Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Knowledge, Attitudes, and Behavioral Risk Patterns Associated with Cybercrime Involvement Among Nigerian University Undergraduates

ADEDEJI ABDULRAHMON ALAYANDE

alayandedeji@gmail.com

University of Ibadan

ADEBISI OLUWAJUWON ADENIRAN

Osun State University

TAIWO DORCAS ADEBOWALE

Osun State University

DAMILARE ADEOLU OLAWUNI

University of Ibadan

MARVELLOUS ADEOLA ADEDEJI

Atiba University

HABEEBULAH ABDULLAHI

ITMO University

Research Article

Keywords: Cybercrime, Knowledge, Attitude, mental health, Nigeria

Posted Date: May 22nd, 2026

DOI: https://doi.org/10.21203/rs.3.rs-9467639/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

KNOWLEDGE, ATTITUDES, AND BEHAVIORAL RISK PATTERNS ASSOCIATED WITH CYBERCRIME INVOLVEMENT AMONG NIGERIAN UNIVERSITY UNDERGRADUATES

BY

ALAYANDE ADEDEJI ABDULRAHMON[1]., ADEBISI OLUWAJUWON ADENIRAN[2]., ADEBOWALE TAIWO DORCAS[2]., OLAWUNI DAMILARE ADEOLU[1]., ADEDEJI MARVELLOUS ADEOLA[3]., ABDULLAHI HABEEBULAH[4]

Address:

1. Department of Epidemiology and Medical Statistics, Faculty of Public Health, College of Medicine, University of Ibadan, Ibadan, Oyo State, Nigeria.
2. Department of Public Health, Faculty of Basic Medical Sciences, College of Health Sciences, Osun State University, Osogbo, Osun State, Nigeria.
3. Department of Public Health, Faculty of Health Sciences, Atiba University, Oyo Town, Oyo State, Nigeria.
4. Department of Public Health Sciences Institute of International Development and Partnership, ITMO National Research University, Russia.

Correspondence to:

Alayande Adedeji Abdulrahmon, Department of Epidemiology and Medical Statistics, Faculty of Public Health, College of Medicine, University of Ibadan, Oyo State, Nigeria.

Email address: alayandedeji@gmail.com;

Telephone: 09168663904

Abstract

Background: Cybercrime is increasingly perpetrated across all age groups; however, young people remain disproportionately involved, with rising participation over time. This trend presents a growing public health concern, given its associated psychological distress, financial harm, and broader social consequences. Investigating cybercrime among youth is therefore essential for informing preventive strategies and interventions that protect mental and psychosocial well-being. This study assessed the knowledge, attitudes, and practices related to cybercrime, as well as factors influencing its practice among undergraduate students of Osun State University.

Methods: A descriptive cross-sectional study of 423 undergraduates ages 15-29 years in a tertiary institution, recruited using a multi-stage sampling technique. A self-administered questionnaire was used to collect data from the study respondents. Data collected from the research were processed and analyzed using Statistical Product and Service Solutions (SPSS) Version 23.0. Descriptive statistics using means, SD, frequency tables, percentages, and charts were used to report frequencies of the variables. Chi-square test, Fisher's exact test, and binary logistic regression were used to determine the factors influencing respondents' involvement in cybercrime. The level of statistical significance was set at a p-value <0.05 with a 95% CI.

Results: The prevalence of cybercrime practice amongst the study respondents ranged from (2.8%) to (36.6%). About 2/3 (63.6%) of the respondents had good knowledge of cybercrime, while 30.50% had fair knowledge, and (5.90%) had poor knowledge. The majority (84.4%) of the respondents had a negative attitude (did not support) towards cybercrime, while (15.6%) were in support of cybercrime; (6.9%) of the respondents practiced cybercrime. Respondents with a side business are less likely to practice cybercrime (OR=0.36; P=0.029), and those with a positive attitude towards cybercrime were very likely to engage in cybercrime (OR=11.55; p =0.001).

Conclusion: Most respondents demonstrated good knowledge of cybercrime and expressed negative attitudes toward its practice. Despite this, efforts to discourage engagement should be strengthened within the school community, particularly in tertiary institutions, as part of broader public health strategies to reduce crime and its associated social and psychological impacts in Nigeria and beyond.

Keywords: Cybercrime, Knowledge, Attitude, mental health, Nigeria.

Introduction

The rapid expansion of Information and Communication Technology (ICT) has transformed communication, education, commerce, and social interaction globally. However, alongside these benefits, ICT has facilitated the emergence of cybercrime criminal activities conducted using computers, digital devices, or internet networks. Cybercrime encompasses a wide range of offenses, including unauthorized access, identity theft, fraud, phishing, malware attacks, and cyberstalking [1, 2]. These crimes may target computer systems directly or use digital platforms as tools to perpetrate illegal acts.

Globally, the increasing reliance on internet-based systems has been accompanied by a corresponding rise in cybercrime. Evidence suggests that cybercrime victimization has surpassed conventional crime in several countries, with significant financial and social consequences [3]. For instance, cybercrime cost the global economy approximately $600 billion in 2018, while billions of personal records have been compromised through large-scale data breaches [4]. High-profile incidents, including ransomware attacks and data breaches affecting major corporations, further highlight the scale and evolving sophistication of cyber threats.

In Nigeria, growing internet penetration and digital adoption across sectors such as banking, education, healthcare, and e-commerce have increased both opportunities and vulnerabilities. While these technologies enhance efficiency and productivity, they also expose individuals and institutions to cyber risks. Nigeria has been identified as one of the countries significantly affected by cybercrime, with a notable proportion of internet users contributing to fraudulent activities [5]. Studies indicate that cybercrime is particularly prevalent among young people, especially those aged 18–30 years, many of whom are students in tertiary institutions [6,7].

Cybercrime is increasingly recognized as a public health concern due to its wide-ranging social, economic, and psychological consequences [8]. Beyond financial losses, victims often experience stress, emotional distress, depression, and reduced well-being, as well as financial strain and reduced quality of life, especially in cases involving financial fraud and identity theft, all of which can negatively affect overall health [9]. These adverse outcomes are occurring within the context of a rapidly increasing global mental health burden, with over one billion people currently living with mental health conditions worldwide [10]. Suicide, a severe consequence of mental health deterioration, accounts for more than 720,000 deaths annually and is among the leading causes of

death among young people aged 15–29 years globally. This burden is disproportionately higher in low- and middle-income countries, where approximately 73% of global suicide deaths occur [11]. In Nigeria, mental health challenges are increasingly recognized as a major public health concern, with estimates suggesting that up to 20% of the population may be affected by mental disorders, which are often linked to socioeconomic factors and insecurity [12, 13]. Furthermore, recent evidence indicates a rising trend in suicidal behaviors, particularly among young people, driven by socio-economic stressors and exposures to cybercrime such as online fraud [14].

Although these outcomes are well documented, preventive efforts require an understanding of behavioral factors such as knowledge, attitudes, and practices. Among undergraduates, who are frequent users of digital technologies, these factors may influence both susceptibility to victimization and engagement in cybercrime-related activities. Therefore, this study assessed the level of knowledge, attitudes, and prevalence of cybercrime practices, as well as the factors influencing such practices among undergraduate students of Osun State University.

Methods

Study Area: This study was conducted at Osun State University, a multi-campus public institution located in Osun State. The state capital is Osogbo, and Kwara State borders the state to the north, Ekiti State and Ondo State to the east, Ogun State to the south, and Oyo State to the west. Established in 2006, Osun State University operates across six campuses distributed within the state's geopolitical zones. The university comprises colleges located in Ejigbo (Agriculture), Ifetedo (Law), Ikire (Humanities and Culture), Ipetu-Ijesa (Education), and Okuku (Social Sciences). At the same time, the main campus at Oke-Baale hosts the Colleges of Science, Engineering and Technology, and Health Sciences. The institution has an estimated student population of approximately 15,000 across all campuses.

Study Design and Duration: A descriptive cross-sectional study conducted between the periods of June and October 2022, among 423 undergraduates of Osun State University.

Eligibility Criteria: Respondents who have completed at least one academic session in Osun State University, and whose consent to participate in the study has been obtained, were included in this

study. However, respondents who cannot participate in the study due to illness or other health conditions were excluded.

Sample Size Determination: With a 50% proportion of cybercrime practice adapted from [15], a total of 423 undergraduates were recruited after adjusting for a 10% non-response rate, using Leslie Fisher's formula [$n = Z^2\ pq/d^2$] for estimating proportions in a population > 10,000. Where:

n = required sample size
z = standard normal deviate (1.96 at 95% CI)
p = prevalence of cybercrime (50%)
q = 1-p
d = margin of error

Sampling Technique

A multistage sampling technique was employed to select study participants.

