Turkish Journal of Computer and Mathematics Education Vol.12 No.12 (2021), 3739-3752

Research Article

Cybersecurity Awareness of University Students in Nigeria: Analysis Approach

Adamu Abdullahi Garba[a], Maheyzah Muhamad Siraj[b], Siti Hajar Othman[c], Waleed A. Zogaan [d]

[a] Department of Computer Science, Yobe State University Damaturu, Nigeria
[a,b,c]School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia, Malaysia
[d] Department of Computer Science, Jazan University, 82822-6649 Jazan, Kingdom of Saudi Arabia

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 23 May 2021

Abstract: Today, the internet has become the backbone to empower and facilitate our daily activities, including educational, financial, and social activities. Nigeria is among the top list of countries that suffered economically from cybercriminals. Many researchers have turned their attention to identifying the cybersecurity awareness of students but limited to the North-eastern universities in Nigeria. University students are prime targets of cyberattacks as research shows frequent access to the internet compared to normal users. The main aim of this paper is to identify the current cybersecurity awareness on the following items (Cyberbully, Personal Information, Internet Banking, Internet Addiction, and Self-protection) of students at the North-eastern universities. The quantitative method was adopted for data collection through a questionnaire that was administered to randomly selected students. The designed questionnaire covers the above items,), based on the holistic result analysis using OrignPro Software the majority of result shows the students have some basic knowledge of cybersecurity in an item like personal information, internet banking, while other items like cyberbully, self-protection and, internet addiction result show moderate awareness. Subsequently, based on the in-depth analysis performed with a control variable "Major Discipline" as specialization, surprisingly, it indicates that engineering, humanity, and law faculties tend to have more awareness of cybersecurity. This survey provides a roadmap toward the design of effective cybersecurity awareness programs and implementation guidelines.

1. Introduction

The advancement of technology has brought opportunities for businesses to perform transactions online via the internet, which is constantly increasing worldwide. The internet has become a prime medium for cybercriminals to perform a variety of cybercrime-related activities. Studies show that a lack of awareness of the threat of cybersecurity attacks is one of the driving factors that contribute to the increasing number of Internet-related attacks (McCrohan et al., 2010; Troia, 2018) (Siddiqui et al., 2020)(Mohammad Ubaidullah Bokhari et al., 2014). Researchers described cybercrime as any criminal activity in which computers or other network devices are used as a tool or a target to commit illegal activities (Finnie, T., Petee, T., & Jarvis, 2010; Gercke, 2012; Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., & Ignatuschtschenko, 2013; Monsurat, 2020; Siegel, 2010). Today, online chat forums, web-sniffing and emails are common ways by which attackers target their victims to launch cyber-attacks, including phishing, IP spoofing, social engineering, denial of service attack, child pornography. According to (Clement, 2020), Africa is becoming more internet-connected than ever before; for example, in Nigeria, alone internet users have reached 99.5 million in 2020. The figure is projected to grow to 131.7 million by 2023. Therefore, it is expected that cybercrime rates will increase simultaneously.

In the past decade, cybersecurity attacks have become daily occurrences in Nigeria, which presents a more significant challenge to the economy, national security and damage to the reputation of the county (F. A. Reegu et al., 2021). To minimize the cybersecurity attacks, security countermeasures and strategies were developed by the Globe Cyber Security Agenda(Gercke, 2012; Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., & Ignatuschtschenko, 2013). These strategies are expected to be implemented globally in the campaign to fight cybercrime activities (Mohammad Ubaidullah Bokhari et al., 2012)(M U Bokhari & Alam, 2013). However, cybersecurity awareness campaigns have not received much attention from both the government and private organizations as a means of fighting against cybersecurity attacks. A few studies have proposed an overview of cybersecurity awareness targeting a small number of participants (Al-Janabi & Al-Shourbaji, 2016; Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., & Ignatuschtschenko, 2013; White, 2011).

Nigeria has a popular crime syndicate known as *yahoo-boys.* These yahoo boys involve using the internet to conduct illegal activities, including account hacking, identity theft, fake relationship, and spreading malware(Ibrahim, 2016). Many individuals, both locally and internationally (foreigners), have been victims of these activities. These activities have led many researchers to analyze the impact of cybercrime and cybersecurity awareness levels on individuals or as a group of a target audience; however, most conducted research has focused on the particular state in which the participants shared the same social, economic, and cultural values (Akanle & Shadare, 2020; Monsurat, 2020; Nzeakor et al., 2020). Moreover, the government has also given much research grants and funding to conduct such studies as many victims of cybercrimes were reported from the southern part of the country.

However, this study aims to identify the current cybersecurity awareness on the following items (*Cyberbully, Personal Information, Internet Banking, Internet Addiction, and Self-protection*) of students at the North-eastern universities on a large number of participants of different cultural background, religion, exposure to the internet

and lifestyle environment, i.e. Universities students from the North-eastern part of Nigeria as many reports have shown cybercrime is increasing exponentially in the region(Sesan Gbenga, B. Soremi, 2015). Therefore, there is an urgent need to conduct this research to assess the level of cybersecurity awareness of people (students) living in those areas. A few studies have been published but have focused on selected state in Nigeria(Adamu A Garba, Siraj, et al., 2020).

Research in the cybersecurity domain is gaining momentum, focusing on designing and implementing end-to-end security mechanisms to ensure the integrity and confidentiality of data and information (Masoodi et al., 2011). However, cybersecurity awareness programs are considered the first security defence line to avoid security attacks and threat confrontation (Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., & Ignatuschtschenko, 2013). The motivation behind this research includes limited research aiming to identify cybersecurity awareness of university students located in the northeast part of Nigerian and also the continues cyberattacks reports. Another motivation of this study is the provision of grants via the tertiary education trust fund (Tetfund) to conduct such research to provide a solution to minimize and increase cybersecurity awareness knowledge in the North-eastern part of the country (Nigeria). Hence, the importance of this study is targeting a larger number of participants with different cultural background and religious exposure. This method would give a clear picture of how cybersecurity knowledge is known to the student, and also, a recommendation on cybersecurity awareness can be proposed.

The remainder of the paper consists of 7 sections. Section 2 discussed the existing literature, Section 3 presents the research methodology, Section 4 explains the results and discussion, Section 5 concludes the findings, and lastly, Section 6 presents the future research direction, section 7 Compliance with Ethical Standards.

2. Literature review

Cybersecurity awareness programs and training are regarded as one of the first defence lines and the most effective means of improving cybersecurity practices. Most cybersecurity awareness programs aim to change the security of individuals. Many theories have been adopted from human psychology that discusses understanding human behaviour. Such theories include General Deterrence Theory (GDT)(D'Arcy et al., 2009; Straub, 1990), Protection Motivation Theory (PMT), and Theory of Planned Behavior (TBP)(Taha & Dahabiyeh, 2020). All these theories are designed to understand human behaviour. For example, GDT focuses on threat severity and susceptibility to threat to predict behavioural intention while PMT emphasizes rational choices and that individuals take calculated action to protect their interest(Bada et al., 2014). These theories have been used mostly in the information system domain and cybersecurity awareness, since the aim is to change an individual's behaviour to instil security consciousness.

