African Multidisciplinary Journal of Development (AMJD)

Page: 70-84 https://amjd.kiu.ac.ug/

# PRESERVICE MATHEMATICS TEACHERS' KNOWLEDGE, ATTITUDE, AND PRACTICE OF CYBERSECURITY

**[1] Michael A. Adewusi, [2]Adeneye O. A. Awofala, [3]Gbolahan E. Awofala & [4]O.V. Fakuade**

[1] Department of Information Technology, School of Mathematics and Computing, Kampala International University, Kampala, Uganda, Email: mikeade3000@yahoo.com

[2] Department of Access, Special Needs, and Early Childhood Education, College of Education, Open, and Distance Learning, Kampala International University, Kampala, Uganda, Email: awofala.adeneye@kiu.ac.ug

[3] Department of Computer and Information Science, College of Science and Information Technology, Tai Solarin University of Education, Ijagun, Nigeria, Email: edawofal@gmail.com

[4] Department of Distance Education, College of Education, Open, and Distance Learning, Kampala International University, Kampala, Uganda, Email: lubusayo.fakuade@kiu.ac.ug

## Abstract

Associations between knowledge, attitude, and practice (KAP) are extensively documented in the international literature that relates to health and construction occupations. While few investigations had been carried out on KAP of cybersecurity in the international literature, such studies are scarce in Nigeria. Therefore, this study investigated the predictive association betwixt knowledge, attitude, and practice of cybersecurity among preservice mathematics teachers in Nigeria through a cross-sectional, correlational research design. The sample included 550 preservice mathematics teachers in one coeducational public university in Nigeria and data were collected using one psychometrically sound instrument (Cronbach alpha=0.97). Three research questions were stated and answered using Pearson product-moment correlation, multiple regression analysis, and independent samples t-test at 5% level of significance. The results showed that there was a significant relationship between knowledge and attitude ($r = 0.98$, $p<0.05$), between knowledge and practice ($r = 0.27$, $p<0.05$), and between attitude and practice of cybersecurity ($r = 0.16$, $p<0.05$). The ANOVA regression analysis revealed a significant association between knowledge, attitude, and practice of cybersecurity ($F(2, 547) = 163.67$, $p=0.000$) and knowledge and attitude produced a joint contribution of 37.4% to the prediction of cybersecurity practice. The attitude showed the highest contribution ($\beta=3.23$) and followed by knowledge ($\beta=3.02$). The regression equation is: Practice = 19.03 + 3.81 attitude + 3.22 knowledge. Gender had a significant influence on preservice mathematics teachers' knowledge ($t548=-4.74$, $p=0.00$) and attitude ($t548=-4.42$, $p=0.00$) toward cybersecurity in favour of males. However, gender had no significant influence on preservice mathematics teachers' practice of cybersecurity ($t548=-1.25$, $p=0.21$). In conclusion, effort should be made to explore how cybersecurity education can be integrated across subjects or courses, not just mathematics.

**Keywords:** Attitude, Cybersecurity, Knowledge, Mathematics, Practice, Preservice teacher

## Introduction

No doubt, the world is agog with people that work and live digitally and virtually. In July 2024, there were 5.45 billion internet users worldwide, which is about 67.1% of the world population (Statista, 2024). While the online transformation carries a lot of advantages, it also has risks connecting to the confidentiality, integrity, and availability of virtual data. It is clear that many people worldwide have been victims of cyberthreats in form of malware, identity theft, spam, and phising (Sfakianakis,

Douligeris, & Marinos, 2019). The Nigerian populace seems to be less fortified against many of these cyberthreats. In 2020, 73% of Nigerians were victims of cybercrime (Nigerian Cybercrime Report, 2020). 61% of Nigerian businesses fell victim to cyberattacks (PwC Nigeria Cybersecurity Survey, 2020). 45% of mobile phone users in Nigeria fell victim to mobile-related cyberthreats (Kaspersky Mobile Threats Report, 2020). 25% of Nigerian children have experienced cyberbullying or online harassment (UNICEF Nigeria Report, 2020). In 2019, 36% of Nigerians were victims of online scam (Nigerian National Cyber Security Awareness Survey, 2019). All these statistics show that a significant portion of the Nigerian population is vulnerable to cyberthreats and that there is a wide gap between how people view their cybersecurity skills and their cybersecurity behaviour. This study is aimed at understanding why people either do or do not exhibit cybersecure behaviours. Clearly, knowledge is a necessary condition for engaging in good behaviour in any given context (de Kok, Oosting & Spruit, 2020). Possessing good knowledge is an antidote for ignorance and a way of bringing about behavioural modification.

In the field of cybersecurity, knowledge is needed in order to comprehend cyberthreats and to recognise the connected risks (Ben-Asher, & Gonzalez, 2015; Bitton, Boymgold, Puzis, & Shabtai, 2019). As necessary as knowledge of cybersecurity is, it is not enough to explain behaviour (Ahlan, Lubis, & Lubis, 2015; Bada, Sasse, & Nurse, 2017; Caldwell, 2016). A person understanding of cybersecurity controls and cyberthreats may not translate to executing the relevant cybersecurity controls (Siponen, Mahmood, & Pahnila, 2014). Thus, in addition to knowledge, attitude is very vital in predicting behaviour (Aronson, & Wilson, 2017; Fiske & Taylor, 2013). Prior investigation on cybersecurity behaviour showed that attitude had a significant influence on intended behaviour (Lebek, Uffen, Neumann, Hohler, & Breitner, 2014; Sommestad, Hallberg, Lundholm, & Bengtsson, 2014). While knowledge and attitude have been assessed both separately and together in prior investigations on cybersecure behaviour (Kruger, & Kearney, 2006; Parsons, Calic, Pattinson, Butavicius, McCormac, & Zwaans, 2017), they were not assessed in conjunction with cybersecurity practices. Cybersecurity practices refer to specific habits and actions a person or an organisation takes to protect theirself from cyberthreats and vulnerabilities.

This study is important because assessing knowledge, attitude and practices (KAP) of cybersecurity may help in identifying gaps and areas for improvement in cybersecurity behaviours and awareness. Assessing KAP could also inform the enactment of effective cybersecurity awareness, training, and education programmes. This study, therefore, adopted a KAP assessment of cybersecurity. The research question is as follows: What is the contribution of cybersecurity knowledge and attitude in explanation of variance in cybersecurity practices?