At the first stage, two out of the six campuses of Osun State University (Okuku and Osogbo) were selected using simple random sampling (balloting). The Osogbo campus comprises two colleges (College of Science, Engineering and Technology, and College of Health Sciences), while the Okuku campus houses the College of Management and Social Sciences.

In the second stage, two faculties were selected from each college using simple random sampling, resulting in a total of six faculties.

In the third stage, two departments were randomly selected from each faculty, yielding a total of twelve departments.

In the final stage, a list of students in each selected department (stratified by level of study) served as the sampling frame. Students were then selected using simple random sampling. Proportional allocation was applied to determine the number of participants recruited from each department based on the size of the student population in each stratum.

Data Collection Methods and Classification

A pre-tested, semi-structured, self-administered questionnaire partly adapted from [15] was used to obtain information from the respondents in this study. The self-administration enabled the respondents to feel free in expressing their perspectives and opinions on the subject matter. The questionnaires were administered to the students in their various Faculties during school hours by the researchers, and consisted of four (4) sections as follows:

Section A: Socio-demographic characteristics of study respondents, which collected information on variables such as respondents' age, Sex, Religion, Tribe, Study level, Monthly Income or allowance, and Fathers' and mothers' educational and employment status.

Section B: Respondents' knowledge of cybercrime was assessed using a 10-item questionnaire with response options of "Yes," "No," and "Not sure." Each correct response (items Q21–Q30) was scored 1, while incorrect or "Not sure" responses were scored 0. Total scores ranged from 0 to 10 and were categorized as poor (0–3), fair (4–7), or good (8–10) knowledge.

Section C: Respondents' attitudes toward cybercrime were assessed using a 5-point Likert scale ranging from "Strongly Agree" to "Strongly Disagree." Responses were dichotomized, with appropriate (non-supportive) attitudes scored as 1 and inappropriate (supportive) attitudes scored as 0. Total scores ranged from 0 to 5 and were categorized as positive attitude (0–2), indicating support for cybercrime, and negative attitude (3–5), indicating non-support for cybercrime.

Section D: Respondents' involvement in cybercrime was assessed using a 10-item questionnaire with response options of "Yes", "No", and "Prefer Not to Answer". Each response was simply presented as a pattern of cybercrime involvement based on the type of cybercrime act each respondent said "yes" to.

Pre-Test Study

To ensure that the research instrument maintained consistency in measuring what it intended to measure, 10% (43) of questionnaires were pre-tested at Fountain University, Osogbo, Osun state. The pre-test results showed a high degree of internal consistency, suggesting that the questionnaire was sufficiently dependable. Experts in the field also evaluated the questionnaire's validity and verified that it was suitable for the study.

Data Management and Analysis

Data collected were checked for completeness, coded, and entered into IBM SPSS Statistical Software for analysis. Data cleaning was performed to identify and correct errors and inconsistencies before analysis. Descriptive statistics such as mean, standard deviation (SD), frequencies, and percentages were used to summarize respondents' sociodemographic characteristics and study variables (knowledge, attitude, and involvement level), and results were presented in tables and charts.

Inferential analysis was conducted using the Chi-square (χ^2) test and Fisher's exact test (for cells with value less than 5) to examine associations between categorical variables, including knowledge, attitude, and involvement in cybercrime. Statistical significance was determined at a 95% confidence level ($p < 0.05$).

Binary logistic regression analysis was performed to identify factors associated with involvement in cybercrime. Only variables that were statistically significant at the bivariate level were included in the multivariable model, and results were reported as odds ratios (ORs) with 95% confidence intervals.

Results

Table 1 shows the socio-demographic characteristics of the study respondents. There was a total of 423 respondents, of which 230 (54.4%) were females, while 193 (45.6%) were males. About one-half, 217 (51.3%) of the respondents were aged 15-19 years (adolescent), 181 (42.8%) were aged 20-24 years, while only very few of them, 25 (5.9%) were between 25 and 29 years. About 2/5 of the respondents, 179 (42.3%), were from the Faculty of Basic Medical Sciences. The majority were Christians, 296 (70%), while 124 (29.3%) were Muslims, and 3 (0.7%) were traditional religion worshipers. Most 414 (97.9%) of the respondents were single, with the majority of their fathers and mothers married 406 (96%) and 411 (97.2%) respectively. Most 386 (91.3%) of the respondents were Yoruba, and in terms of mothers' and fathers' education, the majority of the respondents' parents had attained tertiary education. It was also observed that about 3/4 (77.1%) came from monogamous families. Moreover, about four-fifths of the respondents had

cordial relationship with their fathers 341 (80.6%) and with their mothers 377 (89.1%). More than half of the respondents 231 (54.6%) were receiving 5,000-20,000 as their monthly allowances. Majority 254 (60%) of the respondents said their monthly allowances was not enough to meet their needs. About a third, 138 (32.6%) of the respondents had side jobs.

Table 2 presents the respondents' knowledge of cybercrime among 423 undergraduates. All respondents (100%) reported awareness of the term "cybercrime." A majority (83.9%) correctly identified that cybercrime evolves with technological advancement, and most (85.8%) recognized that a cybercriminal is anyone who unlawfully intrudes into a computer system with malicious intent. However, some misconceptions were observed. While most respondents (83.5%) correctly disagreed that only males commit cybercrime, a considerable proportion still held incorrect beliefs regarding offenders' demographics, with 74% disagreeing that cybercriminals are not usually teenagers or adults. Similarly, 72.1% disagreed that cybercriminals are not students, lecturers, civil servants, or other professionals. Furthermore, 79.9% correctly acknowledged that cybercrime can lead to exploitation of individuals, groups, and institutions. In addition, 83.5% agreed that student involvement in cybercrime can expose other undergraduates to cyberbullying. However, responses were more divided on certain items, such as whether cybercriminals commit forgery using computers for legitimate purposes, where 50.1% answered "Yes" and 41.8% answered "No," indicating mixed understanding.

Figure 1 shows that nearly 2/3 (63.6%) of the respondents had good knowledge of cybercrime, while 30.5% and 5.9% had a fair and poor knowledge of cybercrime, respectively.

Table 3 shows that the majority, i.e., 357 (84.4%) of the respondents agreed that undergraduates of higher institutions caught in the act of cybercrime should be tried in the court of law and punished by appropriate legislation, while a total of 66 (15.6%) of the respondents were either undecided or disagreed. In addition, 58 (13.7%) agreed that undergraduates of higher institutions caught in the act of cybercrime should be set free and not punished by appropriate legislation, while most, i.e., 333 (79.2%) disagreed, and 32 (7.6%) were not sure about it. About one-tenth 41 (9.7%) agreed that Students who abandon their studies to get fully involved in cybercrime are on the right path, while most 344, 81.3%) disagreed, and 38 (9%) were not sure. Furthermore, only 51 (12%) of the respondents agreed that cybercrime should be a generally accepted side job for students while in the University in order to meet their needs and make a living, while about ¾ 348

(82.3%) disagreed, and 24 (5.7%) were not sure. Finally, about one-fifth 101 (23.8%) agreed that undergraduates who forge documents and certificates using the computer system should be apprehended by the law, 295 (69.8%) disagreed, while 27 (6.4%) were not sure about it.

Figure 2 shows that 357 (84.4%) of the study respondents had a negative attitude (i.e., they did not support involvement in cybercrime) towards cybercrime, while 66 (15.6%) supported involvement in cybercrime.

Table 4 shows that a total of 155 (36.6%) of the respondents have intentionally had a virus or other harmful software on their phones or laptops, while the majority of 268 (63.4%) had not. A total of 19 (4.5%) had created a virus or other harmful software and distributed it online, while most 404 (95.5%) represented a greater proportion that had not. In addition, 27 (6.4%) of the respondents had tried to hack or had hacked into someone else's computer. The majority, 396 (93.6%) of the respondents had not. Likewise, 23 (5.4%) of the respondents had carried out a fraud online, and the other person/organization lost money. A total of 400 (94.6%) had not. Further findings showed that 12(2.8%), 16 (3.8%), 38 (9%), 33 (7.8%), 13 (3.1%) and 32 (7.6%) of the respondents had been involved in cybercrime activities while most i.e, 411 (97.2%), 407 (96.2%), 377 (89.1%), 390 (92.2%), 410 (96.9%), 391 (92.4%) of the respondents had not.

