, F. (2016). E-banking Service Quality Parameters‟ Impact on Customer Satisfaction. *4*(2), 01-10.

Ahmed, N., Islam, M. R., Kulsum, U., Islam, M. R., Haque, M. E., & Rahman, M. S. (2019). *Demographic factors of cybersecurity awareness in Bangladesh.* Paper presented at the 2019 5th International Conference on Advances in Electrical Engineering (ICAEE).

Al-Janabi, S., & Al-Shourbaji, I. (2016). A study of cyber security awareness in educational environment in the middle east. *Journal of Information Knowledge Management, 15*(01), 1650007.

Al Shamsi, A. A. J. I. J. I. T. L. S. (2019). Effectiveness of cyber security awareness program for young children: A case study in UAE. *3*(2), 8-29.

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data Cognitive Computing, 5*(2), 23.

Annansingh, F., Veli, T. J. I. t., & education, s. (2016). An investigation into risks awareness and e-safety needs of children on the internet: a study of Devon, UK. *13*(2), 147-165.

Aurigemma, S., & Panko, R. (2012). *A composite framework for behavioral compliance with information security policies.* Paper presented at the 2012 45th Hawaii International Conference on System Sciences.

Bagozzi, R. P., & Yi, Y. J. J. o. t. a. o. m. s. (1988). On the evaluation of structural equation models. *16*, 74-94.

Catal, C., Ozcan, A., Donmez, E., & Kasif, A. (2023). Analysis of cyber security knowledge gaps based on cyber security body of knowledge. *Education Information Technologies, 28*(2), 1809-1831.

Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *The African Journal of Information Communication, 20*, 133-155.

Chin, W. W. J. M. q. (1998). Commentary: Issues and opinion on structural equation modeling. In (pp. vii-xvi): JSTOR.

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. J. C. i. I. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *137*, 103614.

Cuthbertson, A. J. N., September. (2017). Ransomware attacks rise 250 percent in 2017, Hitting US Hardest. *28*, 2017.

Fornell, C., & Larcker, D. F. J. J. o. m. r. (1981). Evaluating structural equation models with unobservable variables and measurement error. *18*(1), 39-50.

Hair Jr, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. J. E. b. r. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. *26*(2), 106-121.

Hartwig, K., & Reuter, C. (2022). Nudging users towards better security decisions in password creation using whitebox-based multidimensional visualisations. *Behaviour Information Technology, 41*(7), 1357-1380.

Henseler, J., Fassott, G., Aluja, T., Casanovas, J., Esposito Vinzi, V. J. P., & Methods, R. (2005). Article in monograph or in proceedings PLS'05. 371-377.

Herbst, T. H. J. S. J. o. I. P. (2020). Gender differences in self-perception accuracy: The confidence gap and women leaders' underrepresentation in academia. *46*(1), 1-8.

Ihmouda, R., & Alwi, N. H. M. (2014). *E-government development models: Review of social-technical security aspects.* Paper presented at the International conference on Intelligent Systems, Data Mining and Information Technology.

Ihmouda, R., Alwi, N. H. M., & Abdullah, I. (2015). Successful factors on e-government security social-technical aspect.

Ismailova, R., & Muhametjanova, G. J. I. S. J. A. G. P. (2016). Cyber crime risk awareness in Kyrgyz Republic. *25*(1-3), 32-38.

Jeske, D., & Van Schaik, P. (2017). Familiarity with Internet threats: Beyond awareness. *Computers Security, 66*, 129-141.

Junior, C. R., Becker, I., & Johnson, S. J. a. p. a. (2023). Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity.

Kaloudi, N., & Li, J. J. A. C. S. (2020). The ai-based cyber threat landscape: A survey. *53*(1), 1-34.

Karim, A. A., Shah, P. M., Khalid, F., Ahmad, M., & Din, R. J. C. E. (2015). The role of personal learning orientations and goals in Students' application of information skills in Malaysia. *6*(18), 2002-2012.

kaspersky. (2024). What is cybersecurity? Retrieved from https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

Khalid, F. (2017). Understanding university students 'use of Facebook for collaborative learning. *International Journal of Information*

Education Technology, 7(8), 595-600.

Kim, E. B. (2014). Recommendations for information security awareness training for college students. *Information Management Computer Security, 22*(1), 115-126.

