International Journal on Emerging Technologies **11**(5): 41-49(2020)

ISSN No. (Print): 0975-8364
ISSN No. (Online): 2249-3255

A Study on Cybersecurity Awareness Among Students in Yobe State University, Nigeria: A Quantitative Approach

Adamu A. Garba[1], Maheyzah Md. Siraj[2], Siti Hajar Othman[2] and M.A. Musa[3]
[1]Faculty of Engineering, School of Computing, Universiti Teknologi Malaysia, Skudai, Johor Bahru, 81310, Malaysia.
[2]Senior Lecturer, Faculty of Engineering, School of Computing, Universiti Teknologi Malaysia, Skudai, Johor Bahru, 81310, Malaysia.
[3]Senior Lecturer, Faculty of Science, Department of Computer Science, Yobe State University, Damaturu, Nigeria.

(Corresponding author: Adamu A. Garba)
(Received 03 June 2020, Revised 06 July 2020, Accepted 18 July 2020)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: The emergence of the internet and also the use of various online applications and the exposure to the social platforms that are evolving day by day have positioned students to online risk. Online fraud, cyber-bully, phishing are among those risks students are exposed to in their daily activities. To find a solution to that, cybersecurity awareness can prepare them to protect themself against such risk. This research aims to investigate the students' awareness of basic knowledge of cybersecurity. A quantitative approach was used for data collection using a set of designed questionnaires, this method was used to investigate the students' cybersecurity knowledge and observe their behavior toward using the internet, from the survey a total of 201 Computer Science students in the Department of Computer Science at Yobe State University, Nigeria participated in the study. The research has encountered moderate responses from the students as all universities are close at this period due to the COVID 19 pandemic, only students living in urban were able to reach out in the study. The result obtained from the experiment were analyzed and it shows the University students' cybersecurity awareness is at a satisfactory level and more than average of the students are not well aware of how to protect their data. The research contribution is, there is no active cybersecurity awareness program in place, and also females' students are more likely to be the victim of cyber-attack. Besides that, the survey alsoindicated a high enthusiasm for students to learn more about cybersecurity.

Keywords: Cybersecurity, Awareness program, Information Security, Authentication, organizational Security, Cyber risk, university education, Yobe State University.

I. INTRODUCTION

Cybersecurity threats have become a major setback to many organizations and individuals as well as most activities are now successfully carried out online with less physical contact. Therefore, the existence of the internet had significantly changed the way people learn, get information, and also construct knowledge[1-2]. This new method of doing things has provided a new method through which people communicate and also engage in societal activities [2]. The birth of the internet was widely considered as one of the most valuable ever created innovations that are used globally, with all these advantages, it also comes with negative side as the result of using it wrongly by the users[3]. The use of the internet has come with many cyber-related risks, these risks include cyber addiction[4], personal information exposure[5], personal information exposure [6], and online fraud addiction [7-8].

Many organizations constantly receive numerous attacks as a result of allowing access to their internal network. A study was conducted by Serianu company and revealed almost $649million was lost by banking and telecoms companies, this report also shows that $3.5 billion was lost in Africa and Nigeria is among the most affected country. This shows that many organizations lack a cybersecurity awareness program. Nigeria is having about 181million population and 60% are youth with 92,699,924 Internet users. According to [9] stated that 97% of organizations in Africa spend less than $10,000 in cyber-Security, Nigeria being the highest. Also 64% lack cyber-Security training of their employees, 83% lack cyber-security management in their organization, and lastly, 97% lack skills to comeback cyber-attacks, sadly Nigeria has the highest in all. This indicated there is a lack of cybersecurity awareness across the country.

In higher institution students are active internet users, many depend on it for information and social media too [10]. Using the internet for a long time can put students into a vulnerable condition by exposing them to online risks and threats. This research aims to investigate the students at the Computer Science Department in Yobe State University to identify their knowledge and awareness of cybersecurity. The objective of this paper to include the following:

– To investigate the cybersecurity basic knowledge among male and female students of the computer science department at Yobe State University Damaturu Nigeria.
– To identify which gender is more likely to be avictim of a cybersecurity attack.
– To identify the desire to learn more about cybersecurity.

There is insignificant amount previous study being conducted to identify the cybersecurity awareness of students at the university level specifically to Nigeria context, however, countries like USA, Malaysia, India UK, and New Zealand have conducted a similar study but only peculiar to their region as they are more advance in information technology and innovations. This research advantage would serve as the first stepping stone for other researches to build on when it comes to cybersecurity awareness in the education section in Nigeria. Therefore, the research gap here is the lack of cybersecurity awareness programs to students at the university level for identifying their awareness level in Nigeria. This paper is divided into sections, the next section will be literature review as section 2, section 3 will be the methodology, section 4 will be results and discussion and section 5 will be the conclusion of the paper.

