Journal of Information Technology Education: Innovations in Practice

An Official Publication of the Informing Science Institute
InformingScience.org

JITEiip.org

Volume 25, 2026

THE INVESTIGATION OF STUDENT SELF-EFFICACY AND PERCEPTIONS IN THE USE OF THE INTERNET IN SOMALIA

Nuriye Sancar*	Near East University, Department of Mathematics, Nicosia, Cyprus, via Mersin, Turkey	nuriye.sancar@neu.edu.tr
Abdiwahab Abdillahi	Near East University, Department of Computer Information Systems, Nicosia, Cyprus, via Mersin, Turkey *and* Amoud University, Borama, Somalia	abdiwahab@amoud.edu.so
Charles Zulu Yonmah	Near East University, Department of Computer Information Systems, Nicosia, Cyprus, via Mersin, Turkey	20243761@std.neu.edu.tr
Ghufran Fareed	Near East University, Department of Computer Information Systems, Nicosia, Cyprus, via Mersin, Turkey	20236225@std.neu.edu.tr
Nadire Cavus	Near East University, Department of Computer Information Systems, Nicosia, Cyprus, via Mersin, Turkey	nadire.cavus@neu.edu.tr

* Corresponding author

ABSTRACT

Aim/Purpose	The purpose of this study is to determine Somali university students' self-assurance in their ability to use the internet securely, as well as their perceptions of safe internet use across the following four areas: computer security, malicious software, web security, social engineering, and social media.
Background	While universities globally have rapidly adopted internet technologies as a valuable tool for enhancing student learning, students in vulnerable areas like Somalia are left behind, unable to use them safely and effectively due to limited digital literacy initiatives and a lack of college or university cybersecurity policies. This

Accepting Editor Bahman Gorjian | Received: October 8, 2025 | Revised: December 15, 2025; January 2, January 4, 2026 | Accepted: January 12, 2026.
Cite as: Sancar, N., Abdillahi, A., Yonmah, C. Z., Fareed, F., & Cavus, N. (2026). The investigation of student self-efficacy and perceptions in the use of the internet in Somalia. *Journal of Information Technology Education: Innovations in Practice, 25,* Article 4. https://doi.org/10.28945/5697

	leaves many Somali university students vulnerable to additional risk of harm or exploitation when they engage with others online.
Methodology	A quantitative, cross-sectional survey design was used, and data were collected via convenience sampling from 388 students across the academic levels and faculties of Somali universities. Nonparametric tests (Mann-Whitney U and Kruskal-Wallis) were used to evaluate differences in students' self-efficacy and perceptions of the internet by gender, age, and level of education.
Contribution	The results of this study provide empirical evidence regarding Somali university students' digital self-efficacy and perceptions of internet safety. The results indicate that these students differ in demographics, self-efficacy, and perceptions of internet safety regarding social media. Therefore, this study will inform and develop specifically tailored cybersecurity education and digital literacy policies in Somali higher education.
Findings	This research found that Somali university students demonstrated a very high degree of self-confidence across all four areas studied. There were also slightly higher levels of awareness of web security and social engineering than of computer security and malicious software ($M = 3.39$) and social networking sites ($M = 3.38$), compared with computer security ($M = 3.25$) and malicious software ($M = 3.28$). Significant group differences were observed. Male students reported higher self-efficacy across all domains than females ($p < .001$; WSS $p = .014$), older age groups (27-30 and 30+) demonstrated significantly higher levels than younger groups ($p \leq .002$), and undergraduate students reported higher self-efficacy than postgraduates ($p < .001$).
Recommendations for Practitioners	To improve academic performance and encourage safer online behaviour, Somali universities should offer students structured cybersecurity and internet safety courses, as well as additional tools to protect their personal information and detect online threats. Increasing the availability of these courses will also help reduce differences in access to cybersecurity and digital literacy among students from different demographic groups.
Recommendations for Researchers	Future research should evaluate how the implementation of structured cybersecurity interventions influences students' behaviours and attitudes regarding their online activities, and use mixed-methods research to capture the ongoing impact of these interventions on students' digital practices.
Impact on Society	As Somalia continues to develop, strengthening digital literacy and internet safety among Somali university students will encourage greater academic performance and contribute to improving national educational quality and technological advancement.
Future Research	Further studies should evaluate the sustainability of cybersecurity awareness programmes over time and explore cross-country comparisons within East Africa to identify trends and best practices regarding the provision of cybersecurity education and awareness among students in fragile higher education contexts. It is important to establish a foundation for the continued growth and development of technology in the region.

Keywords internet self-efficacy, cybersecurity awareness, digital literacy, Somalia, higher education, safe internet use

INTRODUCTION

In recent years, the internet has revolutionized the operation of higher education institutions around the world, including emerging countries such as Somalia. The development of online platforms is now one of the hallmarks of an institution of higher learning's capability to develop students as academically excellent individuals (Somali Research and Education Network [SomaliREN], 2024; Unwin et al., 2010). Digital technologies have redefined how and where knowledge is created and disseminated. Therefore, the ability of university students to independently navigate the digital web with confidence and freedom is now a highly valued competency (UNESCO, 2023). The ability to critically evaluate information in digital environments and to practice good cybersecurity practices will be important skills in today's world, especially in a country like Somalia, where strategic development programmes or initiatives to build electronic literacy are still in their infancy.