A study conducted by Serianu Agency's Nigeria Cyber Security Study (2016)pointed out that the increase in cyber threats and attacks had cost the Nigerian government $550 million. This indicated that most users are not aware of the danger posed by cybercrime and its implications to the economy of a country. However, the study*Awareness and Training, Continuous Monitoring and Log Analysis, Vulnerability and Patch Management, Continuous Risk Assessment and Treatment, and Managed Services and Independent Reviews*identified the top five 2017 cybersecurity challenges (Serianu, 2017).

From the African point of view and in the Nigerian context, the best approach in addressing or mitigating cybersecurity issues from the survey was that almost 95 percent of respondents agree that: *Awareness training* is the primary driving force that will make everyone aware of the problems and danger of cyber-attacks on their businesses. Some respondents also have the view that the IT budget will increase so that technical measures will also be included.

Respondents also agree that "*Education and knowledge is the best way, once a common man is aware of this, he will be vigilant*". The best approach in dealing with cybersecurity in Nigeria is educating both public and private individuals about the possibility of cyber-attacks before it happens. Therefore, according to Ben Robbert, Liquid Telecom Group Chief Technical Officer, Kenya, "My top 3 priorities are *education, education, and education*". All companies need to make sure that all staff are aware of the danger of cybersecurity and should have a basic knowledge of cybersecurity irrespective of their department.

2.1. Cybersecurity Awareness Program in Education Domain

The university system is becoming increasingly digitized day by day. One reason is the current COVID-19 epidemic, as online courses and degrees are much more prevalent, and new learning methods that fully depend on technology have been adopted (Alam et al., 2021). Existing research on the security of the online learning system has illuminated some of the challenges in using online platforms for educational purposes; such are attacks on protecting students' examination and processes, content filtration, and virus and malware attacks. There are many motives toward targeting educational institutions as large databases contain valuable information about students (Shuaib et al., 2021)(M U Bokhari et al., 2011). There is also a lack of security controls in university on what devices students can bring and use in their learning process environment (Monrad, 2019). This issue makes

it important to create a secure learning environment. Many researchers have focused on identifying the antecedent of cybersecurity awareness. Some authors have adopted the theories explained above to assess the impact of individual factors, such as age and gender, on cybersecurity knowledge and behaviour (Ahlan et al., 2015; Al-Alawi et al., 2016).

Cybersecurity awareness has been implemented in the educational domain to either identify the level of awareness or implement a program to increase the level of awareness among students and academics (Al-Janabi & Al-Shourbaji, 2016; Adamu A Garba, Othman, et al., 2020). Educational establishments offer to use the internet in research; therefore, they can be victims of cyber-attack, especially the students whose knowledge of cybersecurity is limited, as some previous research has indicated. Students mostly engage in social networking using the university internet. Their personal information can be compromised or made vulnerable to cyberbullying as there is much available information about hacking skills that can equip potential offenders with knowledge and tools to hack (Van Nguyen, 2020) (Abdus et al., 2018)(Alam et al., 2019). Therefore, universities must provide preventive measures to counter any attack as there is a relationship between preventive measures and information security awareness (Knapp et al., 2006). Cyber-attacks can only be minimized if people (students) have adequate knowledge and practise good behaviour when using the internet as a relationship exists between the two(Kruger et al., 2010).

3. Methodology

This section explains the methodology adopted for this research and how it was conducted; the section includes: data collection, Measures and data analysis.

3.1. Data collection

The quantitative data collection approach is commonly used in data collection and analysis, as reported in (Al-Janabi & Al-Shourbaji, 2016; Aloul, 2012; Gabra et al., 2020; Adamu A Garba, Othman, et al., 2020; Kim, 2014; Slusky & Partow-Navid, 2012; Yang et al., 2017)(Adamu Abdullahi Garba et al., 2021). Similarly, this study adopted a similar research method for data collection and analysis from participants. The question used in this research was adapted from a study of (Khalid et al., 2018) where they try to investigate University students' cybersecurity awareness level on the following items: Personal Information, Internet Banking, Cyberbully, InternetAddiction, and Self-protection in Universiti Kebangsaan Malaysia. Based on the context of this research objective, the following items were investigated: *Personal Information, Internet Banking, Self-protection, Cyberbully and, Internet Addiction* of university students in the North-eastern states of Nigeria. The paper adopted (Son et al., 2014) for data collection and processing to make it easier to be repeated and generalized. The surveyed states include *Adamawa, Borno, Bauchi, Gombe, Taraba, and Yobe*. Due to Covid 19 pandemic, all universities are closed, therefore the questionnaire was designed using Google form and distributed via various platforms.

3.2 Measures

The questions were organized based on the item explained, consisting of four questions making a total of twenty questions (All these questions were asked to answer the research aim to identify cybersecurity awareness of the students in north-eastern universities in Nigeria. The paper measures students' level of awareness of cybersecurity based on the above item discussed. To answer the question, each participant is required to indicate the level of agreement and disagreement with the statements using the concept of a five-point Likert scale from strongly disagree (1) to strongly agree (5) as shown in Table I More than 500 participants were selected to participate (July to September 2020). The expected time to complete the questionnaire is estimated to be 20 minutes**.** Figure 1 shows the Research Survey Design model used in the paper.

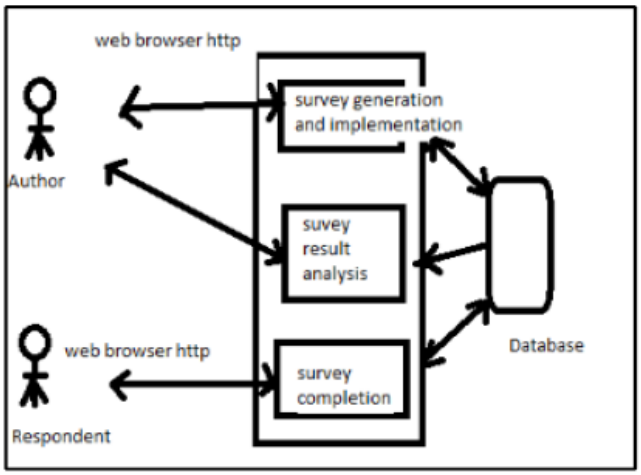

Figure 1. Research Survey Design Model

3.3. Data Analysis

The questionnaires was distributed to states consisting of both private and government universities. The responders were selected from all universities within the northeast, as indicated in table 1, the method of recruiting responders was a random approach so as to get responders from a different social, economic and religious background. This method was used to get divers opinions on the subject being asked. All responders were asked for participation using email address and 600 shows interest in participating in the research voluntary and withdrawal from being part in the study can happen at any point, also the study guarantees the anonymity of participants. Filling in the questionnaire was considered as an indication of participants' consent to take in the study. More than 600 questionnaires were sent using various platforms. A total of 500 was received. After analyzing the data, a total number of 59 were discarded as some did not answer all the questions given. The answered and valid questionnaires were 441 out of the 500 sent; therefore the 441 was used for analysis and interpretation in the next section.