II. LITERATURE REVIEW

The advance on the internet technology has made organizational activities easier than its use to be, clients, stakeholders, and managers can communicate anytime and also anywhere, this technology has also brought a negative impact to some organization where they receive cyber threats frequently. Cybersecurity awareness and training can make people be aware of the danger of cyberattacks and can minimize the impact. However, most criminals use a different channel of attacking, the most commonly used are: phishing email, network traffic, user profiling in launching an attack [11], this attacks are mostly focused on the most vulnerable or fewer inexperienced people. According to [12] they reported that 4.9% of students had experienced cyberstalking. Cybersecurity awareness can be applied to help minimize some basic attacks to individuals, it also indicated that students are more vulnerable to cyber-attacks.The use of online sources for the intention of learning by students and educators helps extend their learning capabilities but also poses threats [13]. Therefore knowing what to access and how to access it is important to all. Also [14] suggested that there is a strong relationship between preventive measures and information security which help toincrease individual security performance. While [15] advised that the knowledge and behavior of an individual has a strong relationship when it comes to cybersecurity threat mitigation. Therefore, individuals must have both the knowledge and also good behavior before cybersecurity can be achieved. Elements such as security policies must be included when designing a cybersecurity program to enable any organization to achieve its desired outcome[16]. Researchers have developed many cybersecurity programs to tackle this issues, [17] surveyed students of the business department at new England to determine their attitude toward information security awareness, which will help assist in designing an effective awareness training program, the survey result indicated the need of the program as it increases their knowledge toward cybersecurity. Another study was carried out by [18] to study the security awareness of academic from the Arab continent, this survey was conducted to students and professionals, the results show less insight on how it was conducted and also didn't show how it manages to reduce cyberattacks, however, it shows the need of continues cybersecurity awareness program.

Cybercriminals target universities, therefore when creating an organization security management plan cybersecurity programs must be included. Another researcher has design simulation tools to provide or enhance the cybersecurity level of students, staff, and other personnel [19]. The result shows simulation tools has a significant impact on increasing cybersecurity awareness level. furthermore, another researcher utilizes Games as students are addicted to online Games, Games like CyberCIEGE were designed to enhance cybersecurity knowledge for the Navy IT training in the US and the preliminary results show the tools can be an effective means of improving the cybersecurity knowledge[20]. This research indicated that software design for this purpose can be used to improve students' cybersecurity knowledge.

A survey was also conducted at California State University by [21] and it found out the main problem is not the lack of basic knowledge but the method students use it in real life, it also shows compliance with information security knowledge is lower than understanding it. Likewise, students from Tamil Nadu India were surveyed to identify how aware are they on various security threat, the result indicated a total number of 500 students participated in the survey, 70% are aware of basic virus attacks and they are using anti-virus, and 11% uses outdated anti-virus, also more than 97% uses free available antivirus online [22]. These results show students use software that is not original and this can lead to malware intrusion to their system. In Malaysia also [23] conducted a study to understand how students are aware of the risk related to a social networking site, a total number of 295 participated in the study, and the result indicated that one-third had been victims of social networking sites scam. This indicated that students are less aware of the risk of cyber threats. Also in the US, some college students at Pacific Northwest were surveyed to see how cyber aware are they, the result indicated students were not able to define malware, trojan horse, phishing, and worms [24]. However, in Bangladesh cybersecurity research was conducted by [25], the survey indicated there is an inconsistency in the level of cybersecurity awareness and the result is at a satisfactory level.

Similarly from New Zealand, a cybersecurity awareness survey was conducted on the use of the internet among students of various ages, the final results show that the students are not familiar with the term phishing and other cybersecurity terms, and this revealed lack of knowledge in cybersecurity [26]. The majority of university students are more vulnerable to cyber attacks, this shows they lack security concern on using the internet, at the same time they lack the knowledge of security threats and the methods necessary to avoid it [27]. Many researchers have a focus on how to design cybersecurity awareness programs to raise the knowledge of cybersecurity as explained above, while other researchers have been engaged in how effective the cybersecurity program islike [28-32].

Cybersecurity has become a necessity for all to learn the basic tricks on how to protect their personal information.In this research paper,Computer Science student at Yobe State University are the target of the

survey, this is important to the researcher to know the level of cybersecurity awareness as they are the potential employees in the futures in the areas of computer science and other IT industries in Nigeria.

III. METHODOLOGY

This research adopted and uses a quantitative approach to prepare the questionnaire as a means of data collection. The medium of the collection is online-based due to the current situation of the COVID 19 pandemic. The questionnaire was organized in such a way to identify the level of cybersecurity knowledge of computer science students at Yobe State University. The students were selected as they are future employees in organizations. The questions were developed to achieve the above objectives. The questionnaire consists of 19 questions using a close-ended approach. Other questions were demography questions. The questionnaire estimated time to be completed is 10 to 15 minutes. The questions were grouped into themes for easier identification, those themes are *cybersecurity* knowledge, privacy*, trust, password management, desire to learn cybersecurity* and acceptance of awareness program. These questions were adopted and customize to fit the study group based on the studies carried out by [13, 11]. Fig 1 shows how the survey was designed.

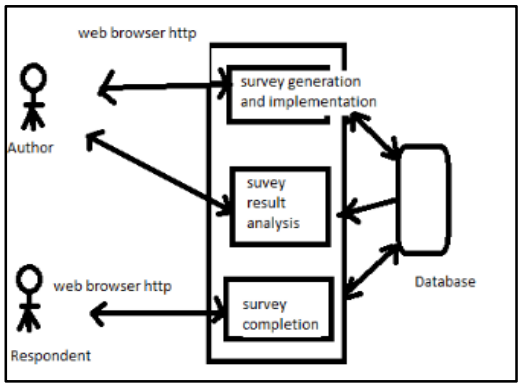


Fig. 1. Research Survey Design [33].

