Information Sciences Letters

Volume 12
Issue 1 *Jan. 2023*

Article 13

2023

Cybersecurity Awareness in African Higher Education Institutions: A Case Study of Sudan

M. E. Eltahir
College of Humanities and Sciences, Ajman University, Ajman, UAE\\ Humanities and Social Sciences Research Center (HSSRC), Ajman University, Ajman, UAE, m.babiker@ajman.ac.ae

O. S. Ahmed
College of Humanities and Sciences, Ajman University, Ajman, UAE\\ Humanities and Social Sciences Research Center (HSSRC), Ajman University, Ajman, UAE, m.babiker@ajman.ac.ae

Information Sciences Letters
An International Journal

http://dx.doi.org/10.18576/isl/120113

Cybersecurity Awareness in African Higher Education Institutions: A Case Study of Sudan

M. E. Eltahir[1,2,*] *and O. S. Ahmed*[1,2]

[1]College of Humanities and Sciences, Ajman University, Ajman, UAE
[2]Humanities and Social Sciences Research Center (HSSRC), Ajman University, Ajman, UAE

Received: 10 Jul. 2022, Revised: 23 Jul. 2022, Accepted: 3 Aug. 2022.
Published online: 1 Jan. 2023

Abstract: The crisis caused by the rapid spread of the coronavirus (COVID-19) has imposed a swift and profound change on teaching and learning methods. Consequently, most higher education institutions around the world, including African higher education institutions, have moved from face-to-face teaching to online learning and teaching, which has made the use of the internet by university students necessary and obligatory regardless of the risks associated with unsafe use. This quick move to online teaching and learning has exposed African universities to a greater risk of cybercrime. This prompted the researchers to investigate the cybersecurity awareness levels among undergraduate students at African higher education institutions based in the case country, Sudan. In an exploratory research approach, a survey was conducted on a convenience sample of 1,200 undergraduate students at six public universities in Sudan. The results show that most undergraduate students in Sudan higher educational institutions have low cybersecurity awareness levels. Further investigation using inferential statistics reveals that male students at the universities in Sudan have slightly higher levels of cybersecurity awareness than female students. Most of the participants believe that cybersecurity should be taught in schools; they are also willing to learn about cybersecurity. In addition, the results showed that students with advanced computer skills significantly differ from students with intermediate or basic computer skills in practicing cybersecurity.

Keywords: awareness, Africa, COVID-19, cybersecurity

1 Introduction

Information and communication technology (ICT) has become part of our working, social, and educational environment, particularly after the crisis resulting from the rapid spread of the coronavirus. COVID-19 imposed a process of rapid and profound change that included various political, economic, social, and educational levels [1]. This change was related to a group of new variables; notable among them is the need imposed by the crisis for the strict and universal application of the principle of "social distancing." This prompted the educational community in general, and researchers in the ICT field in particular, to think and research the implications of this crisis and its fate and the extent of its impact on the education sector.

The education sector represents one of the most prominent systems that has had to deal with the repercussions of the crisis [2]. Imposing the application of the principle of social distancing prevents face-to-face teaching and depends mainly on online teaching and learning systems [3]. However, these e-learning systems need to be effective and safe to ensure a regular and continuous course of interaction among students and between students and their teachers [4].

Most higher education institutions in different countries have exploited and employed ICTs to support e-learning through various e-learning applications [5]. With this increasing spread of ICT devices and tools, the number of users of the internet networks in African countries is constantly increasing, especially among undergraduate students, and access to the internet has become easier and less expensive [6], [7]. This fast move to online teaching and learning as an attempt to reduce the spread of COVID-19 has exposed African higher education institutions to a greater risk of cybercrime. A report published by Mimecast revealed an increase in cyberattacks within the beginning of the 2020 quarter across the world, including sub-Saharan Africa as well as the East Africa and North Africa regions. Among the continent's most recent targets are the Zimbabwe National University of Science and Technology and the Harare Institute of Technology. Between January and

*Corresponding author e-mail: m.babiker@ajman.ac.ae

March 2020, Mimecast found that the number of cyberattacks of all types has increased by 33%.

Along with discovering more than 60,000 fake COVID-19 websites out to steal information. Overall, discoveries rose by a third [8]. On the other hand, and according to the Brookings report released in 2018, the cybercrime threatening the business of African countries is greater than in any other country in the world. Although Africa is relatively limited in terms of its communication infrastructure, the low level of its residents' cybersecurity awareness has made it a prime target for cybercriminals [9]. Another study conducted by the Business Software Alliance in 2018 showed that 57% of business software installed in African countries and the Middle East has been hacked, which encouraged cyberattacks and caused a possible loss of $3.7 billion. The study concluded that these cyberattacks were closely related to the use of unlicensed software [10].

Cybercrime affects all aspects of life in Africa. According to the Africa Cybersecurity Report [11], published by Africa's leading cybersecurity consulting firm, Serianu, banks, and financial services in Africa have been hit; nearly a quarter of the losses are caused by cybercrime on the continent, followed by governments, e-commerce, transactions, and communications mobile phone menu. The nations of Africa will not prosper without dealing with cyberspace. However, most of the internet users in general and undergraduate students in particular in African countries are not properly educated about the safe use of cyberspace [12], which exposes these students to several risks related to the unsafe use of the internet, which can range from loss of information to cyber threats [13], [14]. The proper and safe use of the internet is thus crucial for all undergraduate students.

1.1. Significance and aim of the study

For most of the higher education institutions around the world moving towards online teaching and learning during the breakout of the coronavirus, awareness of cybersecurity is more important now than ever before. This study aims to shed light on the existing levels of awareness of cybersecurity among undergraduate students and suggests further work on this social and educational problem in an attempt to develop a culture of cyber safety among undergraduate students in African countries in general and Sudan in particular.