3.4. Demographic Analysis

This section explains the demographic information of participants in the survey and included gender, age, and university type. The three categories of age groups of respondents fall between 18 – 20 age group is 17.9 % i.e.79; the age group between 21-25 is 45.6%, i.e. 201 respondents; and lastly, the age group between 26-30 is 36.6%, which is 161 respondents. Moreover, the number of participants based on gender shows, males constitute 77.1%, i.e. 340, and females constitute 22.9%, i.e. 101 individuals. The three categories of age groups and the number of participants in each age group. The number of respondents between 18 – 20 age group is 17.9 %, i.e. 79 respondents; the age group between 21-25 is 45.6%, i.e. 201 respondents; and lastly, the age group between 26-30 is 36.6%, which is 161 respondents. Moreover, the number of participants based on gender shows, males constitute 77.1%, i.e. 340, and females constitute 22.9%, i.e. 101 individuals.

3.5. University Type Analysis

This section explains the type of responders' university, as in Nigeria, there are three types of university: private, state and federal. Figure 2 shows the university categories.

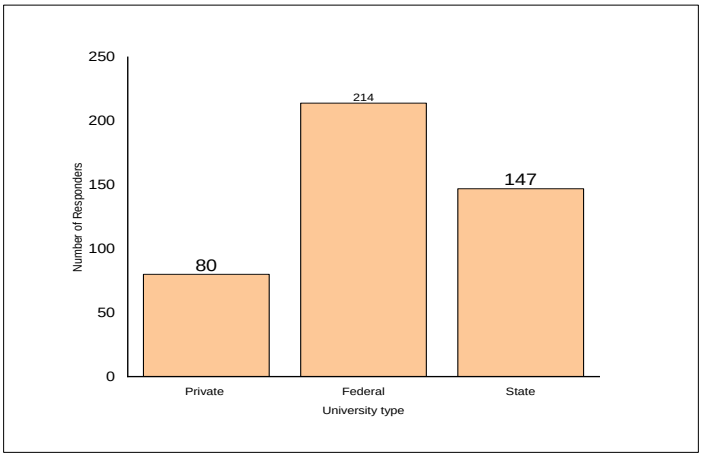

Figure 2. Responders University Categories

Fig 2 shows the type of universities the survey responders come from. As shown, students from the private university are 18.1%, i.e. N=80; State Universities are 33.1%, i.e. N=147, and federal Universities are 48.5%, i.e. N=214. Fig 4 indicated more federal universities have participated than the other Universities.

3.5Major Discipline Analysis

This section shows the type of faculties from where the students surveyed study. Based on the feedback received, there are six faculties, as shown in Figure3.

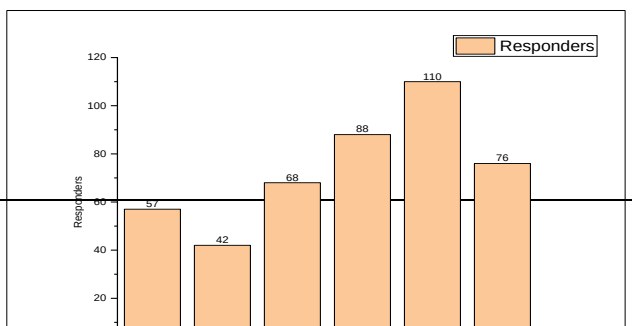

Figure 3. Responders'Major Discipline

The feedback received indicates a total number of 57 respondents are from Science faculty, 42 from Art and education,68 from Humanity, 88 from Engineering, 110 from the law, and 76 from medical Science. It indicates that students from the faculty of law have participated more than students from any other faculty in this research.

4. Result and Discussion

The objective of the study is to identify the level of cybersecurity awareness regarding the following items*: Personal Information, Internet Banking, Self-protection, Cyberbully and, Internet Addiction* of university students in the north-eastern states of Nigeria. This section analyzes the result from the feedback and discusses the outcome base on the research objectives.

4.1 Students Awareness of Personal Information

This subsection analyses participants' feedback on the impact of cybersecurity on personal information. Personal information is a driving factor that led to social engineering, which might result in cyber-attacks when revealed to unintended parties. Such cyber-attacks include *identity theft, Ransomware, internet fraud,* cyber*bullying*, *social engineering.* Therefore, there is a need to identify how the students can protect their personal information when using the internet. Figure 4 represents the analysis of the results for the student's personal information.

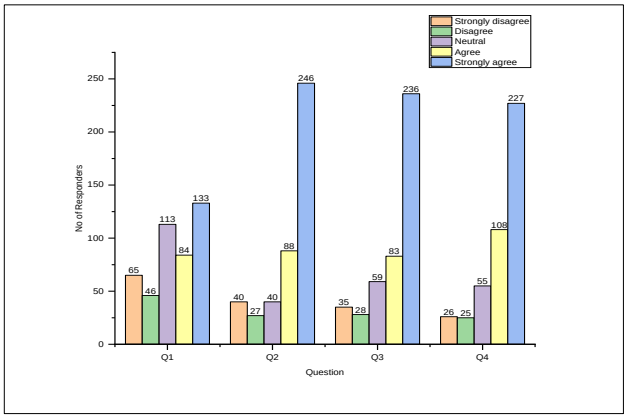

Figure 4. Respond to Personal Information items

Q1: I am worried that my personal information might be misused. From the figure, it can be seen that around 30% of the respondents strongly agree to the question *"I am worried that my personal information might be misused*", accounting for number(N) =133, while only (N=65, 14%) admitted to not being worried if their information might be misused. However, a significant proportion of respondents (N= 113, 25.6%) admitted to being "neutral" to the question asked.

This results analysis reveals that 30% of the students have some basic knowledge on how to protect their personal information when using the internet; however, because 23% of respondents selected "neutral", there is a need for a cybersecurity awareness program that will discuss how to protect personal information and the dangers of revealing it.

Q2: I am not comfortable when my personal information was shared without my permission. Figure 6 shows how the respondents express their thoughts regarding whether they feel comfortable when their information is shared without their permission. The results show that the majority of the respondents strongly agree (N=246, 55.8%) to not feeling comfortable when their personal information was shared without their permission, while (N=40, 9.1%) feel it is ok if their information is shared without their consent.

The outcome of the result has indicated approximately 55.8% have an idea of the concept of identity theft. However, the students also expressed concern about the issue of not being comfortable when their information is shared without their consent.

Q3, I am worried if my personal information was not securely kept online. The result vividly indicates the majority of the students are worried about the security of their personal information online. (N=236, 53.5%) strongly agree, while a small proportion (N=35, 7.9%) disagree with the question. The analysis of the result has indicated many students are engaged with online activities and are worried their information might be stolen. This analysis displays that students are being careful of what information they save and send via social medium.

Q4, I will only provide my personal information when I was asked by an organization that I know well. When asked what information students will provide, (N=227, 51%) admitted to only reveal the information when asked, and only (N=26, 5.9%) disagree with the question.

Basic cybersecurity knowledge is essential to all individuals. However, this result has indicated that the surveyed students have some basic idea of protecting their personal information as 51% said that they would only reply to a legitimate organization that they know and trust.

4.2 Students Awareness of Internet Banking

This part also analyses the students' feedback from the conducted survey on how students behave when using internet banking. Internet banking has now become a major part of everyone's life; therefore, more cybercrimes have been reported regarding internet banking. Cyber-attacks related to internet banking include *internet Scams, Denial of Service attacks, phishing emails* (F. Reegu et al., 2020). Hence, students need to be aware of the dangers of using internet banking and how to protect their financial information. Figure 5 illustrates all the question results from the survey.

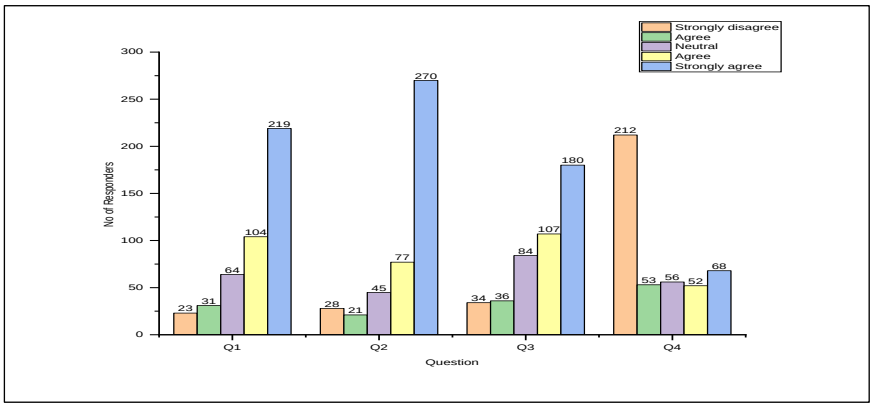

Figure 5. Respond to Internet Banking

Q1, I will only make an online purchase after inspecting the seller's background.

The question is about making a purchase online without understanding the background of the seller. (N=219, 49.7%), the majority of the students make sure they are familiar with the seller before making any purchase, while (N=23, 5.2%) make online payment without checking the seller information.

The analysis has demonstrated that around 50% of the respondents are careful when making any online transaction, and seller information is checked before making payment. The participants have indicated they are aware of online scammers and are diligent when making an online payment.

Q2, I will not make any online purchase if I found the quality of the good is unreliable. The result indicates a higher awareness when it comes to online purchases. (N270, 61.2%) strongly agree with only buying what is reliable, while (N=28, 6.3%) show less interest in checking items before buying.

It indicates that the majority of the students have some basic knowledge of internet scammers, like the previous question analysis, as more than 60% purchase good quality products only after knowing the sellers' information, which further indicates knowledge of online fraud.

Q3, I am worried when I received any suspicious online advertisement. The answer to the question on receiving any suspicious online advertisement indicated (N= 180, 40%), which is a large number of students, are worried about receiving unwanted messages across their account, while (N=107, 24.3%) also agree with the statement, and (N=34, 7.7%) do not worry or care about receiving any kind of message.

This result proves that students are careful about what they see and receive from an unwanted source as phishing emails have become the simplest way criminals use to get information from their target. Thus, it is shown that a large percentage of the respondents are aware of such attack.

***Q4, I will provide my personal information whenever I received calls from banking organizations*,** describes how the students feel or act when they received a call from banks asking for personal information. (N=212, 48.1%) disagree with the questions while only (N=68, 15%) agree to the questions.

The analysis confirms that most students are very aware and familiar with yahoo- boys' methods of scamming victims, as 68% attested to that; however, more cybersecurity awareness programs are needed to educate the remaining students.

4.3 Student Awareness on Self Protection

Awareness of self-protection is significant, as many attacks can be successful if individuals have fallen to protect their data. Therefore, this section evaluates the respondents' responses on how well they are aware of self-protection when it comes to cybersecurity. Figure 6 shows all four questions with their analyzed results.

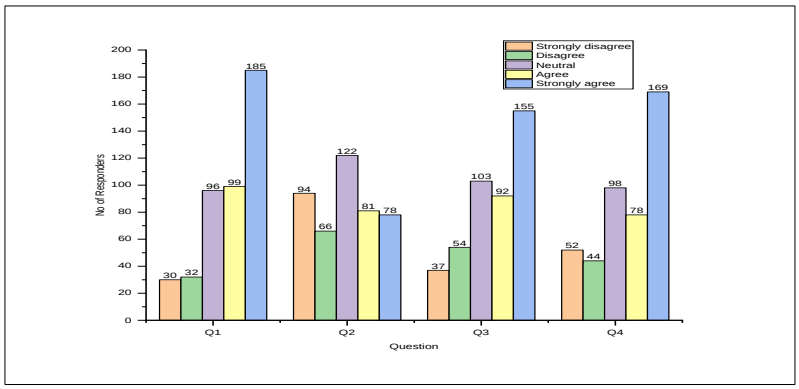

Figure 6. Respond to Self-Protection

Q1 I will only add new friends to my social media after inspecting their background. The results shows (N=185, 42.2%) have strongly agreed to check any friend request before adding, while (N=96, 21.5%) are neutral, and only (N=30, 6.8%) strongly disagree.

The analysis shows that 50% of the students check friend request background before accepting or rejecting as many cybercriminals use social media to launch social engineering attacks. It has confirmed the respondents are aware of such attacks and are careful of who to befriend. However, more awareness is needed to demonstrate how such an attack occurs practically.

Q2 I think I will consider meeting my new online friend alone. The results on whether students would meet a friend made online alone (N=122, 27.7) selected "neutral", which indicates they do not mind. However, another (N=94, 21.3%) and (N=66, 15%) disagree on meeting a friend made online alone.

The analysis revealed around 50% have agreed while another 50% disagreed on meeting new online friends alone. It has indicated urgent awareness is needed here to enlighten the danger of that to the students who agree to the question as many criminals take advantage of this to kidnap and demand a ransom.

Q3 I will not share my contact number with a person whom I newly know when asked. (N=155, 35.1%) and (N=94, 20.9%) have agreed (both "strongly agree" and "agree") not to share contact number with a new person made online, while only (N=37, 8.4%) strongly disagree with the question.

The outcome of the analysis has indicated that the majority of the students are vigilant about whom they can share their personal information with, as more than 50% affirmed that this is a clear indication that reveals the respondents have basic awareness on how to interact with people that they have met on social media platforms.

Q4 I will inform my parents when my online friends want to meet me up. The analysis of the question shows (N=169, 38.3) and (N=78, 17.9%) have selected "agree", which shows that they would notify their parents when meeting an online friend, while (N=98, 22.2%) are neutral and (N= 52, 11.8%), (N=44, 10%) have disagreed with the question.

The result indicated that the respondents could meet an online friend with their parents' consent, as 56.2% agreed. This implies parents are aware when it comes to meeting new people, and it is good to avoid being kidnapped or harassed.

