Education

Cybercrimes and sustainable development in deposit money banks in Nigeria

Njidofor Obiageli C[1], Iyke-Ofoedu Maureen Ifeoma[1*] and Adaora Chinelo Uzochukwu[1]

[1] Department of Management, University of Nigeria, Enugu Campus, Nigeria

Correspondence Author: Iyke-Ofoedu Maureen Ifeoma

Received 8 May 2025; Accepted 23 June 2025; Published 4 July 2025

DOI: https://doi.org/10.64171/JAES.5.3.01-08

Abstract

This study examined effect of cybercrimes on sustainable development in deposit money banks in Nigeria. The specific objectives were to: evaluate the effect of Automated teller machine (ATM) skimming on sustainable development of deposit money banks DMBs in Nigeria and (ii) ascertain the effect of phishing scams cybercrime on sustainable development of deposit money banks DMBs in Nigeria. Study area was Enugu State Nigeria. The research design of the study was descriptive survey design. The study used structured questionnaire to obtain data. The population of the study comprised of 773,000 bank users in Enugu State. The sample size of 371 respondents was drawn from population of the study using Freund and Williams sampling technique. Research questions were answered using frequency, mean and standard deviation. The hypotheses stated were tested using single regression statistic. The empirical result showed that: automated teller machine (ATM) skimming has negatively significant effect on sustainable development of deposit money banks DMBs in Nigeria (t-statistic; -8.954; *p*-value; 0.000 < Sig-value; 0.05) and phishing scams cybercrime has negatively significant effect on sustainable development of deposit money banks DMBs in Nigeria (t-statistic; -6.491; *p*-value; 0.000 < Sig-value; 0.05). The study concluded that cybercrime has negatively significant effect on sustainable development of deposit money banks DMBs in Nigeria. The study recommended that government should provide digital national identification card for each Nigerian, as well as a centralized national database of citizens and immigrants, should be provided to detect fraudsters.

Keywords: Cybercrime, Sustainable development, Automated Teller Machine (ATM) skimming, Phishing cybercrime

1.1 Background of the study

Cybercrime has taken a back seat in the Nigerian banking sector. Hardly does a day pass without one form of cyber-attack or the other on the bank customers. In recent times, our society is increasingly relying on the internet and other information technology tools to engage in personal communication and conduct business activities among other several benefits. While these developments allow for enormous gain in productivity, efficiency and communication they also create a loophole which is cybercrime. Cybercrime has been a social problem as its perpetrators are mostly the youths who are supposed to be the leaders of tomorrow. This aligns with the position of Ama, Onwubiko and Nwankwo, (2024) [3] who noted that cyber terrorism has become one of the biggest threats to the survival of mankind on the planet. Olalekan, Rakiya and Ayanwuyi, (2024) [12] also noted that the global village currently records an increasing criminal behavior. News of cybercriminal activities such as fraud, theft, blackmail, forgery, and embezzlement continue to fill the pages of the newspaper, it is central to world news and has become a global problem.

Cybercrime is a new form of crime with its own forms which according to Okonkwo, Emayomi and Akamike, (2023) [11] includes; cloning of websites, false representations, internet purchase and other e-commerce kinds of fraud (Ribadu, 2020) [14]. Financial fraud, identity theft, credit card theft, cyber theft, cyber harassment, cyber laundering and virus/ worms/ Trojans respectively now abound in Nigeria (Fadairo-Cokers and Ibrahim, 2021) [6] which is denting and drilling holes in the economy of the nation. In Nigeria, the disturbing trend of increase in electronic fraud (e-fraud) cybercrime across major sectors of the Nigerian economy especially deposit money banks are alarming. The incidence of electronic fraud cybercrime which resulted in massive acceptance of new mode of mobile money and electronic banking and payment systems has been discovered to cost Nigeria a huge sum of money annually (Akintoye, Ogunode, Modupe, Abimbola, 2022) [2]. Nigeria Electronic Fraud Forum (NeFF) in its annual report for 2018, reported electronic fraud of N5.571 billion between 2015 and 2017.

Most of these electronic fraud cybercrimes are achieved via hacking of banks customer account and data base, and these have been targeted both locally and internationally, thus precipitating losses in billions of naira. The Central Bank of Nigeria (CBN) in 2018 classifies e-fraud as the highest risk in the banking sector which involves different e-payment classifications, which in itself have encountered hacking by electronic fraudsters. The growth experienced from the possible enhancement of the electronic banking and its juicy services that has continued to facilitate ease of monetary transactions among customers is however challenged by the continuous presence and threat of cybercrime. This study intends to ascertain how cybercrime has affected the sustainable development in deposit money banks DMBs in Nigeria.

