Education and Information Technologies (2024) 29:3699–3727
https://doi.org/10.1007/s10639-023-11973-5

A Structural Equation Approach and Modelling of Pre-service Teachers' Perspectives of Cybersecurity Education

Musa Adekunle Ayanwale[1] · Ismaila Temitayo Sanusi[2] · Rethabile Rosemary Molefi[3] · Adekunle Olusola Otunla[4]

Received: 29 January 2023 / Accepted: 13 June 2023 / Published online: 26 June 2023

Abstract

The increasing technology reliance in today's world has amplified the need for cybersecurity education for all. Hence, initiatives regarding the integration of cybersecurity education within the pre-college level have begun to emerge in recent times. However, limited research exists regarding in-service or pre-service teachers' perspectives on this phenomenon. More importantly, the need to understand pre-service teachers' perceptions; since their perceptions may significantly influence how the prospective teachers respond to cybersecurity issues and also affect their behavior toward learning and promoting cybersecurity education in the future. Consequently, in order to gain insight into how candidates entering the teaching profession regard cybersecurity, 451 pre-service teachers were sampled in a major public university in Lesotho. The prospective teachers recruited across various departments in the faculty of education responded to an online survey that comprised 33 items gauged from five constructs which include personal cybersecurity awareness, perceived self-efficacy of learning cybersecurity, personal relevance of cybersecurity knowledge, behavioral intention towards learning cybersecurity and actual learning of cybersecurity. We analyzed the response from the survey by utilizing the structural equation modelling approach. Our findings showed that our hypothesized model was mostly accepted. The result suggests that practitioners and researchers in the related field need to raise the pre-service teacher's behavioral intention to learn cybersecurity by helping them realize the implication for their personal lives and society. We discussed our findings in relation to the proposed research model and highlighted the implication for teacher education programs. Finally, the article concludes with limitations and identifies future research agenda.

Keywords Cybersecurity education · Pre-service teachers · Behavioral intention · Teacher education · Lesotho

Extended author information available on the last page of the article

1 Introduction

With the increasing technology reliance in the world, it is imperative to raise everyone's awareness about cybersecurity issues, impacts, and implications along with measures of safe practices in cyberspace. Exploring ways to secure "the computers, networks, data and algorithms that run our digital and physical lives is becoming crucial" (Feng et al., 2017). In order to democratize cybersecurity knowledge, researchers and practitioners recommend that cybersecurity content be integrated in the school curriculum to prepare the future generation for the challenges ahead. Institutionalizing a national cybersecurity strategy across regions and establishing cybersecurity as part of school subjects is a step to addressing cybersecurity-related issues. Equally important is the need to understand the personal and interrelated factors that contribute to learning and behavior toward cybersecurity concepts. This will reveal the perspectives that may hinder the pursuit of cybersecurity and factors that can influence their decision to learn or specialize in the field in the future. The call for cybersecurity education in K-12 education has given rise to the need to develop teachers' capacity and find innovative ways to educate the workforce of tomorrow better on cybersecurity. In keeping with this, researchers have been adopting approaches, such as game-based learning methods to introduce cybersecurity concepts and practices to secure online behavior of elementary and middle school (Tseng et al., 2022) including students in high school (Jin et al., 2018; Yett et al., 2020). Relatedly, Handeli and Robila (2018) developed a high school-level curriculum on cybersecurity due to curricular constraints, while Mourning et al. (2023) conducted workshops to prepare teachers for cybersecurity lessons owing to a dearth of teacher education programs. Even though efforts are ongoing on educational opportunities for K-12 cybersecurity, Dawson et al. (2022) noted that the "need to increase the number and diversity of cybersecurity professionals present a challenge to teacher education."

While cybersecurity receives increasing attention within the compulsory level of education, few empirical studies discuss cybersecurity from pre-service teachers' perspectives. Existing research includes Pusey and Sadera (2011), who asked teacher candidates to rate their ability to give lessons on 75 cyberethics, cybersafety, and cybersecurity topics. Other works are based on a scale developed by Erol et al. (2015) tagged the personal cybersecurity provision scale used to elicit internet users' self-reported behavior related to cybersecurity. The scale was adopted by Haseski (2020) and Karagozlu (2020) to investigate prospective teachers to ascertain the impact of their individual cyber security skills on attitude and the behaviors of students' teachers concerning cybersecurity, respectively. This study focuses on future teachers, considering personal cybersecurity awareness constructs from earlier studies and other psychological constructs that have not been established in relation to cybersecurity and pre-service teachers. As cybersecurity education continues to find its way to K-12 levels, we need to investigate the pre-service teachers' perspectives of the phenomenon in relation to their intention to learn about the technology security issue. To this end, this

study examined pre-service teachers' perceptions of cybersecurity in a public University in Lesotho with a focus on the intention to learn cybersecurity, among other personal and psychological factors.

The dearth of studies about cybersecurity education in the Global South makes Lesotho a unique case to study. While few studies have focused on cybersecurity awareness for school learners in African schools (Kritzinger, 2016; Kritzinger et al., 2017), we have not found any study on cybersecurity education in Lesotho, especially in teacher education context. With the concern of the Lesotho Government on cyber-crime threat (Lesotho News Agency, 2020), understanding how future teachers can be prepared to provide awareness and knowledge to learners within the compulsory level of education is important. We adopted the planned behavior theory, TPB (Ajzen, 1991) infused with personal cybersecurity behavior constructs (Erol et al., 2015). We particularly focused on personal cybersecurity awareness (PCA), perceived self-efficacy (SE), personal relevance (PR), behavioral intention(BI), and actual learning (AL) of cybersecurity. Based on the constructs, we adapted survey items from existing literature and validated them for our use. We extended TPB to measure the associations of personal cybersecurity awareness, perceived self-efficacy, personal relevance, behavioral intention, and actual learning behavior factors in relation to cybersecurity considering pre-service teachers. We sampled 451 prospective teachers that consented to partake in our study and analyzed their responses with structural equation modelling approach (SEM). Based on the factors this study seeks to explore; our research question is: Are there positive effects of personal cybersecurity awareness, self -efficacy, personal relevance, and behavioral intention on actual learning of cybersecurity?

This paper is structured as follows. Having introduced the study background and the necessity of our study, we review existing literature in the next section, specifically on the need to study cybersecurity, the situation of cybersecurity in Lesotho, and studies on cybersecurity and pre-service teachers. Hypotheses development was then introduced, followed by the research method, which includes the participant information, measure, and data analytical approach. Further, we presented the findings of the data analysis followed by a discussion of the research findings, including the implications for teacher education programs. Finally, we concluded our study with limitations and suggested direction for future work.

2 Literature Review

2.1 Why study Cybersecurity?

The need to educate people in this digital era about cybersecurity is becoming more important since individuals or groups want to access others' information illegally. As a result, these criminals could harm other people, the government as well as private organizations using different methods in a computer-generated setting (Walters et al., 2019; Wirtz, 2017). Cybercrime is likely to become an increasingly important issue in the coming years due to the rapid rise of cyberattacks worldwide. Consequently, the World Economic Forum (2020) estimates that cyber-attacks will

threaten $5.2 trillion in global value. Well-known cyber threats consist of malicious software (malware) like viruses, keyloggers, as well as trojans, and techniques for example, phishing and social engineering designed to hurt individuals economically or emotionally and taking away private details without permission (Chakraborty, 2019; Erbschloe, 2019; Kara & Aydos, 2019; Mosola et al., 2019; Prem & Reddy, 2019). To safely meet all of their demands and operate for various reasons without being harmed in this period, it is against this backdrop that people should have ample and sufficient information and abilities to sustain personal cyber security (Furnell & Vasileiou, 2017; Kemper, 2019). Therefore, it is important to understand that cyber security is a model whose goal is to safeguard the information and resources that institutions and people own online (Prasad & Rohokale, 2020; van Schaik et al., 2017). In essence, Mack (2018) emphasizes cyber security as a method for defending against unauthorized access and attacks on computers, networks, software, and data whose target is to misuse. It is of great importance that society be educated about cybersecurity and cybercrime. Amankwa,(2021); Rahman et al. (2020) opines that parents should be more concerned about cybersecurity for kids and teenagers because they may not always realize that their child is a victim of online crime. Numerous guardians are oblivious of the actions their kids do on the internet (Ahmad et al., 2019). Many a time, on social media, kids are oppressed through remarks and abuses; be frightened, harassed, ill-treated or sexually assaulted. The figures shown by the Royal Malaysian Police (PDRM), portray that approximately 80% of sexually assaulted cases reported in Malaysia for two years were of friends which started on social media, and most of the victims are under-aged (Rahman et al., 2020). This demonstrates the need for schools to teach critical digital literacy and to inform parents about their children's internet use.

2.2 Cybersecurity Education in Lesotho

Lesotho, a southern African country has her educational curriculum reform many times to meet its societal needs. The last reform known as Curriculum and Assessment Policy (CAP) shows a better hope and future of education to Lesotho citizens at large. Despite the fact that this policy emphasizes a shift in pedagogy towards teaching and learning strategies that cultivate creativity, independence, and survival skills among learners, it also emphasizes the need for learners to assume greater responsibility for their own learning (Ministry of Education and Training, 2009). One of CAP's aims is to offer knowledge, attitude, and skills that students might need to conform to socio-economic and technological changes (Ayanwale et al., 2023; Ministry of Education and Training, 2009). On emphasis, CAP highlights that since technology is rising and growing more in the economic sector, education should consequently issue technological skills to learners in response to their individual and societal needs (Ministry of Education and Training, 2009). It is worth noting that the primary aim of cybersecurity education is to inform and train technology users of any threats they might encounter when utilizing online communication tools, including social media, chat, online gaming, email and instant messaging (Amankwa, 2021; Rahman et al., 2020). In addition, cybersecurity education is also

necessary to regulate the habit of playing video games. This addiction has detrimental effects because youths are always preoccupied with their computers and meet people via their devices (Rahman et al., 2020). This habit of online games cannot be escaped when time goes on, and teenagers' time to do other important things like studying is taken up by the addiction to their gadgets (Ahmad et al., 2019). It is an undeniable fact that with the increase in Information and Communication Technology (ICT), there is a need for people, especially teachers to know more about cybersecurity.