4.4 Students Awareness of Cyberbully

Cyberbully is among the top cybercrime that affects the young generation, i.e. students, due to their excessive usage of social media platforms, may become victims, who are usually threatened to do or give something in exchange for their stolen information; therefore, there is an urgent need to know the impact of this attack on the students as there are few programs that tackle cyber harassment awareness courses that focus the perpetrators of these crimes (Conradie et al., 2020). Figure 7 shows the analysis of all the questions' feedback**.**

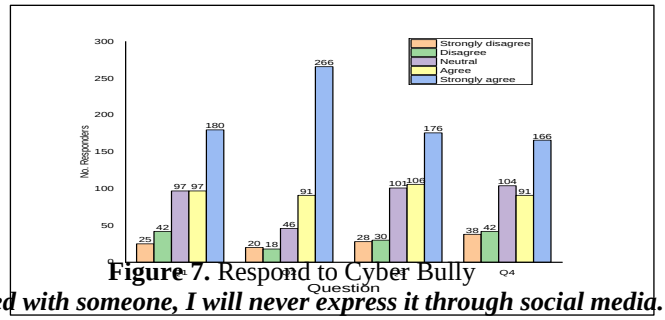

Figure 7. Respond to Cyber Bully

Q1, although I felt unsatisfied with someone, I will never express it through social media. The result shows that (N=180, 40%), (N=97, 22%) have agreed not to express their hatred to some online, while the same proportion (N= 97, 22%) are neutral to the expression. (N=42, 9.5%) and (N=25, 5.7%) disagree with the question.

This shows that students don't mind expressing their feelings to a person through social media. Overall indication concludes that the majority of the respondents agreed not to express dissatisfaction with someone via social media. This analysis also proves that students are not likely to be involved in that act of cyberbully.

Q2 I think giving harsh comments to my friends on social media is not a good thing to do. The analysis indicated (N=266, 60.3%) and (N=91, 20.6%) have agreed that it is not a good idea to write a harsh comment to a friend when replying to his/her post or message. However, a small percentage have disagreed with the question (N= 20, 4.5%) and (N18, 4.1%).

The outcome shows that 80% of the respondents have agreed not to use harsh wording when replying to a post. This question also indicated the surveyed students are not likely to be involved in a cyberbully act.

Q3 ***I think it is not acceptable to criticize someone when they uploaded their controversial photos***. The analysis shows (N= 176, 39.9%) and (N=106, 24%), which accounts for 63% of the respondents, have agreed it is not good to criticize someone for uploading a provocative photo on social media, while only a few have disagreed with the question and those account for 8.6% of the total respondents. Similarly, 22.9% are neutral, which implies they can either agree or disagree.

The overall analysis displays majority would not be involved in criticizing someone simply because they uploaded a provocative photo or statement, which means the surveyed respondents are well-mannered individuals.

Q4 ***I will never express my anger to someone through social media***. This question was asked to know if the students would ever express their anger in social media and the results indicated (N=166, 37.65) and (N=91, 20.6%) have agreed to that, while (N= 104, 23.6%) are neutral to the question. However, 17% of the respondents have disagreed with the question.

This outcome shows respondents would not express their anger to anyone through social media as 57% have agreed to that, which implies that the respondents can control their anger via social media.

4.5 Students Awareness of Internet Addiction

The internet has become part of almost everyone's lives, as many businesses, works, interactions are now performed through the internet. In this context, and the internet is a vital medium of research by educational initiations. To identify the impact of internet addiction, students were asked questions concerning their use of the internet. Figure 8 shows an analysis of the surveyed feedback collected from the participants.

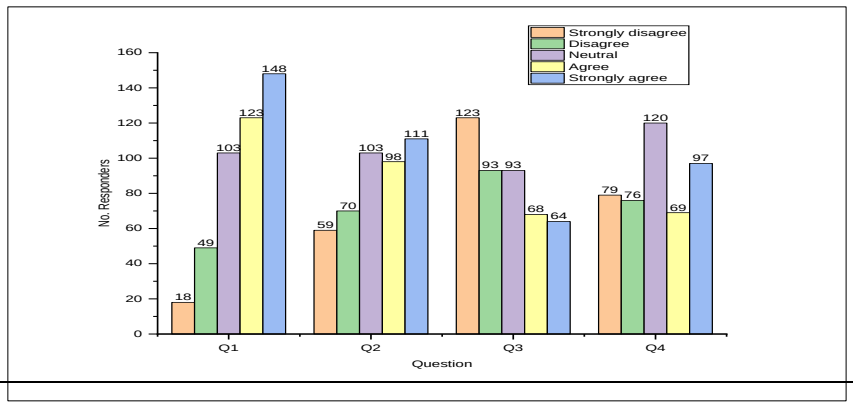

Figure 8. Respond to Internet addiction

Q1I will be extra excited when I use the internet. This question would determine how occupied students are with using the internet. The results show (N= 148, 33.6%) and (123, 27.9%) have agreed that they are excited when using the internet, while 11% of the respondents disagree with the question and 23.4% have shown less interest in the question.

The analysis shows that almost 60% of respondents are happy when using the internet. It entails that if cybersecurity awareness is less, they may be at risk of cyber-attacks. Therefore proper enlightenment on how to use the internet safely without being a victim of cyber threat is needed.

Q2 The time spent without surfing the internet is the most boring moment. The result affirms that (N=111, 33.6%) and (N=98, 22.25) have agreed that they are happier when spending their time on the internet, while 29% disagree with the question and a fraction of the students, 23.3%, are neutral to the question.

The feedback indicated that 55% of the students feel that their life is boring when not using the internet. However, it also supports the previous question in that almost 60% of the respondents are extra excited when using the internet. This implies that students should be careful when interacting with people as many criminals turn to the internet to find their victims.

Q3 ***without the Internet, there is nothing I can do. T***he result remarkably indicates students can be engaged in other things if there is no internet as the result shows (N=122, 27.9%) and (93, 21.1%) disagree with the statement that they cannot do anything without the internet, while a small percentage, i.e. 29.9% have supported the question and another 21.1% are neutral to the statement.

The last question was asked to see if students prefer outdoor activities or just spending time on the internet at home. Looking at the feedback from Q1 and Q2, where it indicates how happy they are when using the internet, it is also shown here they can still do other things apart from spending much of their time surfing the internet.

Q4 I would spend more time on social media than having outdoor activities. The result surprisingly indicates (N=120, 27.2%) are neutral, which shows a majority can do both, i.e. can spend time on the internet and also do some other outdoor activities, but the overall results of those that agreed with the statement are 37%, which is higher than the neutral respondents. However, a small segment that accounts for up to 35.1% has disagreed with the question.

This question is among the narrowest range of respondents to each Likert scale, with the highest one being the agreed section with 37%, which shows that quite a number of students can do other outdoor activities. These show the relationships between each question and the link between them in order to identify how addicted students are to the internet.

4.5 Result and discussion Analysis of Based on Major Discipline

This section explains more on the feedback analysis based on a control variable "Major Discipline". This analysis will give more in-depth knowledge on the cybersecurity awareness level among the students and also would identify the students that have more knowledge on cybersecurity, with this analysis proper cybersecurity will be design for the appropriate audience. Table 1 displays the results of the analysis.

Faculty	Question	N	Science		Art and Education		Humanity		Engineering		Law		Medical Science							
Items			**Mean**	**SD**	**Mean**	**SD**	**Mean**	**SD**	**`Mean**	**SD**	**Mean**	**SD**	**Mean**	**SD**	**Mean**	**SD**	**Mean**	**SD**	**Mean**	**SD**
Personal Infor	Q1	441	3.95	1.394	4.12	1.194	4.07	1.194	4.08	1.271	3.95	1.240	4.11	1.332						
	Q2	441	3.86	1.563	4.07	1.197	3.99	1.409	4.24	1.165	4.09	1.253	4.09	1.308						

matio n	Q3	441	3.23	1.536	3.50	1.330	3.2 9	1.40 4	3.4 3	1.30 2	3.4 4	1.40 5	3.4 5	1.4 18
	Q4	441	4.26	1.078	4.05	1.168	4.0 5	1.16 8	4.0 9	1.19 0	3.9 7	1.16 1	4.1 1	1.1 84
Cumul ative Mean/ SD	3.82 5	1.39 275	3.93 5	1.222 25	3.85	1.2937 5	3.9 6	1.23 2	3.8 625	1.26 475	3.9 4	1.31 05		
Intern et Banki ng	Q1	441	3.98	1.295	4.02	1.199	4.2 1	1.08 7	3.9 8	1.29 5	4.1 8	0.96 9	3.8 9	1.2 17
	Q2	441	4.05	1.481	4.10	1.265	4.2 4	1.21 1	4.2 0	1.24 3	4.4 2	0.93 2	4.1 6	1.1 89
	Q3	441	3.86	1.315	3.52	1.366	3.9 7	1.24 6	3.9 3	1.18 2	3.7 0	1.28 9	3.8 8	1.2 22
	Q4	441	2.42	1.647	2.45	1.485	2.2 9	1.60 3	2.2 8	1.53 1	2.4 1	1.51 6	2.2 5	1.4 80
Cumul ative Mean/ SD	3.57 75	1.43 45	3.52 25	1.328 75	3.677 5	1.2867 5	3.5 975	1.31 275	3.6 775	1.17 65	3.5 45	1.27 7		
Self- Protec tion	Q1	441	4.02	1.217	3.74	1.211	3.7 4	1.34 5	4.0 6	1.19 7	3.8 2	1.22 8	3.7 2	1.1 96
	Q2	441	2.96	1.388	2.93	1.314	3.0 9	1.48 4	2.9 3	1.39 6	3.0 5	1.39 4	2.7 6	1.2 74
	Q3	441	3.81	1.315	3.26	1.380	3.5 0	1.41 9	3.8 8	1.19 2	3.5 6	1.3. 3	3.5 8	1.2 14
	Q4	441	3.58	1.362	3.67	1.319	3.5 0	1.45 1	3.7 8	1.32 6	3.4 3	1.43 6	3.7 5	1.3 67
Cumul ative M/SD	3.59 25	1.32 05	3.4	1.306	3.457 5	1.4247 5	3.6 625	1.27 775	3.4 65	1.01 45	3.4 525	1.26 275		
Cyber bully	Q1	441	3.70	1.253	3.95	1.188	3.8 7	1.30 3	4.0 1	1.16 9	3.6 9	1.19 4	3.8 0	1.2 44
	Q2	441	4.14	1.187	4.21	1.180	4.3 7	1.11 8	4.2 4	1.17 4	4.2 7	1.03 1	4.4 1	0.9 69
	Q3	441	3.63	1.422	3.98	1.259	3.8 1	1.22 5	3.9 3	1.19 2	3.7 7	1.08 1	3.9 6	1.1 71
	Q4	441	3.79	1.306	3.81	1.292	3.7 2	1.29 1	3.7 3	1.41 2	3.6 9	1.17 1	3.4 9	1.3 42
Cumul ative Mean/ SD	3.81 5	1.29 2	3.98 75	1.229 75	3.942 5	1.2342 5	3.9 775	1.23 675	3.8 55	1.11 925	3.9 15	1.18 15		
Intern et Addict ion	Q1	441	3.74	1.142	3.83	1.208	3.7 8	1.28 0	3.8 4	1.17 3	3.7 1	1.07 0	3.6 8	1.1 22
	Q2	441	3.14	1.369	3.43	1.364	3.1 9	1.50 9	3.3 9	1.33 4	3.4 2	1.30 2	3.1 7	1.3 10
	Q3	441	2.26	1.330	2.60	1.380	2.8 7	1.50 5	2.6 6	1.44 5	2.9 0	1.32 7	2.5 5	1.3 70
	Q4	441	2.89	1.410	3.00	1.414	3.1 5	1.44 8	3.1 9	1.40 5	3.1 5	1.30 8	2.8 8	1.4 04
Cumul ative Mean/ SD	3.00 75	1.31 275	3.21 5	1.341 5	3.247 5	1.4355	3.2 7	1.33 925	3.2 95	1.25 175	3.0 7	1.30 15		

Table 1. Result analysis of based on major discipline

Key

From 3.6 -5.0 High	From 3.0 – 3.5 moderate	2.0- 3.0 Low

4.6 Discussion on Science Students' Awareness

The result from the feedback obtained from science students indicates the students have high basic knowledge of personal information and cyberbully with a cumulative mean of more than 3.8, while moderate in internet banking and internet addiction. This result has given insight into what cybersecurity program should address for the science students as moderate and low shows there is a need for awareness.

4.7 Discussion on Art and Education Students' Awareness

The Art and education students analyzed results shows the students have a high understanding of the items personal information and cyberbully while having moderately low in internet banking, self-protection and internet addiction with a mean of <=3.5. This result shows that most education students lack basic awareness of some important cybersecurity items, which prompts them to be cyber-attack victims. However, this calls for urgent planning of a cybersecurity awareness program to explain and practically show how to minimize the impact of the threats.

4.8 Discussion on Humanity Students' Awareness

The analyzed results received from humanity students indicate a high awareness of personal information, internet banking and cyberbully, while a moderately low awareness of self-protection and internet addiction, and from these results, implies Humanity students lacks knowledge of self-protection and internet addiction vulnerability. Therefore, a need to plan a cybersecurity awareness program is important to the students for awareness in those items.

4.9 Discussion on Engineering Students' Awareness

The engineering students' feedback shows awareness in personal information, self-protection and cyberbully, while moderately average awareness in internet banking, internet addiction. Surprisingly, this result shows engineering students having less awareness of internet banking with a cumulative mean(CM) of 3.5. This indicates some students need to undergo cybersecurity training to become familiar with the concepts of all these items and how to protect their information when using the internet.

4.10 Discussion on Law Students' Awareness

The outcome of the analyzed result obtained from the faculty of law shows students have a high understanding of personal information, internet banking and cyberbully, while moderately low in self-protection and internet addiction. Therefore, these surveyed students need awareness of self-protection and internet addiction specifically.

4.11 Discussion on Medical Sciences Students' Awareness

Medical sciences students' evaluated results show high awareness of personal information and cyberbully, while in internet banking, self-protection, and internet addiction, the result is moderately low. These items with moderate awareness need to be included in the cybersecurity awareness program courses to be discussed.

Table IX has summarized the results and also indicated where a cybersecurity awareness program is required or not. It also pointed out the similarity in the results across the faculties and also the faculties that require fewer programs.

