Society for Multidisciplinary & Advanced Research Techniques (SMART)
Trinity University, Lagos, Nigeria
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Harmarth Global Educational Services
ICT University Foundations USA
IEEE Computer Society Nigeria Chapter

33rd ECOWAS iSTEAMS ETech Multidisciplinary Conference (ECOWAS-ETech)

Cybersecurity Awareness amongst Students in a Public University In Ghana

Ellen Akongwin Abanga
Ghana Institute of Management & Public Administration
GreenHills Accra, Ghana
E-mail: ellen.abaga@st.gimpa.edu.gh

ABSTRACT

Internet-based attacks have become common and are anticipated to become more commonplace as technology becomes more widely available. As a result, cybersecurity has evolved as a critical notion in everyday life. Cybersecurity awareness (CSA) is an important line of defense in the defense of people and systems. The study described in this article sought to analyze the levels of CSA among students a public university in Ghana. A questionnaire was used to assess students' cybersecurity knowledge, self-perception of cybersecurity skills, and cybersecurity attitudes. The responses revealed various misalignments, including instances of "cognitive dissonance" between variables, which exposes the students to cyber-attacks. The findings highlight the necessity for specialized CSA initiatives that address the distinct limitations of specific user communities.

Keywords: Cybersecurity, Cybersecurity Awareness, University, Ghana

Proceedings Citation Format
Ellen Akongwin Abanga (2022): Cybersecurity Awareness amongst Students in a Public University in Ghana. Proceedings of the 33rd ECOWAS iSTEAMS Emerging Technologies, Scientific, Business, Social Innovations & Cyber Space Ecosystem Multidisciplinary Conference. University of Ghana/Academic City University College, Ghana. 29th Sept – 1st Oct, 2022. Pp 142-148. www.isteams.net/ghanabespoke2022. dx.doi.org/10.22624/AIMS-/ECOWASETECH2022P29

1. INTRODUCTION

This study seeks to understand cybersecurity awareness amongst students in a public university in Ghana. Cybersecurity a suite of security ideas, regulations, tools, security mechanisms, guidelines, laws, risk management techniques, training, activities, best practices, assurance, education and technology that may be used to secure the cyber environment, as well as the assets of organizations and computer users (Craigen et al., 2014). Information and computer literacy is described as an individual's capacity to use computers to study, create, and communicate in order to engage effectively and safely at home, school, the workplace, and society (Törley, 2020).

The capacity to share information is defined as a person's ability to use email, wikis, blogs, instant messaging, sharing media, and social networking websites. Internet-based communication platforms offer several opportunities for users to share information. This facility carries the risk of misuse, particularly when dealing with sensitive information on the internet/cyberspace (Törley, 2020.).

Advancements in information and communications technology (ICT) and societal transformation have fundamentally altered how people think, work, and live (Ghavifekr et al., 2013). Schools and other institutions of education that are responsible for preparing pupils to live in a "knowledge society" must consider incorporating ICT into their curricula (Ghavifekr & Rosdy, 2015). As a result, a variety of technology solutions are being used in the educational sector, and students are becoming more vulnerable to these innovations as they enroll into institutions of higher learning (O'Connor & Domingo, 2017). Students in Universities are exposed to a variety of technological dangers and vulnerabilities as a result of ICT use. Students must be aware of various information security dangers and attacks, as well as how to use technology securely without jeopardizing themselves or the University. People (the human factor) are the most common source of information technology (IT) security issues, according to security professionals (O'Connor & Domingo, 2017).

According to statistics, a huge percentage of students enrolling in higher education nowadays are mainly digital literates, having been raised interacting with technology in many aspects of their lives (Cerretani et al., 2016). The Commission for University Education (CUE) in Kenya, for example, expects universities to develop, deploy, and sustain IT services that enable their fundamental functions (Paniagua, 2019). This rising use of IT in the academic setting brings with it a slew of new dangers. There is a need to promote cybersecurity awareness (CSA) within various academic groups has never been urgent. Ransomware attacks are the largest danger to colleges (Hansch & Benenson, 2014). According to Hänsch and Benenson (2014) the average cost of a ransomware assault in 2020 will be $447,000, or over 3,7 million. Not only have ransomware attacks against Universities and educational institutions gotten more costly and frequent, but the attack surface at Universities has also grown as a result of the Covid-19 outbreak and the use of digital learning tools. Following ransomware, data breaches and data theft by foreign countries are the second and third most common threats, respectively (Hansch & Benenson, 2014).