As outlined in Mosola et al.'s (2019) study, there is little research concerning cybersecurity research in Lesotho or research aimed at protecting the country from known and future cyber-attacks. The study further asserts that this puts the country at risk of attacks since there is no knowledge of cybersecurity from previous research in Lesotho. Former Deputy Prime Minister, Dr. Moleleki, in a symposium with ministers, parliamentarians, and stakeholders noted that Basotho faces the danger of being a prey of cybercriminals owing to the rapid growth in the internet and technology use. Additionally, he issued a warning that sophisticated individuals and highly skilled criminal organizations are attempting to disrupt and take advantage of digital interactions (Lesotho News Agency, 2020). In addition, developed nations, as well as developing ones, are suffering from a shortage of skills. In Lesotho, for example, there is a lack of technical skills in cybersecurity due to its status as a developing country. Furthermore, information communication and technology (ICT) and other related industries have been the most affected. Among organizations, Serianu (2018) notes that 43% are very reactive toward cybersecurity training. The employees of these organizations are only trained when needed, making it difficult for cybercriminals to do their job. Besides that, they spend much more time understanding their target organizations' inner workings. The development of professional cybersecurity abilities is quite limited and at the moment, there is no tertiary institute that offers teaching and learning of cybersecurity (Mosola et al., 2019; Serianu, 2018). According to the Group World Bank (2020) report, Lesotho's cybersecurity readiness is comparatively low. Digitalization has been thwarted in Lesotho due to a lack of cybersecurity and inadequate legislation, according to Dr. Moleleki. Therefore, Basotho cannot benefit from the digital economy (Lesotho News Agency, 2020). Mosola et al. (2019) pointed out that without technical skills, Lesotho cannot execute any national cybersecurity plan or have any type of cybersecurity defense.

Furthermore, Mosola et al. (2019) suggest that Lesotho may have to hire personnel with such skills from other countries since it cannot train its own due to financial concerns. It has been demonstrated by Moyo (2022) that Lesotho benefited from international expertise when drafting the first version of the cybercrime and cybersecurity bill. According to the World Bank's February report titled Lesotho News Agency (2020) the draft bill was reviewed by the Council of Europe in 2019. A bill proposed by Moyo (2022) describes cyberspace monitoring, cybercrimes, and punishments including fines and lengthy prison sentences. Among the services provided by the National Cyber Security Incident Response Team will be cybersecurity intelligence, notifications, warnings, technical aid, threat eradication and recovery from cyber-attacks for Lesotho, as well as raising awareness among Basotho about how to stay safe in cyberspace and building capacity for the country to manage

cybersecurity risks sustainably. There are some barriers to local training, such as low basic education standards or limited turn-over among ICT-related area graduates. Many developing nations encounter a number of difficulties when developing as well as implementing cybersecurity measures into practice due their inadequate knowledge, lack of competence, and lack of understanding of cybersecurity (Zucule de Barros & Lazarek, 2018).

In addition, many Lesotho citizens are unaware of the inherent risks associated with accessing services through electronic means, which illustrates that there is a lack of campaign awareness in the country (Mosola et al., 2019). No leading organization, public or private, is responsible for educating the public about cybersecurity matters the country comes across. It is important to raise awareness when it comes to cyber defense because, on most occasions, cyberattacks are not caused by faulty systems, but rather by a lack of understanding on the part of the user. Educating people about the hazards and perils associated with cyberspace is crucial in the contemporary world of rising use of cyberspace (Kabanda et al., 2018). As Mr. Nick Keen from Microsoft pointed out, hackers can acquire important information, such as passwords to access one's personal information. Thus, using fingerprints as a password or changing passwords regularly is recommended by him (Lesotho News Agency, 2020). It is worth noting that the primary aim of education about cybersecurity is to inform and train technology users for any threats they might encounter when utilizing online communication platforms like social media, chat, online gaming, email and instant messaging (Amankwa, 2021; Rahman et al., 2020). In order to create a culture of cybersecurity, it is crucial to teach and empower users, particularly kids, about the responsible and safe use of online tools and platforms (Ahmad et al., 2019).

2.3 Cybersecurity Education and pre-service teachers

Few studies demonstrate how pre-service teachers perceive cybersecurity. For instance, in the study of Karagozlu (2020) which focuses on behaviors of pre-service teachers towards cybersecurity, pre-service teachers rarely took precautions to protect their personal privacy or leave no traces of their online activities. However, they took regular measures to avoid untrusted applications and information, as well as protect payment information (Karacı et al., 2017). Additionally, the findings of the study indicate that some behaviors of pre-service teachers relating to cybersecurity cannot be assured. Agamba and Keengwe (2012) found that student teachers failed to protect their personal privacy in accordance with the sub-dimensions of cybersecurity behavior. This resulted in live conversation with unknown individuals, incoming e-mail attachments, and passwords being protected as personal information (Agamba & Keengwe, 2012). However, it is evident that prospective teachers are cautious about transacting over the internet and logging off after using the computer (Karagozlu, 2020).

Regarding precautions, pre-service teachers indicated that they rarely check the authenticity, identity and reliability of websites or web applications. They also bought goods and services on their laptops to protect their payment information.

They sometimes take precautions to avoid leaving a digital footprint, for instance, not saving data when using laptops (Haseski, 2020). Again, it has been asserted that students' cybersecurity behaviours are similar amongst male and female pre-service instructors, and there are no statistically momentous differences. In contrast, male students' attitudes toward cybersecurity in online media are more positive than their female counterparts. Compared to male students, female students rarely update their software based on statements. Male students are more likely to have antivirus software installed on their computers than female students (Karagozlu, 2020). Pre-service teachers are expected to take proactive measures to prevent cybercrime in another study conducted by (Agamba & Keengwe, 2012). Pre-service teachers, however, viewed password changes as unnecessary. In addition, most participants used the same password on multiple websites, indicating a dearth of preventive actions to avoid cybercrime. Also, when it comes to installing intrusion detection software on laptops, most pre-service teachers in this study see no need for it. To keep student data and activities for a long time in the future, pre-service science educators believe blockchains, cloud computing, and cybersecurity will play a large role.

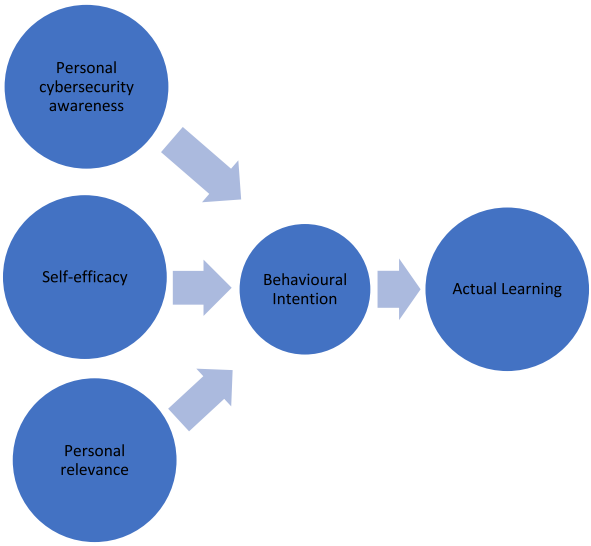
Moreover, Subramaniam (2017) found that college students have a moderate level of cybersecurity awareness. In contrast, Karacı et al. (2017) found that undergraduate students in computer education-oriented programs demonstrated a high level of personal cybersecurity awareness as a whole. Results from Haseski's (2020) study indicated that pre-service teachers appeared to have higher scores when it came to protecting payment information and avoiding untrusted sources. Additionally, leaving a trace, protecting personal information, and taking precautions scored poorly. There might be an explanation for this observation because pre-service teachers prioritize security in their most common virtual activities. According to Yigilt and Seferoğlu (2019) study, college students prioritize preventing untrusted sites, leaving no trace, preserving their privacy, and taking precautions as part of their personal cybersecurity provision. Considering the importance of cybersecurity provision skills for people (Bodea et al., 2019; Neumann, 2017), it may be argued that pre-service teachers are under-trained in cybersecurity, and they should receive support to improve their knowledge and skills. Also, research has shown that pre-service teachers who own their own computers are more likely to possess cybersecurity skills and develop positive attitudes toward computer-assisted instruction. Similar research has revealed that people who own personal computers are probably to use educational computers and have greater skills in digital security than individuals who do not own personal computers (Akgün & Topal, 2015; Chiua & Hob, 2019). Furthermore, there is also a theoretical assumption that the development of a positive attitude can be attributed to the ownership of a personal computer since it can lead to spending a lot of time with interrelated technologies and, as a result, gaining more knowledge and skills. Conversely, it is possible to argue that pre-service teachers with or without personal computers have a relatively higher attitude toward computer-assisted education. The availability of ICT courses in teacher training, along with the inspiration of faculty to employ online learning, may explain the relatively higher attitudes toward computer-assisted education. Even though pre-service teachers own personal computers, their cybersecurity training is inadequate, and their skills could be enhanced.

