Cyber-attacks and Impacts on the Educational Cyber Infrastructures

Olawale Surajudeen Adebayo, PhD

Cyber Security Science Department, Federal University of Technology Minna

Computer Science Department, Islamic University In Uganda

waleadebayo@futminna.edu.ng, o.sadebayo@iuiu.ac.ug

The impacts of cyber-attacks in the field of education over the years cannot be overemphasised. Cyber-attacks are defined as criminal activities perpetrated through the use of internet and electronic gadgets to cause financial loss or damages of properties. The attacks have been responsible for huge data and financial loss in the education sector of economy over the years. Therefore, these attacks have seriously affected the information and communication facilities in education sectors and require adequate attentions. This research examines the effects of these cyber-attacks on the ICT facilities of education sectors and how the trends can be curbed. Research instruments were administered to gather necessary information from the target respondents. Quantitative analysis was applied on the collected information. The results show that the effects of cyber-attacks on the ICT facilities of educational institution need urgent cyber security attentions to curb attacks. Reasons like financial gain and disgruntlement were identified for the attacks. Recommendations were given to ensure the safe use of ICT facilities, institutions' data and other vital information of these educational institutions.

Keywords:

Cyber-attacks, Cybercrime, Information and Communication Technology, ICT infrastructures, Cyber-attacks Impact

1. Introduction

Cyber-attacks are sophisticated criminal activities being perpetrated through the use of electronic gadgets and network facilities. These attacks can be broadly categorized as cyber-dependent attacks and cyber-enabled attacks [1]. The cyber-attacks include; Phishing attack, distributed denial-of-service (DDoS), malware attack, password cracking attack, zero-day exploit, business email compromise/email account compromise, spyware attacks, online hate speech, vishing attacks, system/phone/social media hacking, malicious apps, spamming, identity theft, cryptocurrency scam, cyberstalking, adware attacks, WhatsApp number swapping, and denial of service attacks [2],[3],[4], [5]. Due to the lucrative nature and low risks involved, cybercrimes occasioned by cyber-attacks can be conducted anywhere across the globe through the use of remote unsecure internet. Cybercrime is described by the crime triangle which states that for a cybercrime to occur, three factors must be in play: a victim, a motive and an opportunity. In this scenario, the victim is the entity the attack is targeting, the motive is the reason behind the attack and the opportunity is the vulnerability of the target [6].

Recently, Cyber-attacks have also targeted critical infrastructure such as sensors and actuators, RFID systems, industrial equipment, video surveillance cameras, basic personal computers and networking devices. These ICTs bring cutting-edge services, enhance controllability, reliability and safety, and enable the implementation of innovative infrastructure models like the smart grid. Critical infrastructure assets such as power plants, water supply systems and electric power grids are no longer working in isolated environments but rather working as "systems-of-systems" fused with significant information and communications technology infrastructures such as the Internet [7]. The attack of the ICT infrastructure leads to compromising of the integrity, confidentiality and availability of ICT networks and information [8].

The FBI cybercrime report 2021 shows that cybercrime has been on a drastic rise for the last five years (2017-2021) with 2.67 million complaints in the United States of America alone leading to financial loss of $18.7 billion and $6.9 billion in 2021 alone [26]. The African cyberthreat assessment report 2021 states that 38% (500 million) of the Africa's population are connected on the internet and the number is expected to raise given the accelerated digitalization. This has augmented the cybercrime environment especially during the Covid-19 pandemic with increasing cybersecurity vulnerabilities. 90% of African businesses worked without the essential cybersecurity protocols [27].

In Africa, the East African countries experience the highest rate of cyber-attacks, according to the latest Africa Cyber Security Outlook 2022 report by KPMG. This is credited to the rise in cashless payments and remote working after the Covid-19 pandemic and also the rapid adoption of digital technology across businesses with limited expertise and awareness in technology, digital infrastructure and cyber security.

Considering the current sophistication of cyber-attacks, the frequency of occurrence and the rapid adoption of the information and communication technologies and internet in the education sectors for important activities such as vital information storage, students' record keeping, staff information management, results' processing and storage, among others important activities related to these are being threaten, it becomes a necessity to assess the impacts of these cyber-attacks on the ICT infrastructures in order to identify the causes, effects, and provide possible measures for mitigation.