IV. RESULTS AND DISCUSSION

The link of the survey was created using Google docs and was distributed via emails and WhatsApp groups for students to get access to it. The survey took two months before it was disabled, a total of 201 valid responders were able to fill the survey without missing data, other responders have missed or left some questions blank so it was filtered and deleted. Therefore, the total number of 201 was used for this analysis. This sample is sufficient for the analysis as described by Morgan and Krejcie [34] in their paper where a total of 201 is enough for 420 numbers of N= is population size. This survey only focuses on computer science students at Yobe State University.

A. Demography

The survey distributed to the participants consist of demography data, these data include Age and gender, the participants were divided into three age groups, from 18 -20 are group A, from 21- 25 age are group B and 26- 30 age are group C. Fig. 2 and 3 describe the respondent.

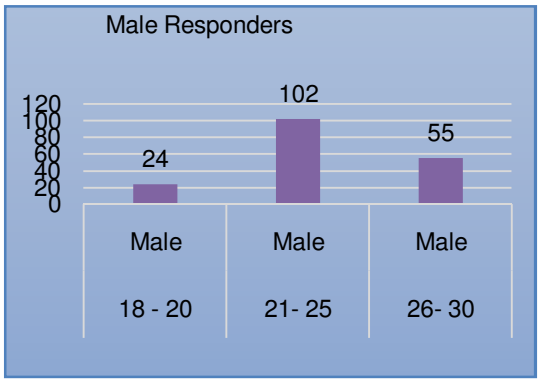


Fig. 2. Male Responders.

Fig. 2 shows group A male responders are 24, group B is 102, and group C is 55 respectively out of the total number of 201 participants, the remaining choose to be anonymous. This result indicated that the majority of the responders are between the age of 21 to 25, therefore the survey would indicate those that have more or less knowledge on cybersecurity. These results also show that more awareness is needed across all groups.

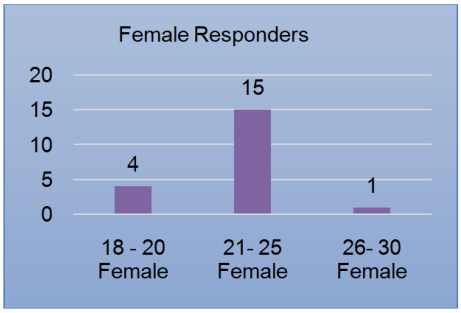


Fig. 3. Female Responders.

Fig. 3 shows group A female responders are 4, group B is 15, and group C is 1, out of 201 responders, while others selected maybe option. This result portrayed again group B of age between 21 to 25 are the majority.

B. Gender Proportion

The survey was conducted and both males and females have participated in the study, figure 4 shows the number of participants based on gender-wise.

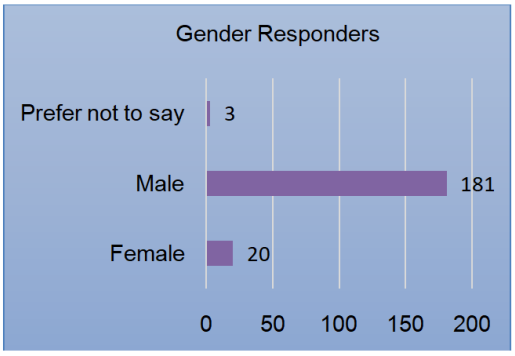


Fig. 4. Respond to Gender Proportion.

The above Fig. 4 indicated that a total of 181 males and 20 females and others who chooses not to say have participated in this survey. Fig. 4 also indicated that males are more into learning or responding to cybersecurity awareness surveys than females students, from this we can boldly forecast that female student are likely to be victims of basic cyber attacks.

C. Cybersecurity Knowledge

The cybersecurity question was asked to know the current level of awareness of the students and the figure below shows the response. The question is "*do you consider your self knowledgeable about cybersecurity*".

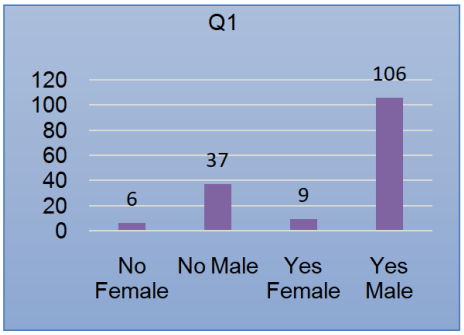


Fig. 5. Respond to Cybersecurity Knowledge.

Fig. 5 indicated that a total number of 106 and 37 male and female responders agree while 9 and 6 responders disagree out of the 201 total participants. from Fig. 4 it indicated that majority of males have some basic idea on what cybersecurity is, while only a few females are aware too, this might be true or not as the number of female participants is low compared to that of males, its can change or not depending on the size of the sample, however from this sample that we have, its shows males have better knowledge than the females. Q2 is "*When using the computer system and the Internet, what do you feel secure*" Fig. 6 shows the results.

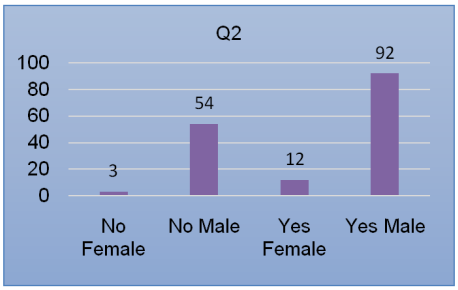


Fig. 6. Respond to feeling sure when using the internet.