As previously mentioned, while internet use continues to grow among Somali universities, students often struggle to use internet technologies effectively and safely (SomaliREN, 2024). Current research indicates that Somali students are frequently exposed to cyber risks, such as phishing scams, identity theft, and malware, due to limited awareness and knowledge of how to protect themselves from potential harm (Ahmed et al., 2023). Additionally, Gure and Rasool (2024) have documented that there is a high prevalence of Somali students using social media and social networking sites, but that there is not a commensurate awareness of how to maximize this use from a cyber safe perspective, thus revealing a lack of both perceived and actual self-efficacy in the Somali context regarding the use of the internet.

The growth of digital technologies in education and communication in Africa has prompted growing interest in the safe use of the internet by university students within the African higher education sector, as these technologies increasingly shape educationally delivered content through both instructional pedagogy and communication (Jauhiainen et al., 2025). Research shows that demographic characteristics such as gender, age, and education level significantly impact students' understanding of computer security and their responses to the risks associated with computer security threats (Aithal & Aithal, 2019; Fatokun et al., 2019). In addition, recent studies indicate that awareness of cybersecurity differs significantly across demographics, including gender and educational level, suggesting that university students differ in their preparedness for safe internet use based on these factors (Bromall et al., 2025). In Somalia, studies have reported that although internet penetration has grown rapidly, students' knowledge and behaviours regarding internet safety have been insufficient, leaving them at risk. They are particularly vulnerable to phishing, malware, and social engineering (SomaliREN, 2024).

The research will also examine how differences in the perception and practice of cybersecurity and digital risk management may be linked to the previously identified demographic factors including gender, age, and educational level examined in PricewaterhouseCoopers (2024), Adala (2016), and Oroma et al. (2013), which have been identified as influencing perception of cybersecurity and digital risk management across eastern Africa. This study explores Somali university students' beliefs about and confidence in using the internet correctly through four lenses: computer security (CS), malicious software (MS), web security (WS), and social networking sites (SNS). The hope is to provide a better understanding of how students think and feel about internet safety, fill an important knowledge gap, and develop targeted efforts to increase internet literacy and cybersecurity among Somali students, which will likely have far-reaching effects on higher education systems across East Africa. As such, it is vital to understand the differences between students' opinions and confidence levels on each dimension. Thus, this study will explore and compare university students' confidence levels and opinions regarding safe internet use (CS, MS, WS, SNS) to determine whether these sentiments vary by demographic characteristics (sex, age, educational level). The importance of the study is that it focuses on Somalia, where the majority of students lack access to formal cybersecurity education due to

systemic underfunding; therefore, this study adds to the literature on digital self-efficacy and digital literacy in under-researched areas.

Research Questions

This study is conducted in accordance with the following research questions:

1. What are university students' opinions and perceptions regarding safe internet use in the context of computer security, and do these opinions and perceptions differ according to gender, age, and education level?
2. What are university students' opinions and perceptions regarding safe internet use in relation to malicious software, and do these opinions and perceptions differ according to gender, age, and education level?
3. What are university students' opinions and perceptions regarding safe internet use in relation to web security and social engineering, and do these opinions and perceptions differ according to gender, age, and education level?
4. What are university students' opinions and perceptions regarding safe internet use on social networking sites, and do these opinions and perceptions differ according to gender, age, and education level?

Literature Review

The Perception of Self-Efficacy

Self-efficacy is the belief that enables an individual to perform specific activities effectively in a digital environment (Ulfert-Blank & Schmidt, 2022). Moreover, self-efficacy encompasses using digital equipment effectively, making effective use of online resources, and problem-solving in an online environment. Research indicates that learners who possess the highest proficiency and most powerful mobile technology proficiency are more adaptable and demonstrate greater resilience in the face of hurdles to achieving higher academic performance in digital environments (Tadesse & Gillies, 2015). Li (2020) identified a high degree of correlation between the level of engagement in online education and the development of a student's sense of self-efficacy. Students who are driven to take responsibility for their participation in online education are more likely to succeed and be resilient in completing and adapting to online tasks than non-self-motivated students. Liu et al. (2023) found that students with strong self-efficacy not only achieve academic success but also can address challenges innovatively and use many forms of digital technology to improve their educational outcomes.

Understanding students' opinions and confidence in their ability to navigate online environments successfully is crucial for educators and academic institutions as e-learning continues to grow in popularity. Regardless of their current level of proficiency, students who believe they can use the internet and related digital tools and resources are more motivated to do so (Putriani & Apriani, 2022). This helps them improve their digital capabilities and academic abilities (Getenet et al., 2024). On the other hand, students who see accessing the internet favorably demonstrate resilience in the face of hardship (Wu & Tsai, 2006). Additionally, this will promote critical abilities, such as understanding and problem-solving, in digital environments (Li, 2020). With increasing global evidence indicating that students' self-efficacy is a contributing factor to both digital engagement and academic success, there remains very limited context-specific research examining how university students from Somalia perceive and develop these skills, offering an opportunity for additional research to better understand their self-efficacy and perceptions of internet use.

Security Issues

Students should be aware of the risks associated with using the internet, including security issues such as identity theft, data breaches, malware, and phishing. Students are often overwhelmed when

they encounter these risks due to their lack of technical knowledge and insufficient cybersecurity training. As such, it is imperative that educational institutions assist students in becoming more aware of these risks, so they can develop preventive measures to safely and effectively use the internet. Research by Cavus and Ercag (2016) has shown that most students have some basic understanding of computer interaction risks; they have very little or no knowledge, understanding, or experience of web security, malware, or safety on social networking sites. Given the rapid increase in student internet use, there is an urgent need for educational institutions to integrate cybersecurity training into their higher education curricula (Caudill & Terrell, 2010).