As stated by Ustundag et al. (2017), a developed level of digital literacy skills was demonstrated by the Department of Teacher Training in Sciences pre-service teachers than by other pre-service teachers. The faculty in this department's support and drive to use technology may be related to the constancy of the abilities demanded in this field of study. Additionally, it may be that the pre-service teachers have extensive experience in cybersecurity within their own lives or that sample methods were used in the study that explains this difference. Despite a weak positive correlation between pre-service teachers' attitudes toward computer-aided instruction and personal cybersecurity capability scores (Haseski, 2020), attitudes were positively correlated with cybersecurity competency scores (Haseski, 2020). Additionally, attitudes toward computer-assisted education were significantly influenced by personal cybersecurity skills. Haseski (2020) argues that safety is considered a basic need, while education is an essential part of meeting high-level demands. The feeling of security in a virtual environment encourages individuals to embrace computer-assisted education. In addition to courses that develop their capabilities in computer usage and computer-aided learning, pre-service teachers should also receive courses on personal cybersecurity in the faculty of education.

3 Hypothesis Development

This section focuses on hypothesis development, variables for measurement and discusses the factors considered in the literature with a proposed research model as shown in Fig. 1. Inspired by TPB (Ajzen, 1991), we focused on perceived self-efficacy, personal relevance, behavioral intention, and actual learning behavior factors. We expanded the theory to include three factors of personal cybersecurity awareness, PCA (Erol et al., 2015) to investigate the perspectives of pre-service teachers.

Fig. 1 Research Model



Based on the widely applicability and utilization of TPB constructs to understand pre-service teachers' perspectives of computing related concepts (Günbatar and Bakırcı, 2019; Li et al., 2016), this study adopted some TPB factor that is deemed relevant for our study. PCA constructs were also considered based on its evidence in previous studies to be appropriate for measuring behavior related to cybersecurity (Erol et al., 2015; Karagozlu, 2020). Also, in previous studies, some variables were examined independently using correlation or regression, but in this study, these underlisted variables were combined into a single model to analyze their inter- and intra-causal relationships with cybersecurity education intentions, resulting in the need for hypotheses to be developed.

3.1 Personal cybersecurity awareness (PCA)

3.1.1 Protecting Privacy (PP)

In this context, privacy protection refers to the notion that one should prevent the information that one wishes to keep private from falling into the hands of hackers, or other wrong doers. More so, keeping personal data and privacy secure is crucial in today's digital world. Data breaches and other forms of cybercrime can easily occur due to the increased use of online services and social media. Consequently, protecting privacy is essential for personal and financial security. Individuals, businesses, and even entire nations may be affected by cybersecurity threats. Physical harm and financial loss can result from cyberattacks. Thus, learning cybersecurity skills can mitigate these risks and protect individuals and organizations. Cybersecurity is also a rapidly growing field, and professionals are in high demand. Educating individuals and organizations about these issues will help them better protect themselves against cyber threats and make the digital world safer and more secure. Despite the apparent logical connection between protecting privacy and learning cybersecurity education, many factors (such as access to technology, level of trust in technology, and personal values) can influence this relationship. Studying this relationship and developing strategies to promote privacy protection and cybersecurity education must consider these factors. In general, students' behavior when using the internet and protecting their privacy are not always protected by the necessary precautions, based on an examination of their cybersecurity behaviour (Haseski, 2020). Based on the premise that protection of privacy is an indication of personal cybersecurity awareness, we intend to ascertain if individuals' understanding of privacy protection can motivate them to learn cybersecurity. Hence, we hypothesize that:

H1a. PCA (Protecting Privacy) predicts pre-service teachers' BI to learn cybersecurity

3.1.2 Avoiding the Untrusted (AU)

In this study, avoiding the untrusted is whereby one evades the process, information, online platform that has not been evaluated or examined for correctness and

adherence to the security policy. Cybersecurity requires caution and a critical eye but does not necessarily translate into high levels of trust in information. Cybersecurity learning involves multiple factors, including the availability of resources, instructional methods, and motivation. Pre-service teachers' BI and their ability to learn cybersecurity education are unlikely to be solely determined by avoiding untrusted sources. The relationship between avoiding untrusted sources and BI is further complicated by the fact that what one context considers reliable in another may be untrusted in another. It is complex and may not be obvious how avoiding untrusted sources affects pre-service teachers' cybersecurity learning. When evaluating cybersecurity education for pre-service teachers, it is important to consider multiple factors. Since it has been established in literature that avoiding the untrusted online sources or links shows cybersecurity awareness of individuals (Erol et al., 2015), this study aimed to determine if avoiding the untrusted will influence learning of cybersecurity. It is therefore hypothesized that:

H1b. PCA (Avoiding the Untrusted) predicts pre-service teachers' BI to learn cybersecurity

3.1.3 Precaution (PC)

As per this study, precaution can be defined as an action taken in advance to prevent harm that might occur as result of breach of security in an online transaction or engagement. Establishing a relationship between precaution and intention to learn cybersecurity is important on several grounds. Since taking precaution has been shown to be an indication of personal cybersecurity awareness, it is logical to find out if this will prompt people to learn cybersecurity contents, specifically pre-service teachers who are the focus of this study. Exploring pre-service teachers is necessary, since literature revealed that 40% of pre-service teachers seldom or never took any step to protect their devices thus putting themselves at risk (Moyo et al., 2022). Hence, this study set out to investigate if taking precautions can influence pre-service teachers to learn about cybersecurity. Thus, it is hypothesized that:

H1c. PCA (Precaution) predicts pre-service teachers' BI to learn cybersecurity

3.2 Self -efficacy (SE)

Perceived self-efficacy is the conviction that one has the capacity to use abilities relevant to IT security or privacy, a psychological trait that has a direct impact on security behaviors. Self-efficacy beliefs influence motivation and, as a result, executing behaviors through having an impact on objectives, outcome expectations and socio-structural factors (Angela et al., 2021). In addition, Adıyaman and Sert (2018) examined pre-service science teachers' perceptions of computer self-efficacy and attitudes towards computer-aided education. As a result of the study, pre-service science teachers were found to have positive attitudes toward computer-aided education and positive perceptions of their self-efficacy. There was a positive correlation

between their perceptions of their self-efficacy and their attitudes towards computer-aided education. The use of computers in pre-service teachers' classrooms was influenced by attitudes toward technology, perceived computer competence, and computer anxiety, according to Celik and Yesilyurt (2013). According to Yeşilyurt et al. (2016), "teachers' attitudes toward computer-supported education were significantly influenced by their self-efficacy, academic self-efficacy, and computer self-efficacy." Thus, we propose that:

H2. SE in learning cybersecurity predicts teachers' BI to learn cybersecurity.

3.3 Personal relevance (PR)

Personal relevance is the extent to which cybersecurity knowledge is applicable to pre-service teachers' daily lives and knowledge. Since establishing relevance of a subject to students' personal lives helps to motivate them by showing them the real-world connection (Vennix et al., 2017, 2022), it is important to consider the factor. Previous researchers have discovered relevance as an important factor in the acceptance of a system or a technology (Weerathunga et al., 2021; Agudo-Peregrina et al., 2014). In the context of this study, we define personal relevance of cybersecurity knowledge as the student's perception concerning the degree of significance of learning cybersecurity for either their personal lives such as career development or societal development. When a learner considers the learning of cybersecurity as significant and establishes links to real world applications, they could find learning the subject very useful. Pre-service teachers who understand cybersecurity knowledge as more relevant to them may be encouraged to pursue cybersecurity lessons and have the behavioral intention to learn cybersecurity. Personal relevance has been earlier established as an antecedent to behavioral intention in related subjects. Our study further validates the relationship in the context of cybersecurity. Hence, we hypothesized that:

H3. Personal relevance of cybersecurity knowledge predicts pre-service teachers' BI to learn cybersecurity

3.4 Behavioral intention (BI)

In this context, behavioral intention is explained as the level of future intention of pre-service teachers to actually learn cybersecurity. It has been hypothesized by Moyo et al. (2022) that pre-service teachers devote most of their time self-studying and that any cybersecurity challenges they encounter harshly impede their learning progress. In Agamba and Keengwe's (2012) study, pre-service teachers were found to be lacking proactive behavior when it came to preventing cybercrime. Pre-service teachers show no difference from general computer end-users when it comes to their attitudes toward cybercrime prevention, and curricula for pre-service teachers can address this by providing fundamental information about what it means to be proactive about cybercrime prevention. By adopting such education, pre-service teachers

can be motivated to teach fundamental cybersecurity measures to their students based on their pedagogical beliefs (Agamba & Keengwe, 2012). Therefore, we propose the hypothesis below:

H4. BI toward learning cybersecurity predicts pre-service teachers' AL of cybersecurity.

4 Methodology

This study focuses on pre-service teachers regarding their perspectives on cybersecurity education. We specifically explore a large metropolitan public university in Lesotho, a Southern African country. Lesotho is ranked among the least populated countries in Africa, with about 2 million people. While little is known about cybersecurity and pre-service teachers' perspective globally, considering the phenomenon among the target population in an African context is important. Even though the country is plagued with a myriad of challenges, like many other African countries, ICT devices, the internet, and other emerging technologies are used extensively in Lesotho. These and many more make it important to understudy the context.

4.1 Sample

The study sample consisted of four hundred and fifty-one (n = 451) pre-service teachers from Science Education, Educational Foundation and Language Art Education in a large public University in Lesotho. The students enrolled in the teacher education program of the university are the targeted population of our study. We surveyed the participants that consented to be part of our study through an online survey. The link to the survey was shared through media platforms (e.g., WhatsApp). The researchers believe that only pre-service teachers filled our survey since the survey link was shared through a closed social media platform created solely for communications between the teacher educators and the pre-service teachers in the institution. The survey was designed such that it can only be filled once. Our respondents were randomly sampled, and they represent the target population. We assume this position since we had representations across all levels of the program and the three departments in the faculty of education under investigation. The instruction on the survey reads that if the participants agree to be part of the study, they should fill the survey with assurance of keeping their information confidential. The data collection was carried out within October and November 2022. As shown in Table 1, female students (77%) participated more in our study and most of the participants (60%) are within the age of 21–30 years. About 41% claimed to have "emerging" proficiency in using ICT while most of them (45%) had increasing confidence in ICT use. All the trainee teachers have equal representation across levels with most of the students in the Educational Foundation department.