Figure 3 shows that the prevalence of cybercrime ranged from (2.8%) to (36.6%) across all the cybercrime-engaged activities.

Table 5 shows the relationship between the socio-demographic characteristics and knowledge of the study respondents on cybercrime. A higher proportion (70.5%) of the male respondents had good knowledge of cybercrime when compared with the female (57.8%), and thus the difference is statistically significant ($\chi^2 = 7.544$, p=0.023). Also, respondents between the age group 25-29 years had good knowledge of cybercrime (80%) when compared with the other age groups, and thus the differences are statistically significant (X^2=9.657, p=0.008). The majority (85%) of the respondents from the faculty of engineering had good knowledge when compared with the other faculties, and thus the differences are statistically significant (X^2=78.471, p<0.001). Also, respondents who are Christians happen to have good knowledge of cybercrime (65.9%), and thus the differences are statistically significant (X^2=11.556, p=0.021). Furthermore, respondents whose mother and father attained primary education had good knowledge (75%) and (79.2%) respectively, when compared with the others, and thus the differences are statistically significant

(X^2=29.898, p<0.001) and (X^2=26.924, p<0.001). Respondents who had a terrible relationship with their mother had good knowledge (100%) when compared with the others, and thus the differences are statistically significant (X^2=17.715, p=0.023). Also, respondents who received 61000-80000 has their monthly had good knowledge of cybercrime (100%) when compared with the others, and thus the differences are statistically significant (X^2=29.898, p= 0.002). Other socio-demographic characteristics have no statistically significant relationship with respondents' knowledge of cybercrime.

Table 6 shows that a higher proportion of the respondents from the faculty of engineering (96.3%) had a negative attitude towards cybercrime when compared with the others, and thus the differences are statistically significant (X^2=47.345, P=0.001). Also, the majority (91.7%) of the respondents whose mother had attained primary education had a negative attitude towards cybercrime when compared with the others, and thus, the differences are statistically significant (X^2=11.186, P=0.011). Also, respondents who received 61000-80000 has their monthly had negative attitude towards cybercrime (100%) when compared with the others, and thus the differences are statistically significant (X^2=12.585, P=0.013). A higher proportion (87%) of the study respondents who had no side business while studying are found to have a negative attitude towards cybercrime when compared with others, and thus the differences are statistically significant (X^2=4.555, P=0.033). No statistically significant relationship exists between other socio-demographic and categorized attitudes of the study respondents.

Table 7 shows that respondents who are traditional religion worshippers (100%) were involved in cybercrime more often than the other religious worshippers, and thus the differences are statistically significant (χ^2 = 16.716, p<0.001). Also, a higher proportion (53%) of the Igbo practiced cybercrime more often when compared with the other and thus the differences are statistically significant (X^2= 11.645, p=0.009). The majority (71%) of the respondents whose mother had attained primary education were involved in cybercrime more often when compared to the others, and thus the differences are statistically significant (X^2= 9.980, p=0.019). Also, respondents who received >80000 monthly (25%) were involved in cybercrime more often when compared with the others, and thus there is a statistically significant relationship (X^2= 19.691, p=0.001). Finally, respondents who had a side business while studying (13%) practiced cybercrime

more often than those without side businesses, and thus the differences are statistically significant (X^2= 12.281, p=0.001). Other socio-demographic characteristics had no statistically significant relationship with respondents' involvement in cybercrime.

Table 8: Respondents who had good knowledge and a negative attitude towards cybercrime (91.4%) were more than those with good knowledge and a positive attitude towards cybercrime (8.6%), and thus the differences are statistically significant (X^2=30.413, p<0.001).

Table 9: Respondents who had good knowledge and did not practice cybercrime (96.7%) are higher than those who had good knowledge and practice cybercrime, and thus, the difference is significant (X^2=14.802, p=0.001).

Table 10: Respondents who had a negative attitude towards cybercrime and did not practice cybercrime (97.2%) are higher than those who had a negative attitude and practiced cybercrime (2.8%). Likewise, respondents who had a positive attitude and did not practice cybercrime (71.2%) are higher when compared to those who had a positive attitude and practiced cybercrime (28.8%), and thus the differences are statistically significant (X^2=54.907, p<0.001).

Table 11 shows factors influencing involvement in cybercrime among the study respondents. Respondents who have no side business aside from school were less likely to get involved in cybercrime compared to those who do. (CI = 0.146 - 0.903; p=0.029; OR=0.363) and students who had a positive attitude of practicing cybercrime were 11.552 times more likely to practice cybercrime compared to those with a negative attitude (CI = 4.379 - 30.473; p<0.001).

Discussion

The present study provides important public health insight into cybercrime as a growing behavioural risk among young people in tertiary institutions. The findings revealed a predominantly young population, largely adolescents and young adults, consistent with the demographic group most vulnerable to risky digital behaviours globally. The high proportion of respondents reporting insufficient monthly allowance and engagement in side jobs highlights underlying socio-economic pressures that may predispose youths to maladaptive coping strategies, including cybercrime. Similar observations have been reported in Nigeria and other low- and

middle-income countries, where economic strain and youth unemployment are strongly linked to engagement in cyber-related fraud and other online deviant behaviours [10,16]. The study demonstrated a high level of awareness and knowledge of cybercrime, with all respondents having heard of the concept and a majority demonstrating good knowledge. This aligns with findings from Nigerian and international studies, such as that of Abanikannda and Tata [15,17], where the investigators consistently report high awareness levels of cybercrime among university students due to increased internet penetration and digital exposure. However, despite this high level of awareness, notable misconceptions persisted, particularly regarding the demographic profile of cybercriminals and the nature of cybercrime activities. This gap between general awareness and accurate knowledge has been widely documented and suggests that knowledge alone may not be sufficient to deter risky behaviour [18]. From a public health perspective, this reflects a classic knowledge–behaviour gap often seen in other risk domains such as substance use and sexual health, where awareness does not necessarily translate into protective behaviour.

Attitudinal findings revealed that the majority of respondents had negative attitudes toward cybercrime, with most supporting legal sanctions against offenders and rejecting cybercrime as an acceptable means of livelihood. This is consistent with previous studies conducted by Nwosu et al. (2017) and Uche & Uche (2023) among undergraduates in a Nigerian higher institution, where they found that while the respondents were aware of cybercrime and its consequences, many still morally disapprove of it [19, 20]. Nevertheless, a concerning minority expressed permissive attitudes, including acceptance of cybercrime as a survival strategy. This highlights the influence of socio-economic and environmental factors in shaping behavioural intentions. Public health theory suggests that attitudes are key determinants of behaviour, particularly within the framework of the Theory of Planned Behaviour, where favourable attitudes can significantly increase the likelihood of engagement in risky acts [21]. Despite the high level of knowledge and predominantly negative attitudes, the study found that a proportion of respondents were involved in cybercrime-related activities, with prevalence varying across behaviours. While more serious forms, such as hacking and fraud, were relatively low, less severe or indirect forms, such as exposure to malware, were more common. This pattern mirrors findings from other studies conducted by [22,23], which found that cybercrime exists along a continuum, with many youths engaging in low-level or opportunistic acts that may escalate over time. From a population health

perspective, even low levels of engagement are significant, as they indicate normalization of deviant digital behaviour within youth populations.

The observed association between socio-demographic factors and cybercrime-related outcomes further reinforces the role of structural determinants in shaping behaviour. Male respondents, older students, and those in technologically inclined faculties demonstrated higher knowledge levels, consistent with studies showing that digital literacy and exposure increase both awareness and capability for cyber activities [15]. Similarly, financial factors such as higher income and engagement in side jobs were significantly associated with cybercrime involvement. This finding supports existing literature, such as that of Reyns et al [24], where the investigators concluded that both financial need and financial opportunity can drive cybercrime behaviour among youths. The association between family background and cybercrime involvement also underscores the influence of early socialization and parental education on behavioural outcomes, a well-established concept in public health research.

A key finding of this study is the strong relationship between attitude and practice, with respondents who held positive attitudes toward cybercrime being significantly more likely to engage in such activities. This is consistent with behavioural science evidence demonstrating that attitudes are among the strongest predictors of behavioural intention and actual behaviour [17]. Additionally, students without side businesses were less likely to engage in cybercrime, suggesting that structured engagement and legitimate economic activities may serve as protective factors. This aligns with the social control theory, which posits that individuals with stronger ties to conventional activities are less likely to engage in deviant behaviour [25].