Table 2. Result comparison based on faculty

Faculty items	Science	Art and education	Humanity	Engineering	Law	Medical sciences
Personal Information	NR	NR	NR	NR	NR	NR
Internet Banking	R	R	NR	R	NR	R
Self-protection	R	R	R	NR	R	R
Cyberbully	NR	NR	NR	NR	NR	NR
Internet addiction	R	R	R	R	R	R
Total required	**3**	**3**	**2**	**2**	**2**	**3**

Note: R= required, NR= Not required

Table 2 indicated that none of the faculties requires cybersecurity awareness in personal information and cyberbully as the results obtained show high awareness, and subsequently, all the faculties require awareness in internet addiction. However, Science, Art and education, and medical sciences require awareness of internet banking and self-protection. Meanwhile, humanity and law require awareness of self-protection. Similarly, engineering requires awareness of internet banking. Surprisingly, the comparison results indicate engineering, humanity, and law faculties tend to have more awareness based on the surveyed items as students show moderate awareness of only two items, unlike the other faculties that require three programs.

5.Conclusion

Cybersecurity knowledge is a must for all individuals irrespective of gender, education, organization, and age group, as now many activities are performed via the internet. Many developed countries have implemented strategies on the cybersecurity awareness of their citizens. Also, much research was conducted to identify the level of cybersecurity awareness of organizations' staff of an educational institution. In general, factors such as searching for knowledge, keeping in touch with family and friends, searching for a job, and students engaging with the connected world make them the prime target of cybersecurity attacks and threats. Research shows the current level of cybersecurity awareness among Nigerian students, particularly in the North-eastern part, required urgent attention to reduce the risk of potential victims.

The study has adopted quantitative methods in data collection. SPSS software was used to analyze the data and presented using OrignPro Software. A total of 600 questionnaires were sent out, and 500 were received; however, after filtering the uncompleted questions, a total of 441 were used for data analysis. As discussed, the analysis is based on cybersecurity items being investigated, which are Personal information, Internet banking, Self-protection, cyberbully and Internet addiction. Each item consists of four questions to determine the awareness level of the respondents. Based on the general analysis performed on the feedback, the overall results have indicated the majority of the students who participated in the study have some *basic knowledge* of cybersecurity in items like *personal information, internet banking*, while other items like *cyberbully, self-protection and, internet addiction* result shows moderate awareness.

However, in the second section of the analysis, a control variable, "Faculty", was used to analyze further the results based on specialization. The analysis shows that students from all faculties have a higher knowledge of *personal information and cyberbully* and moderately low knowledge of *internet addiction*. However, faculties like Science, Art, education, medical sciences, humanity, and law require awareness in self-protection. Similarly, engineering, Science, Art and education, and medical sciences all require awareness in internet banking. Those having a higher chance of understanding cybersecurity are engineering, humanity, and law faculties.

This has given a hint to further the study in the North-eastern part of the country on designing and implementing cybersecurity awareness programs as a proactive approach to increase cybersecurity awareness among students and make students identify how to defend themselves from some basis cyberattacks and also as a benchmark to internet users for identifying the current level of cybersecurity knowledge to help cyber experts to decide what program is appropriate to the users.

6. Future direction

The case study results and discussion indicates the students have some basic knowledge of cybersecurity terminologies. However, in other areas, their results indicated an urgent intervention to address those issues. Therefore, the next paper will focus on planning, designing, and implementing an effective cybersecurity awareness program that will address those issues, increase cybersecurity knowledge, and reduce network attacks and threats to the students and internet users in the northeast using theories and hypotheses. In addition, other analysis such as regression and Structural equation modelling (SEM) would be performed to identify the impact of the programs. Other possible research directions include assessing the methods used to assess the effectiveness of cybersecurity awareness programs, the best method to deliver the effectiveness of cybersecurity awareness programs, and lastly, cybersecurity awareness maturity framework design and implementation.

7. Compliance with Ethical Standards

Ethical approval and consent to participate Participants were asked to fill an online questionnaire through various platforms, which was completely optional. We considered filling in the questionnaire as an indication of participants' consent to take part in the study. Therefore, a section was created for the participant to tick for consent before filling the questionnaire.

References

1. Abdus, S., Shadab, A., Mohammed, S., & Mohammad.Ubaidullah, B. (2018). Internet of Vehicles (IoV) Requirements, Attacks and Countermeasures. 5 International Conference on "Co Mputing for Sustainable Global Development, March, 4037–4040.

2. Ahlan, A. R., Lubis, M., & Lubis, A. R. (2015). Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. Procedia Computer Science, 72, 361–373. https://doi.org/10.1016/j.procs.2015.12.151
3. Akanle, O., & Shadare, B. R. (2020). Why has it been so difficult to counteract cyber crime in Nigeria? Evidence from an ethnographic Study. International Journal of Cyber Criminology, 14(1), 29–43. https://doi.org/10.5281/zenodo.3738962
4. Al-Alawi, A. I., Al-Kandari, S. M. H., & Abdel-Razek, R. H. (2016). Evaluation of Information Systems Security Awareness in Higher Education: An Empirical Study of Kuwait University. Journal of Innovation and Business Best Practice, 2016, 1–24. https://doi.org/10.5171/2016.329374
5. Al-Janabi, S., & Al-Shourbaji, I. (2016). A Study of Cyber Security Awareness in Educational Environment in the Middle East. Journal of Information and Knowledge Management, 15(1). https://doi.org/10.1142/S0219649216500076
6. Alam, S., Abdullah, H., Ayoub, Y., Abdulhaq, R., Alshaikh, A., & Hayawi, A. (2021). A Blockchain-based framework for secure Educational Credentials. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(10), 5157–5167.
7. Alam, S., Shuaib, M., & Samad, A. (2019). A Collaborative Study of Intrusion Detection and Prevention Techniques in Cloud Computing. In Lecture Notes in Networks and Systems (Vol. 55). Springer Singapore. https://doi.org/10.1007/978-981-13-2324-9_23
8. Aloul, F. A. (2012). The Need for Effective Information Security Awareness. Journal of Advances in Information Technology, 3(3). https://doi.org/10.4304/jait.3.3.176-183
9. Bada, M., Sasse, A., & Bada, M., Sasse, A., Nurse, J. (2014). Cyber Security Awareness Campaigns: Why They Fail to Change Behavior. International Conference on Cyber Security for Sustainable Society, 11.
10. Bokhari, M U, Ahmad, S., Alam, S., Masoodi, F., & Science, C. (2011). Modern Tools and Technologies for Interactive Learning. 5th National Conference; INDIACom-2011, 5–8.
11. Bokhari, M U, & Alam, S. (2013). BSF-128: a new synchronous stream cipher design. Proceeding of International Conference on Emerging Trends in Engineering and Technology, 541–545.
12. Bokhari, Mohammad Ubaidullah, Alam, S., & Hasan, S. H. (2014). A Detailed Analysis of Grain family of Stream Ciphers. International Journal of Computer Network & Information Security, 6(6).
13. Bokhari, Mohammad Ubaidullah, Alam, S., & Masoodi, F. S. (2012). Cryptanalysis techniques for stream cipher: a survey. International Journal of Computer Applications, 60(9).
14. Clement, J. (2020). Nigeria: Number of internet users 2025.
15. Conradie, L., Pitchford, M., Myers, E., Barnes, T., & Short, E. (2020). Cyberharassment awareness course (cybac): Influences from domestic abuse perpetrator programmes for its design and function. International Journal of Cyber Criminology, 14(1), 220–235. https://doi.org/10.5281/zenodo.3750140
16. D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information Systems Research, 20(1), 79–98. https://doi.org/10.1287/isre.1070.0160
17. Finnie, T., Petee, T., & Jarvis, J. (2010). The Future Challenges of Cyber-crime. Proceedings of the Futures Working Group. US, Virginia Quantico: Federal Bureau of Investigation.
18. Gabra, A. A., Sirat, M. B., Hajar, S., & Dauda, I. B. (2020). Cyber security awareness among university students: A case study. Journal of Critical Reviews, 7(16). https://doi.org/10.31838/jcr.07.16.108
19. Garba, Adamu A, Othman, S. H., & Musa, M. A. (2020). A Study on Cybersecurity Awareness Among Students in Yobe State University, Nigeria: A Quantitative Approach 1. 11(5), 41–49.
20. Garba, Adamu A, Siraj, M. M., Othman, S. H., & Musa, M. A. (2020). A Study on Cybersecurity Awareness Among Students in Yobe State University, Nigeria: A Quantitative Approach. International Journal on Emerging Technologies, 11(5), 41–49.
21. Garba, Adamu Abdullahi, Jeribi, F., Al-shourbaji, I., Alhameed, M., Reegu, F., & Alim, S. (2021). An Approach To Weigh Cybersecurity Awareness Questions In Academic Institutions Based On Principle Component Analysis : A Case Study Of Saudi Arabia. 04, 319–326.
22. Gercke, M. (2012). Understanding cybercrime: Phenomena, challenges and legal response purpose. Geneva: International Communication Union.
23. Ibrahim, S. (2016). Causes of socioeconomic cybercrime in Nigeria. 2016 IEEE International Conference on Cybercrime and Computer Forensic, ICCCF 2016. https://doi.org/10.1109/ICCCF.2016.7740439
24. Khalid, F., Daud, Y., Jasmy, M., Rahman, A., Khalid, M., & Nasir, M. (2018). An Investigation of University Students' Awareness on Cyber Security. International Journal of Engineering & Technology, 7, 11–14.
25. Kim, E. B. (2014). Recommendations for information security awareness training for college students. Information Management and Computer Security, 22(1), 115–126. https://doi.org/10.1108/IMCS-01-2013-0005
26. Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: Management's effect on culture and policy. Information Management and Computer Security, 14(1), 24–36. https://doi.org/10.1108/09685220610648355

