

Nigerian Journal of Technology (NIJOTECH) Vol. 43, No. 1, March, 2024, pp.71 - 79 www.nijotech.com

> Print ISSN: 0331-8443 Electronic ISSN: 2467-8821 <u>https://doi.org/10.4314/njt.v43i1.10</u>

EXPLORING THE PREVALENCE OF INTERNET CRIMES AMONG UNDERGRADUATE STUDENTS IN A NIGERIAN UNIVERSITY: A CASE STUDY OF THE UNIVERSITY OF ILORIN

AUTHORS:

N. A. Balogun¹, M. D. Abdulrahaman^{2,*}, and K. Aka³

AFFILIATIONS:

^{1,2,3}Department of Information Technology, University of Ilorin, Ilorin, Nigeria

*CORRESPONDING AUTHOR: Email: <u>rahaman.md@unilorin.edu.ng</u>

ARTICLE HISTORY: Received: 24 December, 2023. Revised: 27 February, 2024. Accepted: 06 March, 2024. Published: 31 March, 2024.

KEYWORDS:

Internet crime, Cybercrime, Cybercrime Prevalence, Cyber Security, Criminology.

ARTICLE INCLUDES: Peer review

DATA AVAILABILITY: On request from author(s)

EDITORS: Ozoemena Anthony Ani

FUNDING: None

Abstract

Internet crime, also known as cybercrime, encompasses various illicit activities conducted through computer system and online platforms. It is a global menace that has become a pervasive issue in our contemporary society. This study delves into exploring the prevalence of internet crime among undergraduate students at the University of Ilorin with the view to examine the level of involvement of undergraduate students, identify the underlying factors, the perceived consequences, and potential control measures associated with undergraduates' involvement in internet crime. The study engaged a sample size of 400 undergraduate students, employing a stratified sample technique for comprehensive data collection using a structured questionnaire. The research revealed that the participants acknowledged the prominence of internet crime within their peer group. It uncovered the multifaceted factors contributing to the prevalence of internet crimes. The respondents acknowledged the perceived consequences of undergraduates' involvement in internet crime, encompassing financial mismanagement, expulsion from educational institutions, societal stigma, loss of personal integrity, legal consequences, and limited access to future opportunities. To mitigate this growing concern, respondents recommended various control and combative measures. These encompass the implementation of stringent rules within educational institutions, effective monitoring of students' financial activities, awareness campaigns against internet crime, provision of employment opportunities, engaging experts to address the issue, banning tools facilitating internet crime, and organizing training workshops to enhance legitimate ICT skills and wealth generation. This study sheds light on the pressing need for proactive interventions to curb internet crime among undergraduate students, emphasizing education, awareness, and policy implementation to foster a safer online environment and deter involvement in criminal activities.

1.0 INTRODUCTION

Internet is one of the greatest technologies ever invented by human in the past decades. It has contributed to the invention of other Information and Communication Technology (ICT) solutions and services such as emails, e-commerce, social media, Internet of Things (IoTs) and its smart services, among others. Aside the numerous positive aspects of the internet such as social networking, worldwide linkages, job creation, improving medical and education access, expansion of commercial landscape and so on [1], it has also contributed to series of criminal activities in our society in form of Internet crimes or cybercrimes [2, 3].

HOW TO CITE:

Balogun, N. A., Abdulrahaman, M. D., and Aka, K. "Exploring the Prevalence of Internet Crimes among Undergraduate Students in a Nigerian University: A Case Study of the University Of Ilorin", *Nigerian Journal of Technology*, 2024; 43(1), pp. 71 - 79; <u>https://doi.org/10.4314/</u> njt.v43i1.10

© 2024 by the author(s). This article is open access under the CC BY-NC-ND license Internet crimes are complex and dynamic in nature, but broadly referred to as online based criminal activities conducted through the use of ICT tools such as computer and Internet [4]. More so, it is a computer or internet-enabled crimes and encompasses series of Cybercrimes activities, some of which include financial fraud, cyber stalking, identity theft, email spamming, cyber bullying, phishing, cyber pornography, network intrusion, hacking, cyber extortion, malware attack, copy right infringement, plagiarism, and defamation [3, 5]. Internet crime has devastating effects on the victims, including financial losses, nonfinancial losses such as emotional trauma and damage of reputation by individual, governmental and corporate organizations across the nations [6, 7, 8, 9].

With the increase in the use of mobile phones and other Internet enabled devices among youths, who are the most volatile and sensitive section of the society, cybercrime activities are becoming more prevalence and worrisome especially in developing countries. This therefore calls for more for research efforts to uncover the prevalence, offensive patterns and the available controlling measures and their effectiveness in curbing the spread of Internet crimes among the youths, whose behaviors shape the security and patterns of development of a nation [10, 11]. Thus, studies on cybercrime prevalence, severity and countermeasures are imperative to aid provision of advice and development of prevention mechanisms to end users [5, 12].