## Knowledge of cybersecurity

Knowledge refers to the skills, facts, and information that a person acquires through training, education, and experience. Knowledge is a necessary condition and foundation for exhibiting correct behaviour in a given context (de Kok, Oosting & Spruit, 2020). In the context of cybersecurity, knowledge includes familiarity with common cyberthreats and vulnerabilities (Ben-Asher & Gonzalez, 2015), understanding cybersecurity concepts and terminology (de Kok, Oosting & Spruit, 2020), and understanding of risk management and incident response (Plessis & Solms, 2002). Nine types of knowledge are identifiable and they include conditional knowledge-knowledge of conditions and contexts; dispositional knowledge-knowledge that influences attitudes and behaviours; embodied knowledge-knowledge that is embedded in physical actions and habits, and meta-cognitive knowledge-knowledge of one's own thought processes. Others include propositional knowledge-knowledge of relationships between concepts; declarative knowledge-knowledge of facts, concepts, and principles;


ISSN: 2518-2951 https://doi.org/10.59568/AMJD-2025-13-2-08 African Multidisciplinary Journal of Development (AMJD)

procedural knowledge-knowledge of procedures, processes, and protocols; tacit knowledge-personalised , experiential knowledge that is difficult to share and document, and explicit knowledge-documented and easily shared knowledge. Knowledge can be acquired at different levels and these levels according to the revised Bloom's taxonomy (Krathwohl, 2002) include (1) remember, (2) understand, (3) apply, (4) analyse, (5) evaluate, and (6) Create. In the field of cybersecurity, remembering is equivalent to identifying common cyberthreats and vulnerabilities and recalling cybersecurity terminology and concepts. Understanding requires explaining the importance of cybersecurity and describing the impact of cyberthreats on individuals and organisations. Applying requires implementing cybersecurity measures to protect against threats and applying cybersecurity principles to real-world scenarios. Analysing involves identifying and analysing cyberthreats and vulnerabilities and comparing and contrasting different cybersecurity approaches. Evaluating refers to assessing the risk of cyberthreats and vulnerabilities, justifying the need for cybersecurity investments and assessing cybersecurity policies and procedures. Creating involves designing and implementing comprehensive cybersecurity plans, integrating cybersecurity into existing systems and processess, and developing new cybersecurity solutions and tools. While the first four levels of the revised Bloom taxonomy require making an inventory of cyberthreats and analysing them (de Kok, Oosting & Spruit, 2020), the last two levels involve meta-knowledge and developing new systems and models and thus would not be considered in this study. The assessment of knowledge in prior cybersecurity investigations were carried out on samples including working adults (Herath, & Rao, 2009; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014), seniors (Arfi, & Agarwal, 2014; Cook, Szewczyk, & Sansurooah, 2011; Grimes, Hough, Mazur, & Signorella, 2010), and children (Giannakas, Kambourakis, & Gritzalis, 2015; Tirumala, Sarrafzadeh, & Pang, 2016) with little or none on preservice mathematics teachers. While people have certain knowledge regarding cybersecurity controls and cyberthreats (Slusky & Partow-Navid, 2012), they are not totally secured against cyberthreats (de Kok, Oosting & Spruit, 2020). Therefore, possession of cybersecurity knowledge is not enough to provide right shield against cyberthreats. Thus, attitude towards cybersecurity is also a very vital factor in predicting and explaining behaviour towards cybersecurity. Knowledge can shape attitude by increasing awareness of risks and benefits of cybersecurity.

## Attitude towards cybersecurity

Attitude is defined in this study as an individual's emotional or mental disposition towards an object, idea or situation which can be positive or negative. Awofala (2020) gave three components of attitude to include: behavioural component-actions, intentions, and behaviours towards the object or situation, cognitive component- beliefs, thoughts, and attributes about the object or situation, and affective component- emotions, feelings, and values connected with the object or situation. Other components include conative which refers to motivations and commitments to act on the object or situation (Hagger & Chatzisarantis, 2005) and evaluative component defined as assessments and judgments about the object or situation including likes and dislikes (Bohner & Wanke, 2002). In the field of cybersecurity, these components could appear in the judgments about the effectiveness of cybersecurity measures (evaluative), motivation to learn and implement cybersecurity best practices (conative), actions taken to protect oneself and one's organisation against cyberthreats (behavioural), concern and worry about cybersecurity risks (affective), and understanding cybersecurity risks and threats (cognitive). Attitude can either be positive or negative. A positive attitude towards cybersecurity may include being responsible and accountable, being aware of the risks and consequences, being committed to following best practices, being open to learning and improvement, and being proactive and vigilant. A negative attitude towards cybersecurity can be manifested in the area of irresponsible behaviour, lack of concern


ISSN: 2518-2951 https://doi.org/10.59568/AMJD-2025-13-2-08 African Multidisciplinary Journal of Development (AMJD)

and awareness, resistance to change and learning, skepticism and denial, and complacency and apathy. A person can display both positive and negative attitude towards an object thereby having a conflicting attitude. For instance, a person may feel that cybersecurity is not a pressing concern, despite working with sensitive data. This shows the case of complacency versus vigilance. Attitude can influence knowledge by motivating individuals to learn more about cybersecurity. In the present study, effort is made to understand the predictive influence of knowledge and attitude on consistent adoption of cybersecurity best practices.

## Practice toward cybersecurity

Cybersecurity practices refer to the specific habits and actions that organisations and individuals take to make themselves immune to cyber vulnerabilities and threats. These actions and habits may include compliance with cybersecurity standards and regulations (Hartwig, & Reuter, 2022), cybersecurity awareness and training (Antunes, Silva, & Marques, 2021; Bhatnagar, & Pry, 2020), continuous monitoring and vulnerability assessment (Hatzivasilis, Ioannidis, Smyrlis, Spanoudakis, Frati, Goeke, Hildebrandt, Tsakirakis, Oikonomou, Leftheriotis, & Koshutanski, 2020), network segmentation and isolation to reduce the spread of cyberthreats (Mamonov, & Benbunan-Fich, 2018), and user access control and authentication (Szumski, 2018). Others include incident reporting and response (Szumski, 2018), secure configuration of devices and networks (Hatzivasilis et al., 2020), data backup and recovery (Szumski, 2018), installing antivirus software and firewalls (Szumski, 2018), safe browsing habits (Szumski, 2018), software updates and patching (Szumski, 2018), and password management (Hartwig, & Reuter, 2022). Prior investigations on Information Security Awareness had used Knowledge, Attitude, and Behavior (KAB) (Kruger & Kearney, 2006). In KAB, increase in knowledge could lead to better attitudes which might in turn produce enhanced behavioural security (Al-Nuaimi & Uzun, 2023).

