Assessment of Knowledge of Undergraduate Social Studies towards Cyber Hacking and Cyber Identity Theft in North-West, Nigeria

By

Muhammad, Nasa'i, PhD
muhdnasai@gmail,com
07036167422
&
Adama Shuaibu Sani
Department of Arts and Social Science Education
Faculty of Education
Ahmadu Bello University, Zaria

Abstract

The study was carried out on assessment of knowledge of undergraduate social studies towards cyber hacking and cyber identity theft in north-west, Nigeria. The study was guided by two specific objectives, two research questions and two hypotheses. Descriptive survey design was employed using a total population of 512 of 400 level Undergraduate Social Studies in Colleges of Education in North-West Nigeria where 217 were used as the sample size. Structured questionnaire was used for data collection. The data collected were analyzed using mean, standard deviation and one sample t-test. The two research questions were answered using mean and standard deviation while the two hypotheses were tested using one-sample t-test at 0.05 level of significance. Findings of the study revealed that social studies undergraduates differ in their knowledge on cyber hacking as cybercrime in North-west, Nigeria and social studies undergraduates differ in their knowledge of cyber identity theft as cybercrime in North-west, Nigeria. Based on the findings of the study, it was concluded that students exhibit positive knowledge towards cyber hacking and identity theft. The significant differences observed in their knowledge indicate a varied level of understanding and awareness among the students. The study recommended that ministry of education should incorporate cyber security education into Social Studies curricula to provide students with a comprehensive understanding of hacking, its historical context, and its impact on society and government should organize workshops or seminars specifically focusing on identity theft

awareness. Government should also invite experts in cybersecurity or law enforcement agencies to speak about the risks, prevention strategies, and legal consequences associated with identity theft.

Keywords: Knowledge, undergraduate social studies, cyber hacking, cyber identify theft

Introduction

Technology has brought together almost all countries of the world into a global village. The economy of most countries in the world is accessible through the aid of electronic by mean of the internet. The advent of internet for the past decades has brought massive improvement in all spheres of human endeavours. The gains of the internet since the inception include: the facilitation of job and employment; accessibility to information for research, education, and businesses; rural integration; enhancement of trade and commerce; and sharing of resources and ideas. Aside from the stated benefits, the Internet poses threat to the equilibrium of the society and the world in general which gave birth to cybercrime. Cybercrimes are offences that are committed against individual or group of individuals with a criminal motive to internationally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly using modern telecommunication networks such as internet and mobile phones. Such crimes may threaten nation's security and financial health (Akogwu, 2012). Among such crime are cyber hacking and cyber identify.

Cyber hacking is the act of compromising digital devices and networks by gaining unauthorized access to an account or computer system. A key part of understanding cyber hacking is understanding the intent behind it, which usually involves the hacker seeking access to digital infrastructure, application data, and stealing sensitive customer information that could damage companies if leaked online. Cyber hacking is not always a malicious act, but it is most commonly associated with illegal activity and data theft by cyber criminals. Cyber hacking according to Fortinet (2023) refers to the misuse of devices like computers, smartphones, tablets, and networks to cause damage to or corrupt systems, gather information on users, steal data and documents, or disrupt data-related activity. Cyber hacking is the activity of identifying weaknesses in a computer system or a

network to exploit the security to gain access to personal data or business data. Equally, over reliance on online transaction without putting appropriate mechanisms has also create an opportunity for fraud like identify theft.

Identity theft consists of obtaining sufficient information about different individual and forged the link which enables the thief to obtain the goods and services while accrediting the burden to another person's account. Merriam-Webster online dictionary define identity theft as the illegal use of someone else's personal information (such as a Social Security number) especially in order to obtain money or credit. Daniel (2015) explained that there are diverse forms of systems which are used by identity fraud offenders to defraud victims. Some of these techniques include technical and social engineering attacks tactics. These ranged from technical and social engineering attacks strategies. The social engineering attacks happens when somebody is either in person, in a phone or computer, implores tactics to deceive different person to reveal sensitive information. In the same manner, cybercriminal who are ICT compliant may trick the internet to redirect people e-mails to a different location without their permission. They could do this by discovery user's passwords through hacking, recovering individual data through social media, or sending phishing emails.