The interplay between knowledge, attitude, and practice observed in this study reflects a complex behavioural ecosystem where individual, social, and economic factors converge. Although good knowledge was associated with non-involvement in cybercrime, it did not eliminate risk, indicating that interventions must go beyond awareness creation to address underlying behavioural drivers. This is particularly important from a public health standpoint, where multi-level interventions targeting individual behaviour, social norms, and structural conditions are required to achieve meaningful impact. Cybercrime among undergraduates should therefore be conceptualized not merely as a criminal justice issue but as a public health concern with implications for mental health, economic stability, and societal well-being. Victims of cybercrime

often experience psychological distress, financial loss, and reduced quality of life, while perpetrators may face legal consequences, social stigma, and disrupted educational trajectories [26]. The normalization of cybercrime within youth populations also threatens broader societal trust and economic development, particularly in countries like Nigeria, where digital economies are rapidly expanding.

Conclusion

This study highlights that while knowledge of cybercrime is high and negative attitudes predominate among undergraduates, a non-negligible proportion of students remain engaged in cybercrime-related activities, driven by behavioural, socio-economic, and attitudinal factors. At the population level, this underscores the need for integrated public health interventions that address not only awareness but also behavioural change, economic empowerment, and digital ethics. Universities should incorporate cyber ethics and digital responsibility into curricula, while policymakers should strengthen youth-focused economic and social support systems to reduce vulnerability to cybercrime. Additionally, multi-sectoral collaboration between public health authorities, educational institutions, and cybersecurity agencies is essential to develop comprehensive prevention strategies. Addressing cybercrime among youths is critical not only for reducing criminal activity but also for safeguarding the mental, social, and economic health of the population, thereby contributing to sustainable development in Nigeria and beyond.

Limitation

Information bias cannot be ruled out as some respondents may have provided responses that they considered “ideal” especially in relation to their attitude towards, and practice in cybercrime. However, they were encouraged to provide honest responses to all the questions, as confidentiality was assured.

Declaration

Ethical approval:

The study protocol was reviewed and approved by the Health Research and Ethics Committee of the College of Health Sciences (CHS HREC), Osun State University (Approval number:

UNIOSUNHREC2022/PBH/015), in accordance with the National Code for Health Research Ethics. All procedures involving human participants were conducted in accordance with the ethical standards of the institutional research committee and with the 1964 Declaration of Helsinki and its subsequent amendments.

Consent to participate:

Written voluntary "individual informed consent" and parental/guardian consent for < 16 years were obtained from all respondents who participated in this study. Participants who wish to exit/withdraw from the study for any reason or other were granted the right to withdraw with no consequences or punishment. All information provided by the participants was handled with strict confidentiality. All procedures involving human participants were conducted in accordance with the ethical standards of the institutional research committee and with the 1964 Declaration of Helsinki and its subsequent amendments.

Consent to publish:

The data collected for this study include no known information that leads to the identification of the participants. However, the intention to publish was made known to the participants, and they agreed to it.

Data Availability Statement:

The datasets generated and analyzed for this study are available from the corresponding author upon reasonable request.

Funding Declaration:

No funding was received for this project. Therefore, all expensive was provided by the authors.

Clinical Trial Number:

Not Applicable

Conflict of Interest:

All authors declare no conflict of interest.

References

1. Mshana, J. A. (2015). Cybercrime: an empirical study of its impact in the society: a case study of Tanzania. *Huria: Journal of the Open University of Tanzania*, *19*(1), 72–87.
2. Sabillon, R., Cano, J., Cavaller, V., & Serra, J. (2016). Cybercrime and Cybercriminals: A Comprehensive Study. *International Journal of Computer Networks and Communications Security*, *4*(6), 165–176. www.ijcncs.org
3. Smith, T., & Stamatakis, N. (2020). Defining Cybercrime in Terms of Routine Activity and Spatial Distribution: Issues and Concerns. *International Journal of Cyber Criminology*, *14*(2), 433–459. https://doi.org/10.5281/zenodo.4769989
4. Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. *Current Psychiatry Reports*, *23*(4). https://doi.org/10.1007/s11920-021-01228-w
5. Omodunbi, B., Odiase, P., Olaniyan, O., & Esan, A. (2016). Cybercrimes in Nigeria: Analysis, Detection and Prevention. *FUOYE Journal of Engineering and Technology*, *1*(1). https://doi.org/10.46792/fuoyejet.v1i1.16
6. Oluwasanmi, A & Igbekoyi, E. (2018). Prevalence and Forms of Cybercrime Perpetrated By Students in Public Tertiary Institutions in Ekiti State. *International Journal of Economics, Business and Management Research*, *2*(04), 568–584. www.ijebmr.com
7. Udelue, M., & Bentina, M. (2017). *International Journal of Health and Social Inquiry, Vol.3, No.1, Nov 2017*. *3*(1), 152–169.
8. Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). *Cybersecurity in healthcare : A systematic review of modern threats and trends*. *25*, 1–10. https://doi.org/10.3233/THC-161263
9. Recio, P., Rico, A., & Manuel, D. (2019). Financial Fraud , Mental Health , and Quality of Life : A Study on the Population of the City of Madrid , Spain. *Financial Fraud , Mental Health , and Quality of Life : A Study on the Population of the City of Madrid ,*

Spain, 10–11.

10. World Health Organization. (2022). *World mental health report: Transforming mental health for all*. https://www.who.int/publications/i/item/9789240049338
11. World Health Organization. (2023). *Suicide*. https://www.who.int/news-room/fact-sheets/detail/suicide
12. Gureje, O., Lasebikan, V. O., Kola, L., & Makanjuola, V. A. (2020). Lifetime and 12-month prevalence of mental disorders in the Nigerian Survey of Mental Health and Well-Being. *The British Journal of Psychiatry, 188*(5), 465–471. https://doi.org/10.1192/bjp.bp.105.010405
13. Fashoto, O. Y., Ayangeaor, J. I., Akinkunmi, F., & Shongwe, N. (2025). *The Nigerian mental healthcare system and mental illness: A systematic review*. *Journal of Clinical & Medical Case Reports, Images, 2*(2). https://jcmcrimages.org/articles/JCMCRI-1052.pdf
14. Bamara NC, Ozongwu OE. The Rising Cases of Suicide among Nigerians: What Are the Risk Factors, Prevention, and Remedies? Consort Psychiatr. 2024 Aug 22;5(3):56-61. https://doi.org/10.17816/CP15497
15. Abanikannda, M. O. (2019). *Awareness and impact of cybercrime among selected university undergraduates in Nigeria*. SMCC Higher Education Research Journal, 1(1), 140–146**.** doi. 10.18868/sherjba.01.060119.12
16. Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2015). *Cybercrime and digital forensics: An introduction*. Routledge. https://www.researchgate.net/publication/314220073_Cybercrime_and_Digital_Forensics_An_Introduction
17. Tata, U. D. (2023). Investigating undergraduate students' levels of cybercrime awareness. *International Journal of Social Sciences and Education Studies, 12*(1), 19–39. https://doi.org/10.23918/ijsses.v12i1p19
18. Ngo, F. T., & Jaishankar, K. (2017). *Commemorating a decade in existence of the International Journal of Cyber Criminology: A research agenda to advance the scholarship on cyber crime*. *International Journal of Cyber Criminology, 11*(1), 1–9. https://www.cybercrimejournal.com/pdf/FawnjaiSAvol11issue1IJCC2017.pdf

19. Nwosu, Jonathan. C., Adebawojo Bolanle, Ifeoma Helen Ayeni, "Cybercrime and Computer Science Undergraduate Students in Private Universities in Nigeria: An Empirical Investigation," *International Journal of Computer Trends and Technology (IJCTT)*, vol. 51, no. 1, pp. 34-37, 2017. *Crossref*, https://doi.org/10.14445/22312803/IJCTT-V51P105

20. Uche, I., & Uche, O. (2023). Perceptions of undergraduates towards cybercrimes. *International Journal of Social Sciences and Humanities Invention, 10*(5), 7839–7852. https://valleyinternational.net/index.php/theijsshi/article/view/3924

21. Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

22. Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice, 38*(3), 227–236. https://doi.org/10.1016/j.jcrimjus.2010.02.002

23. Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Journal of Contemporary Criminal Justice, 32*(3), 263–280. https://doi.org/10.1177/1043986216652594

24. Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle-routine activities theory. *Criminal Justice and Behavior, 38*(11), 1149–1169. https://doi.org/10.1177/0093854811421448

