Exploring The Correlation between Cyber Security Awareness, Protection Measures and the State of Victimhood: The Case Study of Ambo University's Academic Staffs

Bayisa Kune Mamade[1,*] and Diriba Mangasha Dabala[2]

[1]*Department of Electrical and Computer Engineering, Hachalu Hundessa Campus, Ambo University, Ethiopia*
[2]*College of Social Sciences and Humanity, Ambo University, Ethiopia*
E-mail: bayisukiya@gmail.com; dabala.diriba7@gmail.com
[*]*Corresponding Author*

Received 10 October 2020; Accepted 24 March 2021;
Publication 14 June 2021

Abstract

The advancement of information communication technology has triggered a revolution in using the Internet for legitimate educational purposes on university campuses. Therefore, the Internet has changed the way of human communication and contributed to the development of mankind. On the other hand it is regrettable that its revolution has helped malicious users to exploit it for the malign purpose to commit a cyberspace crime that has in turn negatively affected fellow users who were preyed on by cyber predators. This work aimed to examine the awareness of cybersecurity, the measures taken to protect against cyberattacks and the state of victimization among professors at Ambo University. Thus, the present study comes up with the following findings. First, the result shows that the respondents' cybersecurity awareness was significantly influenced by cyber-crime victimization, fields of study, and protection measures. Second, the current study also depicts that the respondents' protection measures were connected to and influenced by cyber-crime victimization, education level, and cyber-security awareness. Finally,

Journal of Cyber Security and Mobility, Vol. 10_4, 699–724.
doi: 10.13052/jcsm2245-1439.1044

the study's findings show that being a cyber-crime victim has been linked to predictors' variables: protection measures and the level of cybersecurity awareness.

Keywords: Cybersecurity awareness, multiple linear regression, protection measures, victimhood to cyber-crime.

1 Introduction

Computer and information technology advances remarkably transfigured human lives, especially by making service provisions so more straightforward. The service offering, which was done manually earlier to the broader international community globally, has become online, which mainly resulted from the evolution of the Internet and other digital technologies [1]. Such computer-based technologies have become an inherent element of today's human life. The vital information, which is Internet-based, continues to grow with ever-expanding digital technologies [2]. The dawn of technology recently, more importantly, the digital one, resulted in the birth of several computers, hardware, Internet services, which allow humanity to undertake data processing easily. Humanity has been benefited profoundly from Internet connectivity and remains dependent on the rising Internet-related innovation. Despite such tremendous contribution to human life, Internet and computer technologies have caused substantial damage to its users [3]. As the world becomes more and more digital and commercial transactions increasingly carried out on the Internet via the use of information technologies, associated risks are also rising high [4]. The menace of Cybercrime becomes border transcending and tends to be international in its very nature [5]. The invention of digital technology, mainly the Internet, boosted cyberspace criminals' position to commit very serious Cybercrime within a short period [6].

In this digital age, the danger of Internet-related crime is spreading throughout Europe. The Global Information Security Survey emphasizes that nearly 80% of European companies have been hit by cyber incidents once to the minimum in 2016. Cyber threats have increased exponentially by 35% compared to 2015 worldwide [7]. It has recently become an area where cyber criminals illegally operate cyber-based crimes with impunity to Africa. The pace of cybercrime incidents has been on the rise in Africa. For instance, in 2016, 24 million Cybercrime and intrusion have targeted Africa [8]. Sadly, countries in Sub-Saharan Africa are classified among a region where cyber-crime incidence reaches its chronic level [9]. The rapid increase in the rate of

Cybercrime in Africa is partly due to a lack of awareness and understanding of cybercrime.

Therefore, the current study intends to appraise how cybersecurity awareness, protection measures against cyber-attacks, and victimhood to cyber-crime interplay and influence one another. It also evaluates whether lecturers' educational background and fields of study impact their cyber security awareness level, preventive measures to be taken, and victimization to Cybercrime.

1.1 Cyber Security

Although there is no generally accepted definition of it, cybersecurity can be simply a protection measure or a safeguard/s that both users and service providers can take to avoid if possible or to the least to reduce latent attacks that could disrupt the data, computer systems: both hardware and software [10]. Cybersecurity precaution intends to protect the confidentiality and one's privacy and plays a crucial role in ensuring the availability and integrity of data that in turn proves pivotal to keep quality and safety of the care one can take. Speaking differently, cybersecurity refers to deploying all the pivotal elements that can best shield and give a swift response to the possible cyberspace threats these would include technologies, tools, legal policies, security safeguards, best risk management practice in place, training and preparation, and another mechanism to effectively thwart the Internet-based crime to be committed in cyberspace [11].

Today, people are becoming increasingly dependent on the information and communication technologies that have had emerged in the last two decades, and it is almost impossible to find a single aspect of societal lives not touched by digital technology [12]. Its impact could range from shaping the way people communicate, interact with each other as well as how the government institutions could obtain highly needed information, our culture of work, and to its positive contribution on the economy by changing the manner of doing business in which the economic growth caused by the introduction of the digital technology entails the improvements of the infrastructure and life standards of the people [13].

1.2 Cyber Crime

Cyber-crime is an Internet-based crime that always directed against individuals, groups, and or state and it's economy motivated by the criminal

intention that can cause damage/destruction that may be of different types including: physical, mental, loss of money and also it involves unlawful accessing information of the victims using electronic devices [14]. Cybercrime may vary based on the potential damage it might cause, its targets, and the nature of its occurrence. Hence, Cybercrime may be harassment, cyber terrorism, child pornography, digital piracy, cyberstalking, computer hacking, or unauthorized access to computer databases, networks, and spam [15]. Others define Cybercrime as a variety of crimes, usually involving computer data and systems designed to disrupt its operation. These crimes may also include forgery and fraud that may be carried out using computers [16]. Despite its positive contribution to mankind, the revolution in information and communication technology has also exposed us to a new type of cyber-based crime that continues to have a devastating impact on mankind. Therefore, knowing about the recurrence of cyberspace crime is essential to avoid its destructive effects on the country, organization, economy, and even individuals.

1.3 The Interplay Between Cyber-security Awareness, Victimhood to Cyber-crime and Safety Measures

A couple of studies have shown that there is an interaction between cyber-security awareness, victimhood to Cybercrime, and interventions measures one may take to combat Cybercrime. With the cyber-crime incident being skyrocketed in recent years, the study by [17] unearthed that combating cyber-crime and taking strategic intervention or pre-empt measures hugely depends on the level of cybersecurity awareness notably; this can be achieved through educating the public about potential dangers or consequences of cyber-attacks. Another study by [18] in which they examined the influence of cyber-crime risk on the e-service adoption of European Internet users exposed that users' intent of taking measure to fend off cyber-attacks is reported to have potentially determined by how people are well-versed and aware of the degree of the severity of the problem.