However, little is known regarding the Knowledge, Attitude, and Practices (KAP) model to measure cybersecurity in Nigeria. The KAP assessment might be beneficial in revealing the knowledge of cybersecurity concepts among the participants. It could also reveal the attitude of the participants towards cybersecurity risks and the degree of inadequate practices such as infrequent software updates and weak password among the participants. This study investigated knowledge and attitude as predictors of cybersecurity practice. Cybersecurity practices are important for protecting sensitive information, preventing financial loss, maintaining privacy, building trust, compliance with regulations, protecting reputation, ensuring business continuity, safeguarding national security, preventing cyberbullying, and staying ahead of threats (Szumski, 2018; Mamonov, & Benbunan-Fich, 2018; Hartwig, & Reuter, 2022). The enactment of husky cybersecurity practices, could enable organisations and individuals to significantly lessen the danger of cyber attacks and ensure the protection of their invaluable privacy, reputation, and assets. The present study used cybersecurity practice because it is more amenable to questionnaire-based measurements. In this case, participants were allowed to fully express themselves regarding the practice related to cybersecurity.

## Gender differences in KAP of cybersecurity

Gender is defined as socially constructed expectations, behaviours, and roles connected with being female or male. It is a complex and multifactor construct that goes beyond biological sex and embraces gender norms-unspoken rules that guide how a person should behave based on their gender, gender stereotypes-overly simplistic and often inaccurate beliefs about what men and women are like, and gender roles-societal expectations and norms around what is considered masculine or feminine. Gender also encompasses gender expression-how a person presents themselves to the world, and gender


ISSN: 2518-2951 https://doi.org/10.59568/AMJD-2025-13-2-08 African Multidisciplinary Journal of Development (AMJD)

identity- a person's internal sense of being female, male or something else. Research has shown some gender differences in KAP of cybersecurity (Ruggiero & Boehm, 2016; Aikelewicz & Matusiak, 2017; Shah & Woodward, 2018; Wang & Wang, 2019; Knezek & Christensen, 2016; Gratian, Bandi, Cukier, Dykstra, & Ginther, 2018). Women tend to have lower levels of cybersecurity awareness and knowledge than men. Women are more likely to be concerned about cybersecurity risks and take fewer risks online than men (Knezek & Christensen, 2016). Women are more likely to use strong passwords, enable two-factor authentication, and keep software up-to-date than men (Intel Security Group, 2017; Symantec Corporation, 2019). Women may be more influenced by social norms and relationships when it comes to cybersecurity behaviours than men (Kray, & Waaijenborg, 2019). Men tend to be more confident in their cybersecurity abilities and take more risks online than women (Norton, 2019). Women may be more likely to use language related to security and protection, while men may use language related to technology and functionality (Taylor, & Hutton, 2018; Mouheb, & Zulkernine, 2019). Women are underrepresented in the cybersecurity workforce, but show increasing interest in pursuing cybersecurity careers (McKinsey, 2020).

The major goal of this study was to examine preservice mathematics teachers' self-reported knowledge, attitudes, and practices of cybersecurity. In particular, the investigation examined the association between preservice mathematics teachers' knowledge, attitudes and practices of cybersecurity. The predictive influence of knowledge and attitude towards the explanation of variance in preservice mathematics teachers' practice of cybersecurity was examined. Gender as a factor in preservice mathematics teachers' knowledge, attitudes, and practices of cybersecurity was also investigated. This study found it worthy to connect mathematics education with cybersecurity for the following reasons. First, cryptography, a fundamental aspect of cybersecurity, relies so much on mathematical concepts such as geometry, algebra, and number theory. Second, mathematics education develops problem-solving skills, critical thinking, and analytical reasoning (Ajao & Awofala, 2024; Ajao & Awofala, 2022), essential for cybersecurity professionals. Third, mathematics teaches logical reasoning (Okunuga, Awofala & Osarenren, 2020; Awofala & Lawal, 2022), necessary for understanding cybersecurity principles and protocols. Lastly, preservice mathematics teachers should be prepared to address cybersecurity concerns and promote online safety in their future classrooms.

## Research Questions

The following research questions were answered in this study.

RQ1. What is the relationship between preservice mathematics teachers' knowledge, attitude and practice of cybersecurity?

RQ2. What is the predictive influence of knowledge and attitude towards the explanation of variance in preservice mathematics teachers' practice of cybersecurity?

RQ3. What is the influence of gender on preservice mathematics teachers' knowledge, attitude, and practice of cybersecurity?

## Methods

### Research design

The study adopted a quantitative research paradigm of a cross-sectional descriptive survey of a correlational type (Awofala, Modiu, Fatade & Arigbabu, 2024; Awofala, Lawal, Arigbabu, & Fatade, 2022). This research design allowed the authors to investigate the relationships among the variables of the study. This study was non-experimental as the authors did not manipulate variables in the study.


ISSN: 2518-2951 https://doi.org/10.59568/AMJD-2025-13-2-08 African Multidisciplinary Journal of Development (AMJD)

## Participants

The total respondents composed of 550 preservice mathematics teachers in the Department of Science Education, Faculty of Education, University of Lagos. There are five teaching units in the Department of Science Education and a purposive sampling technique was used to select mathematics education teaching unit. All the 550 preservice mathematics teachers were used as the sample of the study. This sample size was considered sufficient assuming a margin of error of 0.05 and a confidence level of 0.95. There were 260 male and 240 female preservice mathematics teachers and their age ranged from 16 to 31 years ($Mean_{age}$=24.5 years, SD=3.1 years). 90% of the sample were Yorubas while the remaining 10 % were Ibos. The Yorubas dominate Lagos, the centre of excellence and Nigeria's commercial nerve centre.

## Instrument for Data Collection

One research instrument tagged Knowledge, Attitude and Practices of Cybersecurity Scale (KAPCS) was used for data collection in this study. The instrument was adapted from previously validated scales (Bognár, & Bottyán, 2024; Chen, & Li, 2017; Howard, 2018; Li, & Chen, 2019; Parsons, McCormac, & Butavicius, 2018a). The KAPCS contained 30 items where 10 items measured Knowledge, 10 items measured Attitude while the remaining 10 items measured Practice of cybersecurity. The items were anchored on a five-point Likert scale ranging from 5-strongly agree, 4-agree, 3-undecided, 2-disagree to 1-strongly disagree for positive statements while the reverse was the case for negatively worded items. The items of the instrument were pilot-tested with a small sample of 90 students not part of the main sample and the computed Cronbach alpha value was 0.97. This value was adjudged good for the study. The following reliability coefficients of 0.96, 0.98, and 0.99 were computed for Knowledge, Attitude, and Practice respectively.