25. Hirschi, T. (1969). *Causes of delinquency*. University of California Press. https://archive.org/details/causesofdelinque00hirs

26. Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal, 27*(1), 36–54. https://doi.org/10.1057/sj.2012.11

TABLES

Table 1: socio-demographic characteristics of study respondents (n=423)

Variable	Category	Frequency (n)	Percentage (%)
Age group (years) Mean (SD) =20 (±3)	15-19 years	217	51.3
	20-24 years	181	42.8
	25-29 years	25	5.9
Sex	Male	193	45.6
	Female	230	54.4
Faculty	FABAMS	179	42.3
	Engineering	80	18.9
	Social science	80	18.9
	FABAS	44	10.4
	Management science	32	7.6
	FACS	8	1.9
Religion	Christianity	296	70
	Islam	124	29.3
	Traditional	3	0.7
Marital status	Single	414	97.9
	Married	7	1.7
	Divorced	2	0.5

Variable	Category	Frequency (n)	Percentage (%)
Mothers' marital	Married	406	96
	Divorced	3	0.7
	Separated	4	0.9
	Cohabitating	2	0.5
	Widowed	8	1.9
Fathers' marital	Married	411	97.2
	Divorced	3	0.7
	Separated	4	0.9
	Cohabitating	1	0.2
	Widowed	4	0.9
Ethnicity	Yoruba	386	91.3
	Igbo	19	4.5
	Hausa	8	1.9
	Others	10	2.4
Mother's education	No formal education	52	1.2
	Primary	28	6.6
	Secondary	120	28.4
	Tertiary	270	63.8
Father's education	No formal education	5	1.2
	Primary	24	5.7
	Secondary	81	19.1
	Tertiary	313	74

Variable	Category	Frequency (n)	Percentage (%)
Family type	Monogamous	326	77.1
	Polygamous	97	22.9
Relationship between you and Father	Cordial	341	80.6
	We manage to get along	66	15.6
	Indifferent	7	1.7
	Terrible/bad	5	1.2
	Not applicable	4	0.9
Relationship between you and Mother	Cordial	377	89.1
	we manage to get along	32	7.6
	Indifferent	6	1.4
	Terrible/bad	1	0.2
	Not applicable	7	1.7
Monthly allowance	5000-20000	231	54.6
	20,000-40,000	104	24.6
	40,000-60,000	45	10.6
	60,000-80,000	7	1.7
	80,000 and above	38	8.5
Is your monthly allowance meets your needs	Yes	169	40
	No	254	60

Variable	Category	Frequency (n)	Percentage (%)
Do you have any side business or job while studying	Yes	138	32.6
	No	285	67.4
Main source of income	Parents	351	83
	Guidance/other relatives	22	5.2
	Business/side job	42	9.9
	Boyfriend or spouse	8	1.9
Have you ever been oppressed by friends or mates	Yes	141	33.3
	No	282	66.7
How often	Not at all	283	66.9
	Sometimes	58	13.7
	Always	82	19.4

Table 2: Knowledge of the study respondent on cybercrime (n=423).

Variable	Yes	No	Not sure
Are you aware of the term cybercrime	423(100%)	0(0%)	0(0%)
Cybercrime evolved and continue to evolve as a result of improved technology	355(83.9%)	35(8.3%)	33(7.8%)
Men/guys are only the committers of cybercrime	45(10.6%)	353(83.5%)	25(5.9%)
A cybercriminal is not usually a teenager or an adult	52(12.3%)	313(74%)	58(13.7%)
A cybercriminal is not usually a student, lecturer, civil servant, military man or self employed	59(13.9%)	305(72.1%)	59(13.9%)
A cybercriminal is anyone who intrudes any part of a computer with bad intention	363(85.8%)	36(8.5%)	24(5.7%)
A cybercriminal is anyone who commit forgery using the computer as a tool for good deeds	212(50.1%)	177(41.8%)	34(8%)
Cybercrime cannot lead to exploitation of individual, groups, organization, institution and the community at large	55(13%)	338(79.9%)	30(7.1%)
In recent times, excluding the general population, student in higher institution is not often involved in cybercrime	160(37.8%)	214(50.6%)	49(11.6%)
Student involvement in cybercrime can make some newly acquired undergraduates become victims of cyber-bullying	353(83.5%)	26(6.1%)	44(10.4%)

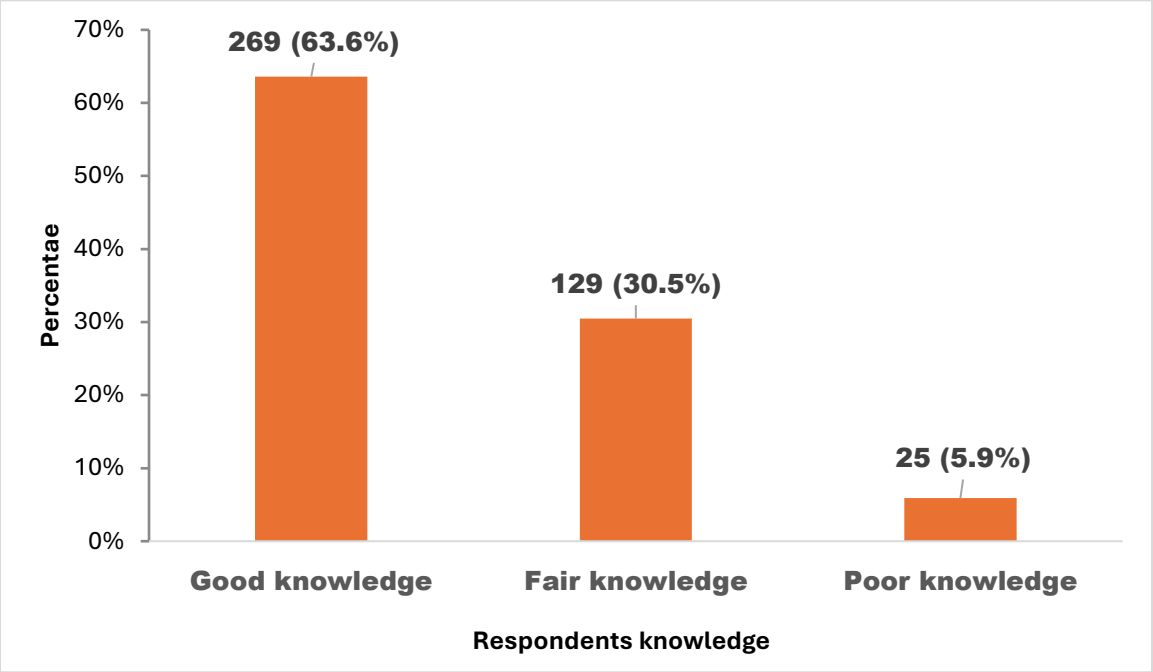

Fig. 1: Summarized knowledge of study respondents on cybercrime. (n= 423)

Table 3: Attitude of the study respondents towards cybercrime (n=423).

Variables	SA	A	U	D	SD
Undergraduate of higher institution caught in the act of cybercrime should be tried in a court of law and punished by appropriate legislation	244 (57.7%)	113 (267%)	36 (8.5%)	13 (3.1%)	17(4%)
Undergraduate of higher institution caught in the act of cybercrime should be set free and not punished by appropriate legislation	30(7.1%)	28(6.6%)	32(7.6%)	117(27.7%)	216(51.1%)
Students who abandon their studies to get fully involved in cybercrime are on the right path	21(5%)	20(4.7%)	38(9%)	122(28.8%)	222(52.5%)
Cybercrime should be a generally accepted side job for students while in the university in other to meet their needs and make a living	31(7.3%)	20(4.7%)	24(5.7%)	124(29.3%)	224(53%)
Undergraduates who forge documents (results) and certificates using the computer system should be apprehended by the law	62(14.7%)	39(9.2%)	27(6.4%)	98(23.2%)	197(46.6%)