1.2. Research Questions

The researchers sought to address the following research questions to achieve the aims of this study:

1. RQ1. What are the students' attitudes towards cybersecurity awareness?
2. RQ2. Is there any significant difference in cybersecurity awareness levels according to students' gender?
3. RQ3. Is there any significant difference in cybersecurity awareness levels between students with different levels of computer skills?

2 Theoretical Framework

2.1 What is Cyberspace?

The word *cyber* is derived from *cybernetics*, and its Greek origin means directing and controlling [15]. Norbert Wiener defined it in 1948 as "*the scientific study of control and communication in the animal and the machine*" [16]. Weiner used the ancient Greek word *Kubernetes*, which means steersman, the man who operates the longship's rudder, to describe the principle of governing or directing a machine or system; the word translated into English as *cybernetics*. [15].

As for *cyberspace*, the US National Institute of Standards and Technology defines it as "*the complex environment resulting from the interaction of people, software and services on the internet using technology devices and networks connected to it, which does not exist in any physical form*" [17]. The US Department of Defense defines cyberspace as "*a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers*" [18]. Others define cyberspace as the environment in which communication over computer networks occurs [19]–[21]. The uses and forms of control over cyberspace or cyber sovereignty differ from one country to another depending on the priorities of those countries. Some of those priorities are security-related, political, intelligence-related, civil, or professional, or maybe purely information-related. The overall entity of cyberspace is formed by three basic components: the technical tools used, the procedures followed, and the human factor of programmers and users.

2.2 What is Cybersecurity?

According to the US National Institute of Standards and Technology, "*cybersecurity is the ability to protect or defend the use of cyberspace from cyber-attacks*" [22]. Cybersecurity can be defined as protecting networks, devices, electronic systems, and data from any penetration, disruption, modification, or illegal entry, use, or exploitation by cyberattacks on

victims ranging from business enterprises to personal devices. Network security, application security, information security, organizational security, disaster recovery, and business continuity are some of the categories that need to be protected. Network protection and application security are concerned with protecting computer networks as well as ensuring that software and hardware are free of threats and vulnerabilities. Disaster recovery is an organization's response in the event of data loss and the effort to regain operating capabilities to continue the organization's work [23], [24].

2.3 Types of cybersecurity threats

According to [23] there are four common types of cybersecurity threats.

Phishing: Phishing is the act of sending fake emails that look like they come from a trustworthy source. The aim is to steal confidential information such as credit card numbers and login credentials. It is the most common cyber threat. One can protect oneself from this type of threat by dealing properly with unknown source emails or using a technical solution that filters malicious emails.

Malware: Malware is a type of program designed to gain unauthorized access or harm a computer.

Ransomware: Ransomware is a sort of malware. It aims to extort money by preventing access to files or the computer system before a ransom is paid. Paying the ransom does not ensure that the files or device will be restored.

Social engineering: Social engineering is a method utilized by attackers to steer users toward exposing private information. They may call about a financial charge or for access to one's personal information. Social engineering may be blended with any of the threats noted above to make users much more likely to click on links, download malware, or believe a malicious source is genuine.

2.4 ICT and Cybersecurity Trends in Africa

All countries, whether developing or developed, are affected by ICT. African countries are no exception; they also seek to resolve ICT challenges' social, economic, educational, cultural, and political issues [25], [26]. According to the International Telecommunication Union Yearbook of Statistics [6], African countries as a group score below world averages on the internet user indicators. While the world average of individuals using the internet was around 53.6 per 100 inhabitants, in 2019, the average in African countries was about one-half of this (Figure 1). However, African internet usage is growing rapidly. Figure 2 provides an overall picture of the increasing number of internet users in African countries during the past 15 years.

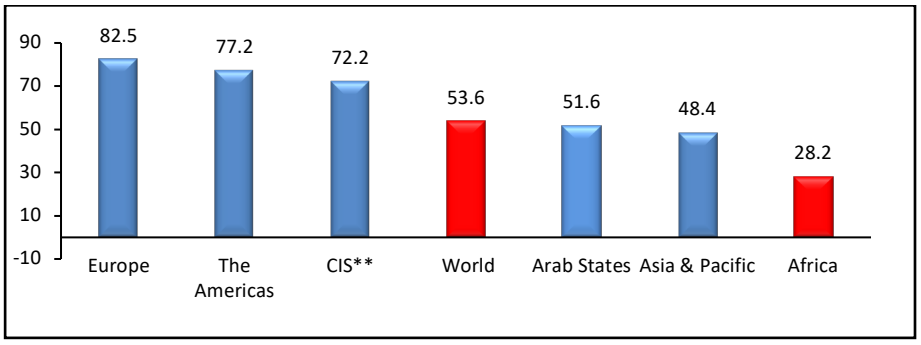

Fig. 1: Individuals Using the Internet per 100 Inhabitants in African Countries as Compared to 2019 World Averages

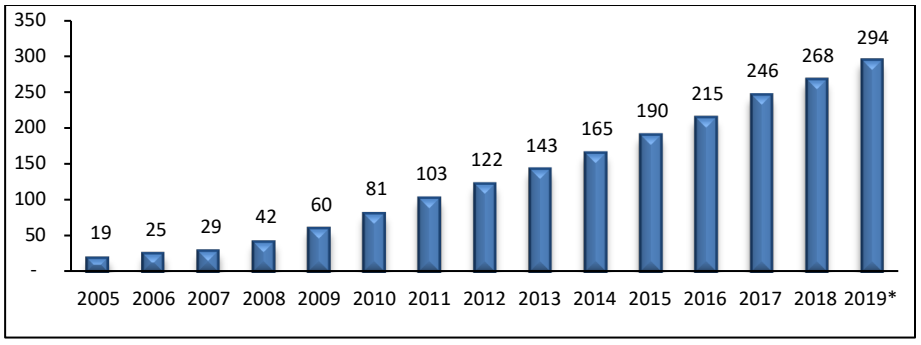

Fig. 2: Individuals Using the Internet in African Countries (In Millions), 2005–2019

Because of the global nature of cybercrime, many patterns of cybercrime seen globally also affect Africa, including violations of privacy, bullying, hacking and phishing, publishing illegal content, digital piracy, cyberextortion, identity theft, and social media scams [27] (Marcum, & Higgins, 2019). However, because internet users are increasing significantly in Africa, many of these cybercrime trends will become particularly acute and pose a significant risk [28] (African Union Commission, 2016).