In 2020, Nigeria was ranked 16th in the world among the countries with high rate of cybercrimes in 2020 by the US Federal Bureau of Investigation (FBI) [15]. As one of the developing countries with high rates of cybercrimes among the youths [13, 14], most cases, the cybercriminals take advantage of lack of cyber security awareness, and other forms of socialeconomic influences such as political, social, religion, and economic factors among the victims to commit crimes [2, 16, 17]. Meanwhile, several researches have been conducted with the view of investigating the prevalence of Internet crimes among the youths or cyber criminals in the last two decades [4, 7, 18, 19], however, the recent growth in internet connectivity and continuous rise in the cases of cybercrimes among Nigerian youths necessitates more research efforts in the context of Nigeria.

The aim of this study is to explore the prevalence of internet crime among undergraduate students at the University of Ilorin, and the specific objectives are to: examine the prevalence and level of undergraduate students' involvement; identifies the underlying

© 2024 by the author(s). Licensee NIJOTECH. This article is open access under the CC BY-NC-ND license. http://creativecommons.org/licenses/by-nc-nd/4.0/ factors; the perceived consequences, and potential control measures associated with undergraduates' involvement in internet crime in Nigeria. The outcome of this study is to serve as a guide for government agencies, security personnel, researchers and practitioners who are in charge of making and enforcing security policies and protocols to be able to provide adequate protection measures for end users against cybercrimes. The summary of our contribution is presented as follows:

- i. Assess the prevalence of Internet crimes among undergraduate students in Nigeria.
- ii. Reveal the perceived underlying factors that contribute to the prevalence of cybercrime among students in Nigeria
- iii. Investigate the consequences of Internet crimes as perceived by students in Nigerian university.
- iv. Assess the countermeasures associated with the prevalence of Internet crimes in Nigeria.

The other parts of this paper is organized thus: Section 2 presents some related work and Section 3 describes the research methodology employed for this study. Furthermore, Section 4 presents the analysis and discussion of the findings according to the set objectives. Finally, Section 5 concludes the article and highlights the study recommendations.

2.0 INTERNET CRIMES

Internet crime is a global menace that is causing financial and non-financial havocs to many Internet users on a daily basis, especially in the developing countries like Nigeria [2]. A number of research efforts have been devoted to different cybercrime related issues and topics with the view of investigating the prevalence, techniques, countermeasures, and victimization of cybercrimes among the Internet users in many countries and study areas. For instance, [5] study investigated the prevalence and severity of cybercrimes among the US citizens. A network scaleup technique was employed to sample a total of 11,953 Internet users to investigate the prevalence of six types of Internet crimes including credit card or bank account compromise, non-delivery, nonpayment, overpayment, digital extortion, advance fee scam.

Their findings revealed no prevalence of the investigated crimes among the US citizens in contrast to the initial assumption of the research. In addition, their study also revealed that both old Americans and black Americans are more vulnerable to cybercrimes. In [2], the author devoted his study to investigating the prevalence of cybercrime in in Dandume Local Government Area of Katsina State, Nigeria. The result of his descriptive and quantitative research approach

with 115 residents of the study area shows the prevalence of cybercrime menace with yahoo attack, credit card fraud, social media hijacking, airtime and government offer scams accounted as the prominent cybercrimes. More importantly, the study revealed that the prevalence of the cybercrimes in the study area is largely as a result of a lack of cybersecurity knowledge and awareness among the users. It therefore suggested for community wide cyber education and awareness among the people who engage in Internet-enabled services or transactions.

A qualitative research approach was employed by [3] to compare and analyze the normative and institutional framework provided by the Ministry of Internal Affairs on cybercrime to combat the prevalence of cybercrimes in the Republic of Serbia and other European countries. The result of their analysis shows that despite a good normative measure, more efforts still need to be put in place in order to combat cybercrimes in the Republic of Serbia. It further suggested for more cybersecurity education for citizens of all ages with regards to the dangers and various forms of cybercrimes and how to guide against them. Similarly, [6] investigated the prevalence of cvbercrimes in Indonesians' corporations in comparison with the legislative rules and enforcement strategies for combating cybercrime in other countries using an inductive qualitative research approach. The analyses revealed that the existing cybercriminal laws in Indonesia is limited to defamation, online cyber threat and other forms of individual cybercrimes, whereas corporate-based cybercrimes such as data protection, illicit transactions among others are provided for in the legal framework. This is said to be a major factor inhibiting the implementation of the various cybercrime laws in their country, and limiting the adoption of online transactions by consumers.