Table 1 Characteristics of the sampled pre-service teachers

		Frequency	Percentages
Gender	Male	103	22.8
	Female	348	77.2
Age	Less than 20	124	27.5
	21–30	269	59.6
	31–40	58	12.9
Department	Science education	123	27.3
	Educational foundation	268	59.4
	Languages and Social Education	60	13.3
Proficiency in using ICT	None	29	6.4
	Novice	60	13.3
	Emerging	186	41.2
	Proficient	176	39
Level of confidence in ICT use	Not confident	66	14.6
	A bit confident	125	27.7
	Increasing confidence	203	45
	Very confident	57	12.6
Level	Year One	105	23.3
	Year two	100	22.2
	Year three	130	28.8
	Year four	116	25.7

4.2 Measures

The questionnaire contained three personal cybersecurity awareness (PCA) subscales, a personal relevance scale, a self-efficacy scale, a behavioral intention scale, and an actual learning scale. The three PCA subscales were 5-point Likert scales in which 1 = Never and 5 = Always while the other four constructs used the 4-point Likert scale of strongly disagree (1) and strongly agree (4). The items utilized in this study are detailed in the Appendix.

PCA subscales. PCA scale by Erol et al. (2015) was used to obtain internet users' self-rated behavior related to cybersecurity. The PCA scale was further distributed to prospective teachers to determine the effect of their individual cybersecurity skills on attitude (Haseski, 2020). PCA scale comprised five subscales of 25 items in total, but three subscales and 16 items were utilized in this study. Protecting Privacy (PP), Avoiding the Untrusted (AU) and Precaution (PC) subscales were specifically considered. We choose to explore the three subscales because we believe they are sufficient to measure the teacher candidate's awareness of cybersecurity.

Self-efficacy belief (SE). SE scale was adapted from Schwarzer et al. (1999) to examine the participants' perceived SE in their understanding of cybersecurity. The items utilized were five items adapted from an existing scale developed originally for pre-service teachers.

Personal relevance (PR). PR scale comprises three items that measured pre-service teachers' viewpoint of the degree to which knowledge of cybersecurity is relevant to them, their needs, and the significant consequences it has for them. The items were adapted from existing work (Li et al., 2022) and verified through confirmatory factor analysis (CFA). Even though the original items were focused on related emerging concepts, we adapted them to fit cybersecurity which is the focus of our study.

Behavioral intention (BI). BI scale was measured with four items generated by Li et al. (2022) were revised and validated through CFA to measure pre-service teachers' intention to learn cybersecurity. We adapted the items such that we contextualized them toward learning of cybersecurity.

Actual learning (AL). This subscale has also revised the survey of Li et al. (2022) and validated it through CFA. AL subscale contained four items that measured pre-service teachers' behavior associated with cybersecurity learning. We specifically request that the teacher candidates reflect on their experience and learning about cybersecurity using the internet, self-directed learning approach, or textual materials.

4.3 Analytical strategy

Data were analyzed using the appropriate statistical methods to address our research objective. We specifically used SmartPLS software version 4.0. Using a measurement model, we examined the validity and reliability of each construct considered in the questionnaire. Further, with a structural model, we confirmed the significance and strength of the hypothesized relationships between the latent variables. Based on our hypothesized model, we conducted confirmatory factor analysis and SEM to establish relationships among the factors under consideration.

5 Results

A measurement model was conducted to validate the seven constructs before a detailed investigation of the structural relationships between them could be conducted. As a result of the analysis, the overall measurement model was found to have a good fit to the data (SRMR = 0.04 < 0.08, d_ULS sat = 0.407 < est = 0.527, and d_G sat = 0.328 < est = 0.452, NFI = 0.924). In terms of descriptive statistics, it is noted that the median value calculated at the item level does not indicate a floor or ceiling effect (See Table 2). Moreover, it was also found that some items in the model of the constructs possess standardized estimates of less than 0.40 (Amusa & Ayanwale, 2021; Bagozzi, 1981; Hair et al., 2014, 2017), which is in accordance with previous research. Protecting privacy (PP), precaution (PC), and actual learning (AL) constructs were found to have average variance extracted (AVEs) below 0.50 in the model. AVE levels are sometimes low in constructs because some indicators underpinning the constructs have low outer loadings.

Table 2 Measurement model result (n = 451)

Measures	Indicators	Median	Standardized estimates	t-statistics
	PP1	3.0	0.97	30.99**
PP	PP2	3.0	0.52	4.21**
	PP4	4.0	0.45	2.86**
	AU1	5.0	0.87	48.69**
	AU2	3.0	0.75	21.90**
AU	AU3	4.0	0.89	44.26**
	AU4	4.0	0.84	28.15**
	PC2	3.0	0.73	4.91**
PC	PC3	4.0	0.81	5.29**
	PC4	4.0	0.76	5.29**
	SE1	3.0	0.75	19.79**
	SE2	3.0	0.78	23.48**
SE	SE3	3.0	0.85	44.86**
	SE4	3.0	0.83	26.60**
	SE5	4.0	0.80	24.81**
	AL2	3.0	0.82	4.89**
AL	AL3	2.0	0.90	6.59**
	AL4	3.0	0.65	2.96**
	PR1	4.0	0.93	49.56**
PR	PR2	4.0	0.97	51.15**
	PR3	4.0	0.96	29.73**
	BI1	4.0	0.93	77.18**
	BI2	4.0	0.96	36.41**
BI	BI3	4.0	0.94	91.69**
	BI4	4.0	0.89	46.13**

*AU = Avoiding the untrusted; PR = Personal relevance, PP = Protecting privacy, SE = Self-efficacy, BI = Behavioural intention, AL = Actual learning, PC = Precaution

Consequently, items with loadings below 0.40 and items with negative loadings could not be used to measure constructs with any degree of reliability. Consequently, using such items in a hypothesis test cannot prove the hypothesized model's validity. This report reveals that several items need to be deleted based on the results; among them are PP3 (-0.104), PP5 (0.194), PP6 (0.279), PP7 (-0.175), PP8 (0.356), PP9 (0.261), PC1 (0.214) and AL1 (0.312). As a result of removing these items from the model, a better description of the hypothesized structure was displayed. As shown in Fig. 2, an improved measurement model has been re-specified and validated to ensure that all standardized estimates for the survived items are significant (see Table 2).

There was an adequate level of internal reliability in the measurement, indicating a Cronbach's alpha value between 0.71 and 0.95. Besides construct reliability, the proposed model was also tested for convergent validity and discriminant validity. Table 3

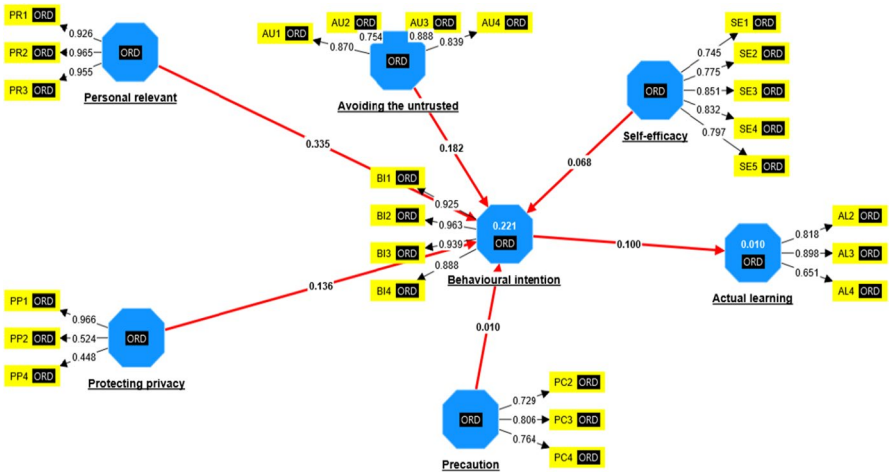


Fig. 2 Validated measurement model

Table 3 Construct validity and reliability

Measure	α	CR	AVE
AL	0.71	0.84	0.63
AU	0.86	0.91	0.70
BI	0.95	0.96	0.86
PR	0.94	0.96	0.90
PC	0.66	0.81	0.59
PP	0.59	0.70	0.48
SE	0.86	0.90	0.64

*AU = Avoiding the untrusted; PR = Personal relevance, PP = Protecting privacy, SE = Self-efficacy, BI = Behavioural intention, AL = Actual learning, PC = Precaution, α = Cronbach's alpha, CR = Composite reliability, AVE = Average variance extracted

indicates adequate construct reliability in the proposed model (CR > 0.70) (Hair et al., 2022; Schreiber et al., 2006), with a composite reliability range of 0.70 to 0.96. As a result, the average variance extracted (AVE) values for all seven constructs were above 0.50, indicating good convergent validity at the construct level, i.e., the model is valid and reliable on a construct-by-construct basis (Hair et al., 2010). The HeteroTrait-MonoTrait ratio of Correlation (HTMT) is presented in Table 4 as a measure of discriminant validity. Due to its superior performance compared to both the Fornell-Larcker criterion and cross-loadings, the HTMT has become one of the most popular criteria for assessing discriminant validity (Henseler et al., 2015). A threshold value of 0.90 was calculated for reflective measurement models in order to establish discriminant validity, but HTMT values must not exceed 0.85 for discriminant validity to be established (that is,

Table 4 Discriminant validity-HTMT

	AL	AU	BI	PR	PC	PP	SE
AL							
AU	0.13						
BI	0.11	0.25					
PR	0.22	0.07	0.40				
PC	0.35	0.38	0.15	0.06			
PP	0.27	0.25	0.20	0.15	0.36		
SE	0.46	0.32	0.26	0.37	0.55	0.23	

*AU = Avoiding the untrusted; PR = Personal relevance, PP = Protecting privacy, SE = Self-efficacy, BI = Behavioral intention, AL = Actual learning, PC = Precaution

HTMT values must be below 0.90 for discriminant validity to be established; Henseler et al., 2015). Based on the analysis of the HTMT ratios, most of the values were below the cut-off of 0.85. Therefore, all seven constructs were discriminantly valid in the proposed model.