Moreover, the fascinating study by [19] that insightfully inquired the perception and awareness of the young Internet users towards cyber-crime recognized that falling victim to cyber-crime is linked strongly to the users' awareness as the line of defense they set up. As such, this research has disclosed that the degree of victimization to cyber-crime would be reduced if the Internet users are highly aware of and cautious about their proper space when they are online and able to take measures to avoid possible breaches

that can compromise personal safety. The study made it clear that being a victim of cyber-crime results either from lack of awareness or failure to install defensive lines even if they have a certain level of awareness that largely emanates from under estimating the destructive impact of cyber-crime. Therefore, to trim down the damage or loss that may occur due to cyber-attacks, increasing awareness through training and safeguarding one's security, which can be done by using various defensive mechanisms, ought to be implemented.

The study by [20] emphasized the need for increasing cybersecurity awareness of those who surf on the Internet page. The study found that having good cybersecurity awareness is essential because it enables the users to take preventive measures, which otherwise may entail defacement of unparalleled scale. The study further indicated that regardless of the nature and types of the attacks staged against the Internet users, cybersecurity breaches can be minimized or limited if not eliminated, given people are aware of always existing threats and able to deploy preventive measures, including up-dating one's system.

1.4 Problem Statement

It is a common activity to expand the Internet infrastructure to promote the development of knowledge or information in higher education institutions. Ambo University has begun to expand the scope of connectivity across all its campuses. Although the Internet's contribution in scaling up the dissemination of knowledge is proven immense, there is a widely observed associated problem with expanding the Internet infrastructure in the University and beyond. Such a problem is a crime committed in cyberspace that arises with the expansion of the Internet. For instance, in Ethiopia, cybersecurity breaches and cyber-crime are on rising tremendously. In particular, the recurring cybersecurity breaches target large-scale financial and infrastructure of the country. In the past three years, Ethiopia has seen more and more cyber-attacks. Thus, the number of attacks jumped from 479 in 2018 to 791 in 2020. On a large scale, these attacks have targeted various organizations and financial institutions for the third consecutive year [10]. In 2017, a cyber-attack and malware targeting the Ethiopian Development Bank paralyzed the entire computer network, which caused customers to feel frustrated because they could not access information and conduct transactions. In the same year, public universities and institution's websites were hacked and targeted by cyber predators, including Dire Dawa University, the Ministry of Education,

the Pharmaceuticals Fund & Supply Agency, the Ministry of Finance & Economic Cooperation, and Commercial Nominees Plc. had come under cyber-attacks [11].

Therefore the Internet can be hijacked by malicious users to commit crimes. Not knowing such users' infiltrating into one's system remains hard for layman users to detect, regardless of tools used to access the connection or the Internet. Users might be outwitted by people with malicious intent that induce others' to commit Internet-based crimes inadvertently. The academic community of the University needs to have know-how about Cybercrime and its potential impact. Thus, it is essential to measure their level of cybersecurity awareness. Therefore, there is a need to evaluate the level of lecturers' cybersecurity awareness, protection measures to be taken, state of cybercrime victimhood, and inform those with a low level of awareness to take precautions to deter possible future attacks.

Thus, this study has developed the following three hypotheses based on the concepts mentioned in the research title.

- Cybersecurity awareness will be significantly affected by protection measure deployed by the respondents, level of cyber-crime victimization, and fields of study,
- Protection measure will be significantly affected by the level of cybercrime victimization, cybersecurity awareness, and education level, and
- Cyber-crime victimization level will be affected by protection measures and cybersecurity awareness taken by the lecturers.

2 Related Work

The rapid spread of the Internet on the African continent makes it possible for the digital economy to emerge, and it also brings unexpected consequences of becoming victims to cybercriminals. In most cases, the increased risk of Cybercrime in Africa is due to the expansion of broadband Internet connections, and a survey conducted in 2000 has shown that a third of spam related to automated information that was sent from computers connected to a broadband network [21]. If someone has a better understanding of cybercrime and cybersecurity measures to be deployed, then the negative impact caused by the Internet penetration can be overcome.

Research conducted by [22], which intended to assess students' cybersecurity awareness in the private Tertiary Educational institution, has found out that students' self-perception about cybersecurity awareness and their actual

knowledge of it has proven considerably vary. Amongst the sampled students, more than 50% of them reported to have a feeble understanding of phishing, which is very concerning given the fact that their response suggested that they have low levels of cybersecurity, yet; conversely, when they spoke out about their self-perception of identifying phishing, they say they are capable enough to do this. Therefore there is a likelihood of falling victim to cyber-crime.

Another study carried out by [23] in the United States, entitled, 'the Shopping on Social Networking Websites', has shown that there exists strong relations between the level of precautions' measures or the attitudes of the consumers' towards privacy and web security would have greatly influenced their e-commerce transaction. In addition, another study conducted in Malaysia by [24] investigates the relationship between consumers' knowledge, attitudes, and practices in e-commerce. The research finding indicated that consumers' knowledge level is positively correlated with their practice of online business transactions.

Although the literature on cybersecurity has been emerging rapidly in other parts of the world, especially in developed countries, in the face of increasing cyber-crime that resulted largely due to the absence of cybersecurity awareness, there are no fully-fledged researches done so far on this issue in Ethiopia. Even the existing scarce literature was confined only to discussing legal measures to be taken to tackle the ever-emerging and rapidly growing threat of cyber-attacks, while those studies discussed nothing about cybersecurity knowledge, awareness, and response to any cyber threats that individuals or community at large can take. In addition to its above shortcomings, the research conducted so far is only qualitative, and no quantitative research on this topic has been conducted in Ethiopia [25] examined the approaches to Internet regulation in Ethiopia, highlighting that Internet regulation has recently become a pressing issue. The government partly wants to take such measures and use it as a tool to overcome the anti-government protests that began to sweep the country in 2014; this was because the protesters rely heavily on the Internet to organize and coordinate their actions. This article clearly explains why the government is so concerned about Internet regulation and finally introduced some laws and the necessity of enacting these laws. However, although to a small extent, this article also puts forward the increasingly severe threat of Cybercrime because it has become an existential threat facing humanity. This work also emphasized that Ethiopia has also adopted some legislation to regulate the Internet.