Further empirical research has confirmed gaps in malware awareness, password management, and the ability to protect against social engineering attempts among higher education students, despite their frequent internet use (Tick & Mai, 2024). Further, Bromall et al. (2025) stated that levels of cybersecurity awareness differ significantly by demographic characteristics, such as gender and education level, suggesting that university students have unequal levels of preparedness for safe internet use. An important study (Yankson et al., 2025) has indicated that students' understanding of cybersecurity issues is a major barrier to using the internet for education. Students lacking essential skills and knowledge to protect themselves from cyber threats are therefore less willing to take advantage of the wide range of online learning opportunities.

Livingstone and Helsper (2010) stated that students should receive specialised training to prepare them for targeted security threats, noting that this training could raise students' levels of awareness and prepare them for such threats through both training and real-life experiences. As a result, the development of structured practicum courses that address all aspects of cybersecurity, as opposed to simply educating students on the subject, is needed to prepare university students in Somalia for the digital world.

Additionally, in addition to the need for technical training for university students, there also needs to be a much larger, more comprehensive approach to developing the structural stability and absorption of such training. This has revealed a large gap in the digital competency of Somali university students. As a result, it is important to examine their perceptions of, and confidence in using, the internet to foster awareness of, and safe participation in, the digital realm of higher education.

Safety in Education

According to Bećirović et al. (2025), as technology advances even faster than the internet, students' ability to use digital resources and communicate online increases exponentially; thus, the need for a safe online environment to support their academic success has never been greater. In addition, researchers' studies of cybersecurity have quantitatively assessed the impact of students' internet safety awareness on their perceptions of online threats and the likelihood that they will engage in Internet safety behaviors (Vortia, 2025). Because of the research yet to be done on Somali university students, it will be important to continue exploring these areas of digital learning to assist them in achieving their educational goals and objectives. By studying these students' self-efficacy and perceptions of how they interact with and use the internet safely and securely, we may find ways to improve their experience accessing and using digital resources.

METHODS

Study Design

Using a quantitative cross-sectional survey design, the purpose of the research was to determine the levels of self-efficacy and perceptions of university students regarding safe internet use as measured by computer security, malicious software, web security, social engineering, and use of social networking sites.

PARTICIPANTS

For this study, 388 volunteer university students from diverse academic disciplines were selected through convenience sampling, of whom 56.2% were male, and 43.8% were female. The demographic data for the study participants are shown in Table 1. Of the students in this sample, 10.57% were 18-20 years old, 27.58% were 21-23 years old, 35.05% were 24-26 years old, 24.48% were 27-30 years old, and 2.32% were over 30 years old. Regarding educational status, 59.3% of participants were undergraduates, while 40.7% were postgraduates. The participants also had diverse academic backgrounds. For example, 35.1% of the respondents were from the Faculty of Business Administration, 39.9% from the Faculty of Software Engineering, 11.9% from the Faculty of Law, 7.5% from the Faculty of Nursing, and 5.7% from the Faculty of Agriculture.

Table 1. Descriptive data of participants

Variable	Frequency	Percentage
Gender		
Male	218	56.2
Female	170	43.8
Age		
18-20	41	10.57
21-23	107	27.58
24-26	136	35.05
27-30	95	24.48
30+	9	2.32
Level of education		
Undergraduate	230	59.3
Postgraduate	158	40.7
Faculty		
Business Administration	136	35.1
Software Engineering	155	39.9
Law	46	11.9
Nursing	29	7.5
Agriculture	22	5.7

DATA COLLECTION TOOLS

The questionnaire used herein is organized into three parts. The first section collects participants' demographics, including gender, age, faculty affiliation, and academic level. This is followed by measuring participants' tech background based on their prior experience, exposure, and knowledge of digital tools and websites. The last section was adapted from Cavus and Ercag (2016) and contains 35 items designed to gauge students' self-efficacy and perceptions regarding the safe use of the internet. Based on the data collected from participants in this research, the scales used to evaluate participants' responses were tested for internal reliability using Cronbach's alpha and found to be very reliable, with a value of 0.96. The scales used were grouped into four dimensions of computer security: web security, social engineering, malicious software, and social network platforms. To gauge the level of agreement or disagreement with participants' responses, a Likert scale (1–5) was created with the following response options: 5 = strongly agree; 4 = agree; 3 = neutral; 2 = disagree; 1 = strongly disagree.

Computer security (CS), comprising 13 questions, was created to assess students' skills and knowledge in securing their computers and devices. CS also focuses on the most relevant areas of protecting computers and devices from data breaches, unauthorized access, and hardware vulnerabilities, as well as securing personal information. The Cronbach's alpha for CS was 0.90.

Malicious software (MS) is made up of nine questions. It is used to measure how actively students identify, avoid, and respond to malware, viruses, worms, spyware, and other forms of malicious software. MS has a Cronbach's alpha reliability Test of 0.89.

Web security and social engineering (WSS): To address pertinent web security and social engineering concerns students may encounter when using the internet to access their emails and online shopping sites, six items were assigned to this dimension, and the Cronbach's alpha reliability was 0.87. The aim is to examine the ability of students to recognize and prevent these threats while using the internet.

Security on social network sites (SNS): To adequately address potential security problems arising from their use, 8 items were designed, yielding an overall Cronbach's Alpha reliability statistic of 0.89. Given that social networking platforms are among the major targets for cybercriminals seeking to carry out dangerous undertakings, this dimension examines how students view privacy and how to protect themselves on platforms such as Facebook, Instagram, and Twitter.

Data Analysis Methods

Data were obtained using a questionnaire, and analysis and interpretation were performed using SPSS version 30.0. The techniques used in the study included frequency and percentage calculations, the Mann-Whitney U test, and the Kruskal-Wallis test. The normality of participants' scores in the computer security, malicious software, web security, social engineering, and security on social networking sites dimensions of safe internet use was assessed using the Shapiro-Wilk test and tests of skewness and kurtosis. The Shapiro-Wilk test results were significant, and those of dimensions' skewness and kurtosis were beyond the ±2 range (Tabachnick & Fidell, 2013).

These findings showed that the data did not have a normal distribution. Therefore, nonparametric tests were more suited to compare groups. In order to estimate differences between two independent groups (e.g., gender, education level), the Mann-Whitney U test was used, whereas multiple-group comparisons (more than two, e.g., age groups) were assessed by the Kruskal-Wallis test. For pairwise comparison of the significance results, Dunn's post hoc test was used. In order to evaluate the magnitude of the group, effect sizes were estimated using eta squared (η^2), calculated for Mann-Whitney U and Kruskal-Wallis tests.

Procedure

The purpose of this research was to explore the gap in the university students' self-efficacy and perception of their capacity to utilize the internet safely and provide a remedy. The systematic research design entailed a literature review to identify the information gaps and data gathering. It was followed by the adaptation of the scale for the accurate assessment of the variables. Ethics committee approval was obtained from the Scientific Research Ethics Committee of Near East University under project number NEU/AS/2025/226 before data collection. Data collection was conducted using only approved methodologies and tools to ensure reliable information; analyses of the collected data were conducted using appropriate statistical techniques to answer the research questions. Last, the findings and conclusions were documented in a detailed research report that presented the objectives, methods, results, and implications. This structured process ensures academic rigor and ethical compliance throughout the study.

RESULTS

The four safe internet behaviors in this study were computer security (CS), malicious software (MS), web security/social engineering (WSS), and social networking sites (SNS), as reported in Table 2. The response to these behaviors was measured by how likely people are to engage with each of them on a scale of very high (4.01 - 5.00), high (3.01 - 4.00), moderate (2.01 - 3.00), low (1.01 - 2.00), and very low (0.00 - 1.00) using a five-point Likert scale. All four dimensions were found to be within the high category (3.01 - 4.00).

The web security/social engineering dimension had the highest mean (M = 3.39, SD = 1.08), indicating that students rate themselves as having a high degree of knowledge regarding phishing, spoof sites, and other deceptive practices. The second-highest mean was from the social networking site dimension (M = 3.38, SD = 0.99), which indicates that students are also highly aware of the need to be cautious regarding their online privacy and safety with regard to social networking sites. The mean for malicious software (M = 3.28, SD = 0.98) was relatively low but still in the high range, indicating appropriate awareness of malware, viruses, and other threats. Finally, computer security (M = 3.25, SD = 0.91) had the lowest mean of the four, although still in a high range, indicating that students recognize the need to secure their devices and information but have relatively less faith in this than in terms of web-related threats.

The reliability analysis confirmed that all four subscales showed strong internal consistency, as their Cronbach's alpha coefficients ranged between 0.865 (WSS) and 0.899 (CS). Composite reliability of the entire scale was very high ($\alpha = 0.963$), confirming the instrument's strength in measuring students' perceptions and self-belief regarding safe internet behavior. Generally, these results show that Somali university students have strong beliefs in their potential to perform across all domains of internet safety, as measured by the developed interpretation scale, and comparatively higher knowledge of web threats and social networking risks than in the technical domains of computer security and malware protection.

Table 2. Descriptive and reliability statistics of the scale and dimensions

Dimensions	Number of items	Mean	Standard deviation	Cronbach's alpha
CS	13	3.249	0.908	0.899
MS	9	3.282	0.980	0.887
WSS	6	3.392	1.075	0.865
SNS	8	3.375	0.987	0.882
Total				0.963

GROUP COMPARISON BY GENDER DIFFERENCES

The Mann–Whitney U test showed significant gender differences across all four dimensions of safe internet use, as shown in Table 3. Male students reported statistically higher levels of self-efficacy compared to females in computer security ($U = 14{,}152$, $Z = -3.93$, $p < .001$, $\eta^2 = .040$), malicious software ($U = 14{,}854$, $Z = -3.29$, $p < .001$, $\eta^2 = .028$), web security and social engineering ($U = 15{,}786.50$, $Z = -2.44$, $p = .014$, $\eta^2 = .015$), and social networking sites ($U = 13{,}233.50$, $Z = -4.83$, $p < .001$, $\eta^2 = .060$).

Although all effects were statistically significant, the magnitude of the differences ranged from small (MS, WSS) to small-to-moderate (CS, SNS), suggesting that gender plays a consistent but relatively limited role in shaping students' self-efficacy toward safe internet practices.

Table 3. Mann-Whitney U test for gender differences

Dimension	Gender	N	Mean rank	Sum of ranks	U	p
CS	Male	221	213.96	46786.00	14152.00	<0.001
	Female	167	168.74	28180.00		
	Total	388				
MS	Male	221	210.79	46584.00	14854.00	<0.001
	Female	167	172.95	28882.00		
	Total	388				
WSS	Male	221	206.57	45651.50	15786.500	0 .014
	Female	167	178.53	29814.50		
	Total	388				
SNS	Male	218	218.80	47697.50	13233.500	<0.001
	Female	170	163.34	27768.50		
Total		388				

GROUP COMPARISON ON AGE DIFFERENCE

Across all four dimensions, Kruskal-Wallis tests, as seen in Table 4, indicated significant age-group differences in computer security ($H(4)=24.982$, $p<.001$,$\eta^2=0.055$), malicious software ($H(4)=17.530$, $p=.002$, $\eta^2=0.035$), web security and social engineering ($H(4)=29.678$, $p<.001$, $\eta^2=0.067$), and security on social network sites ($H(4)=26.016$, $p<.001$, $\eta^2=0.057$). Post-hoc comparisons showed that the 27-30 and especially the 30+ group consistently had higher ranks than younger groups (18-20, 21-23, 24-26) across dimensions.