5.1 Structural model assessment

As a result of structural equation modelling (SEM), the hypotheses relating to the model were tested in respect of the hypotheses proposed in the models, as shown in Table 5. An essential characteristic of path coefficients is their sensitivity to the level of certainty with which a variable can be said to have causal relationships with another variable in the model. It is worth noting that PLS-SEM uses bootstrapped p-values as a method to determine the significance of path coefficients. We used the bootstrapping method to estimate the significance of each of these parameters, and we calculated the student's t-value and p-value. Also reported were the squared multiple correlations (R^2) between the endogenous variables (BI and AL) and the exogenous variables, which were used to estimate the percentage of variance explained by the exogenous variables. BI was found to be influenced by the exogenous variables (PC, PP, AU, SE, and PR), jointly accounting for about 22.1% of the variance

Table 5 SEM results (n = 451)

Hypothesis	Paths	β-values	SD	t- statistics	p- values	remarks
H1a	PP—> BI	0.14	0.03	4.31	0.00	Supported
H1b	AU—> BI	0.18	0.05	3.98	0.00	Supported
H1c	PC—> BI	0.01	0.04	0.22	0.83	Not supported
H2	SE—> BI	0.06	0.05	1.28	0.20	Not supported
H3	PR- > BI	0.34	0.06	5.79	0.00	Supported
H4	BI—> AL	0.10	0.04	2.37	0.02	Supported

AU = Avoiding the untrusted; PR = Personal relevance, PP = Protecting privacy, SE = Self-efficacy, BI = Behavioural intention, AL = Actual learning, PC = Precaution, SD = Standard deviation

observed in the data. Four were found to be supported among the six hypotheses examined in the study, as shown in Table 5. Based on the results of this study, the theoretical hypotheses related to the TPB were well supported. A significant, positive relationship was found between PP ($\beta = 0.14$, $p < 0.05$), AU ($\beta = 0.18$, $p < 0.05$), PR ($\beta = 0.34$, $p < 0.05$), and BI. Conversely, PC and SE did not affect BI directly ($\beta = 0.01$, $p = 0.83$, and $\beta = 0.06$, $p = 0.20$). As a result, H1a, H1b, and H3 were supported, but not H1c and H2. BI also significantly influenced AL ($\beta = 0.10$, $p < 0.05$) and explained 10 percent of its variance. Therefore, H4 was supported.

Further, multiple group analysis (MGA) was conducted to examine whether there are significant differences between groups on the study variables. In the context of this study on pre-service teachers' perspectives of cybersecurity education, the specialization of the participants (Science education, Educational foundations, Languages and Social Education) was used as a grouping variable to explore potential differences in their perspectives. Table 6 presents the result.

In terms of pre-service teachers' perspectives on cybersecurity education, the groups showed significant differences as determined by the preliminary analysis of the study. Specifically, participants with a background in science education had the highest mean score on the importance of cybersecurity education, followed by those in languages and social education and educational foundation, respectively. This finding suggests that cybersecurity contents and its importance in today's world may be more understood by the candidates with a science education background. Furthermore, Table 6 shows that science education and languages and social education differed significantly in their behavioral intention to learn cybersecurity education and actual learning. It appears that BI has a greater impact on AL for participants in languages and social education than for science education. A significant difference was also found between science education and educational foundations in personal cybersecurity awareness and behavioral intention to learn cybersecurity education. As a result, PCA has a greater impact on BI for participants in science education than for participants in educational foundations. Table 6 also reveals that perceptions of cybersecurity education's relevance on behavioral intentions differed significantly between the groups. Candidates in Education foundations and science education specializations have significantly higher behavioral intention scores than languages and social education specializations. This suggests that cybersecurity education may be seen as more directly connected with learning intentions by individuals in science and educational foundation specializations. Additionally, it was found that

Table 6 Multi-group analysis

Relationship	Diff. (Group 1 -2)	p-value	Diff. (Group 1 -3)	p-value	Diff. (Group 2 -3)	p-value
BI—> AL	-0.131	0.092	-0.22	0.028**	-0.089	0.185
PCA—> BI	0.244	0.017**	-0.241	0.056	0.003	0.466
PR—> BI	0.418	0.000**	0.729	0.000**	0.311	0.036**
SE—> BI	0.122	0.102	-0.265	0.032**	-0.386	0.005**

PCA- Personal cybersecurity awareness, PR-personal relevance, SE-Self-efficacy, BI- Behavioural intention, AL- Actual learning, Diff – Difference, Group 1- Science Education, Group 2- Educational Foundations. Group 3- Languages and Social Education

there were significant differences in self-efficacy between the groups regarding behavioral intention to learn cybersecurity. As compared to other specializations, science education has a greater impact on SE and BI. Generally, the MGA provides valuable insights into how pre-service teachers' perspectives on cybersecurity education may differ based on their specialization. Considering the unique needs and perspectives of pre-service teachers, these findings can inform how to design a cybersecurity teacher education program effective for all regardless of specialization.

6 Discussion

Considering the significance of promoting cybersecurity in K-12 learning contexts (Childers et al., 2022; Konak, 2018; Yan et al., 2021) and earlier studies on cybersecurity in pre-service education (Erol et al., 2015; Haseski, 2020), this study further probed into how prospective teachers entering the teaching profession regard cybersecurity in an effort to contribute to knowledge and support the design of an effective cybersecurity teacher education program. As cybersecurity education initiatives aiming at developing a cybersecurity-literate workforce and citizenry are now increasingly focusing on K-12 levels (Childers et al., 2022; Mourning et al., 2022), exploring how to equip educators for the indispensable responsibility of facilitating the lesson in classrooms is imperative. Particularly, in light of limited evidence proving teacher candidates' behavior towards cybersecurity (Karagozlu, 2020), this study sought to examine teacher education students' perceptions of cybersecurity as regards their behavioral intention to learn cybersecurity, among other personal and psychological factors. To gather the participants perspectives, students within teacher education programs in a Lesotho public university were sampled. Furthermore, a 7-factor validated survey scale for measuring teacher candidates' personal cybersecurity awareness (protecting privacy, avoiding the untrusted and precaution), perceived self-efficacy, personal relevance, behavioral intention, and actual learning of cybersecurity drawing on previous literature (e.g., Erol et al., 2015; Li et al., 2022) was administered.

Using the SEM approach, our findings showed that protecting privacy, avoiding untrusted, and personal relevance regarding cybersecurity knowledge directly predicts behavioral intention toward learning cybersecurity, resulting in significant changes in their actual behavior. To validate the reliability of behavioral intention as an antecedent of actual behavior, the participants' actual learning of cybersecurity was incorporated into the structural model. To our knowledge, this study is the first to establish the relationship of the personal cybersecurity awareness (protecting privacy, avoiding the untrusted and precaution), as operationalized in this study in relation to behavioral intention to learn among other constructs. In the three PCA factors, only precaution could not predict behavioral intention which suggests that only taking precaution against cyber threat is not enough. Also, it may be that the respondents are not sure of the precautions to take, perhaps, how are they aware of the precaution tips? This is an important question a follow-up study should provide answers to. Generally, personal cybersecurity awareness is an important factor to be considered in promoting cybersecurity lessons, hence, the need to raise the personal cybersecurity awareness of the prospective teachers through relevance

contents. Based on our result on PCA, the findings mirrored previous studies that examined cybersecurity learning using PCA scale (Karagozlu, 2020; Karacı et al., 2017), establishing the validity of the scale for identifying factors that impact pre-service teachers' behavior towards cybersecurity.

In contrast, precaution and perceived self-efficacy in learning cybersecurity did not impact behavioral intention. This is not in tandem with the submission of earlier findings (Haseski, 2020; Karagozlu, 2020) that pre-service teachers take precautions, leave no trace, and protect their privacy. Karagozlu (2020) and Haseski (2020) study who found that pre-service teachers take cognizance of the PCA considered in this study may have been exposed to cybersecurity content, scuh as through online resources or other means. While the findings is consistent with past research (Sanusi et al., 2021) that reported self-efficacy could not predict behavioral intention, our findings also disagree with the submission of existing results (Celik & Yesilyurt, 2013; Yeşilyurt et al., 2016) that pre-service teacher self, academic and computer self-efficacy were significant predictors of behavioral intention in computer supported education. Self-efficacy was also found to be linked to behavioral intention to learn AI in recent a study (Li et al., 2022). While there is some evidence that establishes self-efficacy's influence, our study showed that prospective teachers' beliefs about their capability and confidence to understand and respond to cyber issues is not sufficient to influence their intention to learn cybersecurity.