[20] Assessed the predictive impact of Internet crimes on commerce by employing a survey research method using Delta state in Nigeria as their study area. From the analysis of the data collected, it was discovered that cybercrime prevalence has negative impact on Nigeria commerce and e-commerce users' confidence and requires a proactive cybercrime countermeasures and implementable appropriate legal framework. The study suggested the need for the law enforcement agencies to be adequately equipped with relevant technological know-how and legal framework to be up-to-date with respect to the current trend and sophistication of in cybercrimes. [21] Conducted a country representative survey of a total of 1,266 citizens of the Republic of Slovenia in Europe with the view of investigating the prevalence and nature of

© 2024 by the author(s). Licensee NIJOTECH. This article is open access under the CC BY-NC-ND license. http://creativecommons.org/licenses/by-nc-nd/4.0/ cybercrimes among the rural and urban dwellers. The study found that there are variations in the purpose of technology use as well as the perceived cybercrime victimization among the two categories of users. It further highlighted the association between the purpose of use and the perceived likelihood of attacks while transacting online across various divides.

[4] Investigated the cybercrime behavior with the view to establish linkages between the criminals and the type of crimes committed. A qualitative research approach including review of offenders' cases documents and interview of prosecuting officers (police agencies) to investigate 37 offenders' network across major European and Northern American countries. The study only focuses on cybercrimes that are financially motivated including phishing, malware attacks, and credit card fraud. The findings from their data analyses categorized the criminals into three specializations, including cybercrime specialist. cybercrime versatile, and traditional cybercriminals. It further shows that it might be difficult to distinctly link certain cybercrimes to a particular offender group due to the dynamic nature of the offenders.

[22][12] Explored the youth level of engagement with money mule recruitment ads on Instagram using quansi-experimental 3x2 factorial design to mimics the actual recruitment techniques employ by cybercriminals to lure Internet users into cybercrime activities in Netherlands. Facebook Ad's manager tool was used to craft and disseminate the adverts to clusters of Dutch Internet users on Instagram. The study crafted three adverts in line with the three common Money mules' techniques: promoting luxury lifestyle, normalization and neutralization. The authors achieved a success with the employed method and discovered that many young users on Instagram are prone to money mule techniques as they are eager to make money through their bank accounts online. In addition, the study suggested for more related researches in this area using social media platforms. It also calls for similar studies in another country in order to compare the outcomes.

More so, [23] examined the efficacy of contextual factors in understanding cybercrime participation among 22 cybersecurity experts using a semistructured interview. The participants were recruited for the study based on stratosphere laboratory and snowballing sampling techniques. The analysis of the collected revealed three contextual factors that may contribute to cybercrime participation to include lack or inadequate employment opportunities, absence of deterrent mechanisms, and availability of drifting which makes individual believe they can partake in cybercrime. The author also discovered four types of cybercrime structures including organized crime, enterprise crimes, loose network, and online community. The work also identified a group of cybercrime participants who are not actively part of the crime but are engaged (knowingly or otherwise) to complete tasks for the criminals in their workplace. Further research efforts to uncover various by recruitment channels or techniques used cybercriminals to lure Internet users to cybercrime, especially the vulnerable users, are suggested by the author.

[16] Investigated the efficacy of data mining to uncover factors contributing to the trend in cybercrime among youths of Ibadan in Nigeria. A mixed research method including interview and survey was adopted, where about four hundred and eighteen (418) cybercriminals in police custodies in Ibadan were randomly selected. Descriptive statistics, Pearson Product Moment Correlation (PPMC) and multiple regression were employed for analysis purposes. The results revealed the prevalence of cybercrimes among the youths, while also showing significant and positive relationship with social influence. It also shows a significant and positive relationship between economic influence and cybercrime prevalence, and significant and negative association between the political influence and the crimes among others. The author advocated for the availability of cybercrime datasets to encourage more data mining-based researches for cybercrime investigations.