For web security and social engineering, the 21-23 and 24-26 groups were similar, but both exceeded the 18-20 group. In computer security and social network sites, both 30+ and 27-30 outperformed all younger groups, and in malicious software, they also exceeded the 21-23, 24-26, and 18-20 groups. The effect sizes ranged from small ($\eta^2 = .035$) to medium ($\eta^2 = .067$), indicating that although statistically significant, age explained a modest proportion of variance in self-efficacy across dimensions.

Table 4. Kruskal-Wallis H test for age differences

Dimension	Age	N	Mean rank	Kruskal-Wallis H	df	p	Post-hoc comparison
CS	18-20	41	168.72				30+ > 27–30, 21–23, 24–26, 18–20; 27–30 > 21–23, 24–26, 18–20
	21-23	107	191.99				
	24-26	136	171.52	24.982	4	<.001	
	27-30	95	232.65				
	30+	9	286.33				
	Total	388					
MS	18-20	41	162.00				30+> 21-23, 24–26, 18–20; 27–30 > 21–23, 24–26, 18–20
	21-23	107	190.52				
	24-26	136	179.24	17.530	4	0.002	
	27-30	95	229.96				
	30+	9	246.06				
	Total	388					

Dimension	Age	N	Mean rank	Kruskal-Wallis H	df	p	Post-hoc comparison
WSS	18-20	41	144.76				27–30, 30+ > 18–20, 21–23, 24–26; 21–23, 24–26 > 18–20
	21-23	107	182.37				
	24-26	136	182.69	29.678	4	<0.001	
	27-30	95	241.77				
	30+	9	244.67				
	Total	388					
SSN	18-20	41	177.89				30+ > 27–30, 21–23, 24–26, 18–20; 27–30 > 21–23, 24–26, 18–20
	21-23	107	185.47				
	24-26	136	171.41	26.016	4	<0.001	
	27-30	95	237.01				
	30+	9	277.78				
	Total	388					

The Mann–Whitney U results indicate that undergraduate students consistently scored significantly higher than postgraduate students across all dimensions: computer security ($U=13{,}477.50$, $p<.001$; $\eta^2 = .055$), malicious software ($U=13{,}297.50$, $p<0.001$; $\eta^2 = .059$), web security and social engineering ($U=12{,}785.00$, $p<.001$, $\eta^2 = 0.071$), and security on social network sites ($U=13{,}233.50$, $p<.001$; $\eta^2 = 0.060$), as seen in Table 5. The effect sizes ranged from small to medium, with the largest difference observed in web security and social engineering, suggesting that, while statistically robust, educational level accounted for only a modest proportion of the variance in students' self-efficacy.

Table 5. Mann-Whitney U Test for education level differences

Dimension	Education level	N	Mean rank	Sum of ranks	U	p
CS	Undergraduate	218	217.68	47453.50		
	Postgraduate	170	164.78	28012.50		
	Total	388			13477.500	<0.001
MS	Undergraduate	218	218.50	47633.50		<0.001
	Postgraduate	170	163.72	27832.50	13297.500	
	Total	388				
WSS	Undergraduate	218	220.85	48146.00		
	Postgraduate	170	160.71	27320.00		
	Total	388			12785.000	<0.001
SSN	Undergraduate	218	218.80	47697.50		
	Postgraduate	170	163.34	27768.50		
	Total	388			13233.500	<0.001

DISCUSSION

In today's global economy, students must be able to use the internet not just safely, effectively, and ethically, but also as validated sources of information. The internet has developed as an integral part of worldwide education, allowing students not only to access validated sources of information but also to participate socially, academically, and professionally with other students. The ability to use the

internet safely is an essential skill, not only for students in an academic sense but also for personal development.

As a result of these factors, it is clear that students are at risk for increased cyber threats if they do not have access to quality Internet/communication technology (ICT) infrastructure, guidance, or policies from universities, and equitable economic and social opportunities such as those found in Somalia. Therefore, this presents an urgent need to conduct research that will evaluate the experiences of Somali university students, assessing their confidence in internet safety, and investigating their beliefs related to internet safety within the areas of computer security, malicious software, website security/social engineering, and social networking sites.

In regard to this study, the research findings confirm that Somali university students demonstrate high levels of awareness across all four dimensions; however, awareness may not be the same throughout the country. This supports previous research findings that Somali university students lack knowledge of web security and malware, as indicated by Cavus and Ercag's (2016) examination of the reliability of the "scale for the self-efficacy and perceptions in the safe use of the internet" for Cypriot university students. Building on these comparative insights, the discussion now turns to the specific research questions.

Research Question 1 examined the opinions and perceptions university students had on their use of the internet safely with regard to computer security. Moreover, to what extent did the perceptions related to computer security vary by gender, age, and educational attainment? In terms of computer security, the mean scores for our Somali sample (M=3.25) were the lowest. Our analysis indicates that Somali students, similar to Cavus and Ercag's (2016) study on Turkish students, have a significantly lower level of competency and access to formalized cybersecurity education than do students from developed countries with better ICT infrastructures. Our findings support the conclusion that the majority of Somali students do not have formalized exposure to structured cybersecurity education. In addition to having poorer access to formalized education, the majority of Somali students rely heavily on informal means of learning (e.g., family, friends, and peers); therefore, we expect a greater number of Somali students to be vulnerable because they rely on informal learning and thus have an inadequate understanding of securing their online activity.