## Procedure for Data Collection

The KAPSC was loaded on a Google Forms for easy distribution. This mode of data collection was considered because it is easy to create and share, it is highly accessible so far there is internet connection, it provides real-time data, it is mobile-friendly and free to use, and it provides automatic data organisation. Before the real time data collection, the participants responded to informed consent and all the 520 preservice mathematics teachers indicated their willingness and readiness to assist in the process of data collection. The participants were told that their participation was voluntary and that they could withdraw from the data collection exercise at any stage of the process. The following ethical considerations which include informed consent, confidentiality, anonymity, voluntary participation, no harm or risk, debriefing, data security, transparency, avoiding bias, compliance with regulations, respect for participants, and cultural sensitivity were all considered and carried out in this study.

## Data Analysis

The data collected through the Google Forms were transferred into the SPSS version 25 for data analysis. SPSS was considered in this study because it ensures reliable and valid results, it allows for efficient data cleaning, transformation, and manipulation, it has a user-friendly interface, and has data analysis capabilities. All statistical test were carried out at 5% level of significance. Research question one was answered using the Pearson Product Moment Correlation. Research question two was answered using the multiple regression analysis while the independent samples t-test was used to answer research question three. Mean and standard deviation were precursor statistics.


ISSN: 2518-2951 https://doi.org/10.59568/AMJD-2025-13-2-08 African Multidisciplinary Journal of Development (AMJD)

## Results

**Research Question One:** What is the relationship between preservice mathematics teachers' knowledge, attitudes and practices of cybersecurity?

**Table 1. Mean, standard deviation and correlation matrix showing the relationship between preservice mathematics teachers' knowledge, attitude, and practice of cybersecurity**

| Construct | K | A | P |
|---|---|---|---|
| 1. Knowledge (K) | 1 | | |
| 2. Attitude (A) | 0.98* | 1 | |
| 3. Practice (P) | 0.27* | 0.16* | 1 |
| N | 550 | 550 | 550 |
| Mean | 47.58 | 47.44 | 47.24 |
| SD | 3.70 | 4.07 | 4.35 |

Table 1 showed the mean, standard deviation, and correlation matrix of the relationship between preservice mathematics teachers' knowledge, attitude and practice of cybersecurity. In line with the Pearson correlation analysis (Table 1), there was a significant relationship among knowledge, attitude and practice of cybersecurity. Furthermore, all associations were significant between attitude and practice ($r = 0.16$, $p<0.05$), knowledge and practice ($r = 0.27$, $p<0.05$) and between knowledge and attitude ($r= 0.98$, $p<0.05$) of cybersecurity. Attitude and knowledge relationship was statistically significant. Thus, there was a significant association between preservice mathematics teachers' knowledge, attitude, and practice of cybersecurity. All the relationships were positive and direct.

**Research Question Two:** What is the predictive influence of knowledge and attitudes towards the explanation of variance in preservice mathematics teachers' practices of cybersecurity?

Table 2 showed the predictive influence of attitude and knowledge towards the explanation of variance in preservice mathematics teachers' practice of cybersecurity. The ANOVA regression analysis (Table 2) revealed a significant influence of knowledge and attitude on preservice mathematics teachers' practice of cybersecurity ($F_{(2,547)} = 163.67$, $p=0.000$). The two factors (knowledge and attitude) investigated contributed as much as 37.4% to practice of cybersecurity.

**Table 2. Predictive influence of attitude and knowledge towards the explanation of variance in preservice mathematics teachers' practice of cybersecurity**

| **R =.612** | **$R^2$ =.374** | **Adjs $R^2$=.372** | **Stand. Error Est=3.45** | **$F_{(2, 547)}$=163.67** | **P < 0.001** |
|---|---|---|---|---|---|
| **Variable** | Unstandardized | coefficients | Standardized coeff. | T | Sig. |
| | **B** | **Std. Error** | **Beta** | | |
| **Constant** | 19.03 | 2.07 | | 9.23 | .000 |
| **Attitude** | 3.81 | 0.22 | 3.23 | 17.44 | .000 |
| **Knowledge** | 3.22 | 0.20 | 3.02 | 16.27 | .000 |


ISSN: 2518-2951 https://doi.org/10.59568/AMJD-2025-13-2-08 African Multidisciplinary Journal of Development (AMJD)

As seen in Table 2, attitude had the highest beta (β) value (3.23), followed by knowledge (β = 3.02). The regression analysis equation is as follows: cybersecurity $practice_{predicted}$ = 19.03 + 3.81 attitude + 3.22 knowledge. According to the equation, one unit increase in attitude results in a 3.81, increase in cybersecurity practice. A unit increase in knowledge of cybersecurity would result in a 3.22 rise in practice of cybersecurity.

**Research Question Three:** What is the influence of gender on preservice mathematics teachers' knowledge, attitude, and practice of cybersecurity?

**Table 3. Gender differences in preservice mathematics teachers' knowledge, attitude and practice of cybersecurity**

| Variable | Gender | N | Mean | SD | T | Df | Sig |
|---|---|---|---|---|---|---|---|
| **Attitude** | Female | 316 | 46.80 | 4.40 | -4.42 | 548 | .00 |
| | Male | 234 | 48.32 | 3.40 | | | |
| **Knowledge** | Female | 316 | 46.95 | 3.96 | -4.74 | 548 | .00 |
| | Male | 234 | 48.44 | 3.11 | | | |
| **Practice** | Female | 316 | 47.04 | 4.40 | -1.25 | 548 | .21 |
| | Male | 234 | 47.51 | 4.28 | | | |

Table 3 displayed a summary of the mean responses of the participants on the gender differences in preservice mathematics teachers' knowledge, attitude, and practice of cybersecurity. Generally, the male participants had more knowledge, attitude, and practice of cybersecurity. The results in Table 3 showed that the male preservice mathematics teachers were more inclined toward KAP of cybersecurity than the female preservice mathematics teachers. With regard to attitude, male preservice mathematics teachers had a mean of 48.32 with a standard deviation of 3.40, while females had a mean of 46.80 with a standard deviation of 4.40. Concerning self-reported knowledge, male participants had a mean value of 48.44 with a standard deviation of 3.11, while females had a mean of 46.95 and a standard deviation of 3.96. With regards to practice, male participants had a mean value of 47.51 (SD=4.28), slightly higher than female participants' of 47.04 (SD=4.40). As shown in Table 3, there was a significant influence of gender on preservice mathematics teachers' attitude (t= -4.42, p=0.00) and knowledge (t= -4.74, p=0.00) of cybersecurity. However, gender did not have significant influence on preservice mathematics teachers' practice of cybersecurity (t= -1.25, p=0.21).