Our study further reveals that personal relevance strongly predicts behavioral intention to learn cybersecurity. The external factor, that is, relevance, was found to be crucial since the factor significantly affects behavioral intention to learn cybersecurity. As a result, a series of approaches should be devised to increase students' perceptions of the relevancy of cybersecurity to their personal lives, future career, and society. This finding is in tandem with recent studies in the related field of artificial intelligence which established a direct and positive association between personal relevance and behavioral intention (Ayanwale et al., 2022; Li et al., 2022). The result suggests that to cultivate a strong intention to learn cybersecurity, teacher educators and designers of teacher education programs need to develop contents and approaches that establish and boost the relevance of cybersecurity for them. For instance, an approach could be experimenting with unconventional cybersecurity awareness training in the form of festivals, art installations and role-playing games. Consequently, the respondents' intention towards cybersecurity may significantly influence their actual learning behavior. As evident in several studies (Ajzen, 2012; Li et al., 2022), our study further corroborates the association between behavioral intention and actual learning as behavioral intention to learn cybersecurity predicts actual learning of cybersecurity. The multi-group analysis along the line of specialization showed that candidates in the science education department had the highest intention to learn cybersecurity. This finding suggests that students in science education are more interested in learning cybersecurity which may be linked to the premise that cybersecurity is science and technology related. The findings of the multi-group analysis indicates that a teacher education program appealing to all students irrespective of their specialization should be designed.

Despite the increasing use of digital technologies in academia and for personal use, pre-service teachers are lacking practical cybersecurity knowledge and

awareness. It is important that pre-service teachers have cybersecurity knowledge as it can prepare them to protect their private information assets. There is evidence that users in different educational institutions are lacking required knowledge and skills in digital technologies used to access online information and applications (Zwilling et al., 2020). In addition, university end-users are unfamiliar with existing tools for protecting themselves against cyber threats, further exacerbating this problem (Abawajy, 2014; Furnell et al., 2007). There is also a potential for cyber security to preserve confidentiality, integrity, and accessibility of information in cyberspace. According to Von Solms and Van Niekerk (2013), cybersecurity focus on protecting the physical and virtual environment of cyberspace, the tangible or intangible technologies that support cyberspace, electronic information, and users on a societal and national level, as well as ensuring that best practices, assurances, and technologies can be used in order to safeguard the cyber environment, organizations, and those utilizing information technology. As a result of using various digital devices to access the internet, personal data stored on such devices can be viewed, tempered with, or even deleted by unauthorized individuals. In all, if empowered with requisite skills, pre-service teachers can mitigate cybersecurity threats and attacks by utilizing basic strategies and knowledge. However, in the case of advanced attacks, the basic strategies may prove insufficient. Hence, the need for a more detailed and effective cybersecurity program to prepare the future teachers with content and pedagogical knowledge to promote cybersecurity in classrooms and solve data theft, phishing, and other threats associated with personal digital devices.

6.1 Implication for teacher education program

This study has several implications for teacher education programs. First, since teacher education programs focusing on cybersecurity education are lacking, especially in the African context, this provides insights into the factors that could be considered to promote cybersecurity education. Based on our findings, personal relevance is the highest predictor of behavioral intention which suggests that there is a need to emphasize and establish the relevance of cybersecurity for an individual's personal lives and activities. In literature, personal relevance has been recognized as a significant factor that motivates and contributes to students' favorable attitude towards STEM (Frymier & Shulman, 1995; Vennix et al., 2017, 2022). Loukomies et al. (2013) further assert that it is imperative that learners regardless of their "motivational profile feel some relevance when participating in science classes'' including other subject domains. As a result, in designing a sequence of lessons with a focus on cybersecurity topics, it is important to include features that would be fascinating to pre-service teachers irrespective of their motivational profiles. Connecting cybersecurity to real-world applications and industrial environments to enhance its personal relevance for students cannot be farfetched. Almost everyone now owns a smartphone among other mobile devices which are vulnerable to cyberattacks. According to The Economic Times (2022), a cybersecurity company known as Kaspersky, detected nearly 3.5 million malicious attacks on mobile phone users in 2021. In 2022, approximately 60 percent of digital fraud is perpetrated through

mobile devices, including phishing attacks, data leaks, use of open WiFi, malicious apps, identity theft, and stolen passwords (Nelson, 2022). Besides the proliferation of mobile devices, highlighting the relevance of cybersecurity knowledge to multiple areas would be beneficial in terms of career development (Pencheva et al., 2020). In addition, designing a program with a component of field experience, for example, developing relationships with industry that would facilitate the process of active learning and further establish relevance.

Our findings also showed that pre-service students' privacy protection and avoiding the untrusted in using a digital device influence their intention to learn cybersecurity. This result is an indication that understanding teacher candidates' existing cyber knowledge and interest in cybersecurity would be valuable for designing an effective cybersecurity module. By this way, we can further establish how the students can be best supported. The article offers some insights into the knowledge base that program designers, researchers and government need to prepare teachers for cybersecurity in K-12 contexts. Currently, there is no policy and curriculum support for K-12 cybersecurity education in Lesotho, let alone included in the school curriculum. Consequently, cybersecurity is not taught in schools or embedded within teachers' education curriculum. Hence, the need for a sustainable strategy to ensure cybersecurity education is democratized to young learners through integration in teachers' education programs. This is particularly important as lack of training through a teacher education program has been identified to be a consequential hindrance to the implementation of cybersecurity in schools (Dawson et al., 2022; Pye, 2016). In order for educators to implement cybersecurity efficiently in schools, they must embark upon training as part of their teacher education program. This study suggests that teacher education curriculum and program designers as well as policymakers could establish a foundation course in cybersecurity education for prospective teachers at Lesotho Universities. This may be designed as a core unit course to be undertaken by student teachers that are registered in the Bachelor of Education (B.Ed.) programs. This unit course should aim at providing the future teachers with a strong foundation in fundamental cybersecurity education through modules that emphasize a range of Cyber issues, cyberethics, and cybersafety.

6.2 Limitation and future work

Some limitations to this study were identified. First, our study was based on the pre-service teacher within a public university. The participants may not be representative of the overall population of pre-service teachers' perspectives and attitudes of cybersecurity in Lesotho. Conducting a similar study with a larger pre-service teacher population will help to validate the findings. Covering more geographical regions or countries could provide more insight. Second, utilizing a quantitative approach may not be sufficient to achieve a rich perspective of teacher candidates on the phenomenon under scrutiny, although it provides us with a broader perspective based on the number of participants. Triangulating the study with a qualitative approach would have allowed the researchers to further understand their disposition and generate a deeper insight into their perspectives. Future studies should also consider analyzing the findings along the lines of gender and specialty (Ayanwale & Sanusi, 2023; Sanusi & Olaleye, 2022) in the teacher training course.

Appendix

Questionnaire items (finalized).

Protecting privacy

PP1. It is important for me to use the same password on all my internet accounts.

PP2. I am responsible for responding to e-mail messages concerning authentication (username, password, etc.).

PP4. When necessary, I share my personal information on the internet (Identity number, date of birth, GSM number, etc.).

Avoiding the untrusted

AU1. Whenever I receive a request for money or credit online, I ignore it.

AU2. My social networks do not allow me to accept friendship requests from people I don't know.

AU3. I won't subscribe to an untrustworthy website.

AU4. Downloading files from websites I don't trust is not something I do.

Precaution

PC2. Whenever I use software, I update it.

PC3. My computer is protected by antivirus software.

PC4. It is important to me not to use weak passwords.

Perceived self-efficacy

SE1. The concept of cybersecurity is something I am confident I can grasp.

SE2. When I receive emails like these, I can identify cyberattack attempts.

SE3. In order to resist cyberattacks, I am confident that I will be able to develop the necessary knowledge.

SE4. It is my confidence that I will be able to respond to cybersecurity concerns.

SE5. It is my hope that over time, I will gain ever-increasing capabilities in the area of cybersecurity.

Actual learning

AL2. My knowledge of cybersecurity comes from my experience working with computer applications.

AL3. By reading books and journal articles, I have gained knowledge about cybersecurity.

AL4. My school or outside school has taught me about cybersecurity.

Personal relevance

PR1. Protecting my personal data will be easier with cybersecurity knowledge.

PR2. I will be able to better protect sensitive data with cybersecurity knowledge.

PR3. The knowledge of cybersecurity will help me become more aware of cybersecurity.

Behavioral intention

BI1. The future holds many opportunities for me to learn more about cybersecurity.

BI2. Cybersecurity issues will be of utmost importance to me.

BI3. Cyber security, cyber safety, and cyber ethics are issues that I expect to be concerned about in the future.

BI4. It is my intention to spend time in the future learning about cybersecurity.

Funding Open access funding provided by University of Eastern Finland (UEF) including Kuopio University Hospital. No funding information.

Data availability The authors declare that data supporting the findings of this study are available upon request.

Code availability Not applicable.

Declarations

Competing interests The authors declare that they have no competing interests.

References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology, 33*(3), 237–248. https://doi.org/10.1080/0144929X.2012.708787

Adıyaman, M., & Sert, H. (2018). An investigation on teacher candidates' self-efficacy perceptions and attitudes towards computer aided education. *Akdeniz Journal of Education, 1*(2), 189–216. https://doi.org/10.20448/journal.522.2019.54.531.537

Agamba, J., & Keengwe, J. (2012). Pre-service teachers' perceptions of information assurance and cyber security. *International Journal of Information and Communication Technology Education, 8*(2), 94–101. https://doi.org/10.4018/jicte.2012040108

Agudo-Peregrina, Á. F., Hernández-García, Á., & Pascual-Miguel, F. J. (2014). Behavioral intention, use behavior and the acceptance of electronic learning systems: Differences between higher education and lifelong learning. *Computers in Human Behavior, 34*, 301–314. https://doi.org/10.1016/j.chb.2013.10.035

Ahmad, N., Mokhtar, U. A., Fariza Paizi Fauzi, W., Othman, Z. A., Hakim Yeop, Y., & Huda Sheikh Abdullah, S. N. (2019). Cyber Security Situational Awareness among Parents. *Proceedings of the 2018 Cyber Resilience Conference, CRC 2018* 7–8. https://doi.org/10.1109/CR.2018.8626830

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*, 179–211.