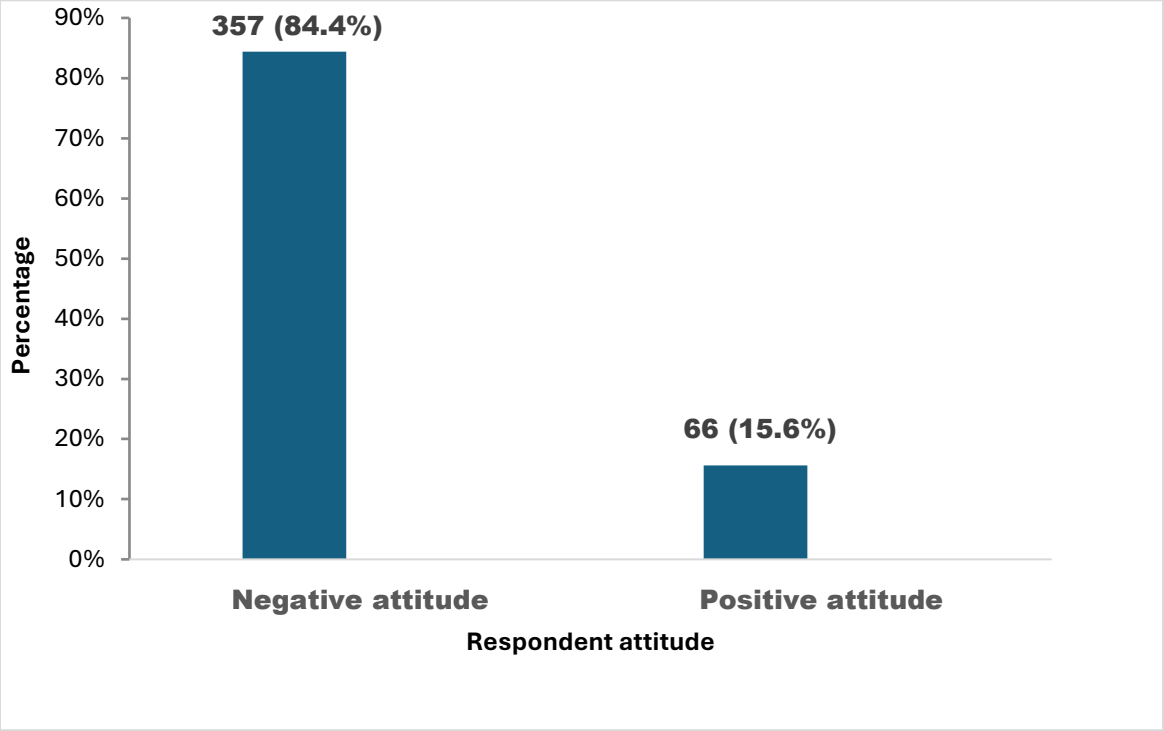

Fig. 2: Categorized attitude of study respondents towards cybercrime

Table 4: Respondents' involvement in cybercrime activities (n=423).

Variable	Yes	No	Prefer not to answer
I have had a virus or other harmful software on my phone/laptop	155(36.6%)	255(60.3%)	13(3.1%)
I have created virus or other harmful software and distributed it online	19(4.5%)	396(93.6%)	8(1.9%)
I have tried to hack or have hacked into someone else's computer	27(6.4%)	379(89.6%)	17(4%)
I have carried out a fraud online and the other person/organization lost money	23(5.4%)	389(92%)	11(2.6%)
I have taken a hospital or other health care Facilities data and then deploy a ransom ware Into the organization	12(2.8%)	400(94.6%)	11(2.6%)
I have shared naked pictures or videos of another Person (blackmail)	16(3.8%)	396(93.6%)	11(2.6%)
I have sent messages with sexual contents to someone older or younger than me	38(9%)	369(87.2%)	8(1.9%)
I have used someone else's bank details to wire money	33(7.8%)	382(90.3%)	8(1.9%)
I have once/always forged my semester result using online software	13(3.1%)	400(94.6%)	10(2.4%)
I have used another person's identity to commit fraud	32(7.6%)	378(89.4%)	13(3.1%)

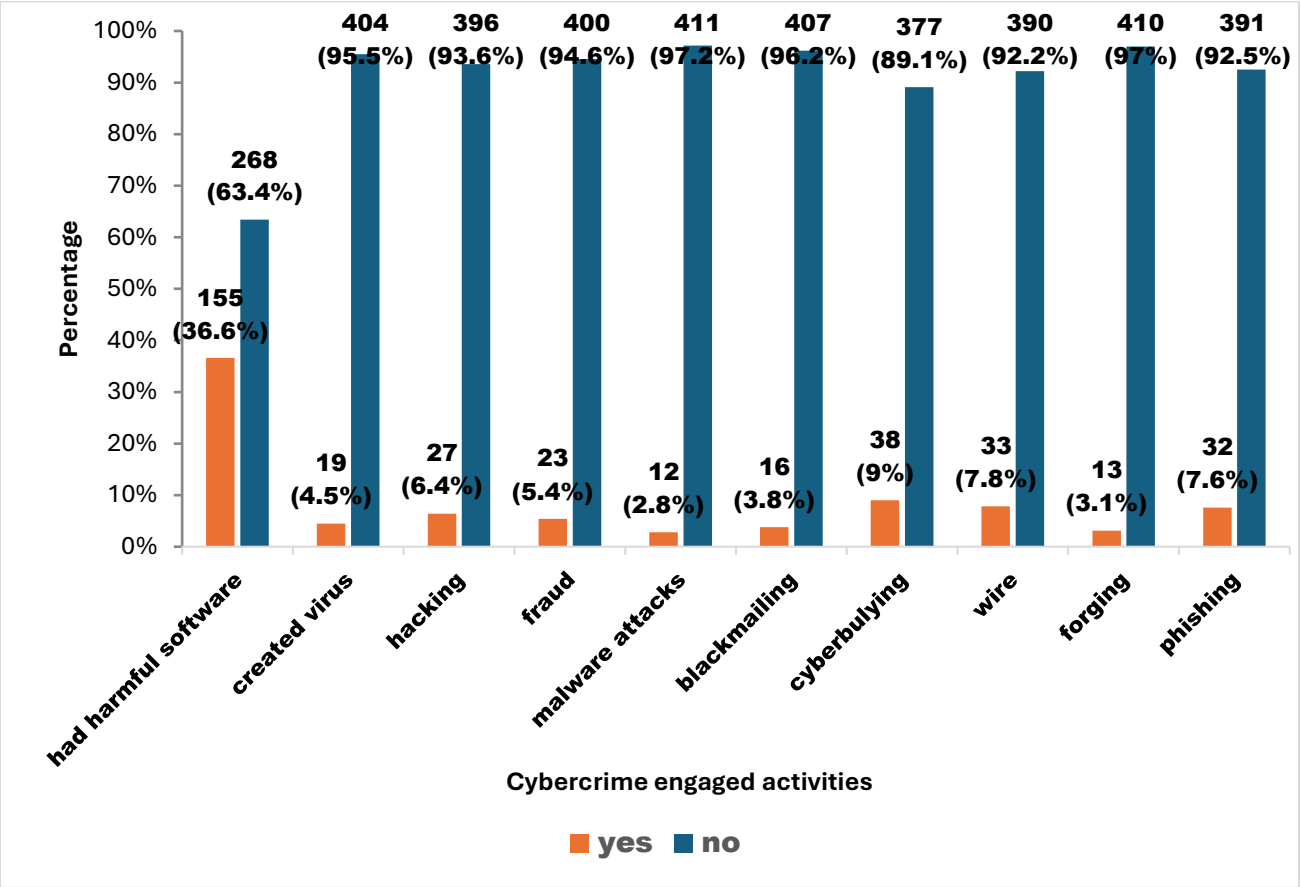

Fig. 3: Categorized pattern of cybercrime involvement among the study respondents (n=423).