The above figure 6 shows 192 and 12 male and female responders feel secure while using the internet while a total of 92 and 3 male and female responders disagree out of 201 total participants. This result indicated that both the participants feel sure when using the internet, however, the percentage of those that do not feel sure is almost to more than half of those that agreed, this indicated that awareness is needed to educate the students on how to sure their internet connection. Q3 is*"Do you know what Two-Factor Authentication (2FA) is and do you use it?*". A total of 77 males and 9 females said "Yes", while 86 males and 10 females Said "No" regarding the understanding of Authentication. This results, without doubt, shows that the majority of both the participants lack the basic knowledge of Two-Factor authentication as is widely applicable to many applications now, this poses the need for awareness programs. The applications that use this method of authentications are many, the popular ones are, Facebook, WhatsApp, gmails, yahoo, twitter, and others as well. This method is highly recommended by many security experts to be used when working on the internet. Q4 is "*When you receive an email from an unfamiliar sender, do you open it?"* figure 7 shows the results.

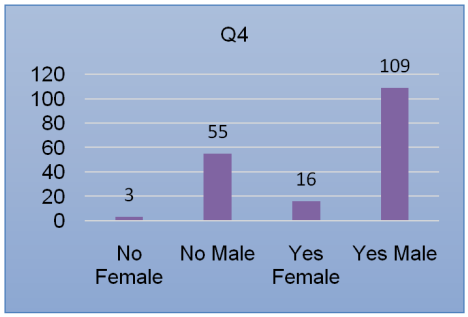


Fig. 7. Respond to email opening?

Fig. 7 indicated that 109 males and 16 females would open an unfamiliar email sent to then while 55 and 3 both responders selected "No" out of the total of 201 participants. This question indicated that both responders are not aware of the concept of phishing emails, therefore urgent cybersecurity awareness program is needed to tackle this problem.Q5 is about "*When you receive an email requiring your credential information such as name, date of birth, age, your credit card number? Do you send it*?. The results show 143 males said " No" and 17 females while 23 males said "Yes" and only 1 female on whether they can reveal their personal information to an unknown person. This question revealed the students at least have satisfactory knowledge of privacy, but more awareness is required. Q6 *is "Do you ever reject app permission*". The results show 61 males selected"No" and 11 females while both 114 participants selected "Yes" on rejecting app permission. We all know that majority of the free application comes with malware embedded in it, as such, they ask for accessing personal information before a user can download it, this question shows that the students occasionally reject this app permission to access their data. Q7 is *"Do you know what is the difference between using HTTP and HTTPS" ?* The results show 109 males and 11 females said "Yes" while 64 males and 8 females said "No"on their knowledge of the difference between HTTP and HTTPS. This question indicated that the majority of responders are aware of the concept of internet protocols. Q8 is *"Do you know, what is the meaning of the concept phishing?*" A total of 131 males and 18 femalesanswered "No" while only 40 males and 2 females are familiar with the concept of phishing.phishing attacks is one of the most widely basic attacks used [11]. Therefore almost all students have an active email account, but from the survey result, it has indicated a lack of basic knowledge of the

concept phishing by both the participants. This poses a greater threat, therefore cybersecurity is desperately required. Q9 is*"Do you use debit or credit cards at an outdoor payment machine?"* the results show 104 males and 10 females agree while 66 males and 8 females disagree on using credit cards for payments at any machine. These results show that most of the students use their card for payment while the overall responders indicated some have less adequate knowledge on cashless payment. Awareness is required to train the studentson how to use their credit cards via a secure medium. Q10 is"*Do you shop/purchase items advertised on social networks or your private email?*" this question shows a total of 81 males and 8 females said "Yes" and another 88 males and 11 females said "No" on whether they buy items shows on their social account. From the above questions we can say that half of the students use an online platform for shopping while another half do not, this indicated that they prefer the traditional method in purchasing items, therefore, more awareness is needed to gain their trust in using such platforms. Q11 is "*Do you think that it is important to read the user agreements for free program/software before clicking,accept*"? the result from this question show 144 males and 20 females agree while only 26 males disagree, this result indicated that the students read the terms before accepting, it shows some basic knowledge of cybersecurity. *(Refer Appendix A for further results***)**

D. Privacy Knowledge

This section question was to determine how the participants perceived privacy and whether they have the basic knowledge of privacy. Fig. 8 shows the result of one of the questions as the question is Q12 "*Do you think that your data on the university system is secure?*"

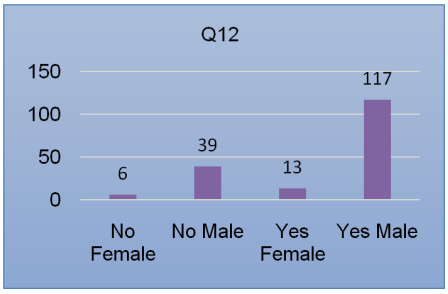


Fig. 8. Respond to Privacy.