Ajzen, I. (2012). The Theory of planned behavior. In Van P. A. M. Lange, A. W. Kruglanski, & E. T. Higgins (Eds.), *Handbook of Theories of Social Psychology* (438–459)

Akgün, Ö. E., & Topal, M. (2015). Information security awareness of the senior teacher students: Sakarya University sample. *Sakarya University Journal of Education, 2*(5), 98–121. https://doi.org/10.1016/SUJE.2021.12.040

Amankwa, E. (2021). Relevance of Cybersecurity Education at Pedagogy Levels in Schools. *Journal of Information Security, 12*(04), 233–249. https://doi.org/10.4236/jis.2021.124013

Amusa, J. O., & Ayanwale, M. A. (2021). Partial Least Square Modeling of Personality Traits and Academic Achievement in Physics. *Asian Journal of Assessment in Teaching and Learning, 11*(2), 77–92. https://doi.org/10.37134/ajatel.vol11.2.8.2021

Angela, M, Borgert Nele,Friedauer Jennifer,Böse, Imke and Elson, M. (2021). The Study of Cybersecurity Self-Efficacy : A Systematic Literature Review of Methodology. *Symposium on Usable Privacy and Security*, 1–4. https://www.usenix.org/system/files/soups21-abstract-poster56-borgert.pdf

Ayanwale, M. A., Sanusi, I. T., Adelana, O. P., Aruleba, K. D., & Oyelere, S. S. (2022). Teachers' readiness and intention to teach artificial intelligence in schools. *Computers and Education: Artificial Intelligence, 3*, 100099.

Ayanwale, M. A., Mosia, P. A., Molefi, R. R., & Shata, L. (2023). Reliability Components of Online Teaching and Learning Tools in Lesotho Higher Education Institutions : A Systematic Review. *Pertanika Journal of Science and Technology, 31*(1), 595–614. https://doi.org/10.47836/pjst.31.1.34

Ayanwale, M. A. & Sanusi, I. T. (2023). Perceptions of STEM vs. Non-STEM Teachers toward Teaching Artificial Intelligence. In 2023 IEEE AFRICON Conference. (Accepted). IEEE

Bagozzi, R. P. (1981). Attitudes, intentions, and behavior: A test of some key hypotheses. *Journal of Personality and Social Psychology, 41*(4), 607. https://doi.org/10.1037/0022-3514.41.4.607

Bodea, C. N., Dascalu, M. I., & Cazacu, M. (2019). Increasing the Effectiveness of the Cybersecurity Teaching and Learning By Applying Activity Theory and Narrative Research. *Issues In Information Systems, 20*(3), 186–193. https://doi.org/10.48009/3_iis_2019_186-193

Celik, V., & Yesilyurt, E. (2013). Attitudes to technology, perceived computer self-efficacy and computer anxiety as predictors of computer supported education. *Computers & Education, 60*(1), 148–158. https://doi.org/10.1016/J.COMPEDU.2012.06.008

Chakraborty, S. (2019). Malware attack and Malware Analysis : A Research. *International Journal of Scientific Research in Computer Science, 5*(3), 268–272. https://doi.org/10.32628/CSEIT195379

Childers, G., Linsky, C. L., Payne, B., Byers, J., & Baker, D. (2022). K-12 Educators' Self-Confidence in Designing and Implementing Cybersecurity Lessons. *Computers and Education Open*, 100119.

Chiua, W. Y., & Hob, H. F. (2019). Time to Educate the Educators: An Evaluation of Cyber Security Knowledge Awareness and Implementation for School Teachers in Taiwan. *Paper Presented at the International Conference on Technology and Social Science 2019, Kiryu, Japan.*

Dawson, K., Antonenko, P., Xu, Z., & Wusylko, C. (2022). Promoting Interdisciplinary Integration of Cybersecurity Knowledge, Skills and Career Awareness in Preservice Teacher Education. *Journal of Technology and Teacher Education*, *30*(2), 275–287. https://www.learntechlib.org/primary/p/221089/.

Erbschloe, M. (2019). *Social Engineering : Hacking Systems, Nations, and Societies*. CRC Press. CRC Press. https://doi.org/10.1201/9780429322143

Erol, O., Şahin, Y. L., Yılmaz, E., & Haseski, H. İ. (2015). Personal Cyber Security Provision Scale development study Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması. *Journal of Human Sciences, 12*(2), 75–91. https://doi.org/10.14687/ijhs.v12i2.3185

Feng, W. C., Liebman, R., Delcambre, L., Lupro, M., Sheard, T., Britell, S., & Recktenwald, G. (2017). {CyberPDX}: A Camp for Broadening Participation in Cybersecurity. In *2017 USENIX Workshop on Advances in Security Education (ASE 17)*.

Frymier, A. B., & Shulman, G. M. (1995). "What's in it for me?": Increasing content relevance to enhance students' motivation. *Communication Education, 44*(1), 40–50.
Furnell, S., & Vasileiou, I. (2017). Security education and awareness: Just let them burn? *Network Security, 12*, 5–9. https://doi.org/10.1016/S1353-4858(17)30122-8
Furnell, S., Bryant, P., & Phippen, A. (2007). Assessing the security perceptions of personal Internet users. *Computers & Security, 26*(5), 410–417. https://doi.org/10.1016/j.cose.2007.03.001
Group World Bank. (2020). Lesotho Digital Economy Diagnostic (Issue February). www.worldbankgroup.org
Günbatar, M. S., & Bakırcı, H. (2019). STEM teaching intention and computational thinking skills of pre-service teachers. *Education and Information Technologies, 24*, 1615–1629.
Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate Data Analysis* (7th ed.). Pearson.
Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2014). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. Sage.
Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM) (2nd ed.). Sage.
Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM) (3rd ed.). Sage.
Handeli, K., & Robila, S. (2018). A Cybersecurity High School Curriculum Course. In *Society for Information Technology & Teacher Education International Conference* (864–869). Association for the Advancement of Computing in Education (AACE).
Haseski, H. İ. (2020). Cyber security skills of pre-service teachers as a factor in computer-assisted education. *International Journal of Research in Education and Science, 6*(3), 484–500. https://doi.org/10.46328/ijres.v1i1.1006
Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *J. of the Acad. Mark. Sci., 43*, 115–135. https://doi.org/10.1007/s11747-014-0403-8
Jin, G., Tu, M., Kim, T. H., Heffron, J., & White, J. (2018). Game based cybersecurity training for high school students. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education* (68–73).
Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce, 28*(3), 269–282. https://doi.org/10.1080/10919392.2018.1484598
Kara, İ, & Aydos, M. (2019). The ghost in the system: Technical analysis of remote access trojan. *International Journal on Information Technologies & Security, 11*(1), 73–84.
Karacı, A., Akyüz, H. İ, & Bilgici, G. (2017). Investigation of cyber security behaviors of university students. *Kastamonu Education Journal, 25*(6), 2079–2094.
Karagozlu, D. (2020). Determination of cyber security ensuring behaviours of pre-service teachers. *Cypriot Journal of Educational Sciences, 15*(6), 1698–1706. https://doi.org/10.18844/cjes.v15i6.5327
Kemper, G. (2019). Improving employees' cyber security awareness. *Computer Fraud and Security, 2019*(8), 11–14. https://doi.org/10.1016/S1361-3723(19)30085-5
Konak, A. (2018). Experiential learning builds cybersecurity self-efficacy in K-12 students. *Journal of Cybersecurity Education, Research and Practice, 1*, 6.
Kritzinger, E. (2016). Short-term initiatives for enhancing cyber-safety within South African schools. *South African Computer Journal, 28*(1), 1–17.
Kritzinger, E., Bada, M., & Nurse, J. R. (2017). A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK. In *IFIP World Conference on Information Security Education* (pp. 110–120). Springer, Cham.
Lesotho News Agency. (2020). *Cyber Crime A Risk To Lesotho*. http://www.gov.ls/cyber-crime-a-risk-to-lesotho/
Li, K., Li, Y., & Franklin, T. (2016). Preservice teachers' intention to adopt technology in their future classrooms. *Journal of Educational Computing Research, 54*(7), 946–966.
Li, X., Jiang, M. Y. C., Jong, M. S. Y., Zhang, X., & Chai, C. S. (2022). Understanding Medical Students' Perceptions of and Behavioral Intentions toward Learning Artificial Intelligence: A Survey Study. *International Journal of Environmental Research and Public Health, 19*(14), 8733. https://doi.org/10.3390/ijerph19148733
London, UK, SageWeerathunga, P. R., Samarathunga, W. H. M. S., Rathnayake, H. N., Agampodi, S. B., Nurunnabi, M., & Madhunimasha, M. M. S. C. (2021). The COVID-19 pandemic and the

acceptance of E-learning among university Students: The Role of Precipitating Events. *Education Sciences, 11*(8), 436. https://doi.org/10.3390/educsci11080436

Loukomies, A., Pnevmatikos, D., Lavonen, J., Spyrtou, A., Byman, R., Kariotoglou, P., & Juuti, K. (2013). Promoting students' interest and motivation towards science learning: The role of personal needs and motivation orientations. *Research in Science Education, 43*(6), 2517–2539.

Mack, M. (2018). Cyber security. In UK: ED-Tech Press. https://www.google.com/search?q=Mack%2C+M.+%282018%29.+Cyber+security.+UK%3A+ED-Tech+Press.&sxsrf=ALiCzsa1HaQ0FV62NOyHoN5B9ikEJxN2pw%3A1670511700821&ei=VPyRY9HmMYnLgAbO7YWYBA&ved=0ahUKEwjR4JSEper7AhWJJcAKHc52AUMQ4dUDCA8&uact=5&oq=Mack%2C+M.+%282018%29.+Cy

Ministry of Education and Training. (2009). *Curriculum and assessment policy framework: Education for individual and social development*. *June*, 1–34.

Mosola, N. N., Moeketsi, K. F., Sehobai, R., & Pule, N. (2019). Cybersecurity Protection Structures: The Case of Lesotho. *International Journal of Computer and Information Engineering, 13*(3), 158–163.

Mourning, C., Juedes, D., Hallman-Thrasher, A., Chenji, H., Kaya, S., & Karanth, A. (2022). Reflections of Cybersecurity Workshop for K-12 Teachers and High School Students. In *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education 2* 1127–1127).

Mourning, C. Chenji, H., Hallman-Thrasher, A., Kaya, S., Abukamail, N., Juedes, D. and Karanth, A. (2023). Reflections of Cybersecurity Workshop for K-12 Teachers. *In Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 1* (Accepted).

Moyo, M., Sadeck, O., Tunjera, N., & Chigona, A. (2022). Investigating Cyber Security Awareness Among Preservice Teachers During the COVID-19 Pandemic. Lecture Notes in Business Information Processing, 437 LNBIP, 527–550. https://doi.org/10.1007/978-3-030-95947-0_38

Moyo, H. (2022). Lesotho's cyber law not well thought-out, potentially violates human rights: Analysts. Lesotho Times. https://lestimes.com/lesothos-cyber-law-not-well-thought-out-potentially-violates-human-rights-analysts/.

Nelson B. (2022). Top Security Threats of Smartphones (2022). Retrieved on 03.01.2022 from https://www.rd.com/article/mobile-security-threats/

Neumann, L. (2017). Human factor in IT security. In F. Abolhassan (Ed.), Cyber security. Simply. Make it happen. Leveraging digitalization through IT security. Switzerland: Springer, 75–86.

Pencheva, D., Hallett, J., & Rashid, A. (2020). Bringing cyber to school: Integrating cybersecurity into secondary school education. *IEEE Security & Privacy, 18*(2), 68–74. https://doi.org/10.1109/MSEC.2020.2969409

Prasad, R., & Rohokale, V. (2020). Cyber Security: The Lifeline of Information and Communication Technology. In Switzerland: Springer. https://link.springer.com/content/pdf/10.1007/978-3-030-31703-4.pdf%0Ahttp://link.springer.com/10.1007/978-3-030-31703-4.

Prem, S. P., & Reddy, B. I. (2019). Phishing and anti-phishing techniques. *International Research Journal of Engineering and Technology, 6*(7), 1446–1452.

Pusey, P., & Sadera, W. A. (2011). Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference. *Journal of Digital Learning in Teacher Education, 28*(2), 82–85. https://doi.org/10.1080/21532974.2011.10784684

Pye, K. (2016). *Teaching cybersecurity in K-12 schools*. A Capstone Project Submitted to the Faculty of Utica College.

Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology, 10*(5), 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393

Sanusi, I. T., & Olaleye, S. A. (2022). An insight into cultural competence and ethics in K-12 artificial intelligence education. In *2022 IEEE global engineering education conference (EDUCON)* (pp. 790–794). IEEE.

Sanusi, I. T., Olaleye, S. A., Agbo, F. J., & Jatileni, C. N. (2021). Global Readiness for Immersive Virtual Space Adoption: The Case of Ohyay. In *2021 XVI Latin American Conference on Learning Technologies (LACLO)* (pp. 244–251). IEEE.

Schreiber, J. B., Nora, A., Stage, F. K., Barlow, E. A., & King, J. (2006). Reporting structural equation modeling and confirmatory factor analysis results: A review. *The Journal of Educational Research, 99*(6), 323–338. https://doi.org/10.3200/JOER.99.6.323-338

Schwarzer, R., Schmitz, G. S., & Daytner, G.T. (1999). The Teacher self-efficacy scale. Retrieved from http://userpage.fu-berlin.de/~health/teacher_se.htm

Serianu. (2018). Africa Cyber Security Report - Lesotho Cyber Security Skills Gap. https://www.serianu.com/downloads/LesothoCyberSecurityReport2018.pdf

Subramaniam, S. R. (2017). Cyber security awareness among Malaysian pre-university students. *Proceeding of the 6th Global Summit on Education*, 1–14.

Suwarna Rami Subramaniam. (2018). Cyber Security Awareness Among Malaysian Pre-University Students | Request PDF. Paper Presented at the *6th Global Summit on Education, Kuala Lumpur, Malaysia*. https://www.researchgate.net/publication/323382802_cyber_security_awareness_among_malaysian_pre-university_students

The Economic Times (2022). 4 in 10 smartphones are vulnerable to cyber attacks. Here's how to protect your device. Retrieved on 03.01.2023 from https://economictimes.indiatimes.com/magazines/panache/can-your-mobile-phone-get-a-virus-yes-and-youll-have-to-look-carefully-to-see-the-signs/articleshow/91314693.cms?from=mdr

Tseng, S. S., Yang, T. Y., Shih, W. C., & Shan, B. Y. (2022). Building a self-evolving iMonsters board game for cyber-security education. *Interactive Learning Environments*, 1–19. https://doi.org/10.1080/10494820.2022.2120015

Ustundag, M. T., Guneş, E., & Bahcivan, E. (2017). Turkish adaptation of digital literacy scale and investigating pre-service science teachers' digital literacy. *Journal of Education and Future, 12*, 19–29.

van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior, 75*, 547–559. https://doi.org/10.1016/j.chb.2017.05.038

Vennix, J., Den Brok, P., & Taconis, R. (2017). Perceptions of STEM-based outreach learning activities in secondary education. *Learning Environments Research, 20*(1), 21–46.

Vennix, J., den Brok, P., & Taconis, R. (2022). Motivation style of K–12 students attending outreach activities in the STEM field: a person-based approach. *Learning Environments Research*, 1–15.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 33*, 97–102.

Walters, R., Trakman, L., & Zeller, B. (2019). *Data Protection Law A Comparative Analysis of Asia Pacific and European Approaches*. Springer. https://doi.org/10.2139/ssrn.3463731

Weerathunga, P. R., Samarathunga, W. H. M. S., Rathnayake, H. N., Agampodi, S. B., Nurunnabi, M., & Madhunimasha, M. M. S. C. (2021). The COVID-19 pandemic and the acceptance of e-learning among university students: The role of precipitating events. *Education Sciences, 11*(8), 436.

Wirtz, J. J. (2017). The Cyber Pearl Harbor. *Intelligence and National Security, 32*(6), 758–767. https://doi.org/10.1080/02684527.2017.1294379

World Economic Forum (2020). Unchecked cyberattacks 'are growing threat to fragile global economy'. Retrieved from https://www.weforum.org/press/2023/01/unchecked-cyberattacks-are-growing-threat-to-fragile-global-economy/. Accessed 15 May 2023

Yan, Z., Xue, Y., & Lou, Y. (2021). Risk and protective factors for intuitive and rational judgment of cybersecurity risks in a large sample of K-12 students and teachers. *Computers in Human Behavior, 121*, 106791.

Yeşilyurt, E., Ulaş, A. H., & Akan, D. (2016). Teacher self-efficacy, academic self-efficacy, and computer self-efficacy as predictors of attitude toward applying computer-supported education. *Computers in Human Behavior, 64*, 591–601. https://doi.org/10.1016/j.chb.2016.07.038

Yett, B., Hutchins, N., Stein, G., Zare, H., Snyder, C., Biswas, G., ... & Lédeczi, Á. (2020). A hands-on cybersecurity curriculum using a robotics platform. In *Proceedings of the 51st ACM Technical Symposium on Computer Science Education* (1040–1046).

Yigilt, M. F., & Seferoğlu, S. S. (2019). Öğrencilerin Siber Güvenlik Davranışlarının Beş Faktör Kişilik Özellikleri ve Çeşitli Diger Değişkenlere Göre Investigating Students ' Cyber Security Behaviors in Relation to Big Five Personality Traits and Other Various Variables. *Mersin University Journal of the Faculty of Education, 15*(1), 186–215.

Zucule de Barros, M. J., & Lazarek, H. (2018). A cyber safety model for schools in Mozambique. *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy*, *2018-Janua*, 251–258. https://doi.org/10.5220/0006573802510258

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł, Cetin, F., & Basim, H. (2020). Cyber security awareness, knowledge and behavior: A comparative study. *The Journal of Computer Information Systems, 00*(00), 1–16. https://doi.org/10.1080/08874417.2020.1712269

Authors and Affiliations

Musa Adekunle Ayanwale[1] · Ismaila Temitayo Sanusi[2] · Rethabile Rosemary Molefi[3] · Adekunle Olusola Otunla[4]

✉ Ismaila Temitayo Sanusi
ismaila.sanusi@uef.fi

Musa Adekunle Ayanwale
ayanwalea@uj.ac.za

Rethabile Rosemary Molefi
rethabile68@gmail.com

Adekunle Olusola Otunla
otunla.adekunle@lcu.edu.ng

[1] Department of Science and Technology Education, University of Johannesburg, Johannesburg, South Africa

[2] School of Computing, University of Eastern Finland, P.O.Box 111, 80101 Joensuu, Finland

[3] Department of Educational Foundations, National University of Lesotho, Lesotho, Lesotho

[4] Department of Mass Communication and Media Technology, Faculty of Communication and Information Science, Lead City University, Ibadan, Nigeria