Table 5: Relationship between socio-demographic characteristics and categorized knowledge of respondents on cybercrime (n=423)

Variable	Sub- variable	Categorized knowledge Good knowledge	Fair knowledge	Poor knowledge	Statistics X^2, p
Age group	15-19 years	129(59.4%)	75(34.6%)	13(6%)	X^2=7.105
	20-24 years	120(66.3%)	51(28.2%)	10(5.5%)	p=0.130
	25- 29 years	20(80%)	3(12%)	2(8%)	
Sex	Male	136(70.5%)	49(25.4%)	8(4.1%)	X^2= 7.544
	Female	133(57.8%)	80(34.8%)	17(7.4%)	**P=0.023**
Faculty	FABAMS	124(69.3%)	51(28.5%)	4(2.2%)	X^2=78.47
	FABAS	21(47.7%)	19(43.2%)	4(9.1%)	1
	Engineering	68(85%)	11(13.8%)	1(1.2%)	**P<0.001**
	FACS	6(75%)	2(25%)	0(0%)	
	Social science	44(55%)	33(41.2%)	3(3.8%)	
	Mgt science	6(18.8%)	13(40.6%)	13(40.6%)	
Religion	Christianity	195(65.9%)	85(28.7%)	16(5.4%)	X^2=11.55
	Islam	74(59.7%)	43(34.7%)	7(5.6%)	6
	Traditional	0(0%)	1(33.3%)	2(66.7%)	**P=0.021**
Marital status	Single	265(64%)	127(30.7%)	22(5.3%)	X^2= 9.464
	Married	4(57.1%)	1(14.3%)	2(28.6%)	P=0.051
	Divorced	0(0%)	1(50%)	1(50%)	
Mother's marital Status	Married	260(64%)	123(30.3%)	23(5.7%)	X^2=10.91
	Divorced	3(100%)	0(0%)	0(0%)	2
	Separated	3(1%)	1(25%)	0(0%)	P=0.207
	Cohabiting	0(0%)	1(50%)	1(50%)	
	Widowed	3(37.5%)	4(50%)	1(12.5%)	

FABAMS: Faculty of basic medical sciences FABAS: Faculty of basic and applied sciences

FACS: Faculty of clinical sciences MGT science : Management science

Variable	Sub- variable	Categorized knowledge Good knowledge	Fair knowledge	Poor knowledge	Statistics X^2, p
Father's marital status	Married	264(64.2%)	124(30.2%)	23(5.6%)	X^2=15.010
	Divorced	3(100%)	0(0%)	0(0%)	P=0.059
	Separated	2(50%)	1(25%)	1(25%)	
	Cohabiting	0(0%)	1(100%)	0(0%)	
	Widowed	0(0%)	3(75%)	1(25%)	
Ethnicity	Yoruba	249(64.5%)	114(29.5%)	23(6%)	
	Igbo	12(63.2%)	7(36.8%)	0(0%)	X^2=
	Hausa	3(37.5%)	3(37.5%)	2(25%)	9.032
	Others	5(50%)	5(50%)	0(0%)	P=0.172
Mother's education	No formal education	0(0%)	2(40%)	3(60%)	X^2=29.898
	Primary	21(75%)	6(21.4%)	1(3.6)	
	Secondary	85(70.8%)	24(20%)	11(9.2)	**P<0.001**
	Tertiary	163(60.4%)	97(35.9%)	10(3.7%)	
Father's education	No formal education	0(0%)	1(20%)	4(80%)	X^2=26.924
	Primary	19(79.2%)	5(20.8%)	0(0%)	
	Secondary	56(69.1%)	20(24.7%)	5(6.2%)	**P<0.001**
	Tertiary	194(62%)	103(32.9%)	16(5.1%)	
Family type	Monogamous	205(62.9%)	103(31.6%)	18(5.5%)	X^2= 1.039
	Polygamous	64(66%)	26(26.8%)	7(7.2%)	P=0.595
Relationship with father	Cordial	226(66.3%)	97(28.4%)	18(5.3%)	
	we manage to get along	36(54.5%)	26(39.4%)	4(6.1%)	X^2=12.695
	Indifferent	4(57.1%)	3(42.9%)	0(0%)	P=0.123
	terrible/bad	1(20%)	2(40%)	2(40%)	
	Not applicable	2(50%)	1(25%)	1(25%)	

Variable	Sub- variable	Categorized knowledge Good knowledge	Fair knowledge	Poor knowledge	Statistics X^2, p
Relationship with mother	Cordial	245(65%)	111(29.4%)	21(5.6%)	X^2=17.715 **P=0.023**
	manage to get along	16(50%)	15(46.9%)	1(3.1%)	
	Indifferent	1(16.7%)	2(33.3%)	3(50%)	
	terrible/bad	1(100%)	0(0%)	0(0%)	
	Not applicable	6(85.7%)	1(14.3%)	0(0%)	
Monthly allowance	5000-20000	135(58.4%)	78(33.8%)	18(7.8%)	X^2=23.787 **P=0.002**
	21000-40000	71(68.3%)	31(29.8%)	2(1.9%)	
	41000-60000	32(71.1%)	13(28.9%)	0(0%)	
	61000-80000	7(100%)	0(0%)	0(0%)	
	>80000	24(66.7%)	7(19.4%)	5(13.9%)	
Allowance meets needs	Yes	105(62.1%)	56(33.1%)	8(4.7%)	X^2= 1.397 P=0.497
	No	164(64.6%)	73(28.7%)	17(6.7%)	
Side job/business While studying	Yes	80(58%)	51(37%)	7(5.1%)	X^2= 4.064 P=0.131
	No	189(66.3%)	78(27.4%)	18(6.3%)	
Ever been Oppressed	Yes	94(66.7%)	40(28.4%)	7(5%)	X^2= 0.948 P=0.622
	No	175(62.1%)	89(31.6%)	18(6.4%)	
How often are you oppressed	Not at all	176(62.2%)	89(31.4%)	18(6.4%)	X^2= 1.566 P=0.815
	Sometimes	38(65.5%)	16(27.6%)	4(6.9%)	
	Always	55(67.1%)	24(29.3%)	3(3.7%)	

Table 6: Relationship between socio-demographic characteristics and categorized attitude of respondents to cybercrime (n=423)

Variable	Sub- variable	Categorized attitude		Statistics
		Negative attitude	Positive attitude	X^2, p
Age group	15-19 years	185(85.3%)	32(14.7%)	X^2= 1.991
	20-24 years	149(82.3%)	32(17.7%)	P=0.370
	25-29 years	23(92%)	2(8%)	
Sex	Male	162(83.9%)	31(16.1%)	X^2 = 0.057
	Female	195(84.8%)	35(15.2%)	P=0.812
Faculty	FABAMS	159(88.8%)	20(11.2%)	
	FABAS	29(65.9%)	15(34.1%)	
	Engineering	77(96.3%)	3(3.8%)	X^2= 47.345
	FACS	4(50%)	4(50%)	**p<0.001**
	Social science	71(88.8%)	9(11.3%)	
	MGT science	17(53.1%)	15(46.9%)	
Religion	Christianity	251(84.8%)	45(15.2%)	X^2= 3.995
	Islam	105(84.7%)	19(15.3%)	P=0.136
	Traditional	1(33.3%)	2(66.7%)	
Marital status	Single	351(84.8%)	63(15.2%)	X^2= 2.081
	Married	5(71.4%)	2(28.6%)	P=0.353
	Divorced	1(50%)	1(50%)	
Mother's marital status	Married	343(84.5%)	63(15.5%)	
	Divorced	3(100%)	0(0%)	
	Separated	3(75%)	1(25%)	X^2= 2.402
	Cohabiting	2(100%)	0(0%)	P=0.662
	Widowed	6(75%)	2(25%)	
Father's marital status	Married	346(84.2%)	65(15.8%)	
	Divorced	3(100%)	0(0%)	X^2= 2.963
	Separated	4(100%)	0(0%)	P=0.564
	Cohabiting	1(100%)	0(0%)	
	Widowed	3(75%)	1(25%)	

FABAMS: Faculty of basic medical sciences FABAS: Faculty of basic and applied sciences
FACS: Faculty of clinical sciences MGT science: Management science

Variable	Sub- variable	Categorized attitude		Statistics
		Negative attitude	Positive attitude	X^2, p
Ethnicity	Yoruba	328(85%)	58(15%)	
	Igbo	15(78.9%)	21.4(2%)	X^2= 1.099
	Hausa	6(75%)	2(25%)	P=0.777
	Others	8(80%)	2(20%)	
Mother's education	No formal education	1(20%)	4(80%)	
	Primary	22(91.7%)	4(14.3%)	X^2= 11.186
	Secondary	68(84%)	15(12.5%)	**p=0.011**
	Tertiary	227(84.7%)	43(15.59%)	
Father's education	No formal education	2(40%)	3(60%)	
	Primary	22(91.7%)	2(8.3%)	X^2=6.251
	Secondary	68(84%)	13(8.3%)	p=0.100
	Tertiary	265(84.7%)	48(15.3%)	
Family type	Monogamous	274(84%)	52(16%)	X^2= 0.131
	Polygamous	83(85.6%)	14(14.4%)	P=0.718
Relationship With father	Cordial	293(85.9%)	48(14.1%)	
	manage to get along	53(80.3%)	13(19.7%)	
	Indifferent	4(57.1%)	3(42.9%)	X^2= 4.653 P=0.325
	terrible/bad	4(80%)	1(20%)	
Relationship with mother	Cordial	321(85.1%)	56(14.9%)	
	manage to get along	25(78.1%)	7(21.9%)	X^2= 7.592
	Indifferent	3(50%)	3(50%)	p=0.108
	terrible/bad	1(100%)	0(0%)	
Monthly allowance	5000-20000	193(83.5%)	38(16.5%)	
	21000-40000	92(88.5%)	12(11.5%)	X^2= 12.585
	41000-60000	41(91.1%)	4(8.9%)	**p=0.013**
	61000-80000	7(100%)	0(0%)	
	>80000	24(66.7%)	12(33.3%)	
Allowance meet needs	Yes	143(84.6%)	26(15.4%)	X^2= 0.010
	No	214(84.3%)	40(15.7%)	p=0.920

Variable	Sub- variable	Categorized attitude		Statistics
		Negative attitude	Positive attitude	X^2, p
Side job/business While studying	Yes	109(79%)	29(21%)	X^2= 4.555
	No	248(87%)	37(13%)	**p=0.033**
Ever been Oppressed	Yes	115(81.6%)	26(18.4%)	X^2= 1.293
	No	242(85.8%)	40(14.2%)	p=0.256
How often are you oppressed	Not at all	243(85.9%)	40(14.1%)	X^2= 2.905
	Sometimes	50(86.2%)	8(13.8%)	p=0.234
	Always	357(84.4%)	66(15.6%)	

Table 7: Relationship between socio-demographic characteristics and categorized practice of respondents in cybercrime (n=423).