The remaining parts of this article are organized as follows: related literatures to the impacts of cyber-attacks on the educational facilities is discussed in section two while methodology to achieve the research aim is discussed in section three. The results of the research is presented in section four while this result is discussed in section five. The research is concluded in section six with the summary of research activities.

2. Related Works

The study in [28] adopts the use of research instrument to gather important information from the target respondent. The data gathered were analysed using factor and relational analysis to determined the effect of incidence and nature of cyber-attacks on the assessment of the effectiveness governance in Nigeria. The results of the study revealed that financial benefits and disgruntlement accounted for most factor responsible for the attacks. The study recommended appropriate actions by government and law enforcement agencies in providing adequate data base and comprehensive research in the area of cybersecurity. The research in

[29] examine the extent to which age, gender and educational level plays a role in mediating the factors affecting tertiary institution students' cybersecurity behaviours. The research conducted cross-sectional survey among 340 students and used Structural Equation Modelling for impacts evaluation. Results show that students cybersecurity behaviors varies based on Age for factors such as: Perceived Severity, Peer Behavior, Familiarity with Cyber Threats, Response Efficacy and Perceived Vulnerability.

[30] assesses the state of cyber security threats and risks in Uganda. The research adopts information gathering technique. The results revealed denial-of-service attacks, Data espionage, natural threats, Sabotage, Computer frauds, malicious attacks, Message falsification or injection, vandalism, copyright violations as parts of cyber emerging security threats. It recommends strategic plans for governments and Information Technology industries to stem the tides of cyber threats. The objective of [31] was to explore the reasons modern learners need to be educated about the risks associated with being active in cyberspace. The paper discussed some strategies on the implementation of cyber security in the schools.

[32] posited cybersecurity as an emerging critical issue confronting schools in the 21st century. The paper identified human factor as an underline reason for successful cyber-attacks on schools' computers and other systems. It recommended formal cyber security awareness to cushion the exploitation of human vulnerabilities by computer hackers and attackers. The study in [33] carried out comprehensive review on the standard threats available in the field of cyber security. The research also investigates the challenges, weaknesses and strengths of the proposed techniques. Types of new descendant attacks are considered in details and standard security frameworks are itemised.

Arina and Anatolie [34] identified classes of attacks with major impact, on the assets. The research also provided recommendations for increasing cyber security in e-learning conditions. The recommendations include up to date system update and security patch management, access policies implemention at the application or resource level, information classification, and use of cryptographic protocols. The research in [35] discussed the current state of cyber security in Education most common reasons for the attack, the highest threats, and the main challenges facing the sector to help understand why needs for cyber security.

3. Methodology

3.1.1 Research Design

The intention in this research is to examine the reasons for the attacks and the reasons for successful attacks. In order to do this, exploratory and survey research techniques were adopted. The research instruments consist of google form questionnaires which were designed and administered to the identified respondents through electronic mail. The survey research was designed to gather the useful data for analysis while the exploratory was used to gain insights into some useful previously available information related to the reasons for the cyber-attacks and the successful operations. In this research, hypotheses were formulated based on the research questions of the research. The research questionnaires were structured to discover whether the reasons of the attacks, which could be financial gains, employee disgruntlement, and/or challenges have impact on the education system. The researcher, in addition, sought to discover whether the reasons for successful cyber-attacks such as the lack of awareness,

vulnerability, use of weak security have impacts on the education system. Finally, the research sought to find out whether the frequency of attacks on the education facilities has impact on the effectiveness of education system.

3.1.2 Research Hypotheses

Hypothesis 1

H0 (Null):

There is no significant correlation between the frequency of cyber-attacks and effective education system

H1 (Alternative):

There is significant correlation between the frequency of cyber-attacks and effective education system

Hypothesis 2

H2 (Null):

The reasons for successful attacks have no significant effects on the effectiveness of education system

H3 (Alternative):

The reasons for successful attacks have significant effects on the effectiveness of education system

Hypothesis 3

H4 (Null):

The motivational factors for cyber-attacks have no significant impacts on the effectiveness of education system

H5 (Alternative):

The motivational factors for cyber-attacks have significant impacts on the effectiveness of education system

3.1.3 Sample and Procedure

The targeted population are the staff and users of the information and communication technology network facilities in three Universities in Uganda namely: Islamic University in Uganda, Kampala International University, and Soroti University. A total number of 220 sample size of the 300 targeted population were randomly selected for analysis. A simple random sampling technique was used to ensure the equal representation of the categories of respondents.

3.1.4 Respondents

The targeted respondents were the staff and users of ICT facilities of the three universities. Google form was designed and sent to the 300 selected respondents. Two hundred and twenty (220) out of these population responded to the questionnaire representing 0.73%. The responses were analysed based on the set coded criteria upon which conclusion was reached.

3.1.5 Research Instruments

The instruments of research are questionnaire designed using google form and administered through the email and social media to the targeted audience. The questionnaire was divided into two part viz the demographic information of respondents and questions related to the cyber-attacks. The demographic information consists the sex, age, occupation, and education of the respondents while the second part was structured into five segments I to V rated on 5-1 scale of reference (Strongly Agree, Partially Agree, Neutral, Agree, Disagree). The first segment was structured to capture the types of attacks, segment II measures the frequencies of the attacks, segment III deals with reasons (motivating factors) for the attacks, segment IV considered the reasons for successful attacks which may contribute to the attacks while segment V relates to the assessment and effectiveness of educational institutions. The questions used were structured by the researchers based on the research hypotheses and existing literatures.

3.1.6 Data Validity and Reliability

In order to validate the instrument of this research (Google forms), the types of the questions were automatically selected and added in the response validation, then the rule was set and the type of error was included. This error will be displayed to the respondents when they want to violate the rule of the data.

4. Results

The responses in segment B were structured into sex, age, occupation, and education of respondents. The sex is to identify the gender percentage participation in the research while the age is to determine whether the respondents are old enough to provide accurate answer. The occupation is to determine whether the respondents are in the field of information and communication technology and involve in the use of ICT. The education part is to examine if the respondents have requisite education to participate in the questionnaire survey.

4.1 Demographic of the Respondents

Table 4.1 Respondents Demographic

Variable (N=220)	Variable Description	Frequency	Percentage (%)	Cumulative Percent
Gender	Male	180	81.8	81.8
	Female	40	18.2	**100**
Age (years)	15 – 30	105	47.7	47.7
	31 – 45	70	31.8	79.5
	45 – 59	35	15.9	95.4
	Above 59	10	4.6	**100**
Occupation	Student	50	22.7	22.7
	ICT Manager	20	9.1	31.8
	System Analyst	50	22.7	54.5
	Computer Operator	100	45.5	**100**
Education	Undergraduate	60	27.3	27.3
	Diploma	50	22.7	50.0
	Degree	70	31.8	81.8
	Master	30	13.6	95.4
	PhD	10	4.6	**100**

Source: Authors' survey, 2023

The results were represented using figures 4.1, 4.2, 4.3, and 4.4.

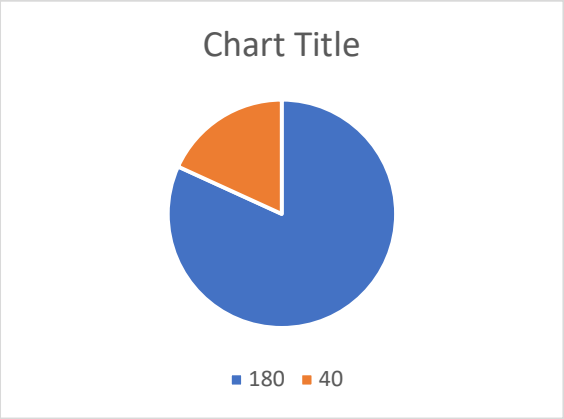

Figure 4.1. Gender distribution of respondents

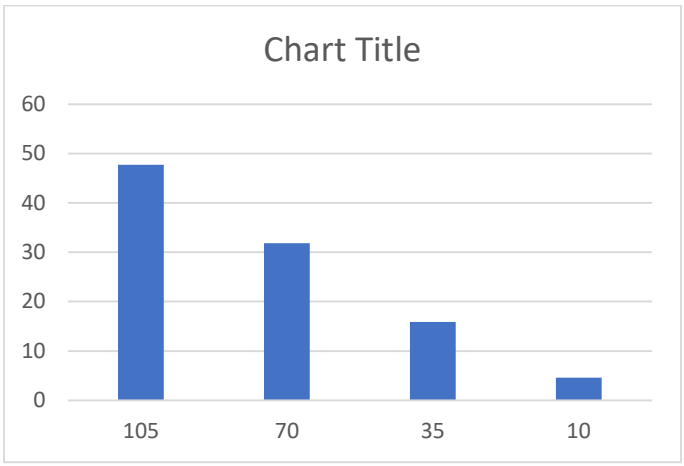

Figure 4.2. Age distribution of respondents

Source: Authors' survey, 2023

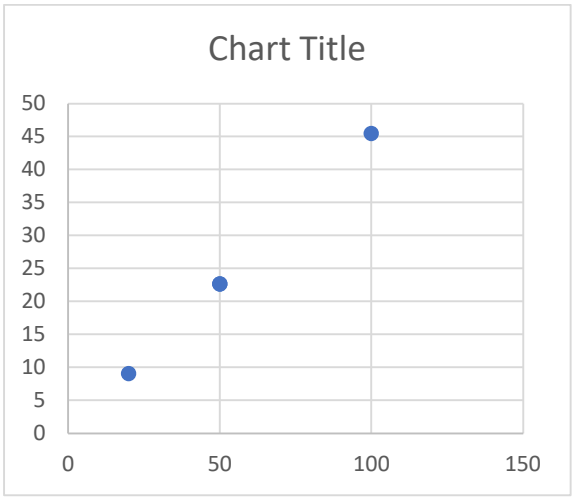

Figure 4.3. Occupational distribution of respondents

Source: Authors' survey, 2023

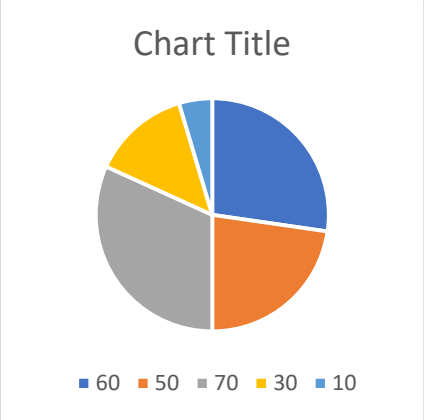

Figure 4.4. Education classification of respondents

Source: Authors' survey, 2023

4.2 Motivations for the attacks and successful attacks

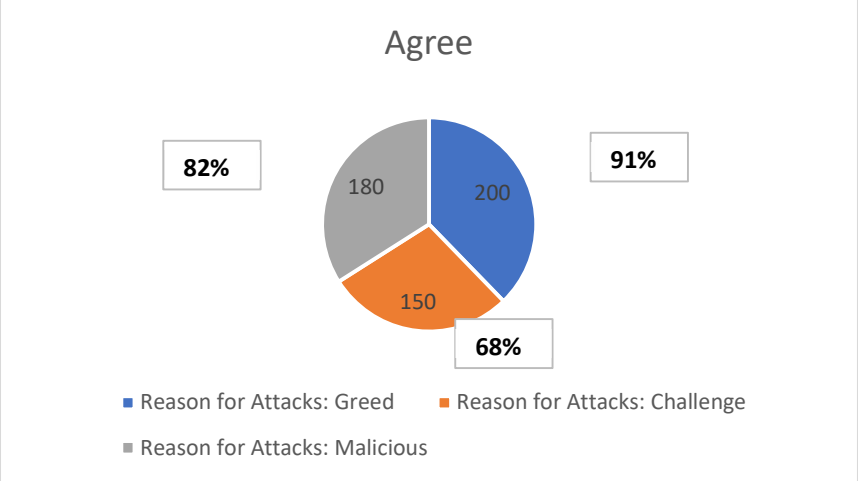

Figure 4.5. Cyber-attack Motivations

Source: Authors' survey, 2023

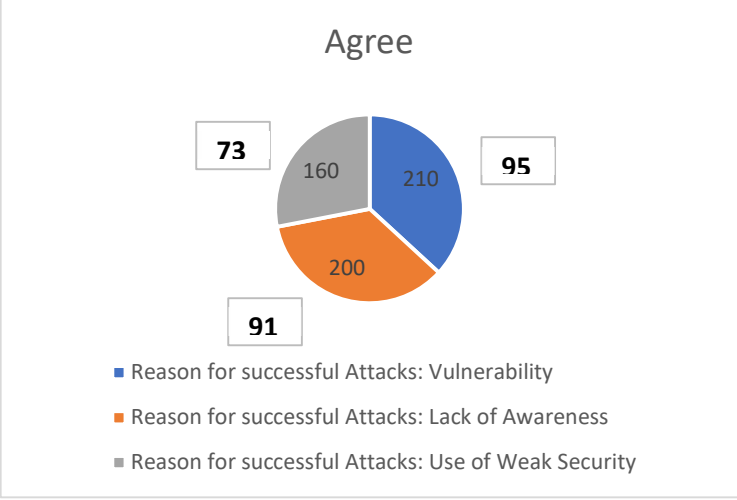

Figure 4.6. Reason for successful Cyber-attack

Source: Authors' survey, 2023

5. Discussion of Results

The results of this research were displaying in table 4.1, and Figures 4.1, 4.2, 4.3, and 4.4. The table is showing the variable parameters considered in the analysis which include the gender of respondents, the age, the occupation, and their educational level. The statistics in figure 4.1 show that 180 males participated in the survey representing 81.8% while 40 females participated with 18.2% representation. Figure 4.2 is showing the age distribution of participant with 47.7 percent of ages between 15 and 30 while 31.8 percent of respondents lies between 31 and 45 years of age. A total of 35 respondents representing 15.9 percent lies between the ages of 45 to 59 years of age while the remaining respondents lies above 59 years of age representing 4.6 percent participated. The total number of students participated in the survey were 50 representing 22.7 percent while 20 were ICT managers of the Universities representing 9.1 percent respondents. The system analyst respondents were 50 representing 22.7 percent while 100 computer operators participated representing 45.5 percent. In terms of respondents' level of education, 60 were undergraduate representing 27.3 percent while 50 respondents were diploma holder representing 22.7 percent. Seventy (70) respondents bagged University degree representing 31.8 percent while 30 respondents were master degree older. The doctoral degree holder respondents were mere 10 representing 4.6 percent population.

The research examined whether the reason of attacks: Greed, Malicious or Challenge and whether the reasons for successful attacks are: Vulnerability, Lack of awareness, or Use of weak Security. Out of 220 respondent participants, 200 representing 91% agreed that greed accounted for the cyber-attacks while 9% disagreed. In addition, 150 respondents representing 68% agreed challenge is the reason for various cyber-attacks while remaining 70 representing 32% disagreed. For malicious reason, 82% of respondents agreed its cause cyber attacks while 18% disagreed. Regarding the reasons for successful cyber-attacks, 210 respondents representing 95% agreed existence of vulnerability accounted for various reasons for successful attacks while 5% disagreed. Moreover, 91% of the respondents agreed that lack of awareness among users responsible for the successful cyber-attacks by the attackers while 9% disagreed. As regards the use of weak security techniques, 73% of the 220 respondents agreed this is responsible for successful attacks while 27% disagreed.

In summary, using the Chi-squared model values for frequency of cyber-attacks, effective education system, and motivation factors show that at significant level of 5% (0.05), the estimated results are statically significant. Therefore, based on these values of results of analysis which are greater than the significant level in the three hypotheses, then the null hypotheses were rejected while the alternative hypotheses were accepted. It was therefore, conclude that there is significant correlation between the frequency of cyber-attacks and effective education system, the identified challenges have significant effects on the effectiveness of education system, and that the motivational factors for cyber-attacks have significant impacts on the effectiveness of education system.

6. Recommendation

Based on the empirical evidence from the analysis in this research, it can be deduced the frequency of cyber-attacks, the identified challenges and motivational factors have severe effects on the educational system of a country. It was therefore, recommended by this research that frequency of attacks should be checked and curbed, the challenges leading to cyber-attacks should be given adequate attention, while the motivational factors should be addressed.

Therefore, there is need for holistic approach by the government and education stakeholders to ensure adequate monitoring, awareness, and timely intervention to curtail the effects of cyber-attacks in educational sectors.

7. Conclusion

This research examined the effects of cyber-attacks on the education system of a nation. The research evaluates this based on the frequency of attacks, challenges, and attacks motivational factors. The results show there is a significant correlation between these factors and effectiveness of education system. The research therefore, recommended holistic approach by the stakeholders in education sectors to curtail the effects of these attacks.

References

[1] G. S. Oreku and F. J. Mtenzi, "Cybercrime: Concerns, challenges and opportunities," in *Studies in Computational Intelligence*, vol. 691, Springer Verlag, 2017, pp. 129–153. doi: 10.1007/978-3-319-44257-0_6.

[2] M. B. Afolabi and G. A. Raji, "Defeating the 21st century demon 'Cybercrime' on corporate bodies in Nigeria: Is security intelligence a weapon? A quantitative study," *F1000Res*, vol. 11, p. 983, Aug. 2022, doi: 10.12688/f1000research.121854.1.

[3] O. P. Badve and B. B. Gupta, "Taxonomy of Recent DDoS Attack Prevention, Detection, and Response Schemes in Cloud Environment," in *Proceedings of the International Conference on Recent Cognizance in Wireless Communication & Image Processing*, Springer India, 2016, pp. 683–693. doi: 10.1007/978-81-322-2638-3_76.

[4] "A Survey of Stealth Malware Attacks, Mitigation Measures, and Steps Toward Autonomous Open World Solutions | Enhanced Reader."

[5] S. Subangan and V. Senthooran, "Secure Authentication Mechanism for Resistance to Password Attacks; Secure Authentication Mechanism for Resistance to Password Attacks," 2019.

[6] H. S. Lallie *et al.*, "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Comput Secur*, vol. 105, Jun. 2021, doi: 10.1016/j.cose.2021.102248.

[7] B. Genge, I. Kiss, and P. Haller, "A system dynamics approach for assessing the impact of cyber-attacks on critical infrastructures," *International Journal of Critical Infrastructure Protection*, vol. 10, pp. 3–17, Sep. 2015, doi: 10.1016/j.ijcip.2015.04.001.

[8] C. Krasznay and B. P. Hámornik, “Analysis of Cyberattack Patterns by User Behavior Analytics,” *Academic and Applied Research in Military and Public Management Science*, vol. 17, no. 3, pp. 101–113, Dec. 2018, doi: 10.32565/aarms.2018.3.7.

[9] “Cyber-Security-Posture-for-the-Period-January-2021-to-December-2021”.

[10] “ASHIRU: Identifying Phishing As A form of Cybercrime in Nigeria IDENTIFYING PHISHING AS A FORM OF CYBERCRIME IN NIGERIA*.” [Online]. Available: https://www.phishing.org/what-is-phishing,

[11] A. K. Jain and B. B. Gupta, “A survey of phishing attack techniques, defence mechanisms and open research challenges,” *Enterprise Information Systems*, vol. 16, no. 4. Taylor and Francis Ltd., pp. 527–565, 2022. doi: 10.1080/17517575.2021.1896786.

[12] D. Javaheri, M. Hosseinzadeh, and A. M. Rahmani, “Detection and elimination of spyware and ransomware by intercepting kernel-level system routines,” *IEEE Access*, vol. 6, 2018, doi: 10.1109/ACCESS.2018.2884964.

[13] R. K. Shazhad, S. I. Haider, and N. Lavesson, “Detection of spyware by mining executable files,” in *ARES 2010 - 5th International Conference on Availability, Reliability, and Security*, 2010. doi: 10.1109/ARES.2010.105.

[14] N. Chetty and S. Alathur, “Hate speech review in the context of online social networks,” *Aggression and Violent Behavior*, vol. 40. 2018. doi: 10.1016/j.avb.2018.05.003.

[15] S. Ullmann and M. Tomalin, “Quarantining online hate speech: technical and ethical perspectives,” *Ethics Inf Technol*, vol. 22, no. 1, 2020, doi: 10.1007/s10676-019-09516-z.

[16] S. Biswal, “Real-Time Intelligent Vishing Prediction and Awareness Model (RIVPAM),” in *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2021*, 2021. doi: 10.1109/CyberSA52016.2021.9478240.