3.0 METHODOLOGY

3.1 Research Design and Sampling Techniques

The research approach employed in this study is quantitative survey method that includes a structured questionnaire as the instrument. This method was chosen to enable researchers elicit useful, representative and relevant information to achieve the study objectives. Meanwhile, the data was collected through a close-ended questionnaire that included a consent approval of the participants. The questionnaire was designed in a bid to elicit information from the respondents with regards to the research objectives. Specifically, the it consists of four sections describes as follows: Section A includes the demographic data of respondents, Section B elicits data on the level of youth's involvement in internet crime, Section C collects data on underlying factors that contribute to the rate of internet crimes amongst youths, Section D is on perceived consequences of undergraduates' involvement in internet crimes, and Section E elicits data on perceived control and combative measures for

© 2024 by the author(s). Licensee NIJOTECH. This article is open access under the CC BY-NC-ND license. http://creativecommons.org/licenses/by-nc-nd/4.0/ undergraduates' involvement in internet crimes. More so, the study was certified and approved by the research and ethical committee of the Department of Information Technology, University of Ilorin and descriptive statistics were performed using relevant frequencies, percentages, mean scores, and standard deviations as reflected in the Tables and Figures, while the data gathered was appropriately coded for ease of use with the Statistical Package for Social Sciences (SPSS) version 21.

3.2 Sample Population and Size

The population for this study includes a total of 44,919 undergraduate students of the University of Ilorin who registered for the 2021/2022 academic session. This includes students in all the fifteen (15) Faculties in the University. The sample size of the population was determined using the Slovin's formula, with a standard error of 5% or 0.05 [24], which gives the minimum sample size of three hundred and ninety-six (396) samples from the 15 faculties in the University of Ilorin. However, this study used a total sample size of four hundred (400) to cater for the possibility of incomplete data entry. The Slovin's formula is given in equation (1):

$$n = \left(\frac{N}{1 + Ne^2} 1\right)$$
(1)
Where n is the sample size, N represents the

Where n is the sample size, N represents the Population, and the e stands for standard error (5% = 0.05).

Furthermore, in order to determine the number of samples per faculty, Slovin's formula (2) was employed as given in equation (2):

$$\frac{RPS}{N} \times n \tag{2}$$

Where RPS represents the respondents' population size, n corresponds to the number of populations, and N is the total population of the study. The result of the equation (2) with respect to the population of students in each Faculty is presented in Table 1.

3.3 Sampling Technique

After the sample size was determined, this study employed a stratified sampling technique to divide the population into strata, which is 15 faculty strata in this case. Then, a convenience sampling method was used to select the participants for this study. The convenience sampling allows the available member of the sample population who are willing to partake in a study be conveniently selected for this study [25]. This method is suitable as it will ensure a completed and revenant information is collected from the particip-

> Vol. 43, No. 1, March 2024 https://doi.org/10.4314/njt.v43i1.10

ants. Therefore, the minimum sample size for each faculty is shown in Table 1.

Faculty	Population	Faculty Sample Size
Arts	4632	41
Agricultural Science	5304	47
Basic Medical Science	1193	11
Clinical Science	1089	10
CIS	2134	19
Education	10377	91
Engineering and Technology	3577	32
Environmental Science	1277	11
Law	979	9
Life Science	3637	32
Management Science	3765	33
Social Science	3094	27
Pharmaceutical Science	336	3
Physical Science	3340	29
Veterinary Medicine	235	2
Total	44919	396

Table 1: Calculation of sample size by faculty

4.0 RESULTS AND DISCUSSION

4.1 Demographic Profile of Respondents

The major demographic profiles sought in this study were the respondent's age group, gender, religion, faculty and level of which these attributes were presented in frequency and percentage formats as shown in Table 2.

i. Gender

Table 2 presents the demographic characteristics of the respondents, as shown on the table, In the data gathered the male respondents in the study were 220 with a percentage of 55% while the female respondents were 180 at 45%.

Table 2: Analysis of socio-demographic characteristics of respondents N=400

Variable	Sub-variable	Frequency	Percentage
Gender	Male	220	55.0
	Female	180	45.0
	Total	400	100.0
Level	100	64	16.0
	200	104	26.0
	300	88	22.0
	400	112	28.0
	500	32	8.0
	Total	400	100.0
Age	Less than 20	88	24.0
	21-25	136	38.0
	26-30	80	22.0
	Above 30 years	56	16.0
	Total	400	100
Religion	Christianity	164	41.0
	Islam	228	57.0
	others	8	2.0
	Total	400	100

ii. Faculty

As depicts in Table 1, Faculty of Education, being the most populated among all the faculties in the University accounted for the highest number of respondents in this study with a total of 91 respondents

© 2024 by the author(s). Licensee NIJOTECH. This article is open access under the CC BY-NC-ND license. http://creativecommons.org/licenses/by-nc-nd/4.0/ (22.97%) while the faculty of Veterinary Medicine accounted for the least number of respondents with a total number of 2 respondents (.51%). Representation from other faculties are; Faculties of Art 10.35% (41), Agricultural Science 11.87% (47), Basic Medical Science 2.78% (11), Clinical Science 2.53% (10), Communication and Information Science {CIS} 4.8% (19), Engineering and Technology 8.08% (32), Environmental Science 2.78% (11), Law 2.27% (9), Life Science 8.08% (32), Management Science 8.33% (33), Social Science 6.82% (27), Pharmaceutical Science 0.76% (3) and Physical Science 7.32% (29).

iii. Age

On the age distribution of the respondents as presented in Table 2, it was revealed that there are 88 students in the dataset who are less than 20 years old, representing 24.0% of the total sample. It was also revealed that there are 136 students in the age group of 21-25, accounting for 38.0% of the total 44 sample. There are 80 students in the age group of 26-30, constituting 22.0% of the total sample. There are 56 students who are above 30 years old, making up 16.0% of the total sample. The age brackets of the sample undergraduates indicate that all the sampled respondents are youths.

iv. Level

On the level distribution of the respondents, it was revealed that there are 64 students at the 100 level, making up 16.0% of the total sample, 104 students at the 200 level, constituting 26.0% of the total sample, 88 students at the 300 level, representing 22.0% of the total sample, there are 112 students at the 400 level, accounting for 28.0% of the total sample and that there are 32 students at the 500 level, making up 8.0% of the total sample.

v. Religion

On the basis of religion, it was revealed that there are 164 students in the dataset who practice Christianity, representing 41.0% of the total sample. It was also revealed that there are 228 students who practice Islam, accounting for 57.0% of the total sample and that there are 8 students who follow religions other than Christianity and Islam, making up 2.0% of the total sample.

4.2 Undergraduate Involvement in Internet Crimes

Research Question One: What is the level of undergraduates' involvement in internet crimes in the University of Ilorin?

In this study, we will make our decision on the respondent's perceptions of the level of undergraduates' involvement in internet crimes in the University of Ilorin using the weighted average value. The value of the weighted average is calculated by summing up the Mean values for the items, divided by the total number of the items.

From Table 3, The data analysis shows that the majority of the respondents have a high level of perception that internet crime is prominent among undergraduates in the University of Ilorin. Also, they felt that internet crime engagement is considered a source of survival by the undergraduates. They also highly perceived that undergraduates consider money laundering as a constant means of survival. They have a high level of perception that undergraduates evade tax purposively in order to prevent tax cost, and they also highly perceive that undergraduates consider

internet crime engagement as the only means of survival. On the other hand, the majority of the respondents had a low level of perception that the undergraduates consider internet crime engagements as a civilized trend to be rated among colleagues and internet crime is as common as eating among undergraduates. The respondents lowly perceived that undergraduates engage in internet crime to meet up with societal demands. They also have a low level of perception that internet crime engagements are believed to be the only source of meeting academic demands and lastly, they have a low level of perception that internet crime engagements are only common among male than the female. This result is in tandem with the findings of [2, 3, 12] who confirmed the prevalence and involvement of youths in cybercrimes in their respective sample areas including Nigeria.

Table 3: Mean and standard deviation analysis of the level of undergraduates' involvement in internet crimes in the University of Ilorin

Item No	Statements	Mean Score	Standard Deviation	Remarks
1.	Internet Crime is prominent among undergraduates in the University	3.43	0.82	Agreed
2.	Internet crime engagement is considered a source of survival by the undergraduates	3.23	0.76	Agreed
3.	Undergraduates considers money laundering as a constant means of survival	3.20	0.82	Agreed
4.	Undergraduates evade tax purposively in order to prevent tax cost	3.10	0.79	Agreed
5.	Undergraduates consider internet crime engagement as the only means of survival	2.91	1.06	Agreed
6.	Undergraduates consider internet crime engagements as a civilized trend to be rated among colleagues	2.77	1.11	Agreed
7.	Internet crime is as common as eating among undergraduates	2.64	0.88	Agreed
8.	The undergraduates engage in internet crime to meet up with societal demands	2.55	1.01	Agreed
9.	Internet crime engagements is believed to be the only source of meeting academic demands	2.61	1.11	Agreed
10.	Internet crime engagements is only common among male than the female	2.64	0.92	Agreed
	Average	2.91	0.93	

Table 4: Mean and standard deviation analysis of the underlying factors that contribute to the rate of internet crimes amongst undergraduates in the University of Ilorin

Item No	Statements	Mean Score	Standard Deviation	Remarks
1.	Undergraduates involve in internet crime due to greed	3.40	0.68	Agreed
2.	Undergraduates engage in internet crime due to high level of poverty	3.38	0.59	Agreed
3.	Undergraduates engage in internet crime due to socialization and leadership among the students	3.35	0.55	Agreed
4.	Undergraduates engage in internet crime due to in-active rules and regulations in schools	3.32	0.73	Agreed
5.	Undergraduates engage in internet crime due to peer group influence	3.32	0.86	Agreed
6.	Undergraduates engage in internet crime due to parenting style and involvement	3.31	0.71	Agreed
7.	Undergraduates engage in internet crime due to the state of the economy	3.29	0.52	Agreed
8.	Undergraduates engage in internet crime due to inability to meet urgent needs	3.24	0.82	Agreed
9.	Undergraduates engage in internet crime due to intimidations from friends	3.21	0.61	Agreed
10.	Undergraduates engage in internet crime due to inability to meet academic needs	3.15	0.73	Agreed
11	Undergraduates engage in internet crime because they can evade punishments	3.14	0.80	Agreed
	Average	3.28	0.69	

Research Question Two: What are the underlying factors that contribute to the rate of internet crimes amongst undergraduates?

From Table 4, the result of data analysis shows that the majority of respondents perceived that high rate of internet crime among students in the University of Ilorin is as a result of greediness, poverty and social

© © 2024 by the author(s). Licensee NIJOTECH. This article is open access under the CC BY-NC-ND license. http://creativecommons.org/licenses/by-nc-nd/4.0/ influence. More so, they also believed that inactive rule and regulation in school, bad parenting, and lack of stringent punishment to cyber criminals are responsible for increase in internet crime.

The respondents also have high perception that the increase in internet crime among students is caused by intimidation from friends, and the anxiety to meet academic needs. These results corroborate the findings of the previous studies such as [1, 2, 3, 6, 20, 21]. This suggests holistic efforts from various stakeholders to ensure that those factors are seriously addressed in order to make Internet safer to use and improve user's trust in online businesses and transactions.

Research Question Three: What are the perceived consequences of undergraduates' involvement in Internet crimes?

As shown in Table 5, majority of the respondents had the perception that students who engage in internet crime are aware of the consequences of their actions. For instance, Table 5 shows that majority of respondents felt that the consequent of internet crime includes funds misplacement, expulsion from school, damaging of school properties, loss of personal integrity, sentencing to jail, societal stigmatization, loss of trust, and limited access to different opportunities. This result is in tandem with findings from [2, 6, 22] that reported various internet crime consequences. *Research Question Four:* What are the control and combative measures for reducing undergraduates' involvement in Internet crimes?

Table 6 presents the analysis of responses from respondents providing various combative measures for internet crime among youths in Nigeria. From Table 6, the weighted average values indicate that majority of respondents are of the opinion that internet crimes can be curbed in the university if strict rule and regulations are put in place by school management. They also opined that regular monitoring of students life styles and spending could go a long way in check mating the evolvement of students in internet crime. Also, they believed that cybercrime can be curbed regular sensitization programmes with and workshops, provision of job opportunities to keep students engaged and productive. More importantly, the respondents believed that by engaging cyber security experts with state-of-the-art security tools and mechanisms, the school authority will be able to arrest the prevalence of internet crime among students on campuses. Majority of respondents also opined that schools need to ban tools that enhance student evolvement in internet crime.

Table 5: Mean and standard deviation analysis of the consequences of undergraduates' involvement in Internet crimes in the University of Ilorin, Kwara state

Item No	Statements	Mean Score	Standard Deviation	Remarks
1.	The consequence of internet crime includes funds misplacement	3.66	0.477	Agreed
2.	Internet crime consequence includes students' expulsion from the school	3.59	0.65	Agreed
3.	Internet crime engagements may lead to Loss and damage of school property	3.51	0.64	Agreed
4.	Internet crime engagement leads to money laundering and wastage	3.47	0.60	Agreed
5.	Loss of personal integrity can occur as a result of engagement in internet crime	3.47	0.60	Agreed
6.	Internet crime engagement may lead to jail terms among other sentences	3.30	0.72	Agreed
7.	Societal stigma and condemnations may also be a consequence	3.25	0.91	Agreed
8.	Internet crime engagement may lead to loss of trust of friends and family	3.08	0.92	Agreed
9.	Internet crime engagement may lead to limited access to opportunities	3.03	0.91	Agreed
	Average	3.37	0.71	

Table 6: Mean and standard deviation analysis of the control and combative measures for reducing undergraduates' involvement in Internet crimes in the University of Ilorin, Kwara state, Nigeria