Fig. 8 shows a total number of 177 males and 13 responders selected "Yes" while 39 males and 6 females selected "No" on feeling sure when using their university system as shown in Fig. 7. This result shows that both participants feel their data is secure in the university system. Furthermore, Q13 is " *Have you ever rejected a mobile app request for accessing your contacts, camera or location?"* Fig. 9 shows the result.

The above figure indicated that a total of 97 males and 6 females said "Yes" while 76 males and 12 females said "No" on how they feel on the app requesting access to the location. The result shows that 50% of the students allow the app to access their location, this indicated a great threat to privacy, therefore a cybersecurity awareness is required to educate students when and how to allow access to location when requested by an application.

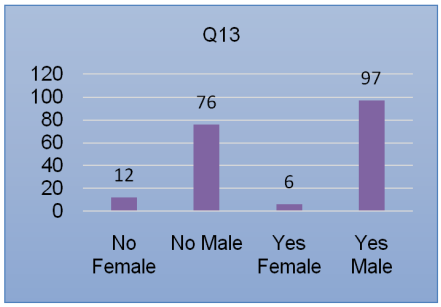


Fig. 9. Respond to Location Access.

E. Trust Knowledge

This section was intended to determine the "trust" knowledge of using the internet and system connected online. Q14 is "*Do you have reason to believe that you are being observed online without your consent?"* figure 10 shows the results.

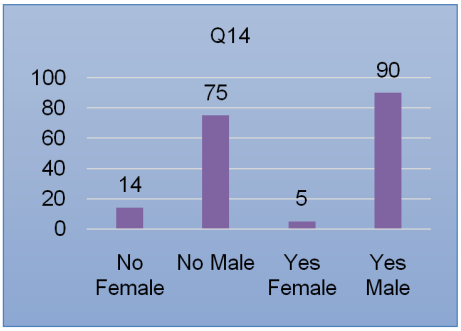


Fig. 10. Respond to Trust.

Fig. 10 shows that a total of 90 males and 5 females said "Yes" and 75 males and 14 females Said "No" on the question of whether the participant on them being observed online. This result shows that more than 50% of the participants feel that they are being monitored online, this will result to trust issues among the students using the internet.

F. Password Management

This section shows how the participants are knowledgeable about password management. Two questions were asked, Q15 is "*Do you use a harder-to-guess password to access your bank account than to access your social networking accounts*?" Fig. 11 shows the result.

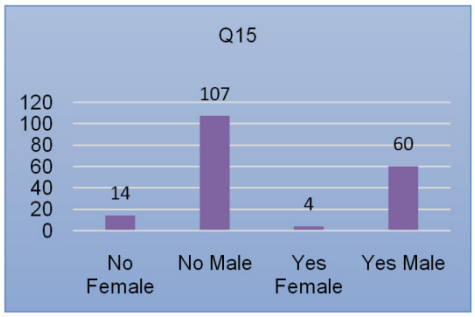


Fig. 11. Respond to Password Management.

Fig. 11 shows 107 males and 14 females selected "Yes" and 60 males and 4 females Selected "No" on whether participants use a strong password or not. The result shows that both responders use an easy-guess password in their accounts, its also indicated that a small brute-force attack can crack their account, therefore awareness is needed to explain the danger of using a simple password and also how to creat hard-guess password.Q16 is "*Do you use the same passwords for both social networks such as Facebook, Twitter, iTunes, and your email accounts?*" the result shows a total of 86 males and 8 females said "Yes" while again 86 males and 11 females said "No" on using the same password on the social network. This result indicated that 50% of the responders use the same password across multiple social platforms, however, the same number answered No, this shows that some use the same while others do not. This indicates that awareness is needed to explain the danger of using the same password across different social sites.

G. Cybersecurity as a Course

This section explains whether the participants are ok if the cybersecurity course is to be added as their curriculum to learn more about cybersecurity or not.program as a core course for all students is important. Q17 is*" Do you think to add a Cybersecurity awareness he University curriculum*". Fig. 12 shows the results.

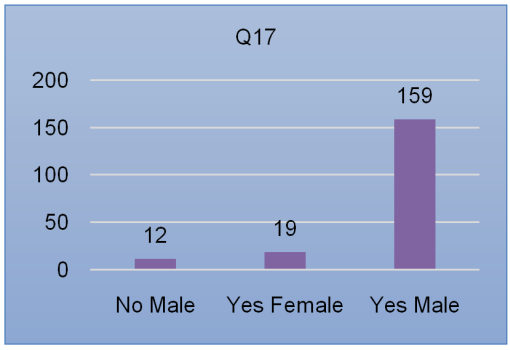


Fig. 12. Respond to Adding Cybersecurity as Course.

Fig. 12 shows a total of 159 males and 19 females answered "Yes" while only 12 males said "No" on the desire to learn more on cybersecurity and also as to make it a curriculum as a course in the university system. This result indicates the enthusiasm and desire to learn more about cybersecurity, more than 95% of the responders have agreed to add cybersecurity as a course, in this result it shows female participants still have less desire to learn cybersecurity Q18 is *"In your opinion, is it important that academic institutions should have an information security officer?*" Fig. 13 shows the results.

The above figure indicated that a total number of 152 males and 19 females said "Yes" while only 14 males and a single female said "No" on having an information security officer at the University. The result also indicated that students agreed on having an information security officer at the university, it shows that if there is any security issues student can go and complain there.