Another study by [26] studied the cybercrime situation in South Africa, Nigeria, and Ethiopia from a comparative perspective and the need to ensure the enforcement of their laws and policies, as Cybercrime is becoming a potential threat to all of them. Like preceding research by [25], this one also delves into re-visiting the legal frameworks and their execution accordingly to combat Cybercrime. The paper shows that the sense of urgency to curb Cybercrime is to enhance the ability of relevant national institutions in their respective countries to effectively implement cybercrime policies because laws and policies cannot be implemented on their own.

A report paper by [27] largely underscored the importance of information security, which is all about ensuring the safety of information from fall into the hands of malignant cyber predators and its vital components that are enablers of its protection—both computer hardware and software that serve as a conduit to transmit and store such critical information. Likewise, some parts of the paper also magnanimously devoted to discussing the status and situation of cyberspace security in Ethiopia and relevant measures that have undertaken to warranty the safety and wellbeing of the data and it also called for having an institution based data center, making available guidelines and procedures that enterprise can rely on to ensure information safety in their organization.

Even if these papers tried to touch on an urgent problem that the world is grappling with, they fail to comprehensively present every aspect of cyber-security, the likely driving factors that pave the way for an occurrence of cyber-attacks, and finally, protection measures to be taken to repel it. Studies carried out in South Africa, Malaysia, and the United States made a huge contribution in assessing cybersecurity awareness in the tertiary educational institution, consumers' privacy precautions, and its role in conducting healthy e-commerce. However, these studies failed to clearly show the interaction between various factors and how they inform each other and fundamentally shape one's cybersecurity awareness, knowledge, and the possibility of being a victim to cybercriminals that our paper tries to fill.

Regards to the researches done so far in Ethiopia, all of them are limited to the need to take legal measures to deal with cyber-attacks and whether the country has an appropriate legal system to deal with such threats as cybercriminals. Examining the interaction between cybersecurity awareness, protection measures needed to deal with Cybercrime, and the likelihood of becoming a victim of Cybercrime and how these factors affect each other is missing in Ethiopia.

3 Methods

3.1 Study Design and Area

This research was conducted to examine cybersecurity awareness, protection measures to be deployed, and the state of victimhood among Ambo University's academic staff. Ambo University is located to the West of the capital city, Addis Ababa, at 119 kilometers in Oromia regional state, in the town of Ambo. The University has three campuses within short distances from each other. Both Main and Awaro campuses are located in Ambo town, while the Guder campus is about twelve kilometers away to the West of the town, in Guder city. The University has five colleges, three institutes, and four schools. It has ninety (90) undergraduate and seventy-three (73) postgraduate programs and six (6) Ph.D. programs in total. One thousand eighty-eight (1088) instructors were employed in the three campuses.

3.2 Sampling and Sample Participants

A cross-sectional qualitative study design was used to collect data from the participants. The population was all active lecturers at the time of data collection. Both female and male lecturers were part of the respondents. Taking into consideration the smallness of the population size, simplified formula for proportional was used. It was assumed to have a 5% margin of error, a 95% level of confidence, and adding 10% non-response rate. Using the simplified proportion formula total sample size was computed to be two hundred eighty-eight (288) with the consideration of 1.5 design effect. The total sample size was proportionately allotted based on the number of entire lecturers in each campus, college, and department. A simple random sampling technique was used to select lecturers from each department with already available lists.

3.3 Data Collection and Tools

A self-administered questionnaire was used as a tool to collect data from all respondents. A review of related literature on the questionnaire assisted in adapting to the context under study. The questionnaire contains three sections. The socio-demographic, lecturers' Internet usage profile, and their cybersecurity awareness sections were part of it. The five Likert-scale questions, which were used to collect lecturers' Internet usage data and their cybersecurity awareness, were adopted from [6]. The questionnaires were categorized into socio-demographic items, lecturers' Internet usage profile with five questions,

cybersecurity awareness containing fourteen questions, cybersecurity protection measure questions being six, and statehood of cyber-crime victimization questions two problems. The questionnaires were distributed to each participant on his/her desk in an office after providing an orientation on the purpose of the study and clarification of terms. The filled questionnaires were checked for completeness on the spot and collected from the participants immediately.

3.4 Data Analysis

Data entry was done on SPSS 22 on Windows 7 operating system. All the questionnaires from two hundred eighty-eight with thirty-four items were entered into the SPSS version 22. The collected data were examined by the use of frequency, mean, standard deviation, and multiple linear regressions. The researcher have done factorial analysis because the data collected was qualitative and discrete, not fitting for multiple linear regression. Besides, the questionnaire's nature calls for grouping or clustering as per what they intend to measure. So, the researchers have undertaken factorial analysis to convert discrete and qualitative data into a continuous type that the researchers believe satisfies multiple linear regression data requirements. The researchers used multiple linear regression because it is an advanced statistic that measures an association between variables. There are three dependent variables and several independent variables.

The principal component analysis extraction method was employed to reduce groups of similar questions, such as cybersecurity awareness, into a single factor score to facilitate necessary regression analysis conditions. Three-factor scores, using the regression method, were created based on the category of the questionnaire. They are cybersecurity awareness, protection measures, and statehood of cyber-crime victimization.

To examine the existence of an association between dependent and independent variables, the regression analysis model was run three times with varying independent variables as per the hypotheses. In the model backward method was used, and from the output tables, only three of them, namely: model summary, ANOVA, and coefficients, were considered for discussion.

3.5 Ethical Consideration

Verbal consent was obtained from all participants by explaining the purpose of the study. All the information given by the respondents has been used for research purposes only, and for the sake of confidentiality, the respondents

were not asked to fill in their details. There is no approval letter and number provided by the University as far as consents were made with the participants.

4 Results

Table 1 shows respondents' age range of 25–35 were 227(78.8%), respondents with the age of 36 and above account for 47(16.3%) while 14 (4.9%) of the total respondents fall below the age of 25. About 143 (49.7%) of the respondents' teaching experience was between 6–10 years. The second with a high percentage of respondents' teaching experience was in the range of 1-5 with 101(35.1%). Respondents with above 16 years of teaching experiences account for 30(10.4%), whereas 11–15 years of teaching experiences were 14(4.9%). Thus, the most dominant age and teaching experience group are 25–35 with 227(78.8%) and 6–10 with 143 (49.7%) respondents. The majority, 212(73.6%), of the respondents' educational background is MSc/MA.