Item No	Statements	Mean Score	Standard Deviation	Remarks
1.	Internet crime engagement can be curbed through creation of strict rules and regulations in the school	3.70	0.46	Agreed
2.	Internet crime engagement can be curbed through effective monitoring of students' expenditure and income by relevant agencies	3.69	0.51	Agreed
3.	Internet crime engagement can be curbed through creation of sensitization programmes and campaigns against internet crime	3.68	0.51	Agreed
4.	Internet crime engagement can be curbed through creating measures that help in preventing students' misconduct	3.68	0.47	Agreed
5.	Internet crime engagement can be curbed through engaging the qualified parties to address students' involvement in internet crime	3.66	0.60	Agreed
6.	Internet crime engagement can be curbed through the creation of job opportunities to discourage students participation in the crime	3.60	0.54	Agreed
7.	Internet crime engagement can be curbed by hiring experts to completely counter the prevalence of the crime	3.59	0.52	Agreed
8.	Internet crime engagement can be curbed through bans of tools that enhance internet crime involvement by students	3.59	0.56	Agreed
9.	Internet crime engagement can be curbed by organizing training workshops on how to use ICT tools and skills to generate legitimate wealth	3.45	0.78	Agreed
	Average	3.63	0.55	



The agreement to the aforementioned cybercrime control measures by the respondents indicates the alignment of this study's outcome with the outcome of the studies like [2, 3, 6, 23].

5.0 CONCLUSION AND RECOMMENDATI-ONS

5.1 Conclusion

This study explores the prevalence of internet crime among youths in Nigeria. The study focuses on the students of university of Ilorin, using a quantitative research approach with a structured questionnaire. The study's demographic characteristics reveal a diverse student population at the University of Ilorin in terms of gender, academic level, age, and religious affiliation. Undergraduates at the university perceive internet crime as a prevalent and potentially lucrative activity, with factors such as financial pressure, peer influence, and perceived lack of consequences contributing to its prevalence. The perceived consequences of internet crime include academic and legal repercussions, damage to personal integrity, and societal stigma. To combat internet crime, the respondents suggest a combination of measures, including stricter rules and regulations, enhanced monitoring, awareness campaigns, and the creation of legitimate income opportunities.

5.2 Recommendations

Based on the above findings, it was recommended that;

- i. The university should continue to monitor and address issues related to internet crime among its student population, considering the factors contributing to its prevalence.
- ii. Efforts should be made to raise awareness about the legal and societal consequences of internet crime, emphasizing ethical behavior and responsible use of technology.
- iii. The university should explore opportunities to create job opportunities, internships, and skillbuilding programs to help students generate legitimate income and reduce financial pressure.
- iv. Collaboration with law enforcement and relevant authorities should be considered to deter internet crime and ensure that legal consequences are enforced when necessary.
- v. Ongoing workshops and training on the ethical use of ICT tools and responsible online behavior can be organized to equip students with the skills and knowledge needed for legitimate wealth generation.
- vi. Continuous research and assessment of the prevalence and underlying factors of internet

© 2024 by the author(s). Licensee NIJOTECH. This article is open access under the CC BY-NC-ND license. http://creativecommons.org/licenses/by-nc-nd/4.0/ crime should be conducted to adapt control and preventive measures effectively.

REFERENCES

- [1] Chen, S., et al., "Exploring the global geography of cybercrime and its driving forces", *Humanit. Soc. Sci. Commun.*, vol. 10, no. 1, pp. 71, 2023. doi:10.1057/s41599-023-01560-x.
- [2] Garba, J., "An approach to cybercrime issues in Dandume Local Government area of Katsina State, Nigeria", *Niger. J. Technol.*, vol. 42, no. 2, pp. 249-256, 2023. doi:10.4314/njt.v42i2.13
- [3] Stošić, L. V., and Janković, A. V. "Cybercrime in the Republic of Serbia: Prevalence, situation and perspectives", *Kpolisa.*, vol. 19, no. 4, pp. 82-99, 2022. doi:10.51738/Kpolisa2022.19.4r. 82sj.
- [4] Leukfeldt, E. R., and Holt, T. J. "Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals", *Comput. Hum. Behav.*, vol. 126, pp. 1-9, 2022. doi:10.1016/j.chb.2021.10 6979
- [5] Breen, C. F. et al., "A large-scale measurement of cybercrime against individuals", *CHI Conference on Human Factors in Computing Systems (CHI '22)*, 2022. doi:10.1145/349110 2.3517613.
- [6] Gojali, D. S., and Mangkurat, U. L. "Identifying the Prevalence of Cybercrime in Indonesian Corporations: A Corporate Legislation Perspective Ten Riskiest Countries in terms of Cybercrime Rate", *Int. J. Cyber Criminol.*, vol. 17, no. 1, pp. 1-11, 2023. doi:10.5281/zenodo. 4766600.
- [7] Nicholson, J., et al., "Prevalence and Trends of Depression among Cyberbullied Prevalence and Trends of Depression among cyberbullied Adolescents—Youth Risk Behavior Survey, United States, 2011-2019", *Int. J. Cybersecurity Intell. Cybercrime*, vol. 6, no. 1, pp. 45-58, 2023.
- [8] Ukam, P. I., et al., "How engagement in internet fraud impact academic activities of undergraduate students in Nigeria: A sociolegal study", *Cogent Soc. Sci.*, vol. 10, no. 1, p. 2280285, 2024. doi:10.1080/23311886.2023.2 280285.
- [9] Deora, R. S., and Chudasama, D. "Brief study of cybercrime on an internet", *J. Commun. Eng. Syst.*, vol. 11, no. 1, pp. 1-6, 2021.
- [10] Adewopo, V., et al., "A comprehensive analytical review on cybercrime in West

Vol. 43, No. 1, March 2024 https://doi.org/10.4314/njt.v43i1.10 Africa", *arXiv Preprint ArXiv:2402.01649.*, 2024.

- [11] Obajobi, J. J., et al., "Impact of cybercrime on national development: A review on Nigeria", *Lapai J. Humanit.*, vol. 13, no. 1, pp. 56-63, 2022.
- [12] Dar, S. A., and Nagrath, D. "Are women a soft target for cyber crime in India?", J. Inf. Technol. Comput., vol. 3, no. 1, pp. 23-31(12), 2022. doi:10.48185/jitc.v3i1.503.
- [13] Ismail, U. "The Nigeria police force and cybercrime policing: An appraisal", *Dutse J. Criminol. Sec. Stud.*, vol. 1, pp. 78-88, 2020.
- [14] Hassan, A. O., et al., "Cybersecurity in banking: A global perspective with a focus on Nigerian Practices", *Comput. Sci. It Res. J.*, vol. 5, no. 1, pp. 41-59, 2024. doi:10.5159 4/csitrj.v5i1.701.
- [15] Olasupo, A. "Nigeria ranks 16th in FBI's global worst affected by internet crimes", 2021, Available at: <u>https://guardian.ng/news/n</u> igeria-ranks-16th-in-fbis-global-worst-affecte d-by-internet-crimes.
- [16] Adesina, A. O., et al., "Investigating data mining trend in cybercrime among youths", in *Pervasive Computing and Social Networking*, *Lecture Notes in Networks and Systems 475*, 2023, pp. 725-741. doi:10.1007/978-981-19-2840-6_55.
- [17] Rawindaran, N., Jayal, A., and Prakash, E. "Exploration of the impact of cybersecurity awareness on small and medium enterprises (SMEs) in Wales using intelligent software to combat cybercrime", *Computers*, 11(12), 174, 2022.
- [18] Curtis, J., and Oxburgh, G. "Understanding cybercrime in 'real world'policing and law

enforcement", *Police J.*, 2023; vol. 96, no. 4, pp. 573-592.

- [19] Loggen, J., et al., "A systematic narrative review of pathways into, desistance from, and risk factors of financial-economic cyber-enabled crime", *Comput. Law Sec. Rev.*, vol. 52, p. 105858, 2024. doi:10.1016/j.clsr.202 3.105858.
- [20] Ugbomah, N., et al., "Cybercrime: Predictive impact on e-commerce in Nigeria," *Sch. J. Soc. Sci. Res.*, vol. 1, no. 1, pp. 1-14, 2022.
- [21] Bernik, I., Prislan, K., and Miheli^{*}, A. "Country Life in the Digital Era : Comparison of Technology Use and Cybercrime Victimization between Residents of Rural and Urban Environments in Slovenia" Sustainability (Switzerland), vol. 14, pp. 1-16, 2022.
- [22] Bekkers, L. M. J., et al., "Understanding cybercrime involvement: A quasi-experiment on engagement with money mule recruitment ads on Instagram", *J. Exp. Criminol.*, pp. 1-20, 2022. doi:10.1007/s112 92-022-09537-7.
- [23] Garcia, M. P. S. "On the dynamics behind pro t-driven cybercrime: From contextual factors to perceived group structures, and the workforce at the periphery", *CrimRxiv*, pp. 1-26, 2023.
- [24] "Statistics How To (n.d)", *Slovin's Formula: What Is It and When Do I Use It?* Available at: <u>https://www.statisticshowto.com/probability-</u> and-statistics/how-to-use-slovins-formula/.
- [25] Dudovskiy, J. (N.D.), "Convenience sampling", Available at: https://researchmethodology.net/sampling-in-primary-datacollection/convenience-sampling/.

© 2024 by the author(s). Licensee NIJOTECH. This article is open access under the CC BY-NC-ND license. http://creativecommons.org/licenses/by-nc-nd/4.0/