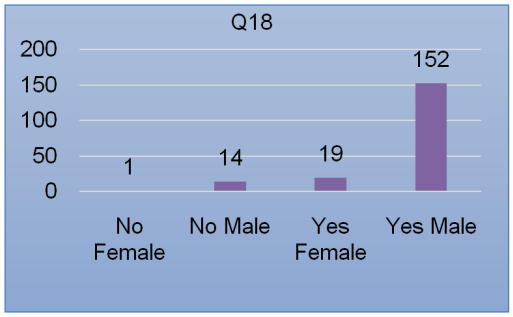


Fig. 13. Respond on Having Information Security Officer.

H. Desire To Learn Cybersecurity

This section explains whether participants have the desire to learn more on cybersecurity, Q19 is *"Do you desire to learn more about Cybersecurity?* Fig. 14 shows the results.

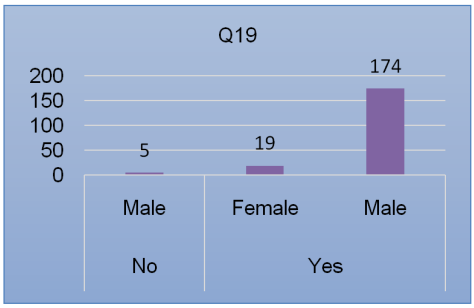


Fig. 14. Respond to Desire to Learn Cybersecurity.

Fig. 14 shows almost 95% of the responders are of the desire to learn more about cybersecurity, a total number of 174 males and 19 females agree (select 'Yes') and only another 5 males disagree (select No'), this is a clear indication how important is to conduct the cybersecurity awareness program at the university. The objectives of this paper further explain below. Objective 1 of the research is to investigate the cybersecurity basic knowledge among male and female students of the computer science department at Yobe State University Damaturu Nigeria. From the above analysis, we can conclude that males students have participated more than female students, and among those that participated males students seem to outsmart the female students to the basic knowledge of cybersecurity. This survey clearly shows that less basic knowledge of cybersecurity, even thousecurity starts with an awareness [35]. Therefore when cybersecurity awareness programs are conducted, the level of awareness would increase. Many authors like [36] suggested that the lack of awareness depicts a serious problem in any organization and it is important for an organization to properly address the issue by conducting cybersecurity awareness programs.while Objective 2 was to identify which gender is more likely to cybersecurity threats, from Objective 1, it is indicated that female students are more likely to be the victim of cyber attack as the results show a lack of basic knowledge on cybersecurity. The last objective was To identify the desire to learn more about cybersecurity, the results show more than 95% of the responders have the

desire to learn more on cybersecurity. This desire to learn more should not limit to only cybersecurity, but rather policies should come from the top management of the academic which would serve as guidanceas suggested both by [37-38]. In addition to this, the policies should be made available to the students, so that they can control their activities and behaviors when using the internet, as awareness improves protective behavior toward the use of computers [39]. This concluded that cybersecurity is highly recommendable to the students in Computer Science Department and also to encourage more females to participate in the program as the results show they are more vulnerable than the males' students, since the situation is known, to minimize the effect of ant breach, cybersecurity awareness through educating, workshop, seminars and other methods within the university is highly encourage as suggested both by [40, 16].

V. CONCLUSION

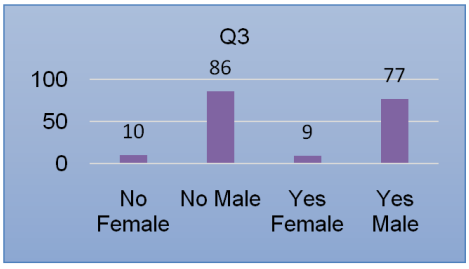
Cybersecurity awareness is essential at all level, but more important to Computer Science Students since most of them will work in IT organizations, therefore, some basic cybersecurity knowledge is needed, not only them but also other students from the various departments as well as organizations that use the internet at their workplaces. The result of this study indicated that even though these student s show a high level of awareness in certain questions like in privacy and trust they are lacking basic knowledge on the aspect of password management, phishing, and Two-Factor Authentication. This research also shows there is no active program for rising cybersecurity knowledge among the students. The National Information Technology Development Agency is the only active agency that focuses on spreading awareness on cybersecurity, this might not be enough for a country of about 181million, population. However, to spread awareness across all levels of communities and organizations more involvement is required from various role players like government and private entities.

VI. FUTURE SCOPE

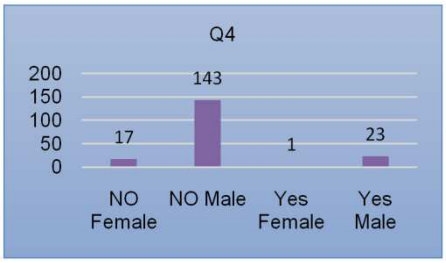
The future scope of this research is to design cybersecurity programs and also implement it to see if the knowledge of cybersecurity would increase especially for the females' participants as the results show they are more vulnerable to cyber-attacks than the males.

Conflict of Interest. This survey research work is mine and there is no conflict of interest.