## Discussion

In this study, the relationships among preservice mathematics teachers self-reported knowledge, attitude and practice of cybersecurity were examined. The predictive influence of knowledge and attitude on preservice mathematics teachers' practice of cybersecurity in Nigeria was also determined. In addition, gender differences in preservice mathematics teachers' knowledge, attitude, and practice of cybersecurity were investigated. The study aimed at extensively determine these relationships in mathematics teacher education context in Nigeria, where there is scarcity of researches on the topic.

**Association between self-reported knowledge, attitude, and preservice mathematics teachers' practice of cybersecurity.**

The study results showed that there was a significant relationship between self-reported knowledge, attitude, and practice of cybersecurity among preservice mathematics teachers. Undoubtedly, there were positive relationships between self-reported knowledge and practice of cybersecurity, self-reported knowledge and attitude towards cybersecurity, and attitude and practice of cybersecurity. These results are very important for the KAP assessment researchers in Nigeria where researches are


ISSN: 2518-2951 https://doi.org/10.59568/AMJD-2025-13-2-08 African Multidisciplinary Journal of Development (AMJD)

very scanty. In the present study, self-reported knowledge and attitude are strong factors in preservice mathematics teachers' practice of cybersecurity. This is because investigating the self-reported knowledge and attitude in relation to practice of cybersecurity is crucial for KAP researchers to develop strategies that promote awareness, knowledge, attitude, and practice of cybersecurity (Benzer, & Karal, 2023; McCormac, Zwaans, Parsons, Calic, Butavicius, & Pattinson, 2017; Ngoqo, & Flowerday, 2015; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014). Preservice teachers' knowledge of cybersecurity principles and best practices can shape their attitude towards cybersecurity, making them more likely to prioritize and practice it.

Preservice teachers' knowledge and attitude towards cybersecurity can influence their confidence and self-efficacy in teaching cybersecurity concepts. Preservice teachers who practice good cybersecurity habits can serve as role models for their students, promoting a culture of cybersecurity. Preservice teachers' good knowledge and attitude towards cybersecurity can impact their ability to teach cybersecurity literacy to their students. Engaging in cybersecurity practices can reinforce preservice teachers' knowledge and attitude, creating a positive feedback loop. A positive attitude towards cybersecurity can motivate preservice teachers to incorporate cybersecurity practices into their teaching, while a negative attitude can hinder its adoption. The connection between mathematics and cybersecurity can make preservice mathematics teachers more inclined to practice and teach cybersecurity concepts. Preservice teachers' knowledge and attitude towards cybersecurity can impact their willingness to engage in ongoing professional development in cybersecurity. Preservice teachers' practice of cybersecurity can help protect their students from cyberthreats and ensure a safe online learning environment. Preservice teachers' knowledge and attitude towards cybersecurity can impact their ability to effectively integrate cybersecurity into the mathematics curriculum.

**Knowledge and attitude as predictors of preservice mathematics teachers' cybersecurity practice**

The present study revealed the efficacy of attitude in predicting preservice mathematics teachers' cybersecurity practice. This is in agreement with the findings of some investigators (Benzer, & Karal, 2023; Parsons, McCormac, & Butavicius, 2018b). Consistently positive attitudes toward cybersecurity can lead to habitual practice, making it a regular part of their teaching routine. When preservice teachers feel emotionally invested in cybersecurity (e.g., concern for students' safety), they're more likely to practice it. Preservice teachers may be influenced by peers, mentors, or colleagues with positive attitudes toward cybersecurity, leading to adoption of good practices. Attitudes can shape intentions, and intentions predict behavior, including cybersecurity practices. Preservice teachers who perceive cybersecurity risks as high are more likely to take action to mitigate them. A positive attitude toward cybersecurity can motivate preservice teachers to learn and implement best practices. When cybersecurity aligns with preservice teachers' values (e.g., protecting students, maintaining privacy), they're more likely to practice it. Preservice teachers who worry about the consequences of cyber threats are more likely to take action to prevent them. Those who feel confident in their ability to implement cybersecurity measures are more likely to do so. Preservice teachers who believe cybersecurity is important are more likely to prioritize and practice it.

Presently, in this study, preservice mathematics teachers' knowledge of cybersecurity was positively and significantly related with their cybersecurity practice. Additionally, preservice mathematics teachers' knowledge of cybersecurity was a second best forcaster of their cybersecurity practice. These results agreed with the findings of some researchers (McCormac, Zwaans, Parsons, Calic, Butavicius, & Pattinson, 2017; Ngoqo, & Flowerday, 2015; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014; Wahyudiwan, Sucahyo, & Gandhi, 2017). Knowledge of cybersecurity can help preservice teachers stay


ISSN: 2518-2951 https://doi.org/10.59568/AMJD-2025-13-2-08 African Multidisciplinary Journal of Development (AMJD)

current with emerging threats and countermeasures, which could enable them to apply concepts to real-world teaching scenarios. Preservice mathematics teachers who have greater knowledge of cybersecurity and more positive attitudes towards cybersecurity are more likely to engage in good cybersecurity practices, such as: using encryption and secure communication protocols, being cautious when clicking on links or downloading attachments, keeping software and operating systems up-to-date, and using strong passwords and two-factor authentication. By possessing knowledge of cybersecurity, preservice mathematics teachers are better equipped to stay current with emerging threats and technologies, educate students about cybersecurity, implement effective security measures, and identify and mitigate cyber threats. Since this knowledge predicts practice, it could empower preservice mathematics teachers to take action and make informed decisions about cybersecurity in their teaching practices. Knowledge of cybersecurity tools and technologies can help preservice teachers use them effectively and gain confidence in their ability to implement security measures since they would be able to identify vulnerabilities and take corrective action informed by their knowledge of cybersecurity legal and ethical issues for decision-making. Preservice mathematics teachers with limited knowledge and negative attitudes towards cybersecurity may be less likely to prioritize and practice good cybersecurity habits. Knowledge of cybersecurity can help preservice teachers to promote critical thinking about online safety and security that could inform instructional practices, promoting a culture of cybersecurity. Knowledge of cybersecurity threats and risks can make preservice mathematics teachers more aware of potential dangers and implement effective measures to combat the risks.