Table 1 Socio-demographic variables of the respondents

Variables	Range	Frequency (n)	Percent (%)
Age	Below 25	14	4.9
	25–35	227	78.8
	36 and above	47	16.3
	total	**288**	**100**
Teaching Experience	1–5	101	35.1
	6–10	143	49.7
	11–15	14	4.9
	>16	30	10.4
Gender	Male	262	91
	female	26	9
	Total	**288**	**100**
Educational Level	BSc/BA	52	18.1
	MSc/MA	212	73.6
	PhD	24	8.3
	total	**288**	**100**
Field of study	Computing	39	13.5
	Non-Computing	249	86.5
	total	288	100

Table 2 Lecturers' level of Internet use profile

S.No	Items	High (n%)	Moderate (n%)	Low (n%)
1	I always use the Internet.	204(70.8)	70(24.3)	14(4.9)
2	I am addicted to the Internet due to overuse.	72(25.0)	52(18.1)	164(56.9)
3	I use the Internet for education and research.	230(79.9)	42(14.6)	16(5.6)
4	I use the Laptop to browse the Internet.	211(73.3)	51(17.7)	26(9.0)
5	I use the Internet for non-educational purposes like Internet Banking and entertainment.	148(51.4)	37(12.8)	103(35.8)

52(18.1%) of them are BSc/BA, while Ph.D. only accounts for 24(8.4%) of the respondents. The distribution of gender among the respondents stated as follows. 262(91%) of the respondents are male, whereas the remaining 26(9%) are female. Male respondents are the dominants. Out of 288 respondents, 249(86.5%) are non-computing, and only 39(13.5%) are computing. There are three campuses in Ambo town, and two of the campuses with many colleges and teaching staff being non-computing. Only three departments are considered to be computing, namely Information Technology, Computer Science and Computer Engineering.

A five-level Likert scale was used to collect responses from the respondents. However, to do the analysis and make a link with previous research, the Likert scale of five levels downsized to three (3) scale, which is classified as high, moderate, and low.

Table 2 indicates that from the three alternatives given in the above table, a high number of lecturers, 230(79.9%), responded that they had used the Internet for educational and research purposes. In the same vogue, 211(73.3%) of the respondents said they used a laptop to browse the Internet, and 204(70.8%) replied that they always used the Internet. Both numbers are depicted under the 'high' category. On the other hand, addiction to the Internet accounts for 164(56.9%), showing that most of the respondents were not addicted. That is to means the addiction rate is low, as clearly illustrated in the table. In general, most of the respondents' responses confirmed that they used the Internet for different purposes that fall under the 'high' class.

For the purpose of clarity and simplicity, the questionnaires to measure the awareness level of cyber-security were regrouped into three (3) distinct

Table 3 Lecturers' Level of cybersecurity awareness

S.No	Items	High (n%)	Moderate (n%)	Low (n%)
1	I know what Cybercrime is.	96(33.3)	2 (0.7)	190(66.0)
2	I have heard about phishing.	39(13.5)	34 (11.8)	215(74.7)
3	I think that Cybercrime is only a virtual crime.	104(36.1)	36(12.5)	148 (51.4)
4	I would click any link that I receive via email/SMS.	92 (31.9)	63(21.9)	133(46..2)
5	I think that a fraudulent Email/website/link is easy to identify.	70(24.3)	66(22.9)	152(52.8)
6	I know some of the cyber laws.	32 (11.1)	35 (12.2)	121(76.7)
7	I trust any website that asks me to enter my bank account detail.	122(42.4)	57(19.8)	109(37.8)
8	I am aware of some features of a fraudulent email.	122 (42.4)	57 (19.8)	109(37.8)
9	I think that downloading any file from any website is always safe.	36(12.5)	19(6.6)	233(80.9)
10	I believe that big companies are the only victims of Cybercrime	49(17.0)	50(17.4)	189(65.5)
11	I believe those who use the Internet frequently will likely experience cyber-attacks than infrequent users.	161(55.9)	43(14.9)	84(29.2)
12	When I am online, I consider my permissible space and the forbidden space of others.	100(34.7)	110(38.2)	78(27.1)
13	I think that I am able to identify a fraudulent email /website.	101(35.1)	64(22.2)	123(42.7)
14	I think that it is difficult to identify a fraudulent website.	148(51.4)	52(18.4)	88(30.6)

parts. The first part consisted of fourteen (14) items to elicit the concept of cybersecurity awareness. For the sake of reporting and making a comparison with previously done research works, the original five Likert scale questionnaires were recorded at a high, moderate, and low level. Overall the above table 3 shows the level of cybersecurity awareness in terms of high, moderate, and low with each frequency and percentage hierarchically. Out of fourteen (14) questions, eight (8) or 57.14% demonstrated a low level of cybersecurity awareness. Four (4) out of fourteen (14), 28.6%, responded to

Table 4 Lecturers' level of cyber-security protection measure and cyber-crime victimization

S.No	Items	High (n%)	Moderate (n%)	Low (n%)
1	I think that anti-viruses are enough to protect me from Cybercrime.	51(17.7)	48(16.7)	189(65.6)
2	I think that I am protected from Cybercrime.	67(23.3)	64(22.2)	157(54.5)
3	I protect myself from Cybercrime.	92(31.9)	65(22.6)	131(45.5)
4	I care about purchasing the best antivirus software.	123(42.7)	61(21.2)	104(36.1)
5	In general, I do not trust the websites that ask me to enter some details about my bank card.	189(65.6)	39(13.5)	60(20.8)
6	I know the details of my card that I should not enter on any website when shopping online.	122(42.4)	98(34.0)	68(23.6)
7	I have been threatened online to pay money for someone who had stolen my personal photograph.	44(15.3)	74(25.7)	170(59.0)
8	I would report being a victim of Cybercrime if I had been a victim.	140(48.6)	70(24.3)	78(27.1)

a high cybersecurity awareness level. Two (2) out of fourteen (14), 14.3%, replied to have moderate cybersecurity awareness level. These results indicate a high probability of being attacked by malicious users because most of the respondents did not have an intermediate cybersecurity awareness level. Thus, awareness creation programs ought to be implemented to curve the overarching cybersecurity-related problems.

The second and third part of the cyber-security awareness questions' sub-section are shown in the above table 4 with the heading cybersecurity protection measure against cyber-crime. Out of eight (6) questions presented to the respondents, four (4) of them accounted for 50% and responded to have a high level of cybersecurity protection measure against Internet vandalism. On the other hand, 50% of the respondents had a low clue of such protection mechanisms to deploy to safeguard one's Internet-related assets. Thus, the respondents are highly polarized into two groups of having and lacking ample protection measure to best shield his/her self from the highly probable danger of cyber-attacks. The population ought to be given both the tools and techniques to defend themselves in the form of short-term training and seminars to create awareness of the rapidly advancing threat to the overall properties of mankind, including intellectual properties.