Many studies globally have illustrated breakthroughs and shortfalls in CSA inside academic circles (AlTameemy, 2017). Lack of diverse studies focusing on students in universities in developing countries, particularly Africa in literature on cybersecurity awareness makes this study highly relevant. Some efforts to narrow this divide focus specifically on students enrolling in higher education institutions (Rezgui & Marks, 2008). Additionally, the literature search around cybersecurity awareness in Ghana that was conducted utilizing databases including E-Journals, Google Scholar, Education Science, Research Gate, Emerald, and Academic Journals produced insufficient results. This clearly demonstrates the need to conduct cybersecurity awareness studies in under-researched nations such as Ghana. Taking all of this into account, the main goal of this study is to contribute to the existing literature on cybersecurity awareness in developing-country higher education institutions.

2. RELATED LITERATURE

Previous research has shown that cybersecurity is critical in mitigating the risks associated with cybersecurity breaches. Line users' inexperience and inadvertent behavior are regarded as the most common causes of cybersecurity breaches (Kenya et al., 2018). As a result, increasing cybersecurity awareness levels among line users reduces the likelihood of them causing in cybersecurity breaches and, as a result, improves the effectiveness of countermeasures that universities implement to protect themselves and their students from cybersecurity-related threats and exploits. It is critical that persons who utilize information technology (IT) resources understand the importance of cybersecurity and related resources (Kenya et al., 2018). Cybersecurity a suite of tools, regulations, security mechanisms, security ideas, guidelines, risk management tools, activities, education, best practices, assurance, and technology that may be used to secure the cyber environment, as well as the assets of organizations and computer users (Craigen et al., 2014).

Cybersecurity awareness a socially defined and an informal construct (Tsohou et al., 2008). As a result, many definitions exist throughout existing literature, resulting in a lack of common understanding of cybersecurity awareness (Tsohou et al., 2008). This has most certainly enhanced the degree to which the notion has been utilized inconsistently. Such discrepancies may make it difficult for researchers to connect various studies on cybersecurity awareness (Kenya et al., 2018). It is important to note that many works on CSA omit to define the word in specific terms (Kenya et al., 2018). The literature has extensively covered the usage of IT in academics. For instance, national developments, expanding supportive laws, and support structures in Africa continue to encourage the use of IT in higher education institutions (Carr, 2013). The use of IT to help teaching and learning is thus still embraced by a number of African higher education institutions. The dangers and vulnerabilities brought on by such use are as widespread in the educational sector as technology itself (Carr, 2013).

Cybersecurity is still receiving attention, with many academics and professionals putting emphasis on the topic (Budzak, 2016). Many studies have stressed how important it is to fix any information security chain's flaws. These flaws are more likely to show up when individuals intentionally or unintentionally interfere with the functioning of the current systems. As a result, cybersecurity awareness is required. However, raising awareness and altering behavior in the area of cybersecurity can be a daunting task given that one must be aware of the reality of the escalating threats and be knowledgeable about the methods for identifying and mitigating a variety of cybersecurity-related threats and attacks (Budzak, 2016). The majority of cybersecurity awareness-related measurements used do not always result in the desired behavioral change (Kenya et al., 2018).

For instance, in Kenya, colleges continue to expand their online course offerings, and the demand for virtual universities continues to guide academic institutions' strategic planning (Kenya et al., 2018). On the other side, the Communication Authority of Kenya's 2010 National ICT Survey found that youth between the ages of 20 and 34 were more likely to utilize and have access to IT equipment and facilities (*Annual-Report-for-the-Financial-Year-2016-2017*, n.d.). Munien (2010) looked into the connection between users' knowledge of the issue and their propensity to become victims social engineering (phishing) that utilizes mails to deceptively request sensitive and personal information from users, such as financial account data or login information. The study came to the conclusion that even while individuals were aware of the significance of phishing, they still fell prey to it.

This was ascribed to improper internet security behavior habits. Using replicated emails to raise user awareness was studied by Chandarman and Niekerk (2017). Their research aimed to examine students' levels of awareness at the United States Military Academy in order to inform their awareness programme. The study discovered that, in addition to assisting people in adjusting their awareness drive, the activity itself boosted awareness.