**Preservice mathematics teachers' gender as a factor in their knowledge, attitude, and practice of cybersecurity**

In this study, preservice mathematics teachers' gender was a factor in their knowledge and attitude of cybersecurity in favour of males. This finding corroborated previous results (Benzer, & Karal, 2023; Ruggiero & Boehm, 2016; Aikelewicz & Matusiak, 2017; Shah & Woodward, 2018; Wang & Wang, 2019) that recorded that gender had significant influence on knowledge and attitude of cybersecurity.

The present study finding negated other previous findings (Anwar, He, Ash, Yuan, Li, & Xu, 2017; Karacı, Akyüz, & Bilgici, 2017) that did not find the influence of gender on cybersecurity knowledge and attitude. However, gender difference in knowledge of cybersecurity among the preservice mathematics teachers could be attributed to many factors. First, the traditional gender roles and stereotypes common in Nigeria might have led to difference in interest, confidence, and perceived ability in technology and cybersecurity. Second, broader societal and cultural factors, such as gender roles and expectations, might have influenced preservice mathematics teachers' knowledge and attitudes towards cybersecurity. The female gender in this study might have considered cybersecurity as a male dominated domain. Third, the lack of female role models and mentors in cybersecurity might have discouraged women from pursuing related interest and this could have affected their low level of cybersecurity knowledge and attitude. Fourth, in Nigeria, girls and boys are socialised differently and this might have influenced their attitudes towards technology and cybersecurity. Lastly, addressing these factors can aid the understanding of gender differences in knowledge and attitudes of cybersecurity and enhance inclusive education and training programmes.

Nevertheless, gender was not a determinant of cybersecurity practices among the preservice mathematics teachers. This result was not in consonance with previous investigations (Mamonov, & Benbunan-Fich, 2018; Hoy & Milne, 2010; He & Freeman, 2019; Broos, 2005) that found gender as a factor in cybersecurity practice. Lihammer and Hagman (2021) identified that female preservice teachers had


ISSN: 2518-2951 https://doi.org/10.59568/AMJD-2025-13-2-08 African Multidisciplinary Journal of Development (AMJD)

lower levels of cybersecurity practice due to gender-based stereotypes. However, Knezek and Christensen (2016) found that female preservice teachers had lower levels of cybersecurity practice due to lack of experience. That gender was not a factor in preservice mathematics teachers' practice of cybersecurity could be as a result of the fact that both genders had equal access to cybersecurity resources, thereby reducing their gender-based disparities. Also, the non-significant difference could be as a result of the instrument utilised in assessing cybersecurity practice which could not be sensitive enough to detect gender differences. More so, both male and female preservice mathematics teachers might not have had sufficient experience with cybersecurity practices, thereby reducing their gender-based disparities.

## Conclusions

It is shown in this study that there were significant associations betwixt self-reported knowledge, attitude and practice of cybersecurity. Precisely, there was a significant positive relationship between self-reported knowledge, attitude and practice of cybersecurity. More so, attitude towards cybersecurity was the highest predictor of preservice mathematics teachers' practice of cybersecurity.

Knowledge of cybersecurity was the least contributor to preservice mathematics teachers' practice of cybersecurity. There were gender differences in preservice mathematics teachers self-reported knowledge and attitude towards cybersecurity in favour of males. There was no significant influence of gender on preservice mathematics teachers' practice of cybersecurity. The findings related to KAP of cybersecurity have practical implications. First, educators should integrate cybersecurity education into preservice teacher training, focusing on knowledge, attitude, and practice. Second, curriculum developer should incorporate cybersecurity topics into mathematics and other subjects, highlighting interdisciplinary connections. Educators should offer professional development by targeting training and resources for in-service teachers to enhance their cybersecurity knowledge, attitude, and practice. Lastly, policy makers should develop and implement policies promoting cybersecurity education in schools, aligning with national and international standards. This study is limited because a self-reported data were collected. Dependence on participants' self-reported measures of knowledge, attitude, and practice may be subject to prejudices. Limited generalisability could also be another limitation of the study since findings may not be applicable to other populations or contexts. The study suffered from a lack of qualitative data. Depending so much on quantitative data may overlook rich, contextual insights.

Also, overemphasis on preservice mathematics teachers may overlook interdisciplinary aspects of cybersecurity education. This study could not establish causality because correlational analysis was used and as such there could be other determinants of the associations. More so, it became impossible for this study to assess the contextual elements that might affect KAP of cybersecurity. The limitations of this study notwithstanding, future research should endeavour to expand sample size and diversity by including more participants from various institutions of learning, locations, and backgrounds. Mixed-methods paradigm should be adopted by combining qualitative and quantitative methods to gain deeper insights. In addition, a longitudinal study can be conducted to investigate the changes in knowledge, attitude, and practice of cybersecurity over time. Contextual factors such as school culture and resources should be investigated to determine their influence on cybersecurity knowledge, attitude, and practice. Effort should be made to explore how cybersecurity education can be integrated across subjects or courses, not just mathematics. More so, cross-cultural studies to compare cybersecurity education globally should be conducted. With these areas in focus, future research can provide a more comprehensive understanding of preservice mathematics teachers' knowledge, attitude, and practice of cybersecurity, ultimately informing effective education and training strategies.