The African Union Commission and Symantec released a report analyzing cybersecurity trends and government responses in Africa [28]. The report provides an overview of developments in cybersecurity-related to cybercrime on the African continent. The report notes that Africa can be considered a fertile environment for cybercriminals due to a lack of security capabilities, the absence of appropriate legislation, and insufficient awareness of cybersecurity measures. Another issue raised by the report is that most of the African countries do not have clear legal provisions on cybercrime and applicable electronic evidence. The report concludes that the current state of legislation on cybercrime and electronic evidence in Africa is unsatisfactory and that only 20% of the African states seemed to have the minimum legislation in force. African governments will need to develop and implement successful policy, legislation, and awareness campaigns to combat the increasing wave of cyberthreats to help Africa achieve its full potential.

2.5 Previous Study

Cybersecurity is an important problem affecting internet users not only in African higher education institutions but also in schools around the world, as demonstrated in the study of [29] on determining levels of educator awareness in Turkish schools regarding cyberbullying. Teachers' awareness was measured to determine the extent to which it affects their daily lives, with a focus on personal cybersecurity and possible precautions. A survey was distributed to 184 teachers in various Turkish schools. The study found that teachers had a medium level of awareness about cyberbullying in general. Furthermore, based on gender and frequency of use of the internet, teachers' awareness levels of cyberbullying were significantly different.

A study by [30] examined the information security awareness levels of students in the Kyrgyz Republic. A total of 172 students from different departments of Kyrgyz Universities participated in the study. The study shows that, despite the vast number of reports on cybercrime, awareness of cybercrime was quite poor among students. Study results pointed out that students were often unaware of many aspects of computer crime, even though information technology is widely used. The study recommended that students be taught how to be safe when using information networks to prevent them from becoming victims of cybercrime.

Kim [31] conducted a study aimed at investigating the attitudes of undergraduate and graduate students in a business college in New England toward cybersecurity awareness.

The study found that college students understood the value and the need for information security awareness, but many of them were not involved in practicing it. A study by [32] aimed to explore cybersecurity behavior in five cybersecurity aspects among higher education students in Malaysia. The study depended mainly on a questionnaire distributed to 128 undergraduate students at a private university. The results show that cybersecurity behavior among students was unsatisfactory in all five cybersecurity aspects.

A study by Albarashdi [33] showed that most cybercrime is related to the use of social media, particularly Facebook. The study employed a qualitative approach by analyzing cybercrime statistics released by the Centre for Information Safety of the Sultanate of Oman, additionally, the study interviewed 30 information security experts. The author concludes that further research is needed to develop radical solutions for combating cybercrime by understanding its causes.

Senthilkumar and Easwaramoorthy's study [34], entitled "A Survey on Cybersecurity Awareness Among College Students in Tamil Nadu," relied on the descriptive-analytical approach, as the study used a web-based questionnaire directed at 500 college students from five different cities. The survey examined cybersecurity awareness of three main cyberattacks: virus attacks, phishing with emails, and threats to spread personal details. According to the study's findings, 70% of the students were aware of virus attacks and using antivirus software. The study concludes that the degree of awareness of cybersecurity among college students in Tamil Nadu is at a good level that can help them protect themselves from cyberattacks.

As for African countries, several studies have concerned the awareness of cybersecurity among teachers, students, and internet users in general [14], [35]-[38]. However, few studies investigate the issue of the awareness of cybersecurity among educators and students in higher educational institutions.

Most of these studies show that students are not aware of such threats related to using the internet and that there is a need for cybersecurity awareness campaigns and education initiatives that provide knowledge and skills to students to help them safely surf online. For instance, the [35] study presents an initiative in the form of a play-based curriculum, which helps students to become safer online and teaches learners the risks related to using the internet. The study relied on a quantitative

survey of elementary school students in South Africa to determine whether a game-based curriculum could be used to improve awareness of cybersafety. A significant statistical result from the study shows that 35% of students hid their online activities from their parents and 61% of parents and teachers did not supervise their students' or children's online use.

3 Methodology

An exploratory research approach was used due to its ability to achieve the aims of this study. A questionnaire was designed and distributed to undergraduate students in six public educational institutions in Sudan in the first semester of the 2020–2021 academic year. Since Sudanese university students have different levels of cyber knowledge, we chose to focus on the largest universities with good information technology infrastructure as the baseline for our study. These included undergraduate students in the fields of arts, sciences, and education at the University of Khartoum (n = 221), the Sudan University of Science and Technology (n = 220), Al Neelain University (n = 232), Omdurman Islamic University (n = 171), the International University of Africa (n = 121), and Nile Valley University (n = 203). Overall, the sample included 1,168 subjects who participated in the survey, as shown in Table 2.

The content of the survey tool was based on the literature review of recent studies on cybersecurity awareness [32], [36], and [39]-[42]. Three key aspects were taken into consideration when designing the questionnaire: participants' knowledge of cybersecurity, cybersecurity practice, and cybersecurity education. These aspects were adopted based on a [42] study, which found that participants' levels of cybersecurity awareness were connected to their levels of cybersecurity knowledge, practice, and education.

