Impact of Awareness of Cybersecurity among Tertiary Institution Students in Enugu State, Nigeria

[1]Adesegun Osijirin; [2]Victor Utibe Edmond; [1]Shamsudeen Mohammed

[1]Department of Health Care Management, Federal University of Allied Health Sciences, Enugu
[2]Department of Health Information Management, Federal University of Allied Health Sciences, Enugu

Abstract: Cybersecurity awareness is crucial in today's digital age, especially among tertiary institution students who heavily rely on technology for academic and personal activities. This study investigates the level of cybersecurity awareness among students in tertiary institutions in Enugu State, Nigeria, and examines its impact on their online behavior and security practices. Using a mixed-methods approach, data were collected through structured questionnaires and interviews involving 300 students across three major institutions. Findings reveal a moderate level of awareness, with significant gaps in understanding phishing, password security, and data privacy. The study highlights the need for targeted cybersecurity education programs to strengthen students' digital safety practices.

Keywords: Cybersecurity Awareness, Tertiary Institutions, Enugu State, Nigeria, Digital Security, Student Behavior.

I. INTRODUCTION

In the increasingly interconnected digital world, cybersecurity has become a critical concern, especially among youth populations who are prolific users of the internet. Tertiary institution students frequently engage in online academic research, social networking, and e-commerce, exposing themselves to various cyber threats. Despite growing global awareness of cybersecurity risks, many students in developing countries, including Nigeria, remain vulnerable due to limited exposure to cybersecurity education.

This study aims to assess the level of cybersecurity awareness among tertiary institution students in Enugu State, Nigeria, and explore how awareness impacts their online safety practices. The research is motivated by the increasing rate of cyber incidents affecting students, including identity theft, phishing scams, and data breaches.

➢ *Objectives:*
- To assess the level of cybersecurity awareness among tertiary students.
- To examine the relationship between cybersecurity awareness and students' online safety practices.
- To identify gaps in knowledge and recommend strategies for improvement.

II. LITERATURE REVIEW

➢ *Cybersecurity Awareness and Education*
Cybersecurity awareness refers to the understanding of potential cyber threats and the adoption of safe practices to mitigate risks. Studies by Abawajy (2014) and Alotaibi (2020) highlight that education and training significantly improve users' cybersecurity practices.

➢ *Cybersecurity in Nigerian Tertiary Institutions*
Previous studies (Olabode & Olatunji, 2018) have revealed that many Nigerian tertiary institutions lack structured cybersecurity education programs, leaving students vulnerable. While some institutions integrate basic ICT courses, they often fail to address practical cybersecurity concerns.

➢ *Students' Online Behavior and Risks*
Students are prime targets for cybercriminals due to their frequent use of social media, online banking, and academic portals. A study by Chukwuma (2021) found that 63% of Nigerian university students had fallen

victim to at least one form of cyber-attack, largely due to poor awareness and negligence.

III. METHODOLOGY

> *Research Design*

This study employed a mixed-methods approach, combining quantitative surveys with qualitative interviews to provide a comprehensive analysis of cybersecurity awareness.

> *Population and Sampling*

The study targeted students from three major tertiary institutions in Enugu State:
- University of Nigeria, Enugu Campus (UNEC)
- Enugu State University of Science and Technology (ESUT)
- Federal University of Allied Health Sciences, Enugu

A stratified random sampling technique was used to select 300 students (100 from each institution), ensuring diversity across faculties and academic levels.

> *Data Collection Instruments*

A structured questionnaire with sections on demographic data, cybersecurity knowledge, and online practices.
In-depth interviews with 15 students to gain deeper insights into their experiences with cyber threats.

> *Data Analysis*

Quantitative data were analyzed using SPSS (Statistical Package for Social Sciences) with descriptive and inferential statistics (chi-square tests and regression analysis). Qualitative data from interviews were analyzed thematically.

IV. RESULTS

> *Demographic Profile*

Table 1 Presentation of Results (Gender)

Gender	
Male	55%
Female	45%
TOTAL	100%

Table 2 Presentation of Results 9 (Age)

Age Range	
18–25 years	78%
26–30 years	22%
TOTAL	100%

Programmes of Study: Diverse faculties including Sciences, Arts, Engineering, and Health Sciences

> *Cybersecurity Awareness Levels*

Table 3 Cybersecurity Awareness Levels

Cybersecurity awareness level	
High Awareness	28%
Moderate Awareness	46%
Low Awareness	26%
TOTAL	100%

> *Knowledge of Specific Cyber Threats*

Table 4 Knowledge of Specific Cyber Threats

Knowledge of Specific Cyber Threats	
Phishing Awareness	35%
Password Security Best Practices	42%
Data Privacy (e.g., GDPR awareness)	20%
TOTAL	100%

> *Online Safety Practices*

Table 5 Online Safety Practices

Knowledge of Specific Cyber Threats	
Regular password changes	38%
Use of two-factor authentication (2FA):	27%
Cautiousness with suspicious emails:	41%
TOTAL	100%

> *Relationship between Awareness and Online Practices*

Chi-square tests indicated a significant positive relationship between high cybersecurity awareness and safe online practices ($p < 0.05$).

V. DISCUSSION

The findings reveal that while a majority of students have moderate awareness of cybersecurity issues, there are significant knowledge gaps, especially concerning phishing scams and data privacy regulations. The limited use of strong security measures like 2FA and password managers indicates a need for targeted interventions.

The study aligns with Chukwuma (2021), confirming that Nigerian students face substantial risks due to inadequate cybersecurity knowledge. Interestingly, students in science and engineering faculties showed higher awareness compared to those in arts and social sciences, suggesting that curriculum exposure plays a role.

VI. CONCLUSION

This study underscores the importance of improving cybersecurity awareness among tertiary institution students in Enugu State, Nigeria. Given their heavy reliance on digital platforms, students must be equipped with the knowledge and tools to protect themselves from evolving cyber threats.

RECOMMENDATIONS

In view of the findings, the following recommendation were made:
- Integrate comprehensive cybersecurity education into general ICT courses.
- Conduct regular workshops and seminars on cyber threats and safe practices.
- Encourage institutions to implement policies mandating the use of 2FA and secure academic portals.

REFERENCES

[1]. Abawajy, J. (2014). User preference of cybersecurity awareness delivery methods. Behaviour & Information Technology, 33(3), 237-248.
[2]. Alotaibi, S. (2020). The impact of cybersecurity education on student behavior. Journal of Information Security, 11(2), 102-115.
[3]. Chukwuma, P. (2021). Cybersecurity awareness among Nigerian university students: A survey. African Journal of Information Systems, 13(4), 88-101.
[4]. Olabode, A., & Olatunji, F. (2018). Evaluating cybersecurity practices in Nigerian universities. International Journal of Cybersecurity, 9(2), 65-77.