Variable	Sub- variable	Categorized practice: practiced cybercrime	Categorized practice: Did not practice cybercrime	Statistics X^2, p
Age group	15-19 years	205(94.5%)	12(5.5%)	X^2= 1.707
	20-24 years	167(92.3%)	14(7.7%)	P=0.426
	25-29 years	22(88%)	3(12%)	
Sex	Male	17(8.8%)	176(91.2%)	X^2= 2.119
	Female	12(5.2%)	218(94.8%)	P=0.145
Faculty	FABAMS	9(5%)	170(95%)	
	FABAS	7(15.9%)	37(84.1%)	X^2= 10.374
	Engineering	4(5%)	76(95%)	P=0.065
	FACS	1(12.5%)	7(87.5%)	
	Social science	3(3.8%)	77(96.2%)	
	MGT science	5(15.6%)	27(84.4%)	
Religion	Christianity	17(5.7%)	279(94.3%)	X^2= 16.716
	Islam	9(7.3%)	115(92.7%)	**p<0.001**
	Traditional	3(100%)	0(0%)	
Marital status	Single	26(6.3%)	388(93.7%)	X^2= 6.005
	Married	2(28.6%)	5(71.4%)	p=0.050
	Divorced	1(50%)	1(50%)	
Mother's marital status	Married	28(6.9%)	378(93.1%)	
	Divorced	0(0%)	3(100%)	X^2= 4.861
	Separated	0(0%)	4(100%)	P=0.302
	Cohabiting	1(50%)	1(50%)	
	Widowed	0(0%)	8(100%)	

FABAMS: Faculty of basic medical sciences FABAS: Faculty of basic and applied sciences

FACS: Faculty of clinical sciences MGT sciences: Management science

Variable	Sub- variable	Categorized practice: practiced cybercrime	Categorized practice: Did not practice cybercrime	Statistics X^2, p
Father's marital status	Married	28(6.8%)	383(93.2%)	X^2= 2.425 P=0.658
	Divorced	0(0%)	3(100%)	
	Separated	0(0%)	4(100%)	
	Cohabiting	0(0%)	1(100%)	
	Widowed	1(25%)	3(75%)	
Ethnicity	Yoruba	23(6%)	363(94%)	X^2= 11.645 **p=0.009**
	Igbo	1(53%)	18(94.7%)	
	Hausa	4(50%)	4(50%)	
	Others	1(10%)	9(90%)	
Mother's education	No formal education	3(60%)	2(40%)	X^2= 9.980 **p=0.019**
	Primary	2(71%)	26(92.9%)	
	Secondary	7(5.8%)	113(94.2%)	
	Tertiary	17(6.3%)	253(93.7%)	
Father's education	No formal education	3(60%)	2(40%)	X^2= 13.190 p=0.004
	Primary	0(0%)	24(100%)	
	Secondary	6(7.4%)	75(92.6%)	
	Tertiary	20(6.4%)	293(93.6%)	
Family type	Monogamous	20(6.1%)	306(93.9%)	X^2= 1.157 p=0.282
	Polygamous	9(9.3%)	88(90.7%)	
Relationship with father	Cordial	19(5.6%)	322(94.4%)	X^2= 4.879 P=0.300
	manage to get along	7(10.6%)	59(89.4%)	
	Indifferent	1(14.3%)	6(85.7%)	
	terrible/bad	1(20%)	4(80%)	
	Not applicable	1(25%)	3(75%)	

Variable	Sub- variable	Categorized practice		Statistics X^2, p
		practiced cybercrime	Did not practice cybercrime	
Relationship with mother	Cordial	23(6.1%)	354(93.9%)	X^2= 4.899 P=0.298
	manage to get along	3(9.4%)	29(90.6%)	
	Indifferent	2(33.3%)	4(66.7%)	
	terrible/bad	0(0%)	1(100%)	
	Not applicable	1(14.3%)	6(85.7%)	
Monthly allowance	5000-20000	13(5.6%)	218(94.4%)	X^2= 19.691 **p=0.001**
	21000-40000	2(1.9%)	102(98.1%)	
	41000-60000	5(11.1%)	40(88.9%)	
	61000-80000	0(0%)	7(100%)	
	>80000	9(25%)	27(75%)	
Allowance meets needs	Yes	12(7.1%)	157(92.9%)	X^2= 0.026 P=0.871
	No	17(6.7%)	237(93.3%)	
Side job/business While studying	Yes	18(13%)	120(87%)	X^2= 12.281 **p=0.001**
	No	11(3.9%)	274(96.1%)	
Ever been Oppressed	Yes	11(7.8%)	130(92.2%)	X^2= 0.296 P=0.586
	No	18(6.4%)	264(93.6%)	
How often are you oppressed	Not at all	18(6.4%)	265(93.6%)	X^2= 0.401 p=0.818
	Sometimes	5(8.6%)	53(91.4%)	
	Always	6(7.3%)	76(92.7%)	

Table 8: Relationship between Categorized knowledge and categorized attitude towards cybercrime (n=423).

		Categorized attitude		Statistics
Variable	**Sub- variable**	**Negative attitude**	**Positive attitude**	**X^2, p**
Knowledge	Good knowledge	246(91.4%)	23(8.6%)	**X^2=30.413**
	Fair knowledge	97(75.2%)	32(24.8%)	**p<0.001**
	Poor knowledge	14(56%)	11(44%)	

Table 9: Relationship between Categorized knowledge and categorized practice of cybercrime (n=423).

		Categorized practice		Statistics
Variable	**Sub- variable**	**Did not practice**	**Practiced**	**X^2, p**
Knowledge	Good knowledge	260(96.7%)	9(3.3%)	**X^2=** 14.802
	Fair knowledge	114(88.4%)	15(11.6%)	**p=0.001**
	Poor knowledge	20(80%)	5(20%)	

Table 10: Relationship between Categorized practice and categorized attitude towards cybercrime (n=423).

		Categorized practice		Statistics
Variable	**Sub- variable**	**Did not practice**	**practiced**	**X^2, p**
Attitude	Negative attitude	347(97.2%)	10(2.8%)	**X^2=** 54.907
	Positive attitude	47(71.2%)	19(28.8%)	**P<0.001**

Table 11: Factors influencing respondents' involvement in cybercrime (n=423).

Variable	Odds ratio	p-value	Confidence interval	
			Lower	Upper
Religion				
Christianity **(Ref)**				
Islam	1.045	0.932	0.380	2.877
Traditional	1.288	0.725	0.201	3.217
Ethnicity				
Yoruba **(Ref)**				
Hausa	0.748	0.801	0.709	7.091
Igbo	8.372	0.058	0.928	75.510
Others	1.009	0.860	0.815	12.076
Mother's education				
Primary **(Ref)**				
Secondary	1.757	0.630	0.177	17.417
Tertiary	1.363	0.784	0.148	12.514
None	5.962	0.290	0.218	162.673
Any side business				
Yes **(Ref)**				
No	0.363	**0.029**	0.146	0.903
Knowledge				
Good knowledge **(Ref)**				
Fair knowledge	1.747	0.276	0.640	4.771
Poor knowledge	1.259	0.780	0.250	6.333
Attitude				
Negative attitude **(Ref)**				
Positive attitude	11.552	**<0.001**	4.379	30.473