27. Kruger, H., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. Information Management & Computer Security, 18(5), 316–327. https://doi.org/10.1108/09685221011095236
28. Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., & Ignatuschtschenko, E. (2013). Comprehensive study on cybercrime. In United Nations Office on Drugs and Crime, Tech. Rep.
29. Masoodi, F., Alam, S., & U Bokhari, M. (2011). SOBER Family of Stream Ciphers: A Review. International Journal of Computer Applications, 23(1), 1–5. https://doi.org/10.5120/2857-3672
30. McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. Journal of Internet Commerce, 9(1), 23–41. https://doi.org/10.1080/15332861.2010.487415
31. Monrad, J. (2019). Universities fall into the cross hairs of cyber attacks.
32. Monsurat, I. (2020). African insurance (spiritualism) and the success rate of cybercriminals in Nigeria: A study of the yahoo boys in Ilorin, Nigeria. International Journal of Cyber Criminology, 14(1), 300–315. https://doi.org/10.5281/zenodo.3755848
33. Nzeakor, O. F., Nwokeoma, B. N., & Ezeh, P. J. (2020). Pattern of cybercrime awareness in Imo state, Nigeria: An empirical assessment. International Journal of Cyber Criminology, 14(1), 283–299. https://doi.org/10.5281/zenodo.3753223
34. Reegu, F. A., Mohd, S., Hakami, Z., Reegu, K. K., & Alam, S. (2021). Towards Trustworthiness of Electronic Health Record system using Blockchain. Annals of the Romanian Society for Cell Biology, 25(6), 2425–2434.
35. Reegu, F., Khan, W. Z., Daud, S. M., Arshad, Q., & Armi, N. (2020). A Reliable Public Safety Framework for Industrial Internet of Things (IIoT). 2020 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET), 189–193. https://doi.org/10.1109/ICRAMET51080.2020.9298690
36. Serianu. (2017). Demystifying Africa's Cyber Security Poverty Line.
37. Sesan Gbenga, B. Soremi, B. O. (2015). Economic Cost of Cybercrime in Nigeria.
38. Shuaib, M., Alam, S., Daud, S., & Ahmad, S. (2021). Blockchain-Based Initiatives in Social Security Sector. EAI 2nd International Conference on ICT for Digital, Smart, and Sustainable Development (ICIDSSD), 8. https://doi.org/10.4108/eai.27-2-2020.2303256
39. Siddiqui, S. T., Alam, S., Ahmad, R., & Shuaib, M. (2020). Security threats, attacks, and possible countermeasures in internet of things. In Lecture Notes in Networks and Systems (Vol. 94, pp. 35–46). https://doi.org/10.1007/978-981-15-0694-9_5
40. Siegel, L. (2010). Criminology: Theories, patterns, and typologies (Nelson Education (ed.); 10th ed.). Wadsworth Gengage learning.
41. Slusky, L., & Partow-Navid, P. (2012). Students Information Security Practices and Awareness. Journal of Information Privacy and Security, 8(4), 3–26. https://doi.org/10.1080/15536548.2012.10845664
42. Son, J., Kim, D., Hussain, R., & Oh, H. (2014). Conditional proxy re-encryption for secure big data group sharing in cloud environment. Proceedings - IEEE INFOCOM, 541–546. https://doi.org/10.1109/INFCOMW.2014.6849289
43. Straub, D. W. (1990). Effective IS security: An empirical study. Information Systems Research, 1(3), 255–276. https://doi.org/10.1287/isre.1.3.255
44. Taha, N., & Dahabiyeh, L. (2020). College students information security awareness: a comparison between smartphones and computers. Education and Information Technologies. https://doi.org/10.1007/s10639-020-10330-0
45. Troia, V. (2018). The Cybersecurity Framework as an Effective Information Security Baseline: A Qualitative Exploration. ProQuest Dissertations and Theses, D.I.T.(August).
46. Van Nguyen, T. (2020). Cybercrime in Vietnam: An analysis based on routine activity theory. International Journal of Cyber Criminology, 14(1), 156–173. https://doi.org/10.5281/zenodo.3747516
47. White, G. B. (2011). The community cyber security maturity model. 2011 IEEE International Conference on Technologies for Homeland Security, HST 2011, 173–178. https://doi.org/10.1109/THS.2011.6107866
48. Yang, Y., Zhou, L., Peng, Z., Using, S., Spread, N., Deng, S., & Huang, H. (2017). A Survey on Cyber Security awareness among college students in Tamil Nadu A Survey on Cyber Security awareness among college students in Tamil Nadu. https://doi.org/10.1088/1757-899X/263/4/042043