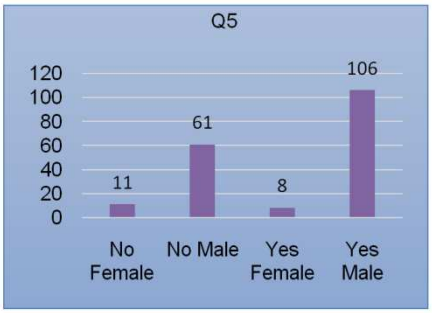
APPENDIX



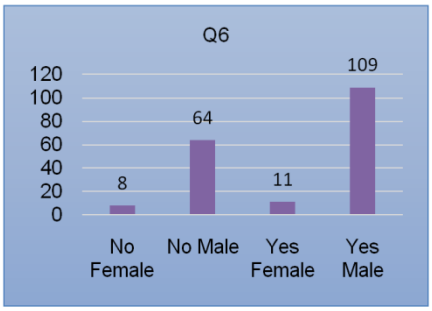
A1.



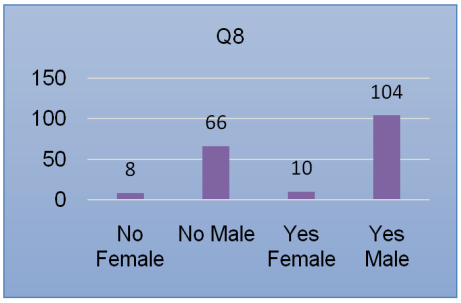
A2.



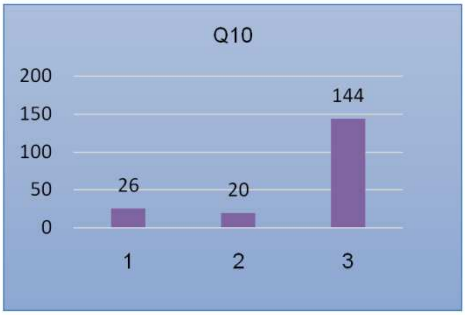
A3.



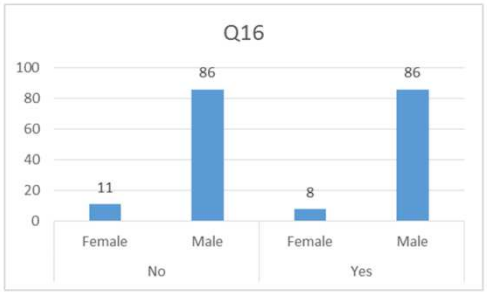
A4.



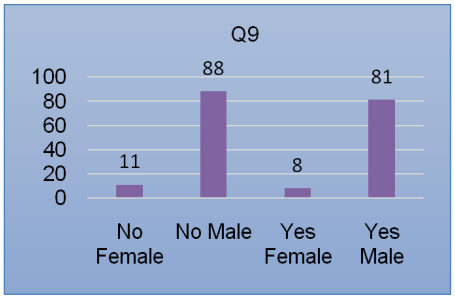
A5.



A6.



A7.



A8.

REFERENCES

[1]. Khalid, F. (2017). Understanding University Students' Use of Facebook for Collaborative Learning. *International Journal of Information and Education Technology, 7*(8), 595–600. https://doi.org/10.18178/ijiet.2017.7.8.938

[2]. Khalid, F., Daud, Y., & Mohamad Nasir, M. N. (2016). "Cross-Cultural Education for Sustainable Regional Development " Bandung perbandingan penggunaan telefon pintar untuk tujuan umum dan pembelajaran dalam kalangan pelajar universiti. *International Conference on Education and Regional Development*.

[3]. Karim, A. A., Shah, P. M., Khalid, F., Ahmad, M., & Din, R. (2015). The Role of Personal Learning Orientations and Goals in Students' Application of Information Skills in Malaysia. *Creative Education*, *06*(18), 2002–2012. https://doi.org/10.4236/ce.2015.618205

[4]. Annansingh, F., & Veli, T. (2016). An investigation into risks awareness and e-safety needs of children on the internet: A study of Devon, UK. *Interactive Technology and Smart Education*, *13*(2), 147–165. https://doi.org/10.1108/ITSE-09-2015-0029

[5]. Muniandy, L. & Muniandy, B. (2012). State of Cyber Security and the Factors Governing its Protection in Malaysia. *International Journal of Applied Science and Technology, 2*(4), 106-112.

[6]. Anderson, G., Ktoridou, D., Eteokleous, N., & Zahariadou, A. (2012). Exploring parents' and children's awareness on internet threats in relation to internet safety. *Campus-Wide Information Systems*, *29*(3), 133–143. https://doi.org/10.1108/10650741211243157

[7]. Mosalanejad, L., Dehghani, A., & Abdolahifard, K. (2014). The students' experiences of ethics in online systems: A phenomenological study. *Turkish Online Journal of Distance Education*, *15*(4), 205–216. https://doi.org/10.17718/tojde.02251

[8]. Ratten, V. (2015). A cross-cultural comparison of online behavioural advertising knowledge, online privacy concerns and social networking using the technology acceptance model and social cognitive theory. *Journal of Science and Technology Policy Management*, *6*(1), 25–36. https://doi.org/10.1108/JSTPM-06-2014-0029

[9]. Adeyemi. (2019). Nigeria: Financial Losses to Cybercrimes. Retrieved from https://allafrica.com/stories/201806070110.html