[17] E. O. Yeboah-Boateng and P. M. Amanor, “Journal of Emerging Trends in Computing and Information Sciences Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices,” *Journal of Emerging Trends in Computing and Information Sciences*, vol. 5, no. 4, 2014.

[18] K. Harrison and G. White, “A Taxonomy of Cyber Events Affecting Communities,” 2011.

[19] M. Bartoletti, S. Lande, A. Loddo, L. Pompianu, and S. Serusi, “Cryptocurrency scams: Analysis and perspectives,” *IEEE Access*, vol. 9, 2021, doi: 10.1109/ACCESS.2021.3123894.

[20] K. Lee and H. Park, “Malicious Adware Detection on Android Platform using Dynamic Random Forest,” in *Advances in Intelligent Systems and Computing*, 2020, vol. 994. doi: 10.1007/978-3-030-22263-5_57.

[21] L. Liang, K. Zheng, Q. Sheng, and X. Huang, “A denial of service attack method for an IoT system,” in *Proceedings - 2016 8th International Conference on Information Technology in Medicine and Education, ITME 2016*, 2017. doi: 10.1109/ITME.2016.0087.

[22] K. S. Jones, M. E. Armstrong, M. K. Tornblad, and A. Siami Namin, “How social engineers use persuasion principles during vishing attacks,” *Information and Computer Security*, vol. 29, no. 2, 2020, doi: 10.1108/ICS-07-2020-0113.

[23] E. O. Yeboah-Boateng and P. M. Amanor, "Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices," *Journal of Emerging Trends in Computing and Information Sciences*, vol. 5, no. 4, 2014.

[24] J. Obuhuma and S. Zivuku, "Social Engineering Based Cyber-Attacks in Kenya," in *2020 IST-Africa Conference, IST-Africa 2020*, 2020.

[25] S. Musman, M. Tanner, A. Temin, E. Elsaesser, and L. Loren, "Computing the impact of cyber-attacks on complex missions," in *2011 IEEE International Systems Conference, SysCon 2011 - Proceedings*, 2011, pp. 46–51. doi: 10.1109/SYSCON.2011.5929055.

[26] "FE DE R A L B U RE A U O F I N VE S TI G A TIO N." [Online]. Available: www.ic3.gov.

[27] "INTERPOL For official use only AFRICAN CYBERTHREAT ASSESSMENT REPORT," 2021.

[28] Fayomi O., Ndubisi O. N., Ayo C., Chidozie F., Ajayi L., Okorie U. Cyber-Attack as a Menace to Effective Governance in Nigeria. 15th European Conference on eGovernment (ECEG 2015) Portsmouth, United Kingdom 18 – 19 June 2015. Editors: Carl Adams. ISBN: 978-1-5108-0911-6

[29] F B Fatokun, S Hamid, A Norman, J O Fatokun. The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities. International Conference Computer Science and Engineering Journal of Physics: Conference Series 1339 (2019) 012098 IOP Publishing doi:10.1088/1742-6596/1339/1/012098

[30] Matovu Davis, Mugeni Gilbert B , Karume Simon, Mutua Stephen, Gilbert Gilibrays Ocen. State of cyber security: the Ugandan perspective. International Journal of Scientific & Engineering Research Volume 10, Issue 4, April-2019 713 ISSN 2229-5518.

[31] Rahman N. A. A, Sairi I. H., Zizi N. A. M., and Khalid F. I. The Importance of Cybersecurity Education in School. International Journal of Information and Education Technology, Vol. 10, No. 5, May 2020

[32] Michael D, Richardson, Pamela A. Lemoine, Walter E. Stephens, Robert E. Waller. Planning for Cyber Security in Schools. The Human Factor. Educational Planning 2020 23 Vol. 27, No. 2.

[33] Yuchong Li a,b , Qinghui Liu. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports 7 (2021) 8176–8186. Available at http://www.elsevier.com/locate/egyr

[34] Alexei Arina, Alexei Anatolie. Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learning. International Journal of Scientific and Technology Reseaech. Volume 10, Issue 03, March 2021, ISSN: 2277-8616

[35] Md. Sadre Alam. Need of Cyber Security in Higher Education in Present Era. International Journal of Creative Research Thoughts (IJCRT) www.ijcrt.org. Volume 10, Issue 3 March 2022 | ISSN: 2320-2882