According to Volkamer et al. (n.d.), students studying in institutions of higher learning are not unaware of smartphone security problems, but they are also not completely aware of all security dangers and essential security procedures. Pretorius and Niekerk (2015) proposed awareness and training campaigns. These studies serve as more examples of how cybersecurity attitudes, understanding, and behavior can be inconsistent. After finding weaknesses in systems caused by users' weak password handling, omitted software updates, and out-of-date or uninstalled anti-virus and malware protection. Kim (2014) observed that a whole lot of students in the America did not take part in it. Another conclusion of the study was that students learned about security in bits and pieces from various sources, and that in order for them to build long-lasting secure behaviors, they needed to take part in more concentrated information security and awareness training. Another example of the mismatch between having enough information and comprehension and excellent security practice.

Users will attempt to bypass safeguards if security procedures are excessively time-consuming or challenging, which may also lessen the impact of earlier and ongoing awareness initiatives. In order to positively influence behaviors and attitudes, influencing techniques must be used in addition to information transmission and awareness (Chandarman & Niekerk, 2017). According to (Peltier, 2005), in order to direct training, it is necessary to have a mark of attitudes , cybersecurity perception levels, competence and knowledge, as well as the linkages among them.

Figure: 2.1. Cybersecurity Awareness
Source: elynx Technologies

Aliyu et al. (2010) identified Malaysia university students identified by to be serious violators of computer security and ethics because they were regularly careless while publishing material and surfing and frequently engaged in unlawful activity by sharing and downloading fake software, TV shows, and movies. The pupils were discovered to not be generally engaging in safe computing due to a number of issues, including lethargy and financial situation (Aliyu et al., 2010). Therefore, the goal of this study is to add to the body of knowledge already available on CSA in African institutions of higher education. We do this by looking into the prevalence of CSA among students at a public university in Ghana.

3. RESEARCH GAP

Many studies globally have illustrated breakthroughs and shortfalls in CSA inside academic circles (AlTameemy, 2017). Lack of diverse studies focusing on students in universities in developing countries, particularly Africa in literature on cybersecurity awareness makes this study highly relevant. Some efforts to narrow this divide focus specifically on students enrolling in higher education institutions (Rezgui & Marks, 2008). Additionally, the literature search around cybersecurity awareness in Ghana that was conducted utilizing databases including E-Journals, Google Scholar, Education Science, Research Gate, Emerald, and Academic Journals produced insufficient results. This clearly demonstrates the need to conduct cybersecurity awareness studies in under-researched nations such as Ghana. Taking all of this into account, the main goal of this study is to contribute to the existing literature on cybersecurity awareness in developing-country higher education institutions.

4. FINDINGS

The link to the survey was issued to students that were readily available on campus as at the time of data collection. Out of the 200 students who completed the questionnaire, a filter was done to see if any questions were left unanswered or blank. Due to not answering any of the provided questions, a total of 17 people were found and eliminated from the results. The analysis will be performed using the 183 samples that have been determined to be genuine.

5. IMPLICATIONS FOR CYBER SAFETY IN AFRICA

From the findings, the implication of Cybersecurity Awareness on Cyber Safety in Africa will mean that more cybersecurity campaigns and trainings should be held by universities and other governmental and non-governmental organizations to help create awareness on Cybercrime and ways to prevent it. This will help reduce the number of cyberattacks in Africa, especially amongst students.

6. CONCLUSION

All internet and computer users in Africa are affected by CSA, hence it is necessary to survey a wide swath of the population to determine the country's knowledge levels. A "generic" CSA survey should be developed to be relevant across population segments, organizations, demographics, and economic groupings in order to establish a baseline for CSA in Ghana. The success of established CSA programmes can be observed over time by conducting bigger longitudinal studies using the baseline data.

To better understand the interactions between these variables within different population segments, more in-depth qualitative approaches in CSA are also required. These studies should look into the underlying causes and motivations for particular users' awareness, personality, actual skills and abilities, and attitudes.