5 Validity, Reliability and Structural Equation Model

Validity can take different forms. For example, one of the forms is content validity, so the degree to which the deployed test metric measures the content as expected[28]. To improve or increase the content validity, it is best to adapt all the research questions from the previous research[28]. Establishing content validity is problematic because it is not easy to determine the degree of certainty, so it can be said that a researcher has drawn an unbiased representative from the whole or content universe. Therefore, an easy way to establish content validity is to review previous work and often have in-depth discussions with professionals and experts. Undertaking to pretest the instrument with expertise is the most realistic and desirable way to establish content validity[29]. Another validity typology is constructed validity, and this one pertains to the possible degree of making inferences from operationalization in one's study, which has justifiable relation to the theoretical constructs on which the operationalization of the research depends[28].In short, the focus of construct validity is whether the measures selected by the researchers are consistent with each other or fit together so that the essence of construct validity can be easily observed between constructs[30].

Unlike validity, reliability is shortly about measurement that is solely confined to a single construct. This is also a statement about the accuracy of the measure used ,i.e., the extent to which the respondent can answer the same or approximately closer questions similarly every time[28]. Even though there are various mechanisms of evaluating reliability, in our case, the researchers only see internal reliability. To assess the internal consistency of reliability between items in a single construct, Cronbach's alpha is the best method of doing it. Internal consistency reliability refers to the degree of consistency between the items contained in a single construct and other constructs. For a long time, Cronbach's alpha has been regarded as a recognized method for evaluating internal reliability, mainly when researchers use Likert scale questions [28]. For the Cronbach alpha's internal consistency reliability to be accepted, its confirmatory should be at least 0.70 [30].

Therefore, here are two tables showing the reliability level of internal consistency between items within a single construct and between different constructs. As clearly indicated in the first table, even though the overall level of internal consistency reliability for all the constructs meets the minimum standard to be accepted, the researcher have eliminated few items from one construct to further improve the strength of relations between items and internal consistency all questions at once. The improvement in overall internal

Table 5 Internal consistency reliability before the elimination of items

Item	Number of Questions	Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items
Total questions	22	0.699	0.702

Table 6 Internal consistency reliability after the elimination of items

Item	Number of Questions	Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items
Total questions	20	0.704	0.715

consistency reliability observed in the second table is due to the omission of two items from the construct named cybersecurity awareness. Thus, these two items are: I trust any website that asks me to enter my bank account detail, and I believe those who use the Internet frequently will likely experience cyber-attacks than infrequent users, are excluded from the construct(See, table.3 above), and the overall internal consistency reliability has been improved to 0.715.

The researcher employed Simultaneous Structural Equation Modeling (SSEM) because it has been proven effective model to answer sets of interrelated questions systematically and comprehensively by simultaneously modeling the relationships between numerous independent and dependent constructs. This modeling clearly involves systematically and simultaneously resolving equations linear in nature by using regression, factorial analysis, and path analysis [30, 31]. To express it simply, the SSEM is all about multiple-equation regression. One variable serves as a response variable in one regression, and another time it appears as an explanatory variable in another equation. These two variables also mutually influence each other, which can occur directly or indirectly through a feedback hoop [32, 33]. The regression analysis executed have done is based on the following framework.

As explicitly indicated in Table 7 herein under all the predictors (cyber-crime victimization, fields of study, and protection measure) in that order significantly influence/affect cybersecurity awareness (DV) with ($\beta = 0.206$, $p < 0.000$, $\beta = -0.120$, $p < 0.036$&$\beta = 0.139$, $p < 0.017$). It is imperative to comprehend that all the items of independent variables (cyber-crime victimization, protection measure, and fields of study) respectively impact cybersecurity awareness with nearly 0.8% of the covariance (Adj.R2 0.080). Although there are subtle differences in the impact of predictors, their effect on DV clearly supports Hypothesis I. There are no multicollinearity problems in all regression analyses.

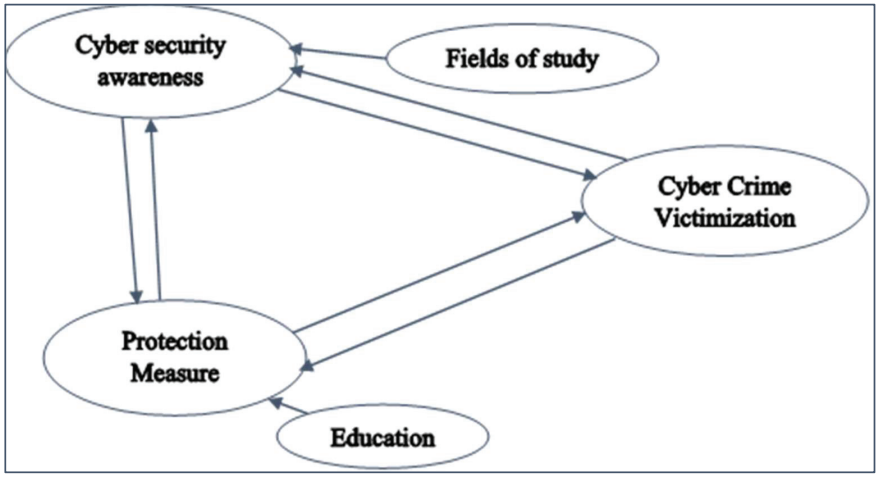

Figure 1 Study hypothesized model.

Table 7 Results of regression analysis run 1

DV-cyber Security Awareness				
IV	Standardized β	Sig	VIF	Supported
Cyber-crime victimization	0.206	0.000	1.041	Yes
Fields of study	−0.120	0.036	1.016	Yes
Protection measure	0.139	0.017	1.055	Yes
Adj.R2		0.080		
F		F(3, 284) = 7.273, P < 0.000		
N		288		

Considering cyber-crime protection measure as dependent variable (DV), it was positively affected by three predictors, which are: cyber-crime victimization, cybersecurity awareness, and education level. As shown in Table 8 below, these three items have primarily affected the protection measures used, explaining the 9.1%of the variance (Adj.R2 = 0.091). From the three predictors given, the DV was influenced highly by all of them with ($\beta = 0.150$, p < 0.019, $\beta = 0.155$, p < 0.006 &$\beta = -0.211$, p < 0.019, supporting hypothesis II.

Cyber-crime victimization is regarded as the dependent variable, as shown in Table 9; it is positively correlated with both items. Therefore, protection measures and the level of cybersecurity awareness significantly

Table 8 Results of regression analysis run 2

DV-Protection Measure				
IV	Standardized β	Sig	VIF	Supported
Cyber-crime victimization	0.150	0.019	0.949	Yes
Cyber-security awareness	0.155	0.006	0.948	Yes
Education level	−0.211	0.019	0.997	Yes
Adj.R2		0.091		
F		F(3,284)=10.554,P<0.000		
N		288		

Table 9 Results of regression analysis run 3

DV-Cyber-Crime Victimization				
IV	Standardized β	Sig	VIF	Supported
Protection measure	0.154	0.008	1.304	Yes
Cyber-security awareness	0.197	0.001	1.304	Yes
Adj.R2		0.067		
F		F(2,285) = 11.275, P < 0.000		
N		288		

affect cyber-crime victimization with 6.7% of the variance (Adj.R2 = 0.067). These two predictors affect the cyber-crime victimization in the order of (($\beta = 0.154$, p < 0.008, $\beta = 0.197$, p < 0.001), which means they support Hypothesis III.

Moreover, as revealed in Table 9 below, cyber-crime victimization, being termed as the dependent variable, was considerably influenced by the level of cyber-security awareness, validating hypotheses III. The results of the regression analysis below show that the predictor variable (cyber-security awareness) greatly influenced cyber-crime victimization with ($\beta = 0.241$, p < 0.000) and with 8.3% of the variance (Adj.R2 = 0.083) as mentioned earlier on above.

6 Discussion

Noting the lack of research investigating the interplay between cybersecurity awareness, protection measure to be taken, and the likelihood of falling victim to cyberspace crime in Ethiopia, this study endeavored to identify the extent to which these variables have had an impact on each other considering them

as the dependent variable in one construct and as independent variables other time. As for the method, a self-administered questionnaire was used with a cross-sectional, qualitative research design. Then, multiple linear regression was used to analyze the data, and factor analysis was performed to make our questionnaire continuous, which was a discrete type before.

The study results clearly show that our sampled university faculty and staff see the advent of the Internet as an opportunity because it has changed people's lives. Likewise, they have never ignored the related cyber-hazards that are becoming more and more threatening than ever. Respondents are very aware that unless they have better cybersecurity awareness and can best deploy protection tools, they are vulnerable to the adverse effects of Cybercrime, which may cause huge damage. Apart from this, it is easily comprehended from the respondents' responses that all of the variables affect each other, despite whether it is taken as dependent or independent variables under a different construct as the researcher hypothesized earlier. The discussion of our paper is based on the three constructs mentioned in the results part.

In the study, the researchers explored the correlation between cybersecurity awareness, protection measures, and the state of victimhood in the premises of the University. Though cybersecurity awareness of the staff/user was positively affected by other factors, it was significantly enhanced by cyber-attack materialization. Thus, inducing a pseudo attack that could offer a lesson might enhance the users' cybersecurity awareness. This result is also aligned with the previous research works by [32, 34], and [35]. The study carried out by [30] shows that the prospect of becoming a victim of Cybercrime or actual victimization is positively related to cybersecurity awareness, and thus it supports our hypothesis. The study by [34] also pointed out that the respondents' education has profoundly impacted their awareness of cyber hazards, and this also supports our hypothesis. Simultaneously, the study by [35] disclosed that the cybersecurity awareness and corresponding protective measures taken by the respondents seem to be closely related and positively impacted each other. This research underscored clearly that employees' actions and normative behavior were said to have influenced their cybersecurity awareness. Therefore this study validates our hypothesis.

As cybersecurity awareness increases due to the impact of cyber-crime, mechanisms to safeguard own system rise too. Victimization by cyber-crime prepares the users well to look for protective measures. Our paper's result is also consistent with the previous study by [36, 37]. The consistency of our work with the prior study is only about the first variable—cyber-crime

victimization. Thus, [36] expounded that the more preventive measures are taken, the more it reduces the possibility of being victimized by Cyber-crime. Equally, the research work of [37] demonstrates that humans, more precisely, those who engaged in any form of online activities, tend to take protective measures to curb cyber-attacks because they have been exposed to such attacks at least once in their lives. The result of the erstwhile study by [34] sharply repudiates our findings, especially concerning the influence of cybersecurity awareness on the protection measure. The study disclosed that tough, the people have become well accustomed to the Internet with the advent of digital technology, yet they lacked the required savvy and fall short of having the least needed awareness level that in turn leads to complete fiasco to take protective measures to safeguard themselves against cyber-attacks. Therefore, there is no statistically significant relationship between these two variables. A recent study by [38] has exhaustively examined factors that affect the adoption of computer security practices among college students. In his findings, the author singled out that the respondents' educational level is one predictor to see whether it has an impact on the students' computer security practices. The result of his paper noted no correlation between the respondents' educational status and the protective measures or cybersecurity practices they take. No matter what level of education they receive, there is no difference in cybersecurity practices or measures they take. Therefore the result was found to be not consistent with our findings and rejects our hypothesis. Even though it was thought that the higher the level of education, the stronger the protection measures deployed to counter-attack or defend one's resources on electronic devices, the opposite had been observed in our findings. Although this idea may seem strange, this inverse relationship is mainly because those who have been in academia for longer tend to be less dependent on computers, and in most cases, do things manually. Since they do not care much about falling victim to cyber-attacks, whenever they use the Internet, although it is infrequent, there is a high probability of falling victim to cyber-attacks.

In contrast to the general truth, protection is better than cure; our finding indicates that being a victim of cyber born attack clears the road for the whole sort of protection measures to be deployed and services as an eye-opener toward cybersecurity awareness. Based on the coefficient index, compared with the level of protection measures, cyber-security attention has greatly affected cyber-crime victimization, which is the outcome variable. This difference is that although this is not the only factor, it is mainly because people neglect to take preventive measures most of the time. This is because they

are prone to wrongly perceive that a good level of cybersecurity awareness alone is adequate to avoid falling victim to cyber-crime and less concerned about deploying precaution measures ahead of time. That is why the cyber-crime victimization index is a bit lower. The previous research by [39], which aimed to explore the relationship between awareness of Cybercrime or being a victim to cyber-criminals and security, also shows that the occurrence of Cybercrime or being a victim of cyber predators was highly related to the level of cybersecurity awareness. On the other hand, the result, the work of [40], in which he investigated the factors the affect the adoption of computer security, indicted that cyber-security awareness does not seem to have significantly affected the perceived security threats/likelihood of being a victim of Cybercrime and therefore have not correlated anyway.