Regarding Research Question 2, the study seeks to examine university students' views and experiences regarding safe internet use from the perspective of malware (malicious software), and whether there are differences by gender/age/level of education. As discussed above, Somali respondents had very low scores for malware (M = 3.28) due to the lack of formalized training in their culture. More comprehensive research conducted elsewhere (for example, the study by Cavus and Ercag (2016)) indicates that although there is an increasing awareness of social networking and web security, significant knowledge gaps remain among the students surveyed.

Compared to the previous, Research Question 3 addresses students' views and experiences regarding safe internet use as it relates to the internet and Web3, Psychology (information technology), and BlackBerry (social networking). Again, there is a slightly higher awareness of WSS in the Somali sample (M = 3.39) than in the technical domains; WSS scores fall within the high range of our study (3.01-4.00). Thus, this indicates that Somali students lack the ability to use or address malware or computer-level security risks (computer-level security risks) available to them, but that previous/current exposure to various social media platforms has helped raise their awareness of the potential risks related to these areas. This finding adds originality by highlighting how socio-digital realities in Somalia, where mobile connectivity and social platforms are dominant, shape students' risk perceptions differently from those in contexts like Cyprus.

Research into countries other than Cyprus (e.g., Africa and other parts of the world) is a prudent way to make comparisons. Research by Magen-Nagar and Shonfeld (2018) indicated that internet self-efficacy is an independent predictor of engaging positively with digital learning, while research by Aithal and Aithal (2019) showed that students from developing countries generally have difficulty

protecting their devices from malware due to inadequate technical expertise. Similarly, we see evidence of this trend in our findings for Somalia. A majority of Somali respondents feel that they are more adept at handling social risks than protecting themselves from malware or technical breaches. As confirmed by Livingstone and Helsper (2010), training people to stay safe online helps reduce unsafe behaviours. This finding is especially true for Somali institutions, many of which do not provide any systematic training.

Research Question 4 further extends our research to examine university students' perceptions and attitudes toward safe internet use when using social networking sites (SNS) and how these attitudes and perceptions differ by gender, age, and higher education attainment. Similar to our findings on web security, the majority of Somali university students reported relatively high levels of internet self-efficacy when using SNS (mean = 3.38), indicating their awareness of privacy risks and the need to use safe practices on these platforms.

Although regional specificity is one of the unique aspects of this study, the inclusion of demographic factors is also considered very important. Most previous research focused on stable geographic environments with access to technical infrastructure; however, this study shows significant variability in perceptions of internet safety self-efficacy among Somali students, based on demographic variables (i.e., gender, age, and educational attainment). In contrast, male students demonstrated higher levels of self-efficacy in almost all areas, except sport; older students reported the highest levels of self-efficacy for the items analysed in this study, and undergraduate students' perceived self-efficacy was significantly greater than that of postgraduate students. These findings provide the first empirical evidence of the influence of socio-demographics on internet safety self-efficacy, particularly in vulnerable educational settings (Oroma et al., 2013; Wu & Tsai, 2006).

From an academic perspective, implications for future research on this topic fall into two categories. The positive implications of this study indicate that the students have a strong understanding of social and web security issues; thus, building upon this foundation through appropriate interventions will allow Somali institutions of higher education to contribute to the development of digital citizenship and resilience. The negative implications of this study indicate that students scored significantly lower in CS and MS, indicating they are significantly more vulnerable to malware infections, data breaches, and unauthorized access. These areas require increased attention in the curriculum during the planning process, through the inclusion of practical modules on password security, antivirus, and malware recognition.

The importance of these findings in Somalia cannot be understated. By increasing students' cyber security self-efficacy, not only will individuals protect their own personal information but also build on a foundation of increased trust and effectiveness within higher education, The integration of digital literacy and cyber security awareness modules into the university curriculum will allow learners to engage in a global digital learning environment, Additionally, through the creation of gender-sensitive and age-appropriate interventions to help close demographic gaps will create more equitable results and eliminate digital divides in Centers of Higher Education in Somalia.

As a result of this study, we provide evidence-based insights into Somali university students' perceptions and self-efficacy regarding internet safety across four primary areas of focus: computer security, malicious software, web security and social engineering, and security on social networking sites. While our findings demonstrate a fairly moderate to high level of awareness across these four areas, they also emphasize the need for localized educational interventions focused on the particular digital literacy and cybersecurity self-efficacy needs of these students, especially in technical areas, in an unstable digital higher education environment.

Last, the discussion demonstrates a clear connection to Research Questions 1 to 4, which provide a direct relationship between students' perceptions of their particular domains and their demographic characteristics, thereby providing the framework for safe internet use.

CONCLUSION

The findings of this research are particularly relevant in Somalia and other emerging nations, as they highlight the potential risks faced by university students through internet use due to the fragility of their ICT infrastructure, the degree of digital literacy of the population, and socio-economic disparities. The research demonstrates how the development of Somali students' perceptions of their ability to use the internet safely and their understanding of the potential threats associated with that use can be improved across four primary areas of computer security: malware, web security, social engineering, and social network security. The information gathered from a volunteer sample of 388 respondents provides insight into the strengths and weaknesses of the digital skills of Somali university students at a critical time of opportunity for development. While there is relative confidence in the ability of Somali university students to use the internet safely, the data indicate many vulnerable areas that expose them to potential threats in the online environment.