Today, the student's population is estimated to form the largest unit of the total population of about 140 million people and more than 2.1 million population of students are currently studying in Nigerian Universities (Idoko, 2021). The students' life could be challenging with peer and socio-economic factor influences. These factors among others have great effect on students on several issues like what is right and wrong. Students like to explore into any area of life, especially interesting and alluring nature. With the breakthrough in information technology through the use of Internet facilities, knowing about the cyber hacking and cyber identity may be assisted through knowledge. Knowledge is a familiarity or awareness of someone or something contributing to one's understanding. A high-level knowledge about the cyber hacking and cyber identity by young people particularly the student should be given in educational institutions. All the security breaches such as cyber identity theft and cyber hacking are the direct cause of carelessness and lack of knowledge and action on the part of users (Chen, 2018).

Cyber identity theft and cyber hacking have become a stubborn mouth sore which causes us a lot of pain and shame because criminally minded individuals in the country are stealing and committing atrocity through the aid of the internet online business transactions. The youths particularly students in every society are of great importance and concern to that society because they are looked upon as the leaders of tomorrow. Olaide and Adewole (2014), observed that a sizeable number of criminals in Nigeria fall within the youthful age. The youths therefore at present have discovered different ways of using the internet in doing different types of criminal activities and these age brackets are usually found in tertiary institutions in Nigeria. Thus, a study on assessment of knowledge of undergraduate social studies towards cyber hacking and cyber identity theft in North-west, Nigeria becomes necessary.

Statement of the Problem

In Nigeria today, young people mostly especially tertiary institution students are the ones who engage in this form of anti-social behaviour for the purpose of living a life of splendour. This menace has created a high level of disinterest in education and touting among young people. The internet has also become an environment where the most lucrative and safest crime thrives for the youths. The researcher observed that so many persons have been duped or fallen victims of cybercrimes. The Individuals now hide under the faceless nature and the ease of access offered by the internet to perpetuate criminal acts. The researcher also observed that cybercrimes has causes a lot of pain and shame to people because criminally minded individuals in the country are stealing and committing atrocity through the aid of the internet online business transactions. The incident can rightly be said to be on the increase in the country due to lack of security awareness and under reportage respectively. Although some people's level of knowledge of the net is observably just for chatting with their friends and may be get information there from, most of them may not be in the position to protect their data or information and computer from malicious programmers. Noting these observations, the researcher is therefore triggered to carryout study on assessment of knowledge of undergraduate social studies towards cyber hacking and cyber identity theft in North-west, Nigeria

Objectives of the study

The following objectives were achieved in this study

i. Assess the knowledge of undergraduate Social Studies towards cyber hacking in North-West, Nigeria.
ii. Assess the knowledge of undergraduate Social Studies towards cyber identity theft in North-West, Nigeria.

Research Questions

The following research questions were answered in this study:

i. What is the knowledge of undergraduate Social Studies towards cyber hacking in North-West, Nigeria?
ii. What is the knowledge of undergraduate Social Studies towards cyber identity theft in North-West, Nigeria?

Research Hypotheses

The following hypotheses were tested in this study:

HO_1: There is no significant difference in the knowledge of undergraduate Social Studies towards cyber hacking in North-West, Nigeria

HO_2: There is no significant difference in the knowledge of undergraduate Social Studies towards cyber identity theft in North-West, Nigeria.

Methodology

This study adopted descriptive survey design. Descriptive survey design sets out to describe and to interpret what is. It aimed to describe the state of affairs as it exists. The study population consisted of all 400 level Undergraduate Social Studies s in Colleges of Education in North-West Nigeria. The total population of 400 level Undergraduate Social Studies in Colleges of Education in North-West Nigeria was 512. The sample size of this study was two hundred and seventeen (217). This sample size was adequate based on the Research Advisors (2010), a sample size of 217 is adequate for population of 512. In order to achieve selection of the sample from the population, multi stage sampling technique which involve purposive sampling technique, Proportionate sampling technique and Simple random sampling technique. A structured questionnaire designed by the researcher on a four-point rating scale of strongly agreed (SA), agreed (A), disagreed (D) and strongly disagreed (D) was used as instrument for data.

The questionnaire was face and content validated by experts from the Department of Arts and Social Science Education, Faculty of Education, Ahmadu Bello University, Zaria. In line with the suggestion given, amendment was made to improve the clarity and relevance of the instrument. Twenty (20) copies of questionnaire were used as a pilot testing for the study to test the reliability of the instrument. A reliability coefficient value of 0.76 was obtained using the Cronbach alpha Coefficient. The data were finally collected by the researcher with the aid of three trained research assistants. The research questions were analyzed using mean and standard deviation. The null hypotheses were tested at 0.05 level of significant using one sample T-test.

Results and Discussion

Table 1: Mean score of respondents on knowledge of undergraduate Social Studies towards cyber hacking in North-West, Nigeria

S/N	Items	SA	A	D	SD	Mean	Std. Deviation
1	I know what to do if my passwords are hacked	197	10	3	7	3.83	0.73
2	I don't have enough knowledge about hacking	140	40	30	7	3.45	0.50
3	I recognize emails that are hacked when I receive them	90	44	35	48	2.81	0.99
4	I know what to do when I witness any sort of hacking	194	10	7	6	3.81	0.57
5	I know that people who commit hacking are very intelligent	189	11	8	9	3.75	0.59
6	I know how to use social networking sites and technology to track hackers	132	44	23	18	3.34	0.73
7	I know how to protect my information from hackers very well.	206	3	3	5	3.89	0.31
8	I know how to secure my account against hackers.	205	5	2	5	3.89	0.31

9	The school curriculum adequately addresses the topic of hacking in Social Studies courses`	140	44	17	16	3.42	0.49
10	I have encountered discussions about hacking in my Social Studies coursework.	160	39	8	10	3.61	0.59
	Cumulative mean					**3.58**	**0.58**

Decision/benchmark mean = 2.50

Table 1 presented result on knowledge of undergraduate Social Studies towards cyber hacking in North-West, Nigeria. Item (1) indicated that, the mean score of 3.83 is higher than the rating scale of 2.50, which mean that the respondents agreed that they know what to do if their passwords are hacked. Item (2) showed that mean score of 3.75 is higher than the rating scale of 2.5 which means respondents agreed that they don't have enough knowledge about hacking. Item (3) showed that mean score of 2.81is higher than the rating scale of 2.5 which means respondents agreed that they recognize emails that are hacked when they receive them. Item (4) showed that mean score of 3.81 is higher than the rating scale of 2.5 which means respondents agreed that they know what to do when they witness any sort of hacking. Item (5) showed that mean score of 3.75 is higher than the rating scale of 2.5 which means respondents agreed that they know that people who commit hacking are very intelligent. Item (6) showed that mean score of 3.34 is higher than the rating scale of 2.5 which means respondents agreed that they know how to use social networking sites and technology to track hackers.

Item (7) showed that mean score of 3.89 is higher than the rating scale of 2.5 which means respondents agreed that they know how to protect their information from hackers very well. Item (8) showed that mean score of 3.89 is higher than the rating scale of 2.5 which means respondents agreed that they know how to secure their account against hackers. Item (9) showed that mean score of 3.42 is higher than the rating scale of 2.5 which means respondents agreed that the school curriculum adequately addresses the topic of hacking in Social Studies courses. Finally, Item (10) showed that mean score of 3.61 is higher than the rating scale of 2.5 which means respondents agreed that they have encountered discussions about hacking

in their Social Studies coursework. From the analysis, the mean score of nine items were found to be higher than the index score of 2.50 for agree, while the mean score of one item is less than the rating scale of 2.5. However, the aggregate mean value was found to be higher than the index score for agree (3.58 >2.50) with standard deviation of 0.58. This implies that undergraduate Social Studies have adequate knowledge towards cyber hacking in North-West, Nigeria.

Table 2: Mean score of respondents on the knowledge of undergraduate Social Studies towards cyber identify theft in North-West, Nigeria

S/N	Items	SA	A	D	SD	Mean	Std. Deviation
11	The topic of identity theft has been adequately covered in my Social Studies coursework.	183	23	5	6	3.77	0.81
12	I know how people use other people information to cheat	151	30	18	18	3.45	0.55
13	I know how to spread wrong info by means of using other person's profile	153	40	10	14	3.53	0.87
14	I know how to ensure that my profile is not used by another person.	148	38	11	20	3.45	0.49
15	I know how to block request from people I cannot identify	140	45	15	17	3.42	0.55
16	I know people forge information to dupe on my behalf	140	49	13	15	3.45	0.55
17	I aware of stealing people information to initiate transaction online	192	13	7	5	3.81	0.46

18	I have enough knowledge on tactics used to deceived people online	201	11	2	3	3.89	0.31
19	I understand the various methods through which identity theft can occur	198	5	11	3	3.83	0.69
20	I am aware of the potential consequences of falling victim to identity theft	191	13	10	3	3.81	0.700
	Cumulative mean					**3.65**	**0.59**

Decision/benchmark mean = 2.50

Table 2 presented the results on knowledge of undergraduate Social Studies towards cyber identify theft in North-West, Nigeria. Item (11) indicated that, the mean score of 3.77 is higher than the rating scale of 2.50, which mean that the respondents agreed that the topic of identity theft has been adequately covered in their Social Studies coursework. Item (12) showed that mean score of 3.45 is higher than the rating scale of 2.5 which means respondents agreed that they know how people use other people information to cheat. Item (13) showed that mean score of 3.53 is higher than the rating scale of 2.5 which means respondents agreed that they know how to spread wrong info by means of using other person's profile. Item (14) showed that mean score of 3.45 is higher than the rating scale of 2.5 which means respondents agreed that they know how to ensure that their profile is not used by another person. Item (15) showed that mean score of 3.42 is higher than the rating scale of 2.5 which means respondents agreed that they know how to block request from people they cannot identify. Item (16) showed that mean score of 3.45 is higher than the rating scale of 2.5 which means respondents agreed that they know people forge information to dupe on their behalf.

Item (17) showed that mean score of 3.81 is higher than the rating scale of 2.5 which means respondents agreed that they aware of stealing people information to initiate transaction online. Item (18) showed that mean score of 3.89 is higher than the rating scale of 2.5 which means respondents agreed that they have enough knowledge on tactics used to deceived people online. Item (19) showed that mean score of 3.83 is higher than the rating scale of 2.5 which means respondents agreed

that they understand the various methods through which identity theft can occur. Finally, Item (20) showed that mean score of 3.81 is higher than the rating scale of 2.5 which means respondents agreed that they are aware of the potential consequences of falling victim to identity theft. From the analysis, the mean score of all the ten items were found to be higher than the index score of 2.50 for agree, this can also be seen in the aggregate mean value found to be higher than the index score for agree (3.65 >2.50) with standard deviation of 0.59. This implies that undergraduate Social Studies students have adequate knowledge towards cyber identity theft in North-West, Nigeria.

Test of Hypotheses

The null hypotheses were tested using one sample t-test at 0.05 level of significance.

Hypothesis one: There is no significant difference in the knowledge of undergraduate Social Studies students towards hacking in North-West, Nigeria.

Table 3: One sample t-test on significant difference in the knowledge of undergraduate Social Studies towards hacking in North-West, Nigeria

Variable	N	Mean	Std. deviation	t-value	Df	p-value	Decision
Knowledge of undergraduate Social Studies towards cyber hacking	217	3.48	0.58	33.289	216	0.000	Rejected

t (216) = 1.972, p <0.05

Table 3 shows the significant difference in the knowledge of undergraduate Social Studies towards cyber hacking in North-West, Nigeria. The observed t-value obtained at 216 degrees of freedom (DF) for the test was 33.289 and it is higher than the critical value of 1.972 indicated at the bottom of the table. The observed level of significance (0.000) is less than the fixed level of 0.05 (P < 0.05). These observations provide enough evidence for rejecting the null hypothesis. This

shows that respondents highly believed that there is significant difference in the knowledge of undergraduate Social Studies towards cyber hacking in North-West, Nigeria. Therefore, the null hypothesis which stated that there is no significant difference in the knowledge of undergraduate Social Studies towards cyber hacking in North-West, Nigeria is hereby rejected.

Hypothesis two: There is no significant difference in the knowledge of undergraduate Social Studies towards cyber identify theft in North-West, Nigeria.

Table 4: One sample t-test on significant difference in the knowledge of undergraduate Social Studies towards cyber identify theft in North-West, Nigeria

Variable	N	Mean	Std. deviation	t-value	Df	p-value	Decision
knowledge of undergraduate Social Studies towards cyber identify theft	217	3.65	0.59	30.686	216	0.000	Rejected

t (216) = 1.972, p <0.05

Table 4 shows the significant difference in the knowledge of undergraduate Social Studies towards cyber identify theft in North-West, Nigeria**.** The observed t-value obtained at 216 degrees of freedom (DF) for the test was 30.686 and it is higher than the critical value of 1.972 indicated at the bottom of the table. The observed level of significance (0.000) is less than the fixed level of 0.05 (P < 0.05). These observations provide enough evidence for rejecting the null hypothesis. This shows that respondents highly believed that there is significant difference in the knowledge of undergraduate Social Studies towards cyber identify theft in North-West, Nigeria. Therefore, the null hypothesis which stated that there is no significant difference in the knowledge of undergraduate Social Studies towards cyber identify theft in North-West, Nigeria is hereby rejected.

Discussion of findings

The finding of hypothesis one revealed that social studies undergraduates differ in their knowledge on hacking as cybercrime in North-west, Nigeria. The result of data analysis on hypotheses one illustrates that the t = 33.289, df = 217, p = 0.000, which indicates that the probability value (p) is less than the alpha level ($p < 0.05$). This showed that social studies undergraduates differ in their knowledge on hacking as cybercrime in North-west, Nigeria. The finding of this study is in line with the findings of Fortinet (2023) who stated the misuse of devices like computers, smartphones, tablets, and networks to cause damage to or corrupt systems, gather information on users, steal data and documents, or disrupt data-related activity shows difference in knowledge about hacking. The findings is supported by Lawrence, (2023) who stated that hacking is the activity of identifying weaknesses in a computer system or a network to exploit the security to gain access to personal data or business data. The findings was also in line with Hiley, (2022) who stated that the knowledge about hacking evolve and increase in sophistication and gave birth to a wide range of types of hacking and hackers.

The finding of hypothesis two confirmed that social studies undergraduates differ in their knowledge of identity theft as cybercrime in North-west, Nigeria. The result of data analysis on hypotheses two illustrates that the t = 30.686, df = 217, p = 0.000, which indicates that the probability value (p) is less than the alpha level ($p < 0.05$). This shows that social studies undergraduates differ in their knowledge of identity theft as cybercrime in North-west, Nigeria. This finding corroborates with that of Bert-Jaap & Ronald (2020), who found that knowledge about identity theft is often perceived as one of the major upcoming threats in crime. The findings are also supported by Daniel (2015) who explained that the diverse forms of systems which are used by identity fraud offenders to defraud victims are done through awareness. The finding is also in line with Anderson, Durbin & Salinger, (2018) who state that the awareness on identify theft leads to over dependence on data for payments and have also breed new prospects for fraud.

Conclusion

Based on the findings from the study, it was concluded that students exhibit positive knowledge towards cyber hacking and identity theft. The significant differences observed in their knowledge indicate a varied level of understanding

and awareness among the students. The rejection of all null hypotheses suggests that there are distinct differences on how the students understand and involve in cybersecurity issues in colleges of education in North-West Nigeria and they prepare better to navigate the digital landscape and safeguard themselves from potential risks by increasing their knowledge and understanding of cybersecurity concerns.

Recommendations

i. Ministry of education should incorporate cyber security education into Social Studies curricula to provide students with a comprehensive understanding of hacking, its historical context, and its impact on society.
ii. Government should organize workshops or seminars specifically focusing on identity theft awareness. Government should also invite experts in cybersecurity or law enforcement agencies to speak about the risks, prevention strategies, and legal consequences associated with identity theft.

References

Akogwu, S. (2012). An Assessment of the Level of Awareness on Cyber Crime among Internet Users in Ahmadu Bello University, Zaria. Department of Sociology, Ahmadu Bello University, Zaria.

Anderson, K. B., Durbin, E., & Salinger, M. A. (2018). Identity theft. *Journal of Economic Perspectives*, *22*(2), 171-192.

Chen, S.Y., (2018). Internet Use and Academic Achievement: *Gender Differences in Early Adolescence*. 44(176). Retrieved January 30, 2022, from: http://goo.gl/ZzkiOW.

Daniel, E. (2015). *Cybercrime in Ghana A Study of Offenders, Victims and the Law.* Doctoral dissertation, University of Ghana.

Fortinet C. (2023). *Hacking—Definition, Types, Security, and More*. Retrieved from https://www.fortinet.com/corporate/about-us/about-us on 10th July, 2023

Hiley C (2022). *Brief history of cybersecurity and hacking*. Retrieved from https://cybernews.com/security/brief-history-of-cybersecurity-and-hacking/ on 7th July, 2023

Idoko, C (2021). *2.1 million Students studying in Nigerian Universities*. Retrieved on February, 2022 from www.tribune Online.htm

Lawrence W. (2023). What is Hacking? Types of Hackers (Introduction to Cyber Crime) retrieved from https://www.guru99.com/what-is-hacking-an-introduction.html on 17th June, 2023

Olaide H. & Adewole Y. (2014). *Cyber Crime Embarrassing for Victims*. Retrieved January 2022 from http//www.heraldsun.com.au