7 Conclusion

The study examined the interaction between cyber-security awareness, protective measures, and cybercrime victimization. To check how they affect each other, it relies on Structural equation modeling. The research used a Cross-sectional, qualitative research design and a self-administered questionnaire used as a data collection tool of this study. Overall, the results of the study evidently suggest that cybersecurity awareness, protection measures, and cyber-crime victimization witnessed on the university campus among the academic staffs seem strongly related, and there was a significant relationship between all of them; despite their changing nature, i.e., once acting as dependent and another time as predictor under different constructs.

This research has the following limitations:-Due to time and resource constraints, our research scope is limited to one University; the researchers think that had been possible to collect data from the population of more than one organization, the researchers might have obtained more accurate data that could produce robust research results. Moreover, this research's focus is only on the academic staff, which the researchers also take as a limitation because there are many administrative staffs that are part of the university community and use computers daily to conduct the university activities. So, had the researchers included administrative staff as part of the sampled population. Indeed, the results would be different.

This article contributes to the existing literature because it uses a multiple linear regression model to explore the correlation between cyber-security awareness, protection measures, and cybercrime victimization. Contrasted with the previous study by [41], this study is also novel regarding its

component variables. Previous research only analyzed the impact of online security measures on the degree of cybercrime victimization. The researchers hope future studies should utilize any of the existing models, for instance, TAM and others, so that the forthcoming studies' results can display high reliability and validity. Future studies should also be carried out in two or more academic and other institutions to observe how these variables affect each other. And if it is going to be conducted in academic institutions, it should include all university communities.

Acknowledgment

This paper would not be finalized without generous financial support from my brother Guta Kune Manmade and technical and material support from Ambo University.

Conflict of Interest

We authors, Bayisa Kune Mamade and Diriba Mangasha Dabala, do not have any interest of conflict of interest (financial and non-financial) with any organizations and individuals in the subject matter or materials discussed in the manuscript.

References

[1] M. Lagazio, N. Sherif, and M. Cushman, "A multi-level approach to understanding the impact of cybercrime on the financial sector," *Comput. Secur.*, vol. 45, pp. 58–74, 2014, doi: 10.1016/j.cose.2014.05.006.

[2] N. Tosun and M. F. Baris, "The place and importance of computer and internet are in secondary school students' life," *Procedia – Soc. Behav. Sci.*, vol. 28, pp. 530–535, 2011, doi: 10.1016/j.sbspro.2011.11.102.

[3] M. Xin, J. Xing, W. Pengfei, L. Houru, W. Mengcheng, and Z. Hong, "Online activities, the prevalence of Internet addiction and risk factors related to family and school among adolescents in China," *Addict. Behav. Reports*, vol. 7, no. June 2017, pp. 14–18, 2018, doi: 10.1016/j.abrep.2017.10.003.

[4] A. Bendovschi, "Cyber-Attacks – Trends, Patterns, and Security Countermeasures," *Procedia Economics and Finance*, vol. 28. pp. 24–31, 2015, doi: 10.1016/s2212-5671(15)01077-1.

[5] M. Gercke, "Cybercrime Understanding Cybercrime?:," *Underst. cybercrime phenomena, challenges Leg. response*, no. ITU, p. 366, 2012, doi: 10.1088/1367-2630/11/1/013005.

[6] M. H. Tibi, K. Hadeje, and B. Watted, "CybercrimeAwareness among Students at a Teacher Training College," *Int. J. Comput. Trends Technol.*, vol. 67, no. 6, pp. 11–17, 2019, doi: 10.14445/22312803/ijctt-v67i6p102.

[7] European Economic and Social Committee, *Cybersecurity?: Ensuring awareness and resilience of the private sector across Europe in the face of mounting cyber risks*. 2018.

[8] N. Kshetri, "Cybercrime and Cybersecurity in Africa," *J. Glob. Inf. Technol. Manag.*, vol. 22, no. 2, pp. 77–81, 2019, doi: 10.1080/1097198X.2019.1603527.

[9] E. Kritzinger and B. Von Solms, "A framework for cybersecurity in Africa," *Innov. Vis. 2020 Sustain. Growth, Entrep. Econ. Dev. - Proc. 19th Int. Bus. Inf. Manag. Assoc. Conf.*, vol. 1, pp. 438–447, 2012, doi: 10.5171/2012.322399.

[10] N. Kortjan and R. Von Solms, "A conceptual framework for cybersecurity awareness and education in SA," *South African Comput. J.*, vol. 52, no. 52, pp. 29–41, 2014, doi: 10.18489/sacj.v52i0.201.

[11] A. García Zaballos and F. González Herranz, "From Cybersecurity to Cybercrime: A Framework for Analysis and Implementation," *Institutional Capacit. State Div. Institutions Dev.*, no. September 2013.

[12] K. R. Lee, "Impacts of Information Technology on Society in the new Century," *Structure*, pp. 1–6, 2002, [Online]. Available: https://www.zurich.ibm.com/pdf/Konsbruck.pdf.

[13] N. Roztocki, P. Soja, and H. R. Weistroffer, "The role of information and communication technologies in socio-economic development: towards a multi-dimensional framework," *Inf. Technol. Dev.*, vol. 25, no. 2, pp. 171–183, 2019, doi: 10.1080/02681102.2019.1596654.

[14] M. M. H. Alansari, Z. M. Aljazzaf, and M. Sarfraz, *On Cyber Crimes and Cyber Security*, no. January. 2019.

[15] J. A. Mshana, "Cybercrime: An Empirical Study of its Impact in the Society- A Case Study of Tanzania," *Huria J. Open Univ. Tanzania*, vol. 19, no. 1, pp. 72–87, 2015.

[16] Conference Support Section, Organized Crime Branch, Division for Treaty Affairs, and Unodc, "Comprehensive Study on Cybercrime," *United Nations Off. Drugs Crime*, no. February, pp. 1–320, 2013, [Online]. Available: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

[17] J. L. Bele, M. Dimc, D. Rozman, and A. S. Jemec, "Raising Awareness of Cybercrime – The Use of Education as a Means of Prevention and Protection," pp. 281–284, 2014.
[18] M. Riek, B. Rainer, and T. Moore, "Understanding the influence of cybercrime risk on the e-service adoption of European Internet users," pp. 1–35.
[19] S. Hasan, R. A. Rahman, S. Farah, H. Binti, T. Abdillah, and N. Omar, "Perception and Awareness of Young Internet Users towards Cybercrime: Evidence from Malaysia," 2015, doi: 10.3844/jssp.2015.395.404.
[20] S. Mensch and L. Wilkie, "Information Security Activities of College Students: An Exploratory Study Scott Mensch, Indiana University of Pennsylvania."
[21] N. Kshetri, "Diffusion and effects of cyber-crime in developing economies," *Third World Q.*, vol. 31, no. 7, pp. 1057–1079, 2010, doi: 10.1080/01436597.2010.518752.
[22] R. Chandarman and B. Van Niekerk, "Students' Cybersecurity Awareness at a Private Tertiary Educational Institution," *African J. Inf. Commun.*, no. 20, pp. 133–155, 2017, doi: 10.23962/10539/23572.
[23] J. Cha, "Shopping on Social Networking Web Sites," *J. Interact. Advert.*, vol. 10, no. 1, pp. 77–93, 2009, doi: 10.1080/15252019.2009.10722164.
[24] E. A. Bakar, L. L. Chang, and A. Z. Saidin, "Knowledge, attitude and practices of consumers in e-commerce transactions," *2013 5th Int. Conf. Inf. Commun. Technol. Muslim World, ICT4M 2013*, no. March 2013, doi: 10.1109/ICT4M.2013.6518903.
[25] H. H. Abraha, "Examining approaches to internet regulation in Ethiopia," *Inf. Commun. Technol. Law*, vol. 26, no. 3, pp. 293–311, 2017, doi: 10.1080/13600834.2017.1374057.
[26] F. E. Eboibi, *Concerns of cyber criminality in South Africa, Ghana, Ethiopia, and Nigeria: rethinking cybercrime policy implementation and institutional accountability*, vol. 46, no. 1. Routledge, 2020.
[27] B. B. Reba, "Ethiopian Telecommunications Agency State of Cyber Security in Ethiopia," no. June 2005.
[28] D. Straub and D. Gefen, "Validation Guidelines for IS Positivist Research," *Commun. Assoc. Inf. Syst.*, vol. 13, no. March 2004, doi: 10.17705/1cais.01324.
[29] D. W. Straub, "Validating instruments in MIS research," *MIS Q. Manag. Inf. Syst.*, vol. 13, no. 2, pp. 147–165, 1989, doi: 10.2307/248922.
[30] D. Gefen, D. Straub, and M.-C. Boudreau, "Structural Equation Modeling and Regression: Guidelines for Research Practice," *Commun. Assoc. Inf. Syst.*, vol. 4, no. October 2000, doi: 10.17705/1cais.00407.

[31] X. Li and J. Li, "Statistical Human Genetics," vol. 850, no. November 2014, pp. 411–421, 2012, doi: 10.1007/978-1-61779-555-8.

[32] J. Jeon, "The strengths and limitations of the statistical modeling of a complex social phenomenon: Focusing on SEM, path analysis, or multiple regression models," *Int. J. Soc. Behav. Educ. Econ. Bus. Ind. Eng.*, vol. 9, no. 5, pp. 1604–1612, 2015.

[33] A. Alavifar, M. Karimimalayer, and M. K. Anuar, "Structural equation modeling VS multiple regression," *Eng. Sci. Technol. An Int. J.*, vol. 2, no. 2, pp. 326–329, 2012, [Online]. Available: http://www.estij.org/papers/vol2no22012/25vol2no2.pdf.

[34] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study," *J. Comput. Inf. Syst.*, no. February 2020, doi: 10.1080/08874417.2020.1712269.

[35] K. J. Knapp, T. E. Marshall, R. K. Rainer, and F. N. Ford, "Information security: Management's effect on culture and policy," *Inf. Manag. Comput. Secur.*, vol. 14, no. 1, pp. 24–36, 2006, doi: 10.1108/09685220610648355.

[36] A. Habirovs, "University of Huddersfield Factors that shape cybercrime victimization and use of prevention measures in England and Wales."

[37] S. Burns and L. Roberts, "Applying the Theory of Planned Behaviour to predicting online safety behavior," *Crime Prev. Community Saf.*, vol. 15, no. 1, pp. 48–64, 2013, doi: 10.1057/cpcs.2012.13.

[38] A. Alqarni, "Exploring Factors that Affect Adoption of Computer Security Practices among College Students," *ProQuest Diss. Theses*, p. 130, 2017, [Online]. Available: https://login.pallas2.tcl.sc.edu/login?url=https://search.proquest.com/docview/2013966819?accountid=13965%0Ahttp://resolver.ebscohost.com/openurl?ctx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF-8&rfr_id=info:sid/ProQuest+Dissertations+%26+Theses+Global&rft_v

[39] A. K. Mokha, "A Study on Awareness of Cyber Crime and Security," *Research Journal of Humanities and Social Sciences*, vol. 8, no. 4. p. 459, 2017, doi: 10.5958/2321-5828.2017.00067.5.

[40] K. Edwards, "Examining the Security Awareness, Information Privacy, and the Security Behaviors of Home Computer Users," *ProQuest Diss. Theses*, no. 947, p. 160, 2015, [Online]. Available: https://nsuworks.nova.edu/gscis_etd%0Ahttps://proxy.cecybrary.com/login?url=https://search.proquest.com/docview/1773308920?accountid=26967.

[41] F. Ngo and R. Paternoster, "Cybercrime Victimization: An Examination of Individual and Situational Level Factors," *Int. J. Cyber Criminol.*, vol. 5, no. 1, p. 773, 2011.

Biographies

Bayisa Kune Mamade has attended Dokuz Eylul University which is found in Turkey, Izmir and received his M.Sc. in Computer Engineering in 2015. He gained diploma in laws in 2010 from Oromia State University. He received B.Sc. in Information Technology in Education from Addis Ababa University in 2005. He has experiences of teaching in higher educational institutions since 2005. Currently he is in the department of Electrical and Computer Engineering, Hachalu Hundessa Campus, Ambo University, Ethiopia.

Diriba Mangasha Dabala has attended Addis Ababa University and received his M.A in International Relations in 2014. He has pursued LL.B in Laws from Ambo University in 2016; He has also gained Bachelor of Education in Civics and Ethical Education from Wollega University in 2010.He had teaching experiences of couples of years and still teaching in Ambo University since 2010 in the College of Social Sciences and Humanity, Ethiopia.