This study finds multiple indications of gender and age differences among the respondents. Male respondents expressed greater confidence than female respondents in managing the potential risks associated with their online presence and that of their peers. Additionally, the findings from this research can serve as a strong basis for developing curricula and systematic cybersecurity training for institutions of higher education in Somalia. Addressing the demographic divide and ensuring equal access to digital training opportunities for young and female university students will be necessary to develop equitable digital skills in Somalia. By identifying the strengths and weaknesses regarding students' internet self-efficacy and perceptions of safety, this study can guide the implementation of targeted support for Somali university students to enhance their digital skills and online protection. University administrators and policymakers will benefit from data-driven recommendations on developing effective cybersecurity education programs for these students, which will improve their academic performance and ultimately create a safer digital learning environment in Somalia and similar environments.

Although this study has many benefits, it has limitations, such as a sample limited to students from the northern regions of Somalia, potentially reducing the generalizability of the results to other regions of Somalia or other contexts. Another limitation is that the collected data consisted only of participants' self-reports; therefore, it is subject to reporting bias or personal opinion, which could affect the reliability of the results. The study provides valuable insights into improving students' digital competence and cybersecurity awareness at Somali universities. These include: (a) integrating comprehensive cybersecurity education into their university curricula; (b) implementing targeted intervention(s) to reduce the gap between males and females and younger students and older students in internet use; (c) ensuring that educational institutions improve access to the internet; (d) and (e) collaborating with internet service providers to provide discounted data packages for educational purposes. It is through such measures that a safer and more effective digital learning environment can be established, leading to enhanced institutional performance and improved technological proficiency among students.

Future research could adopt mixed-methods or longitudinal designs to explore how university students' internet safety self-efficacy and behaviours develop over time and in response to cybersecurity interventions. Additionally, including universities from diverse regions of Somalia and similar resource-constrained higher education contexts would help make the findings more generalizable and enable clearer comparisons of students' perceptions of safe internet use across regions and cultures.

REFERENCES

Adala, A. A. (2016). *Current state of advancement of Open Educational Resources in Kenya.* UNESCO Institute for Information Technologies in Education. http://iite.unesco.org/pics/publications/en/files/3214744.pdf

Ahmed, A. A., Elmi, A. H., Abdullahi, A., & Ahmed, A. Y. (2023). Cybersecurity awareness among university students in Mogadishu: A comparative study. *Indonesian Journal of Electrical Engineering and Computer Science, 32*(3), 1580–1588. https://doi.org/10.11591/ijeecs.v32.i3.pp1580-1588

Aithal, P. S., & Aithal, S. (2019). Analysis of higher education in Indian National Education Policy Proposal 2019 and its implementation challenges. *International Journal of Applied Engineering and Management Letters*, *3*(2), 1-35. https://doi.org/10.47992/IJAEML.2581.7000.0039

Bećirović, S., Dervic, M., & Mattoš, B. (2025). Exploring the factors affecting students' internet habits, self-efficacy in e-learning, and academic achievement: Structural equation modeling approach. *Sage Open, 15*(2), 1–21. https://doi.org/10.1177/21582440251339286

Bromall, N., Draus, P., Mishra, S., Slonka, K., & Trunkos, J. (2025). Cybersecurity awareness among post-secondary students. *Issues in Information Systems*, *26*(3), 149-157.

Caudill, J. G., & Terrell, R. (2010). Integrating online security into the undergraduate curriculum. *Theory of Cryptography Conference.* https://api.semanticscholar.org/CorpusID:113032914

Cavus, N., & Ercag, E. (2016). The scale for the self-efficacy and perceptions in the safe use of the internet for teachers: The validity and reliability studies. *British Journal of Educational Technology, 47*(1), 76–90. https://doi.org/10.1111/bjet.12217

Fatokun, F. B., Hamid, S., Norman, A., & Fatokun, J. O. (2019). The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: an empirical investigation on Malaysian universities. *In Journal of Physics: Conference Series* (Vol. 1339, No. 1, p. 012098). IOP Publishing. https://iopscience.iop.org/article/10.1088/1742-6596/1339/1/012098/meta

Getenet, S., Cantle, R., Redmond, P., & Albion, P. (2024). Students' digital technology attitude, literacy and self-efficacy and their effect on online learning engagement. *International Journal of Educational Technology in Higher Educatio*n, *21*, Article 3. https://doi.org/10.1186/s41239-023-00437-y

Gure, H. O., & Rasool, S. W. (2024). Impact of social media on education and students in Somalia: A comprehensive overview. *International Journal of Human and Society*, *4*(2), 216–229. https://ijhs.com.pk/index.php/IJHS/article/view/551

Jauhiainen, J. S., Ntinda, M. N., & Sutinen, E. (2025). Integrating generative AI to higher education systems in Africa: Reflections from tests in Namibia. *Proceedings of the IST-Africa Conference, Nairobi, Kenya,* 1–8. https://doi.org/10.23919/IST-Africa67297.2025.11060488

Li, D. (2020). A review of the self-efficacy of learners through online learning. *Journal of Humanities and Education Development, 2*(6), 526–533. https://doi.org/10.22161/jhed.2.6.17

Liu, M., Cai, Y., Han, S., & Shao, P. (2023). Understanding middle school students' self-efficacy and performance in a technology-enriched problem-based learning program: A learning analytics approach. *Journal of Educational Technology Systems, 51*(4), 513–543. https://doi.org/10.1177/00472395231174034

Livingstone, S., & Helsper, E. (2010). Balancing opportunities and risks in teenagers' use of the internet: The role of online skills and internet self-efficacy. *New Media & Society, 12*(2), 309–329. https://doi.org/10.1177/1461444809342697

Magen-Nagar, N., & Shonfeld, M. (2018). The impact of an online collaborative learning program on students' attitudes towards technology. *Interactive Learning Environments, 26*(5), 621–637. https://doi.org/10.1080/10494820.2017.1376336

Oroma, J. O., Kiden, S., Maghendha, M. W., & Ntiyani, S. (2013, May). Perspectives on underutilisation of ICT in education in Tanzania, Uganda and Kenya. *Proceedings of the IST-Africa Conference & Exhibition* (pp. 1–11).