The survey tool consisted of two sections. The first section included the demographic background of the students. The second section consisted of 35 statements intended to determine the students' attitudes towards cybersecurity awareness through investigating their knowledge, the practice of cybersecurity, and attitude towards cybersecurity education. Five-point Likert scale statements were used for responses to questionnaire statements.

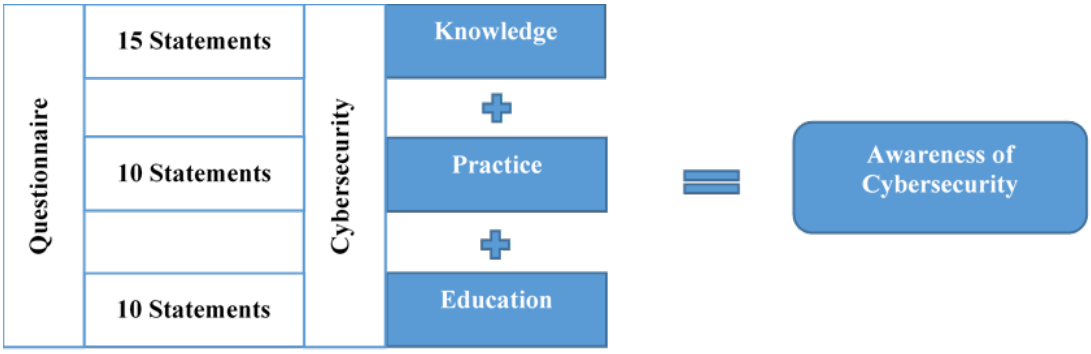

Fig. 3: Design of the Study

3.1. Validity and Reliability

To test the questionnaire's validity, copies of it were sent to four scholars who specialize in methodology, network, and information security, educational technology, and educational psychology. The content was adjusted according to their suggestions and comments. The reliability of the questionnaire was also verified by applying it to a pilot sample consisting of 35 undergraduate students who were not part of the research sample. Using Statistical Package for Social Sciences (SPSS) software, the Cronbach's alpha coefficient was computed, yielding a result of 0.79, which indicated an acceptable level of internal consistency, as shown in Table 1.

Table 1: Cronbach's Alpha Coefficients of Reliability for the Questionnaire

Aspects	No. of Statements	Cronbach's Alpha Reliability Coefficient
Knowledge of Cybersecurity	15	0.798
Cybersecurity Practice	10	0.766
Cybersecurity Education	10	0.740
Total Reliability	35	0.797

3.2. The Sample

Researchers selected 1,200 undergraduate students at six public universities in Khartoum, Sudan's capital city, using convenience sampling, where it was easy to contact these students.

3.3. Procedure

Two versions of the questionnaire were designed; an online copy was created using Google Forms and distributed to the participants by email. The study's aim was explained in full in the invitation email, which also stated that all replies would be kept confidential. Hard copies of the questionnaire were distributed by hand. Of the 1,200 questionnaires distributed, 1,168 valid responses were returned. The following table summarizes the composition of the sample.

Table 2: Demographic Information

Institution Name		University of Khartoum	Sudan University of Science and Technology	Al Neelain University	Omdurman Islamic University	International University of Africa	Nile Valley University	Total
Gender	Male	109	113	121	101	69	142	655
	Female	112	107	111	70	52	61	513
Age	Below 20	97	79	87	81	66	132	542
	20–25	77	52	55	34	24	23	265
	26–30	35	39	41	19	16	25	175
	31–35	4	19	23	18	6	12	82
	36–40	3	23	24	9	4	8	71
	Over 40	5	8	2	10	5	3	33
Academic Status	Freshman	106	118	101	93	63	93	574
	Sophomore	48	69	64	58	35	52	326
	Junior	40	0	35	16	8	38	137
	Senior	27	33	32	4	15	20	131
Computer Skills Level	Basic	70	68	78	70	50	90	426
	Intermediate	122	133	129	98	53	97	632
	Advanced	29	19	25	3	18	16	110
Field of Study	Arts	98	63	64	46	46	59	376
	Education	69	111	112	76	45	100	513
	Sciences	54	46	56	49	30	44	279
Total		221	220	232	171	121	203	1,168
Percent		18.92%	18.84%	19.86%	14.64%	10.36%	17.38%	100%

4 Results and Discussion

The SPSS was used to investigate and answer the study questions. To investigate differences in responses according to participants' gender and computing skills, an independent sample *T*-test, an analysis of variance (ANOVA) for equality of means, and Schiff's multiple comparisons test were used to determine differences in means. The first section of the questionnaire dealt with the participants' demographic information. To find out the participants' attitudes in the second section of the questionnaire, a 5-point Likert scale was used (Strongly Disagree = 1, Disagree = 2, Neutral = 3, Agree = 4, and Strongly Agree = 5). The participants' responses were then categorized into five equal classes and the length of each class was calculated through the following equation: class length = (max. value – min. value) ÷ number of alternatives = (5 – 1) ÷ 5 = 0.80, as shown in Table 3.

Table 3: Distribution of Categories

Score	**Class (Extent of Means)**	**Represents**
5	4.21–5.00	Strongly Agree
4	3.41–4.20	Agree
3	2.61–3.40	Neutral
2	1.81–2.60	Disagree
1	1.00–1.80	Strongly Disagree

4.1. RQ1. What Are the Students' Attitudes Toward Cybersecurity Awareness?

In Section 2 of the survey tool, the researchers aimed to identify participants' attitudes toward cybersecurity awareness.

For each of the three aspects, average scores and standard deviations were calculated for each statement from the questionnaire, as displayed in Table 4.