REFERENCES

1. Aliyu, M., Abdallah, N. A. O., Lasisi, N. A., Diyar, D., & Zeki, A. M. (2010). Computer security and ethics awareness among IIUM students: An empirical study. *Proceeding of the 3rd International Conference on Information and Communication Technology for the Moslem World (ICT4M) 2010*, A52–A56. https://doi.org/10.1109/ICT4M.2010.5971884
2. AlTameemy, F. (2017). Mobile Phones for Teaching and Learning. *Journal of Educational Technology Systems*, *45*(3), 436–451. https://doi.org/10.1177/0047239516659754
3. *Annual-Report-for-the-Financial-Year-2016-2017*. (n.d.).
4. Budzak, D. (2016). Information security – The people issue. *Business Information Review*, *33*(2), 85–89. https://doi.org/10.1177/0266382116650792
5. Carr, T. (2013). Higher Education and Teaching Commons, International and Comparative Education Commons, and the Management Information Systems Commons Recommended Citation Recommended Citation Carr. In *The African Journal of Information Systems* (Vol. 5).
6. Cerretani, P. I., Iturrioz, E. B., & Garay, P. B. (2016). Use of information and communications technology, academic performance and psychosocial distress in university students. *Computers in Human Behavior*, *56*, 119–126. https://doi.org/10.1016/j.chb.2015.11.026
7. Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). *Technology Innovation Management Review Defining Cybersecurity*. www.timreview.ca
8. Ghavifekr, S., & Rosdy, W. A. W. (2015). Teaching and learning with technology: Effectiveness of ICT integration in schools. *International Journal of Research in Education and Science (IJRES)*, *1*(2), 175–191. www.ijres.net
9. Ghavifekr, S., Zabidi, A., Razak, A., Faizal, M., Ghani, A., Ran, Y., Meixi, Y., & Tengyue, Z. (2013). ICT Integration In Education: Incorporation for Teaching & Learning Improvement. In *The Malaysian Online Journal of Educational Technology* (Vol. 2, Issue 2). www.mojet.net
10. Hansch, N., & Benenson, Z. (2014). Specifying IT Security Awareness. *2014 25th International Workshop on Database and Expert Systems Applications*, 326–330. https://doi.org/10.1109/DEXA.2014.71
11. Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007
12. Kenya, K., Ndiege, J. R. A., & Okello, G. O. (2018). Information security awareness amongst students joining higher Information security awareness amongst students joining higher academic institutions in developing countries:
13. Evidence from academic institutions in developing countries: Evidence from. In *The African Journal of Information Systems* (Vol. 10).
14. Munien, R. (2010). *INTERNET PHISHING HOOK, LINE AND HOPEFULLY NOT SUNK…*.
15. O'Connor, E. A., & Domingo, J. (2017). A Practical Guide, With Theoretical Underpinnings, for Creating Effective Virtual Reality Learning Environments. *Journal of Educational Technology Systems*, *45*(3), 343–364. https://doi.org/10.1177/0047239516673361
16. Paniagua, F. A. (2019). Some Thoughts on Preferred Qualifications in the Search for Academic Jobs. *Open Journal of Social Sciences*, *07*(10), 261–268. https://doi.org/10.4236/jss.2019.710021

17. Peltier, T. R. (2005). Implementing an Information Security Awareness Program. *Information Systems Security*, *14*(2), 37–49. https://doi.org/10.1201/1086/45241.14.2.20050501/88292.6
18. Positivist Paradigm. (2008). In *Encyclopedia of Counseling*. SAGE Publications, Inc. https://doi.org/10.4135/9781412963978.n249
19. Pretorius, B., & van Niekerk, B. (n.d.). *Cyber-Security and Governance for ICS/SCADA in South Africa*.
20. Rajesh Chandarman, & Brett Van Niekerk. (2017). Students' Cybersecurity Awareness at a Private Tertiary Educational Institution. *The African Journal of Information and Communication (AJIC)*, *20*. https://doi.org/10.23962/10539/23572
21. Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, *27*(7–8), 241–253. https://doi.org/10.1016/j.cose.2008.07.008
22. Törley, G. (n.d.). *The Level of Information Security Awareness of First-Year University Students*. http://ceur-ws.org
23. Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating Information Security Awareness: Research and Practice Gaps. *Information Security Journal: A Global Perspective*, *17*(5–6), 207–227. https://doi.org/10.1080/19393550802492487
24. Volkamer, M., Renaud, K., Kulyk, O., & Emeröz, S. (n.d.). *A Socio-Technical Investigation into Smartphone Security*. https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSI/