e-palli

American Journal of Multidisciplinary Research and Innovation (AJMRI)

ISSN: 2158-8155 (Online), 2832-4854 (Print)

VOLUME 3 ISSUE 6 (2024)

PUBLISHED BY: E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Multidisciplinary Research and Innovation (AJMRI)

Volume 3 Issue 6, Year 2024
ISSN: 2158-8155 (Online), 2832-4854 (Print)
DOI: https://doi.org/10.54536/ajmri.v3i6.3012
https://journals.e-palli.com/home/index.php/ajmri

Assessment of Internet Safety, Cybersecurity Awareness and Risks in Technology Environment among College Students

Akere Olajumoke Modupe[1*]

Article Information

Received: September 08, 2024

Accepted: October 13, 2024

Published: November 13, 2024

Keywords

Internet Safety, Awareness, Cybersecurity, Technology Risk, College

ABSTRACT

The study examined the internet safety, cybersecurity and risks in technology environment. The study adopted a descriptive survey research design. The sample comprised 100 respondents drawn randomly online were used. College students cybersecurity awareness scale ($r = 0.84$) was used to collect data. Frequency counts and multiple regression analysis were used to analyse the data collected. 52 (52%) of the respondents are of age 16-20 years. Thirty-eight (38%) males responded while 62 (62%) are female and 89 (89%) maintain high levels of internet safety, and seventy-eight (78%) cybersecurity awareness. There is a linear relationship between predictor variables (internet safety and cybersecurity awareness) and risk in the technology environment $r = 0.777$. Internet safety ($\beta = 0.823$; $t (98) = 10.816$; $p < .05$) contributed most followed by cybersecurity awareness ($\beta = 0.099$; $t (98) = 1.299$; $p < .05$). It was deduced from the findings that there more users of high level of internet safety and cybersecurity awareness among college students. There is significant effect of internet safety and cybersecurity awareness on risk in technology environment. Although some of the internet safety measures are not well observed as they were considered not necessary. It is therefore recommended that all safety measures must be taken seriously by college students, as well as other technology users.

INTRODUCTION

The rapid development of technology in the 21st century has changed our lives, especially information and communication methods used to communicate and interact with others over time. Different communication methods are used around the world. As a result, the public and private sectors have begun to offer more services and adopt new technologies to access information anytime and anywhere, according to user demand. The main reason for many automation services and adoption of new technologies is for supporting and meeting a wide range of user needs (Jinadu, 2024; Jinadu, 2024 and Gamreklidze, 2014).

Afterward, there has been a growing number of hackers and cybercriminal groups trying to break into automated systems. These cybercriminals have developed new ways to commit cybercrime (Mohammed, 2022). An attacker's main goal is to make money by stealing sensitive information and holding it for ransom. Hackers can also make money by selling secret data to competitors on the dark web, causing cyberspace damage and serious disruption. Organizations and their customers have become a major threat to the security and economy of the world, targeting critical infrastructure, having a significant financial impact on business operations and leading to the loss of intellectual property (Green, 2015).

Every Internet and technology users (including today's college students, most of who have grown up in cyberspace) are not aware of the risks to their security and individual details with insecure electronic use. Kim (2013) states that, contrary to popular belief, these heavy consumers of virtual tools are mostly those who have very little knowledge about cyber security and issues of prevention, although the security of the body, property and space is a priority for most people, the problem of security of data and property in our online world is not ordinary (Moallem, 2017). This is truly a threat manouvering.

Every organisation has a responsibility. As organizations use automated information technology systems in digital era to process their details in order to better support their programs, risk management plays an important role in protecting the organization's information assets, and therefore its mission, from the connection (Jinadu, 2024). With information technology, there is a risk of harm. Risk is the chance of bearing damage or impairment. It refers to an action, event, or environmental situation that has an unexpected result.it can produce negative results or results. An effective risk management process is an important part of a successful IT security program. The primary goal of an organization's risk management process is to protect the organization and its ability to achieve its mission, not just IT assets (NIST, 2022). Therefore, the process of risk management should not be done primarily as a technical task by IT professionals who manage and manage the IT system, but as a technical task the most important part of managing all IT users in this era of cyber security. Risk management is looking through what can go wrong, and then deciding on how to forestall or reduce the sensed challenges. There are three processes: risk assessment, risk mitigation and evaluation. Studies in the field of cybersecurity suggest that internet

[1] Department of Education Management, University of Ibadan, Ibadan, Nigeria
[*] Corresponding author's e-mail: akereom23@gmail.com

safety and cybersecurity awareness tend to reduce technological risks. These studies examined both the level of cyber security awareness and internet safety. However, studies have not linked the impact to technological risk as is the case in this study. In recent years, many studies have been conducted to assess the level of awareness of university students about details of security issues. Slusky and Partow-Navid (2014) studied students in the College of Business and Economics at California State University, Los Angeles. The results show that lack of security knowledge does not bring about the main problem in security awareness, rather how students apply this knowledge in real-world situations. This is because fundamentally, understanding of information security is way below the respect for the knowledge of information security.

Another study conducted by Samaher and Ibrahim Al-Shourbaji (2016) analysed cyber security awareness among academic staff, researchers, students and education sector workers in the Middle East. The results show that the participants did not possess the required know how and understanding of the essence of information security principles and their application in practical terms on daily basis.

Senthilkumar and Easwaramoorthy (2017) analyzed cyber security awareness among students in Tamil Nadu (a state in India) regarding various security threats; 500 students from five major cities answered a survey online. The result showed that more than 70% of the students were more aware of basic virus attacks and used antivirus software (updated frequently) or Linux platform to protect their system from virus attacks. The other students did not use protection against malware and have received the wrath attacks of viruses. 11% of them used antivirus but did not update their software. More than 97% of them did not know the source of the virus.

Abbas (2019) investigated the early results of a study that aimed to investigate the awareness and attitudes of students towards cyber security and related risks in the most advanced technological environment: Silicon Valley in California, in the United States. The student body in Silicon Valley is very diverse ethnically. The study observed that college students, no matter their notion that they are being monitored at the same time as the usage of the internet and that their information is not secure even in college systems, they are now no longer wary of the way to defend their information. To add to it, evidently, academic establishments no longer have a lively method to enhance the attention of college students to grow their know-how of those issues and a way to defend themselves from probable cyber-attacks, inclusive of identification robbery or undesirable computer effects.

Chelsea and Sagaya (2023) examined the level of awareness of cyber security and to understand the level of basic knowledge of cyber security among female students in the city of Coimbatore. Data were collected using a questionnaire and a sample of 106 female students. Descriptive design was used for this work. Simple random sampling method was used. Data collected were analysed by spearman's rho correlation and chi-square coefficient. The study concludes that there is a growing awareness of cyber security among female students, but there is still a knowledge gap when it comes to implementing the necessary security measures to stay safe online.

Internet safety entails many measures that affect the physical and mental health of internet users. This concept, known as "cyber security", "digital security" or "cyber security" refers to the problems that occur on the internet and the ways in which they can protect themselves against those problems. Researchers across fields (such as communication, psychology, law), educators, media and public institutions have expressed their views. There has been a growing concern about the harm that can be done online every day, and the need for appropriate interventions to reduce the harm that people do online. Activity can create more for students (Kimple *et al.*, 2019; Livingstone *et al.*, 2011).

Three research questions were posed and answered to guide this study. These are:

1. What is the profile of the college students in terms of demographics, internet safety and cybersecurity awareness?
2. What is the joint influence of student internet safety and cybersecurity awareness on risk in technology environment?
3. What is the relative influence of student internet safety and cybersecurity awareness on risk in technology environment?

MATERIALS AND METHODS

The study adopted a descriptive survey research design. This design was adopted because the researchers did not manipulate any variable. It allowed the researcher to collect data on variables that had occurred earlier and draw the inferences from them to generalised to the entire population of the study. This is relevant because it examines the cause-and-effect relationship between independent and dependent variables (Jinadu *et al.*, 2023). This study's population comprised all users of technology gadgets among college students. A total sample of one hundred (100) college students selected randomly participated in the study.

Cybersecurity awareness scale was developed and validated to collect data for this study. The researchers developed the scale to measure Internet safety, Cybersecurity Awareness and Risks in Technology Environment. The instrument has four sections A, B, C and D. Section A is on demographic information such as gender, age, admission sought, daily devices used, daily social media used and knowledge of cybersecurity concept. Section B is on cybersecurity counter measures. Section C is on cybersecurity website tracking and section D is on phishing. To validate the instrument, samples of the instrument were trial tested on small sample of college students different from the main sample. The data collected were analysed for internal consistency and reliability using Chronbach's Alpha which yielded 0.84. The final form of the instrument was administered through an online Google form survey.

The researchers developed an online Google form where responses were collected to measure students' awareness of cyber security. The data/responses were automatically coded and organized online by the Google Form online survey service for easy analysis. In total, data was collected over a period of four weeks. Frequency counting and multiple regression analysis were used to analyze the data. The study focuses on the safety and security of information and technology users. Therefore, the issue of ethical consideration was respected by ensuring that the participants had the freedom to respond to their opinion without imposition or coercion. They were given the freedom to withdraw from participating in the research exercise at any time they felt uncomfortable with the process. To protect your identity from any unforeseen or possible damage in accordance with data protection and governance as stipulated in the policy of the Nigerian Communications Commission (NCC) of the Federal Ministry of Community and Digital Economy, were considered anonymous as their name was not requested or recorded and the data collected is were treated confidentially and for research purposes only.

RESULTS AND DISCUSSION

Result

Research Question 1

What is the profile of the college students in terms of demographics, internet safety and cybersecurity awareness?

Table 1: Profile of the Respondents

S/N	Demographic Variable	Frequency	Percentage
1	**Age (years)**		
	16-20	52	52
	21-25	28	28
	26-30	15	15
	31 and above	6	6
	Total	**100**	**100.0**
2	**Gender**		
	Male	38	38
	Female	62	62
	Total	**100**	**100.0**
3	**Level of Internet Safety**		
	Low	2	2
	Moderate	9	9
	High	89	89
	Total	**100**	**100.0**
4	**Level of Cybersecurity Awareness**		
	Low	9	9
	Moderate	13	13
	High	78	78
	Total	**100**	**100.0**

Table 1 shows the profile of the respondents used in the study. The table indicates that 52 (52%) of the respondents are of age 16-20 years, 28 (28%) are of age 21-25 years, 15 (15%) are of age 26-30 years and 6 (6%) are of age 31 years and above. Thirty eight (38%) male responded while 62 (62%) are female respondents. The table also shows that 89 (89%) of the respondent maintain high level of internet safety, 9 (9%) moderate and only 2 (2%) low. Seventy eight (78%) have high level of cybersecurity awareness, 13 (13%) moderate and 9 (9%) low level of cybersecurity awareness.

Research Question 2

What is the joint influence of student internet safety and cybersecurity awareness on risk in technology environment?

Table 2: Model Summary of Predictors on Risk in Technology Environment

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
	.775	.600	.592	8.67275

Table 3: Regression ANOVA of Predictors on Risk in Technology Environment

Model	Sum of Squares	Df	Mean Square	F	Sig.
Regression	10956.025	2	5478.013	72.830	0.000*
Residual	7296.015	98	75.217		
Total	**18252.040**	**100**			

**Significant at P < 0.05 level*

Tables 2 and 3 show the model summary and regression ANOVA respectively. The multiple regression correlation coefficient (R) show the strong positive linear relationship between predictor variables: internet safety and cybersecurity awareness and the dependent variable (risk in technology environment) as shown in Table 2 is 0.775, the multiple R2 is 0.600 which is 60% and the Adjusted R square value is 0.592 which is 59.2%. This means that the variation in risk in technology environment accounted for by the predictor variables: internet safety and cybersecurity awareness is approximately 59.2% and it is statistically significant at $p < 0.05$ level. Furthermore, indicated in the Table 3 is the analysis of variance of the multiple regression data. This produced an F- ratio of F(2,98) = 72.830 and found to be significant at 0.05 Alpha level.

The result on composite effect of internet safety and cybersecurity awareness on risk in technology environment show that there is linear relationship between predictor variables: internet safety and cybersecurity awareness and the dependent variable (risk in technology environment). This means that the variation in risk in technology environment accounted for by the predictor variables: internet safety and cybersecurity awareness is more and it is statistically significant.

Research Question 3

What is the relative influence of student internet safety and cybersecurity awareness on risk in technology environment?

Table 4: Regression Coefficients of Predictors on Risk in Technology Environment

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig
	B	Std. Error	Beta		
(Constant)	9.136	5.452		1.676	.001
Internet safety	0.867	0.080	0.823	10.816	.000
Cybersecurity awareness	0.086	0.066	0.099	1.299	.003

Table 4 shows the contribution of each of the predictor variable to the prediction of risk in technology environment. Internet safety ($\beta = 0.823$; t (98) = 10.816; $p < .05$) contributed most significantly to the prediction model for risk in technology environment at 0.05 level followed by cybersecurity awareness ($\beta = 0.099$; t (98) = 1.299; $p < .05$).

Discussion of Findings

The result on the profile of the respondents used in the study indicates that there are more respondents who are of age 16-20 years than other age bracket. There are more female respondents than male respondents. The results also shows that majority of the respondent maintain high level of internet safety while few moderate and only a few low level of internet safety. Majority have level of cybersecurity awareness, few moderate and low level of cybersecurity awareness. The result of this study is in line with that of Gamreklidze (2014) who found that there is a growing rate of technologies in the 21st century most especially IT channels however, the results did not agree with that of Kim (2013) who argued that, counter intuitively; it is the heavy users of digital devices who are usually the least knowledgeable and aware of cyber security issues and prevention.

The finding on joint influence of student internet safety and cybersecurity awareness on risk in technology environment revealed that there a linear relationship between predictor variables: internet safety and cybersecurity awareness and the dependent variable (risk in technology environment). This means that the variation in risk in technology environment accounted for by the predictor variables: internet safety and cybersecurity awareness is more and it is statistically significant. The finding of this study does not tally with that of Kim (2013) who reported that, counter intuitively; In general, it is the frequent users of digital devices who are least informed and least aware of cybersecurity issues and keeping. Although concern for the protection of the physical body, assets and space is ordinary for certain individual, concern for the protection of information and assets in cyberspace is not ordinary in the real sense (Moallem, 2017).

The result on relative influence of student internet safety and cybersecurity awareness on risk in technology environment showed that the two predictors contribution to the prediction of risk in technology environment. The result of this study agrees with that of Senthilkumar and Easwaramoorthy (2017) who found out that there are more students who are take care of common attacks from viruses and employ defense from it by keeping it tune to newest version or another platforms that guard their system from virus attacks which prevent risks in technology environment.

CONCLUSION

The study established that there more users of high level of internet safety and cybersecurity awareness than the moderate and low level of internet safety and cybersecurity awareness. The study also established a significant influence of internet safety and cybersecurity awareness on risk in technology environment. The study concluded that college students maintain high level of internet safety and cybersecurity awareness. Although some of the internet safety measures are not well observed as they were considered not necessary by the respondents. It is therefore recommended that all safety measures must be taken seriously and watchful by college students, as well as other technology users. Also, college student should maintain their level of cybersecurity awareness as it is key and germane to risk in technology environment.

REFERENCES

Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. *Science Proceeding Series, 2*(1), 82-86.

Chelsea, A. S., & Sagaya, A. M. (2023). Awareness of cyber security among students in women's colleges with special reference to Coimbatore city. *International Journal of Creative Research Thought, 11*(4), 40-44.

Gamreklidze, E. (2014). Cyber security in developing countries: A digital divide issue—the case of Georgia. *Journal of International Community, 20,* 200–217.

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security, 11,* 74–83.

Green, M. J. S. (2015). *Cyber security: An introduction for non-technical managers.* Ashgate Publishing.

Jinadu, A. T. (2024) Science teachers preparedness for artificial intelligence in practical instruction control and delivery Oyo state public secondary schools. *American Journal of IR 4.0 and Beyond, 3*(1), 44-49 https://doi.org/10.54536/ajirb.v3i1.3488.

Jinadu, A. T. (2024). Automated control and delivery system for science practical instructions to public schools. *Journal of Learning Theory and Methodology, 5*(2), 70-75. https://doi.org/10.17309/jltm.2024.5.2.04.

Jinadu, A. T., Akere, O. M., & Balogun, R. T. (2023). Post COVID-19: New breakthroughs and the future of behavioural research data collection. *Interdisciplinary Journal of Sociality Studies, 3,* 10-18. https://doi.org/10.38140/ijss-2023.vol3.02a.

Kim, E. B. (2013). Information security awareness status of business college: A global perspective of undergraduate students. *Information Security Journal, 22*(4), 171-179.

Kimple, L. D., Walrave, M., Ponnet, K., & Ouytsel, J. V. (2019). *Internet safety.* John Wiley & Sons. https://doi.org/10.1002/9781118978238.ieml0093

Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). *Risks and safety on the internet: The perspective of European children. Full findings.* EU Kids Online, LSE, London.

Moallem, A. (2017). Do you really trust "privacy policy" or "terms of use" agreements without reading them? In *Advances in Human Factors in Cybersecurity* (pp. 290-295). Springer.

Moallem, A. (2019). Cyber security awareness among college students. In *Advances in Human Factors in Cybersecurity* (pp. 79-87). Advances in Intelligent Systems and Computing. https://doi.org/10.1007/978-3-319-94782-2_8

National Institute of Standards and Technology (NIST). (2022). *Computer security: Risk management guide for information technology systems. Recommendations of the National Institute of Standards and Technology.* Special Publication 800-30.

Samaher, A., & Al-Shourbaji, I. (2016). A study of cyber security awareness in educational environments in the Middle East. *Information Knowledge Management, 15,* 1650007. https://doi.org/10.1142/S0219649216500076

Senthilkumar, K., & Easwaramoorthy, S. (2017). A survey on cyber security awareness among college students in Tamil Nadu. *IOP Conference Series: Materials Science and Engineering, 263*(3), 19-24.

Slusky, L., & Partow-Navid, P. (2014). Students' information security practices and awareness. *Journal of Information Privacy and Security, 11*(2), 3-26. http://www.tandfonline.com/doi/abs/10.1080/15536548.2012.10845664