Table 4: Descriptive Statistics for Participants' Responses Toward Cybersecurity Awareness

Statements	***N***	**Mean**	**S. Deviation**	**Description**
Knowledge of Cybersecurity				
1. I know much about internet network security measures	1,168	2.16	1.203	Disagree
2. I think the internet is safe	1,168	3.43	1.354	Agree
3. It's safe to shop online and use internet banking	1,168	3.45	1.300	Agree
4. I think I will never injure someone or be injured by someone due to internet usage	1,168	3.42	1.321	Agree
5. I have no problems with using a computer that does not have antivirus software installed	1,168	3.43	1.366	Agree
6. I know what the risks are when using the internet	1,168	2.17	1.143	Disagree
7. I know the risk of using non-genuine software	1,168	2.17	1.111	Disagree
8. I know the risk of clicking on an unknown email link	1,168	2.23	1.116	Disagree
9. I think using the internet with my mobile is more secure than using it with my PC	1,168	3.43	1.321	Agree
10. I think security measures are up to the provider, not the individual	1,168	3.42	1.333	Agree
11. I know what measures individuals should take for cybersecurity	1,168	1.91	0.839	Disagree
12. I know that cybersecurity is a priority within my institution	1,168	1.93	0.811	Disagree
13. I am aware of the institution's internet use policy	1,168	1.94	0.825	Disagree
14. I do pay attention to my institution material about cybersecurity	1,168	1.87	0.812	Disagree
15. I know to whom and how to report if I face cybersecurity problems in my institution	1,168	1.88	0.858	Disagree
Total mean	**2.59**			Disagree
Standard deviation	**1.11**			
Cybersecurity Practice				
16. I am using antivirus and firewall software to protect my computer	1,168	3.05	1.343	Neutral
17. I regularly scan my computer and storage devices	1,168	2.47	1.542	Disagree
18. I know the characteristics of a strong password	1,168	2.44	1.328	Disagree
19. I change my passwords regularly	1,168	2.70	1.135	Neutral
20. I regularly back up my important files	1,168	2.62	1.203	Neutral
21. I understand the risk of sharing peer to peer (P2P) files	1,168	2.55	1.448	Disagree
22. I ensure that sensitive data is protected on my mobile device	1,168	2.64	1.117	Neutral
23. I use filtering software to restrict access to harmful internet sites	1,168	2.51	1.133	Disagree
24. I don't open emails from unknown senders	1,168	2.68	1.025	Neutral
25. I use a pop-up blocker in my web browsers	1,168	2.31	1.421	Disagree
Total mean	**2.60**			Disagree
Standard deviation	**1.27**			
Cybersecurity Education				
26. People ought to receive cybersecurity education	1,168	3.97	0.931	Agree
27. Undergraduate students should be taught thoroughly about cybersecurity	1,168	3.51	1.091	Agree
28. Cybersecurity should be taught in schools	1,168	3.89	0.785	Agree
29. There ought to be more opportunities for cybersecurity training at higher education institutions	1,168	3.60	1.131	Agree
30. Higher education institutions should provide user-	1,168	3.51	1.081	Agree

Statements	*N*	Mean	S. Deviation	Description
friendly teaching materials online				
31. Individuals ought to teach themselves about cybersecurity	1,168	3.56	1.037	Agree
32. I would like to be taught about cybersecurity	1,168	3.54	1.058	Agree
33. These days, education about cybersecurity is particularly necessary	1,168	3.56	1.053	Agree
34. I use educational resources to educate myself about cybersecurity	1,168	3.18	1.120	Neutral
35. Cybersecurity education is necessary even when using security software	1,168	3.51	1.049	Agree
Total mean	**3.58**			Agree
Standard deviation	**1.03**			
Total mean for the three aspects	**2.92**			Neutral
Standard deviation	**1.14**			

According to Table 4, most respondents do not agree with the statements related to the Knowledge of Cybersecurity aspect, with a total mean of 2.59. The responses to the statements 14 and 15 in Table 4 also reveal that they were the lowest averages (1.87 and 1.88, respectively), which shows that the majority of students do not pay attention to their institution material about cybersecurity and do not know to whom and how to report if they face cybersecurity problems in their institution because they are not acquainted with their institution's internet use policy.

As for the second aspect of the questionnaire about cybersecurity practice, the students' responses reported in Table 4 indicate that the level of practicing cybersecurity among undergraduate students is very low, with a total mean of 2.60 and a standard deviation of 1.27. The responses to statements 25 and 18 had the lowest averages (2.31 and 2.44, respectively), which shows that the majority of students do not know the characteristics of a good password and they do not use a pop-up blocker in their web browsers to prevent unwanted pop-ups from interfering with their browsing experience (this interference is because most of the pop-ups are ads, malware, and other unwanted windows). This result is consistent with the previous studies of both [31], [40] the results of which conclude that cybersecurity awareness has a major impact on cybersecurity practice.

The results of the students' responses related to cybersecurity education presented in Table 4 reveal that all participants hold a positive opinion about cybersecurity education, with a total average value of 3.58. This result confirms the importance of education in the field of cybersecurity and attention to educating students because reliance on modern technologies and the internet will increase, especially in light of crises and disasters such as the COVID-19 pandemic, and thus the risks related to the unsafe use of the internet networks will also increase.

The responses to statements 26 and 28, with average values of 3.97 and 3.89, indicate that most respondents agree that people ought to receive cybersecurity education, and they are also agreed that cybersecurity should be taught in schools. Asked if they use educational resources to teach themselves about cybersecurity (statement 34), participants hesitated to agree or disagree; most of the responses were Neutral. It can be supposed that this is not because of the students' unwillingness to learn about cybersecurity but because educational resources do not exist or, if they do exist, they are not enough, and this finding is in line with the report done by the African Union Commission [28]. That is, cybersecurity education and training centers are not available, and there is a lack of local expertise in most African states. For the other statements, all the participants agreed about the importance of cybersecurity education.

It is clear that the total mean for the three aspects (2.92) related to the students' attitudes toward cybersecurity awareness shows a poor level of student knowledge of cybersecurity in most of the items of the questionnaire, and this result is consistent with previous studies [30], [32], [36] and reveals that most undergraduate students in African countries do not have sufficient awareness about cybersecurity.

4.2. RQ2. Is there any significant difference in cybersecurity awareness levels according to students' gender?

To determine the differences in the mean responses according to the gender of the samples an independent sample T-test was conducted. The results of Levene's test for homogeneity of variances are not significant as shown in Table 5 ($p = 0.427 > 0.05$). It can be concluded that variances for each group were the same. The result also shows that there are significant differences between the mean values of females and males regarding cybersecurity awareness levels ($p = 0.00 < 0.05$), where males score higher than females, as shown in Table 6. This result is consistent with a previous study [38].

Table 5: Independent Sample T-Test of Cybersecurity Awareness Levels Between Student Genders

		Levene's Test for Equality of Variances		***T*-test for Equality of Means**			
		F	**Sig.**	***t***	**df**	**Sig. (two-tailed)**	**Mean Difference**
Mean Awareness	Equal variances assumed	.630	.427	-20.151	1,166	.000	-.36529
	Equal variances not assumed			-20.085	1,085.738	.000	-.36529

Table 6: Means and Standard Deviations of Students' Responses According to Gender

Gender	***N***	**Mean**	**S. Deviation**
Female	655	2.7619	.30379
Male	513	3.1272	.31210

4.3. RQ3. Is there any significant difference in cybersecurity practice levels between students with different levels of computer skills?

A one-way ANOVA was used to determine whether there are any statistically significant differences between students with different computer skill levels (Basic, Intermediate, and Advanced) in their cybersecurity practice levels.

From Table 7, it is clear that the mean and sample size for each computer skills level is not equal. Thus, Levene's test was used to examine the homogeneity of variance. Levene's test (Table 8) shows that the homogeneity-of-variance assumption was not met (p = .000). As such, Welch's F-test and the Brown–Forsythe F-test were used (Table 9). The one-way ANOVA of student's average scores on the measure of cybersecurity practice revealed a statistically significant main effect (Welch's F [2, 319.212] = 85.579, p = 0.00 < .05, the Brown–Forsythe F [2, 554.244] = 77.452, p = 0.00 < .05), indicating that students with different computer skills had significantly different average scores on the measure of cybersecurity practice level.

To determine which level of computer skills differed significantly among the three levels, the Games-Howell post hoc test was applied since the homogeneity-of-variance assumption was violated. Multiple comparisons in Table 10 show that significant differences between students' computer skills levels were driven by significant differences between students with advanced computer skills and students with intermediate computer skills—the mean difference between them was .47050 (p = 0.00)—as well as between students with advanced computer skills and students with basic computer skills; the mean difference between them was .79631 (p = 0.00). The mean difference between students with intermediate computer skills and students with basic computer skills was .32581 (p = 0.00). This indicates that there are significant differences between each of these groups on the measure of cybersecurity practice level.

Table 7: Means and Standard Deviations of the Students' Responses to Cybersecurity Practice Level According to Computer Skills Level

Computer Skills Level	***N***	**Mean**	**S. Deviation**
Basic	426	2.3446	.59853
Intermediate	632	2.6704	.75623
Advanced	110	3.1409	.59851
Total	1,168	2.5959	.72608

Table 8: Test of Homogeneity of Variances

		Levene Statistic	**df1**	**df2**	**Sig.**
Cybersecurity Practice Level	Based on mean	42.813	2	1,165	.000
	Based on median	39.051	2	1,165	.000
	Based on median and with adjusted df	39.051	2	1,157.283	.000
	Based on trimmed mean	44.539	2	1,165	.000

Table 9: One-Way ANOVA Robust Tests of Equality of Means

	Statistic[a]	df1	df2	Sig.
Welch	85.579	2	319.212	.000
Brown–Forsythe	77.452	2	554.244	.000

a. Asymptotically *F* distributed.

Table 10: Games–Howell Post Hoc Test Statistics for Different Computer Skills: Multiple Comparisons

(I) Skill level in Using Computers	(J) Skill Level in Using Computers	Mean Difference (I-J)	Std. Error	Sig.*	95% Confidence Interval	
					Lower Bound	Upper Bound
Basic	Intermediate	-.32581	.04178	.000	-.4239	-.2277
	Advanced	-.79631	.06401	.000	-.9477	-.6450
Intermediate	Basic	.32581	.04178	.000	.2277	.4239
	Advanced	-.47050	.06451	.000	-.6230	-.3180
Advanced	Basic	.79631	.06401	.000	.6450	.9477
	Intermediate	.47050	.06451	.000	.3180	.6230

b. *The mean difference is significant at the 0.05 level.

5 Conclusions and Limitations

Research results show that a minority of respondents are familiar with the term "cybersecurity." Thus, these respondents understand that using the internet may expose them to a variety of risks, including invasion of privacy, loss of money or data, equipment damage, and surveillance of themselves or any institution to which they belong. However, we also found inconsistencies between the respondents' knowledge and practice. As with previous studies [38], [42] we found that respondents only took basic and inadequate security precautions, such as password protection and antivirus installation.

The study examined in detail the literature related to the concepts of cybersecurity as well as the risks of unsafe use of the internet and its impact on the African continent, especially in light of the spread of the COVID-19 pandemic. As far as we know, the novelty of this study is based on being the first to discover the level of cybersecurity awareness among undergraduate students in various higher education institutions in Sudan. Moreover, the study compared the levels of cybersecurity awareness and practice among undergraduate students according to specific variables (gender and level of computer skills) and concludes that male students have slightly higher levels of cybersecurity awareness than female students. In addition, the results reveal that students with advanced computer skills significantly differ from students with intermediate and basic computer skills in practicing cybersecurity. One of the important points of this study is that the majority of its respondents believe that cybersecurity should be taught in schools, and they are also willing to learn about cybersecurity.

Although this study adopted a rigorous research methodology, there are still some potential limitations that need to be addressed in future studies. First, this study deals with one country in Africa: Sudan. Therefore, due to variations in population among African countries, the generalizability of the findings of this study must be approached with caution. This study focuses on and investigates higher education students' attitudes towards cybersecurity awareness. Future studies can develop cybersecurity awareness and education frameworks for African countries.

6 Recommendations and Suggestions

Due to the increasing significance of cybersecurity, its serious threats, and related issues at the international level, awareness of cybersecurity has become extremely important and plays a pivotal role in protecting ourselves, our families, our society, and our countries. African higher education institutions cannot remain passive; they should promote a culture of cybersecurity awareness among their students, and they should raise cybersecurity awareness across the country by launching a youth-focused cybersecurity campaign. They must protect youth and their families and society and create the conditions for educating our future leaders by including cybersecurity awareness courses in undergraduate academic programs.

African governments should be convinced that there is a need for each African country to cooperate, share information, and develop comprehensive legislation and a proactive approach to meet these challenges and risks as well as to strengthen awareness and education mechanisms to stop everything that threatens the safety of their societies.

There should be cooperation between non-governmental organizations, telecommunications companies, civil society

organizations, and higher education institutions in African countries to increase cybersecurity awareness among students by providing educational resources regularly through appropriate communication media.

A unit or center has been established for the professional development of faculty members in many higher education institutions. It is recommended that these centers provide training courses on cybersecurity awareness. This training is vital for development in this field, and it should be an integral part of the ongoing professional development of faculty members and employees. Achieving this goal will reduce the number of people who are exposed to the threats of cybercrime in African states.

Acknowledgment

We would like to express our great appreciation to Professor Ahmed Babiker El-Taher, Chairman of the Nile Valley University Board in Sudan for his exceptional support during the planning and development of this research. In particular, we would like to thank all of his office team members who have given their time to facilitate the distribution of the research instrument. Their willingness to give their time generously was greatly appreciated.

Conflict of interest:

The authors declare that there is no conflict regarding the publication of this paper.

References

[1] Huang, R. H., Liu, D. J., Tlili, A., Yang, J. F., & Wang, H. H. *Handbook on facilitating flexible learning during educational disruption:* The Chinese experience in maintaining undisrupted learning in covid-19 outbreak. Beijing: Smart Learning Institute of Beijing Normal University. (2020), [Online]. Available: http://www.alecso.org/nsite/images/pdf/1-4-2.pdf

[2] Sintema, E. J. Effect of COVID-19 on the Performance of Grade 12 Students: Implications for STEM Education. *Eurasia Journal of Mathematics, Science and Technology Education*, **16(7)**, em1851, (2020).

[3] Crawford, J., Butler-Henderson, K., Rudolph, J., & Glowatz, M. COVID-19: 20 Countries' Higher Education Intra-Period Digital Pedagogy Responses. *Journal of Applied Teaching and Learning* (JALT), **3(1)**, (2020).

[4] Oranburg, Seth. Distance Education in the Time of Coronavirus: Quick and Easy Strategies for Professors. *Duquesne University School of Law Research Paper No. 2020-02*, (2020), [Online]. Available: https://ssrn.com/abstract=3553911

[5] Miguel, J., Caballé, S., & Xhafa, F. *Intelligent data analysis for e-learning: enhancing security and trustworthiness in online learning systems*. Academic Press, (2017).

[6] International Telecommunication Union. *ITU Yearbook of Statistics 2019*. [Online]. Available: http://handle.itu.int/11.1002/pub_series/database/2a8478f7-en

[7] Statista. *Number of internet users worldwide from 2009 to 2019, by region (in millions)*, (2019). [Online]. Available: https://www.statista.com/statistics/265147/number-of-worldwide-internet-users-by-region

[8] Wearn, C., Gaffney, F., Addison, K. & Miles, J. *Threat Intelligence Report: 100 Days of Coronavirus. Mimecast*, (2020). [Online]. Available: https://www.mimecast.com/resources/white-papers/threat-intelligence-report-100-days-of-coronavirus

[9] Signé, L., & Signé, K. *Global cybercrimes and weak cybersecurity threaten businesses in Africa*. Brookings Institute, (2018). [Online]. Available: https://www.brookings.edu/blog/africa-in-focus/2018/05/30/global-cybercrimes-and-weak-cybersecurity-threaten-businesses-in-africa/

[10] Business Software Alliance. *Software management: Security imperative, business opportunity*. BSA Global Software Survey, (2018).

[11] Kaimba, B. (Ed.). *Africa Cyber Security Report: 100 Demystifying Africa's Cyber Security* Poverty Line. SERIANU, (2017). [Online]. Available: https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf

[12] Bada, M., Sasse, A. M., & Nurse, J. R. *Cybersecurity awareness campaigns: Why do they fail to change behaviour?* arXiv preprint arXiv:1901.02672, (2019).

[13] Kwaa-Aidoo, E. K., & Agbeko, M. An Analysis of Information System Security of a Ghanaian University. *International Journal of Information Security Science*, **7(2)**, 90-99, (2018).

[14] Nir Kshetri. Cybercrime and Cybersecurity in Africa, *Journal of Global Information Technology Management*, **22(2)**, 77-81, (2109). https://doi:10.1080/1097198X.2019.1603527

[15] Beer, S. "What is cybernetics?", *Kybernetes*, **31(2)**,209-219, (2002), [Online]. Available: https://doi.org/10.1108/03684920210417283

[16] Wiener, N. *Cybernetics or Control and Communication in the Animal and the Machine*. MIT Press, (2019).

[17] Hogan, M. D., & Newton, E. M. *Supplemental Information for the Interagency Report on Strategic US Government Engagement in International Standardization to Achieve US Objectives for Cybersecurity*, (2015). [Online]. Available: http://dx.doi.org/10.6028/NIST.IR.8074v2

[18] Staff, J. Joint Publication 1-02, 8 November 2010 (as amended through 15 February 2016) *Department of Defense Dictionary of Military and Associated Terms. Department of Defense*, Washington, DC, (2016), [Online]. Available: https://fas.org/irp/doddir/dod/jp1_02.pdf

[19] Kissel, R. (Ed.). *Glossary of key information security terms*. Diane Publishing, (2011).

[20] Canongia, C., & Mandarino, R. Cybersecurity: *The new challenge of the information society*. In Handbook of Research on Business Social Networking: Organizational, Managerial, and Technological Dimensions (pp. 165-184). IGI Global, (2012).

[21] Oxford University Press. *Oxford Online Dictionary*. Oxford: Oxford University Press, (2014), [Online]. Available: http://www.oxforddictionaries.com/definition/english/Cybersecurity

[22] Ross, R., et al., *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication (SP) 800-53 Revision 4, National Institute of Standards and Technology, Gaithersburg, Maryland. http://doi.org/10.6028/NIST.SP.800-53r4

[23] CISCO. *What is cybersecurity?* (2020) [Online]. Available: https://www.cisco.com/c/en_ae/products/security/what-is-cybersecurity.html

[24] Kaspersky. *What is cybersecurity?* (2020), [Online]. Available: https://me-en.kaspersky.com/resource-center/definitions/what-is-cyber-security

[25] Beda, K. F. G. *Information and Communication Technologies in Africa*: *Levels, Trends and perspective*. In Smart Economy in Smart African Cities: Sustainable, Inclusive, Resilient and Prosperous, 447, (2019).

[26] Eltahir, M. E. E-Learning in Developing Countries: Is it a Panacea? A Case Study of Sudan. *IEEE Access*, 7, 97784-97792, (2019).

[27] Marcum C.D., Higgins G.E. Cybercrime. In: Krohn M., Hendrix N., Penly Hall G., Lizotte A. (eds) *Handbook on Crime and Deviance.* Handbooks of Sociology and Social Research. pp. 459-475, Springer, Cham, (2019).

[28] African Union Commission. *Cyber Crime & Cybersecurity Trends in Africa*. Mountain View, CA: Symantec, (2016). [Online]. Available: https://docs.broadcom.com/doc/cyber-security-trends-report-africa-interactive-en

[29] Sezer, B., Yilmaz, R. and Karaoglan Yilmaz, F. Cyber bullying and teachers' awareness. *Internet Research*, **25(4)**, 674-687, (2015), [Online]. Available: https://doi.org/10.1108/IntR-01-2014-0023

[30] Rita Ismailova and Gulshat Muhametjanova. Cyber crime risk awareness in Kyrgyz Republic. *Inf. Sec. J.: A Global Perspective,* **25(1-3)**, 32-38, (2016), [Online]. Available: http://dx.doi.org/10.1080/19393555.2015.1132800

[31] Kim, E. Recommendations for information security awareness training for college students. *Information Management & Computer Security*, **22(1)**, 115-126, (2014), [Online]. Available: https://doi.org/10.1108/IMCS-01-2013-0005

[32] Muniandy, L., Muniandy, B., & Samsudin, Z. Cybersecurity Behaviour among Higher Education Students in Malaysia. J. Inf. Assur. Cyber Secur, **2017**, 1-13, (2017).

[33] Albarashdi H. **الفيسبوك والجرائم الإلكترونية في عمان: هل هناك علاقة؟**[Facebook and the cybercrimes in Oman: Is there a relationship?]. *Journal of Information Studies and Technology*, **2019(2)**, 2-7, (2019), [Online]. Available: https://doi.org/10.5339/jist.2019.7

[34] Senthilkumar, K., & Easwaramoorthy, S. A Survey on Cybersecurity awareness among college students in Tamil Nadu. In Materials Science and Engineering Conference Series, **263(4)**, p. 042043, (2017).

[35] Kritzinger, E., Bada, M., & Nurse, J. R. *A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK*. In IFIP World Conference on Information Security Education (pp. 110-120). Springer, Cham, (2017).

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

[37] Bada, M., Von Solms, B., & Agrafiotis, I. *Reviewing national cybersecurity awareness in Africa: an empirical study*. (2019), [Online]. Available: https://www.repository.cam.ac.uk/handle/1810/293742

[38] Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. Cybersecurity education is as essential as "the three R's". *Heliyon*, **5(12)**, e02855, (2019).

[39] Kansai University. *Survey on the Internet Usage and Security Awareness*, (2010), [Online]. Available: http://www.kansai-u.ac.jp/riss/en/shareduse/data/26_E_questionnaire.pdf

[40] Muhirwe, J., & White, N. Cybersecurity Awareness and Practice of Next Generation Corporate Technology Users. *Issues in Information Systems*, **17(2)**, (2016).

[41] Subramaniam, S. R. *Cybersecurity awareness among Malaysian pre-university students*. E. Proceeding of the 6th Global Summit on Education, 1-14, (2017).

[42] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, **62(1)**, 82-97, (2020).