PricewaterhouseCoopers. (2024). *Strengthening cyber defences: The road to resilience in East Africa.* https://www.pwc.com/mu/en/east-africa-dti/2025-East-Africa-DTI-Survey-Insights.pdf

Putriani, S., & Apriani, R. (2022). Impacts of digital technostress and digital technology self-efficacy on intentions to use fintech in Indonesia. *Jurnal Reviu Akuntansi Dan Keuangan*, *12*(1), 210–227. https://doi.org/10.22219/jrak.v12i1.20801

Somali Research and Education Network. (2024). *State of ICT in Somali universities and research institutions: Current realities and future possibilities.* https://doi.org/10.20374/sorer/508

Tabachnick, B., & Fidell, L. (2013). *Using multivariate statistics* (6th ed.). Pearson.

Tadesse, T., & Gillies, R. M. (2015). Nurturing cooperative learning pedagogies in higher education classrooms: Evidence of instructional reform and potential challenges. *Current Issues in Education, 18*(2), 1–17. https://cie.asu.edu/ojs/index.php/cieatasu/article/view/1374

Tick, A., & Mai, P. T. (2024). Cybersecurity awareness and the behaviors of higher education students using smartphones. *Acta Polytechnica Hungarica*, *21*(2), 7–24. https://doi.org/10.12700/APH.21.12.2024.12.7

Ulfert-Blank, A. S., & Schmidt, I. (2022). Assessing digital self-efficacy: Review and scale development. *Computers & Education, 191,* 104626. https://doi.org/10.1016/j.compedu.2022.104626

UNESCO. (2023). *UNESCO and Somalia moved the needle on digital learning in a conflict-affected country*. UNESCO. https://www.unesco.org/en/articles/unesco-and-somalia-moved-needle-digital-learning-conflict-affected-country

Unwin, T., Kleessen, B., Hollow, D., Williams, J. B., Oloo, L. M., Alwala, J., Mutimucuio, I., Eduardo, F., & Muianga, X. (2010). Digital learning in Africa: Barriers, opportunities and policy options. *International Journal of Educational Development, 30*(6), 553–564. https://doi.org/10.1016/j.ijedudev.2010.04.004

Vortia, W. (2025). Modelling cybersecurity awareness, perceived threats, and secure online behavioural intentions among university students: A PLS-SEM approach. *Magna Scientia Advanced Research and Review*s, *14*(2), 96–111. https://doi.org/10.30574/msarr.2025.14.2.0094

Wu, Y. T., & Tsai, C.-C. (2006). University students' internet attitudes and internet self-efficacy: A study at three universities in Taiwan. *Cyberpsychology & Behavior*, *9*(4), 441–450. https://doi.org/10.1089/cpb.2006.9.441

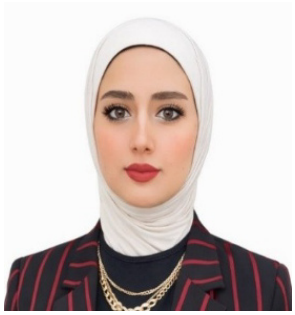
Yankson, R., Bondzie, S., Resciniti, D., Marquez, N., Chow, N., & Atele-Williams, T. (2025). Enhancing digital forensics in higher education: The role of experiential learning in bridging the skills gap. *Proceedings of the 12th IFIP International Conference on New Technologies, Mobility and Security, Paris, France,* 51–57. https://doi.org/10.1109/NTMS65597.2025.11076904

AUTHORS

Nuriye Sancar received her BSc in Applied Mathematics and Computer Science from Eastern Mediterranean University in 2010. She completed her master's and doctorate degrees in the Department of Mathematics at Near East University in 2012 and 2018, respectively. She is presently an Associate Professor in the Department of Mathematics at Near East University. She has authored numerous scientific publications in journals indexed by leading international databases. Her research interests include data analysis, statistical and regression modeling, metaheuristic optimization techniques, validity and reliability studies, and survival analysis.

Abdiwahab Abdillahi (born February 16, 1994) received his BSc in Business and is currently an MSc student in Computer Information Systems at Near East University, where he is in the thesis stage of his graduate studies. His MSc thesis focuses on artificial intelligence soft skills. His current research interests include different aspects of artificial intelligence, IoT devices, and machine learning.

Charles Zulu Yonmah is a Master's candidate in the Department of Computer Information Systems at Near East University. His research focuses on student self-efficacy and perceptions of the safe use of the internet, with particular interest in how digital awareness and confidence influence online behavior in educational contexts.



Ghufran Fareed is a software developer and a Master's student in Computer Information Systems at Near East University. She specializes in designing and implementing intelligent software solutions with a focus on cybersecurity, machine learning, and blockchain technologies.

Since 1995, **Professor Dr Nadire Cavus** has been with Near East University, where she is currently a Lecturer in the Department of Computer Information Systems. She is also a director of the Computer Information Systems Research and Technology Centre. She has published more than 50 scientific articles in world-renowned journals. Moreover, she has published many books and book chapters with world-renowned academic publishers. Her research interests include e-learning, m-learning, learning management systems (LMS), virtual learning environments, educational technologies, artificial intelligence, and information systems.