ISSN: 2518-2951 https://doi.org/10.59568/AMJD-2025-13-2-08 African Multidisciplinary Journal of Development (AMJD)

## References


1) Abdel, F. A., Qaraman, M. E., Edris K., & Ahmed, H. A. (2022). Knowledge, attitudes, and practice towards occupational health and safety among nursing students in Gaza strip, Palestine. *Ethiopian Journal of Health Science, 32*(5), 1007.doi: http:// dx.doi.org/ 10.4314/ejhs. v329i5.17
2) Ahlan, A. R., Lubis, M., & Lubis, A. R. (2015). Information security awareness at the knowledge-based institution: Its antecedents and measures. *Procedia Computer Science, 72*, 361–73, https://doi.org/10.1016/j.procs.2015.12.151.
3) Ajao, E. A., & Awofala, A. O. A. (2022). Learning difficulties in mathematical problem-solving at pre-tertiary levels. *African Journal of Science, Technology and Mathematics Education, 8*(5), 368-374.
4) Ajao, E. A., & Awofala, A. O. A. (2024). Developing problem solving skills in mathematics at primary, secondary and tertiary levels. *Nigerian Online Journal of Educational Sciences and Technology, 6*(1), 136-152.
5) Al-Nuaimi, M. N., & Uzun, A. M. (2023). Socio-cognitive determinants of plagiarism intentions among university students during emergency online learning: Integrating emotional, motivational, and moral factors into theory of planned behavior. *Cogent Psychology, 10*(1), 1–22.
6) Alotaibi, F., & Alshehri, A. (2020). Gender differences in information security management. *Journal of Computer and Communications*, *8*, 53-60. doi: 10.4236/jcc.2020.83006.
7) Antunes, M., Silva, C., & Marques, F. (2021). An integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviours in school context. *Applied Sciences, 11*(23), 1–18.
8) Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69*, 437-443. doi:10.1016/j.chb.2016.12.040.
9) Arfi, N., & Agarwal, S. (2014). A study on level of knowledge regarding cybercrime among elderly residing in homes and old age homes. *International Journal for Research in Applied Science and Engineering Technology, 2*(7), 30–34.
10) Aronson, E., & Wilson, T. (2017). *Sociale Psychologie* (Amsterdam: Pearson Benelux, 2017).
11) Awofala, A. O. A. (2020). Examining components of attitudes towards mathematics among senior secondary school students in Nigeria. *International Journal on Teaching and Learning Mathematics, 3*(2), 54-66.
12) Awofala, A. O. A., & Lawal, R. F. (2022). The relationship between critical thinking skills and quantitative reasoning among junior secondary school students in Nigeria. *Jurnal Pendidikan Matematika (Kudus), 5*(1), 1-16.
13) Awofala, A. O. A., Olaguro, M., Fatade, A. O., & Arigbabu, A. A. (2024). Learning engagement as a predictor of performance in mathematics among Nigerian senior secondary school students. *International Journal of Innovation in Science and Mathematics Education, 32*(3), 40-51.
14) Awofala, A. O., Lawal, R. F., Arigbabu, A. A. & Fatade, A. O. (2022): Mathematics productive disposition as a correlate of senior secondary school students' achievement in mathematics in Nigeria. *International Journal of Mathematical Education in Science and Technology, 53*(6), 1326-1342.
15) Bada, M., Sasse, A., & Nurse, J. (2017). Cybersecurity awareness campaigns: Why do they fail to change behaviour? *Proceedings of the International Conference on Cyber Security for Sustainable Society*, 118–131, https://arxiv.org/abs/1901.02672.
16) Ben-Asher, N. & Gonzalez, C. (2015). Effects of cybersecurity knowledge on attack detection. *Computers in Human Behavior, 48*, 51–61, https://doi.org/ 10.1016/j.chb.2015.01.039.
17) Benzer, A. İ., & Karal, Y. (2023). Pre-service teachers' information security awareness: An analysis based on the knowledge— attitude—behavior model. *Educational Academic Research, 49*, 10-22. https://doi.org/10.5152/AUJKKEF.2023.1034562

18) Bhatnagar, N., & Pry, M. (2020). Student Attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media: An initial study. *Information Systems Education Journal, 18*(1), 48–58.
19) Bitton, R., Boymgold, K., Puzis, R., & Shabtai, A. (2019). Evaluating the information security awareness of smartphone users. http://arxiv.org/abs/ 1906.10229.
20) Bognár, L., & Bottyán, L. (2024). Evaluating online security behavior: Development and validation of a personal cybersecurity awareness scale for university students. *Education Sciences, 14*(6), 588. https://doi.org/10.3390/educsci14060588.
21) Bohner, G., & Wanke, M. (2002). *Attitudes and attitude change*. Psychology Press.
22) Broos, A. (2005) Gender and information and communication technologies (ICT) anxiety: Male self-assurance and female hesitation. *Cyber Psychology & Behavior, 8*, 21-31. https://doi.org/10.1089/cpb.2005.8.21
23) Caldwell, T. (2016). Making security awareness training work. *Computer Fraud and Security, 6*, 8–14, https://doi.org/10.1016/S1361-3723(15)30046-4.
24) Chen, H., & Li, Y. (2017). Development and validation of a cybersecurity knowledge assessment tool. *Computers & Security,* 66, 147-157.
25) Cook, D., Szewczyk, P., & Sansurooah, K. (2011). Seniors language paradigms: 21st century jargon and the impact on computer security and financial transactions for senior citizens. *Proceedings of the 9th Australian Information Security Management Conference*, 63–68, https://doi.org/10.4225/75/57b52 d42cd8b8.
26) de Kok, L. C., Oosting, D., & Spruit, M. (2020). The influence of knowledge and attitude on intention to adopt cybersecure behaviour. *Information & Security,* 46(3), 251-266. https://doi.org/10.11610/isij.4618.
27) Fiske, S., & Taylor, S. (2013). *Social cognition: From brains to Culture* (Thousand Oaks, CA: Sage Publications).
28) Giannakas, F., Kambourakis, G., & Gritzalis, S. (2015). CyberAware: A mobile game-based app for cybersecurity education and awareness. *Proceedings of 2015 International Conference on Interactive Mobile Communication Technologies and Learning, IMCL,* 54–58, https://doi.org/10.1109/IMCTL.2015.7359553.
29) Gratian, M., Bandi, S., Cukier, M., Dykstra, J. & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security, 73*, 345-358. https://doi.org/10.1016/j.cose.2017.11.015
30) Grimes, G., Hough, M., Mazur, E., & Signorella, M. (2010). Older adults' knowledge of internet hazards. *Educational Gerontology, 36*(3), 173–92, https://doi.org/10.1080/03601270903183065.
31) Hagger, M. S. & Chatzisarantis, N. L. D. (2005). *The social psychology of exercise and sport*. Open University Press.
32) 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.
33) Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L.,Hildebrandt, T., Tsakirakis, G., Oikonomou, F., Leftheriotis, G., & Koshutanski, H. (2020). Modern aspects of cyber-security training and continuous adaptation of programmes to trainees. *Applied Sciences, 10*(16), 5702.
34) He, J., & Freeman, L.A. (2019) Are men more technology-oriented than women? The role of gender on the development of general computer self-efficacy of college students. *Journal of Information Systems Education, 21*, 7.
35) Herath, T., & Rao, R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154–65, https://doi.org/10.1016/j.dss.2009.02.005.
36) Howard, D. J. (2018). Development of the cybersecurity attitudes scale and modeling cybersecurity behavior and its antecedents. *USF Tampa Graduate Theses and Dissertations.* https://digitalcommons.usf.edu/etd/7306

37) Hoy, M. G., & Milne, G. (2010) Gender differences in privacy-related measures for young adult facebook users. *Journal of Interactive Advertising, 10*, 28-45. https://doi.org/10.1080/15252019.2010.10722168
38) Intel Security Group (2017). *2017 Norton cyber security insights report: Global results*.
39) Karacı, A., Akyüz, H. İ., & Bilgici, G. (2017). Investigation of cyber security behaviors of university students. *Kastamonu Education Journal, 25*(6), 2079–2094.
40) Krathwohl, D. (2002). A revision of Bloom's taxonomy : An overview. *Theory into Practice, 41*(4), 212–18, https://www.researchgate.net/publication/242400296_A_Revision_of_Bloom's_Taxonomy_An_Overview.
41) Kray, J., & Waaijenborg, S. (2019). Gender differences in cybersecurity behavior: A systematic review. *Computers & Security, 84*, 245-255.
42) Kruger, H. A., & Kearney, W. (2006). A prototype for assessing information security awareness. *Computers and Security,* 25(4), 289–96, https://doi.org/ 10.1016/j.cose.2006.02.008.
43) Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review,* 37(12), https://doi.org/10.1108/MRR-04-2013-0085.
44) Li, Y., & Chen, H. (2019). Development and validation of a comprehensive cybersecurity awareness scale. *Computers & Security, 83*, 241-253.
45) Lihammer, S. & Hagman, L. (2021). *Investigating gender disparity within cyber security: Analysis of Possible factors through a mixedmethod qualitative study and a self-implemented testing program.* A first degree project of KTH Royal Institute of Technology, Sweden.
46) Mamonov, S., & Benbunan-Fich, R. (2018) The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior, 83*, 32-44. https://doi.org/10.1016/j.chb.2018.01.028
47) Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior, 83*, 32–44.
48) McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017) Individual differences and Information Security Awareness. *Computers in Human Behavior, 69*, 151–156.
49) McKinsey & Company (2020). Delivering through diversity: 2020 report on women in tech.
50) Mouheb, D., & Zulkernine, M. (2019). An exploratory study on gender differences in cybersecurity awareness and behavior. *International Journal of Cybersecurity Education, 1*(1), 1-18.
51) Mukhtar, M. & Mat Yusof, A & Lokman, I. (2020). Knowledge, attitude and practice on occupational safety and health among workers in petrochemical companies. *IOP Conference Series: Earth and Environmental Science,* 436. 012029. https://doi.org/10.1088/1755-1315/436/1/012029.
52) Ngoqo, B., & Flowerday, S. V. (2015). Information Security Behaviour Profiling Framework (ISBPF) for student mobile phone users. *Computers and Security, 53*, 132–142.
53) Norton, S. (2019). 2019 Norton lifelock cyber safety insights report: Global results. NortonLifeLock.
54) Okunuga, R. O., Awofala, A. O. A. & Osarenren, U. (2020). Critical thinking acquisition of senior secondary school science students in Lagos state, Nigeria: A predictor of academic achievement. *Journal of Curriculum and Instruction, 13*(1), 44-56.
55) Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers and Security, 66*, 40–51, https://doi.org/10.1016/j.cose.2017.01.004.
56) Parsons, K., McCormac, A., & Butavicius, M. (2018a). The cybersecurity knowledge assessment tool (CKAT): A comprehensive assessment of cybersecurity knowledge. *Journal of Cybersecurity Education, Research and Practice, 2018*(1), 1-15.
57) Parsons, K., McCormac, A., & Butavicius, M. (2018b). The influence of social norms on cybersecurity behavior. *Computers & Security, 76*, 323-333.

58) Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers and Security, 42*, 165–176.
59) Parsons, P., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers and Security, 42*, 165–76, https://doi.org/10.1016/j.cose.2013.12.003.
60) Plessis, L. D., & Solms, R. V. (2002). Information security awareness: Baseline education and certification. *Information Technology on the Move, 8*(8), 1–12.
61) Sfakianakis, A., Douligeris, C., & Marinos, L. (2019). ENISA Threat Landscape Report 2018 15 Top Cyberthreats and Trends. *ENISA*, https://doi.org/10.2824/622757.
62) Siponen, M., Mahmood, A., & Pahnila, S. (2014). Employees' Adherence to Information Security Policies: An Exploratory Field Study. *Information and Management, 51*(2), 217–24, https://doi.org/10.1016/j.im.2013.08.006.
63) Slusky, L., & Partow-Navid, P. (2012). Students information security practices and awareness reproduced with permission of the copyright owner further reproduction prohibited without permission. *Journal of Information Privacy & Security, 8*(4), 3–26, https://doi.org/10.1080/15536548.2012.10845664.
64) Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management and Computer Security, 22*(1), 42–75, https://doi.org/10.1108/IMCS-08-2012-0045.
65) Statista (2024). Number of internet users worldwide from 2009 to 2024.
66) Symantec Corporation (2019). *2019 Internet Security Threat Report*. Symantec Corporation.
67) Szumski, O. (2018). Cybersecurity best practices among Polish students. *Procedia Computer Science, 126*, 1271–1280.
68) Taylor, M., & Hutton, J. (2018). Gender and cybersecurity: A systematic review of the literature. *Computers & Security, 77*, 255-265.
69) Tirumala, S., Sarrafzadeh, A., & Pang, P. (2016). A survey on internet usage and cybersecurity awareness in students. *14th Annual Conference on Privacy, Security and Trust,* 223–28. https://doi.org/10.1109/PST.2016.7906931.
70) Wahyudiwan, D. D. H., Sucahyo, Y. G., & Gandhi, A. (2017). Information security awareness level measurement for employee: Case study at Ministry of Research, Technology, and Higher Education. In *Proceeding of the 3rd International Conference on Science in Information Technology (ICSITech)* (pp. 654–658). Bandung, Indonesia