[10]. Daud, Y., & Khalid, F. (2014). *Nurturing the 21st Century Skills among Undergraduate Students through the Application and Development of Weblog*. *7*(13). https://doi.org/10.5539/ies.v7n13p123

[11]. Moallem, A. (2019). Cybersecurity Awareness Among Students and Faculty. In *Cybersecurity Awareness Among Students and Faculty* (Vol. 2). https://doi.org/10.1201/9780429031908

[12]. Reyns, B. W., Henson, B., & Fisher, B. S. (2012). Stalking in the Twilight Zone: Extent of Cyberstalking Victimization and Offending Among College Students. *Deviant Behavior*, *33*(1), 1–25. https://doi.org/10.1080/01639625.2010.538364

[13]. 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

[14]. 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

[15]. 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

[16]. McDaniel,A. E. (2013). Securing the Information and Communications Technology Global Supply Chain from Exploitation: Developing a Strategy for Education, Training, and Awareness. *Issues in Informing Science and Information Technology*, *10*(2012), 313–324. https://doi.org/10.28945/1813

[17]. 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

[18]. 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

[19]. Pastor, V., Díaz, G., & Castro, M. (2010). State-of-the-art simulation systems for information security education, training and awareness. *2010 IEEE Education Engineering Conference, EDUCON 2010*, 1907–1916. https://doi.org/10.1109/EDUCON.2010.5492435

[20]. Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers and Security*, *26*(1), 63–72.

[21]. 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

[22]. 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
[23]. Kirwan, G. H., Fullwood, C., & Rooney, B. (2017). Risk Factors for Social Networking Site Scam Victimization Among Malaysian Students, 1–6. https://doi.org/10.1089/cyber.2016.0714
[24]. Sarathchandra, D., Haltinner, K., & Lichtenberg, N. (2016). College Students' Cybersecurity Risk Perceptions, Awareness, and Practices. *Proceedings - 2016 Cybersecurity Symposium, CYBERSEC 2016*, 68–73. https://doi.org/10.1109/CYBERSEC.2016.018
[25]. Ahmed, N., Kulsum, U., Bin Azad, M. I., Momtaz, A. S. Z., Haque, M. E., & Rahman, M. S. (2018). Cybersecurity awareness survey: An analysis from Bangladesh perspective. *5th IEEE Region 10 Humanitarian Technology Conference 2017, R10-HTC 2017*, *2018-Janua*, 788–791. https://doi.org/10.1109/R10-HTC.2017.8289074
[26]. Tirumala, S. S., Sarrafzadeh, A., & Pang, P. (2016). A survey on internet usage and cybersecurity awareness in students. *2016 14th Annual Conference on Privacy, Security and Trust, PST 2016*, 223–228. https://doi.org/10.1109/PST.2016.7906931
[27]. Pramod, D., & Raman, R. (2014). A study on the user perception and awareness of smartphone security. *International Journal of Applied Engineering Research*, *9*(23), 19133–19144.
[28]. Chan, H. (2012). Significance of Information Security Awareness in the Higher Education Sector.*60*(10), 23–31.
[29]. Rahim, N. H. A., Hamid, S., Kiah, L. M., Shamshirband, S., & Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes*, *44*(4), 606–622. https://doi.org/10.1108/K-12-2014-0283
[30]. Rantos, K., Fysarakis, K., & Manifavas, C. (2012). How Effective Is Your Security Awareness Program? An Evaluation Methodology. *Information Security Journal*, *21*(6), 328–345. https://doi.org/10.1080/19393555.2012.747234
[31]. Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating information security awareness: Research and practice gaps. *Information Security Journal*, *17*(5–6), 207–227. https://doi.org/10.1080/19393550802492487
[32]. Willison, R., & Warkentin, M. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS Quarterly*, *37*(1), 1–20. Retrieved from http://www.jstor.org/stable/43825935
[33]. 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
[34]. Januszyk, K., Liu, Q., & Lima, C. D. (2011). Activities of human RRP6 and structure of the human RRP6 catalytic domain. *Rna*, *17*(8), 1566–1577. https://doi.org/10.1261/rna.2763111
[35]. Furnell Steven, N. Clarke. (2012). Power to the People? The Evolving recognition of human aspects of security. Computers and Security, 31, 983–988. https://doi.org/10/1016/j.cose.2012.08.004
[36]. Yeo, A. C., Rahim, M. M., & Miri, L. (2007). Understanding factors affecting success of information security risk assessment: The case of an Australian higher educational institution. PACIS 2007 - 11th Pacific Asia Conference on Information Systems: Managing Diversity in Digital Enterprises.
[37]. Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences, 43*(4), 615–660. https://doi.org/10.1111/j.1540-5915.2012.00361.
[38]. Goo, J., Yim, M. S., & Kim, D. J. (2013). A pathway to successful management of individual intention to security compliance: A role of organizational security climate. Proceedings of the Annual Hawaii International Conference on System Sciences, 2959–2968. https://doi.org/10.1109/HICSS.2013.51.
[39]. Wolf, M., Haworth, D., & Pietron, L. (2011). Measuring An Information Security. *Review of Business Information Systems – Third Quarter 2011, 15*(3), 9–22
[40]. Chan, H. (2012). Significance of Information Security Awareness in the Higher Education Sector, *60*(10), 23–31.

How to cite this article: Garba, A. A., Siraj, M. M., Othman, S. H. and 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.