Kim, L. (2018). Cybersecurity matters. *Nursing management, 49*(2), 16-22.

Kirwan, G. H., Fullwood, C., & Rooney, B. (2018). Risk factors for social networking site scam victimization among Malaysian students. *Cyberpsychology, Behavior, Social Networking, 21*(2), 123-128.

Kritzinger, E., Bada, M., & Nurse, J. R. (2017). *A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK.* Paper presented at the Information Security Education for a Global Digital Society: 10th IFIP WG 11.8 World Conference, WISE 10, Rome, Italy, May 29-31, 2017, Proceedings 10.

Kritzinger, E., & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers Security, 29*(8), 840-847.

Kruger, H., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management Computer Security, 18*(5), 316-327.

Kshetri, N. J. J. o. G. I. T. M. (2019). Cybercrime and cybersecurity in Africa. In (Vol. 22, pp. 77-81): Taylor & Francis.

Ktoridou, D., Eteokleous, N., & Zahariadou, A. J. C.-w. i. s. (2012). Exploring parents' and children's awareness on internet threats in relation to internet safety. *29*(3), 133-143.

Li, N., Tsigkanos, C., Jin, Z., Hu, Z., Ghezzi, C. J. J. o. S., & Software. (2020). Early validation of cyber–physical space systems via multi-concerns integration. *170*, 110742.

Manke, S., & Winkler, I. J. S., Retrieved April. (2013). The habits of highly successful security awareness programs: A cross-company comparison. *12*, 2016.

Moallem, A. (2019). *Cybersecurity awareness among students and faculty*: CRC Press.

Muniandy, L., & Muniandy, B. (2012). State of cyber security and the factors governing its protection in Malaysia. *International Journal of Applied Science, 2*(4), 106-112.

Othman, N. A., Alamsyah, D. P., Rustine, M., Aryanto, R., & Setyawati, I. (2021). *ICT and Consumer Behavior: A Study of Students' Self-Perceived Digital.* Paper presented at the 2021 International Seminar on Intelligent Technology and Its Applications (ISITIA).

Pogrebna, G., & Skilton, M. (2019). *Navigating new cyber risks*: Springer.

Rahim, N. H. A., Hamid, S., & Kiah, L. M. J. M. J. o. C. S. (2019). ENHANCEMENT OF CYBERSECURITY AWARENESS PROGRAM ON PERSONAL DATA PROTECTION AMONG YOUNGSTERS IN MALAYSIA: AN ASSESSMENT. *32*(3).

Ratten, V. (2015). 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 Technology Policy Management, 6*(1), 25-36.

SANS. (2017). Retrieved from https://securingthehuman.sans.org/media/resources/STHSecurityAwarenessReport-2017.pdf

Senthilkumar, K., & Easwaramoorthy, S. (2017). *A Survey on Cyber Security awareness among college students in Tamil Nadu.* Paper presented at the IOP Conference Series: Materials Science and Engineering.

Sezer, B., Yilmaz, R., & Karaoglan Yilmaz, F. G. J. I. R. (2015). Cyber bullying and teachers' awareness. *25*(4), 674-687.

Singh, I., & Singh, Y. (2022). Cyber-security knowledge and practice of nurses in private hospitals in northern Durban, kwazulu-Natal. *Journal of Theoretical Applied Information Technology, 100*(1), 246-267.

Suryotrisongko, H., & Musashi, Y. (2019). *Review of cybersecurity research topics, taxonomy and challenges: Interdisciplinary perspective.* Paper presented at the 2019 IEEE 12th conference on service-oriented computing and applications (SOCA).

Szumski, O. J. P. C. S. (2018). Cybersecurity best practices among Polish students. *126*, 1271-1280.

usaid, T. U. S. A. f. I. D. (2024). Retrieved from https://idea.usaid.gov/cd/libya/information-and-communications-technology-ict

Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. J. H. (2019). Cyber security education is as essential as "the three R's". *5*(12).

Wang, D., Wang, P., He, D., & Tian, Y. (2019). *Birthday, name and bifacial-security: understanding passwords of Chinese web users.* Paper presented at the 28th USENIX security symposium (USENIX security 19).

Yıldırım, M., & Mackie, I. J. I. J. o. I. S. (2019). Encouraging users to improve password security and memorability. *18*, 741-759.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. J. J. o. C. I. S. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *62*(1), 82-97.