1.2 Statement of the problem

Deposit money banks in Nigeria have recorded about 3.9 billion users of the internet, owing to that internet has become one of the greatest technological developments. While widely accepted for its ease and efficiency, it is also embedded with a multitude of vulnerabilities, which pose significant security threats to users and has led to the emergence of cybercrime.

Cybercrime, which includes any crime committed with the aid of a computer and network (e.g. phishing, bank verification number scams, fraudulent emails, hacking, cyber harassment, spamming, ATM spoofing, social media hi-jacking etcetera), exploits vulnerabilities of both electronic devices and their users. In Nigeria, a number of key factors - such as a high rate of unemployment, the quest for wealth, a lack of strong cybercrime laws, and incompetent security on personal devices amongst others - have coalesced to make cybercrime a significant problem for the country. The estimated annual financial loss in Nigeria due to cybercrime was N250 billion ($649 million) in 2017 and N288 billion ($800 million) in 2018 (Nigeria Electronic Fraud Forum (NEFF) annual report, 2018). Cybercrime destroys the reputation of a country and make business environment difficult for start-ups small and medium-sized enterprises. It also discourages investment in the economy by foreign companies. For individuals, cybercrime results in the loss of financial resources, intellectual property or personal confidential information, and the damages can be extreme, often targeting senior citizens and people who are vulnerable. Against these backdrops, there is need to examine effect of cybercrime on sustainable development of deposit money banks DMBs in Nigeria.

1.3 Objective of the study

The main objective of this study is to examine the effect of cybercrimes on sustainable development of deposit money banks DMBs in Nigeria. The specific objectives are to:

- Evaluate the effect of Automated Teller Machine (ATM) skimming on sustainable development of deposit money banks DMBs in Nigeria.
- Ascertain the effect of phishing cybercrime on sustainable development of deposit money banks DMBs in Nigeria.

1.4 Research questions

The study aimed to answer the following questions

- What is the extent to which Automated teller machine (ATM) skimming affects sustainable development of deposit money banks DMBs in Nigeria?
- What is the extent to which phishing cybercrime affects sustainable development of deposit money banks DMBs in Nigeria?

1.5 Significance of the study

This would be beneficial and important to the following groups of individuals and groups namely: bank management, staff and customers-

Bank management: The outcome the study would be importance to bank management that involve in the financial services information and network management portfolios because it proposes security measures on how to protect the financial institutions information and network resources against the cybercrimes.

Bank staff and customers of financial institutions: The outcome the study would be importance because it aims to contribute to the existing literature that educates both staff and customers of financial institutions of the potential vulnerabilities and threats associated with financial institutions' IT resources, and online transactions.

2.1 Conceptual literature

2.1.1 Cybercrime

In (Adewumi, 2021) cybercrime was defined as a type of crime committed by criminals who make use of a computer as a tool and the internet as a connection in order to reach a variety of objectives such as illegal downloading of music files and films, piracy, spam mailing and the likes. Cyber-crime evolves from the wrong application or abuse of inter-net services.

Cybercrime is defined as crimes committed on the internet using the computer as either a tool or a targeted victim. However, all cybercrimes involve both the computer and the person behind it as victims, it just depends on which of the two is the main target. Hence, the computer will be looked at as either a target or tool for simplicity's sake. For example, hacking involves attacking the computer's information and other resources (Chukwu, 2021) [5].

Cybercrime is seen as computer crime, computer-related crime, digital crime, information technology crime and cybercrime could reasonably include a wide difference in criminal activities (Onah, Onodugo & Ugwu, 2023) [13]. In the 10th conference on Prevention of Crime and Treatment of Offenders, a conference dedicated to the activities on crimes related to computer networks which were carried out by United Nations Congress, cybercrime activity was subdivided into two definitions. Firstly, Cybercrime in a narrow sense of definition is an illegal activity directed by the process of electronic operations that are targeted towards the security of computer systems and the data processed by them. Secondly, cybercrime in a broader sense of definition is an illegal activity done utilizing, or about, a computer system, which includes crimes as illegal possession and offering or distributing information using a computer system (United Nations, 2020).

2.1.2 Sustainable development

Sustainable development can be defined as the practice of maintaining the productivity by replacing used resources with resources of equal or greater value without degrading or endangering natural biotic systems. Sustainable development binds together concern for the carrying capacity of natural systems with the social, political and economic challenges faced by humanity (Godswill, 2017) [7].

2.2 Contextual literature

2.2.1 Automated Teller Machine (ATM) skimming and sustainable Development in DMBs

ATM skimming refers to a type of cybercrime where criminals steal cardholders' data by attaching unauthorized devices (skimmers) to ATMs to capture card information and PINs, which they then use to create fraudulent payment cards. ATM skimming is a form of financial fraud in which devices called "skimmers" are used to steal credit or debit card information at cash withdrawal terminals. ATM skimming involves installing a device on an ATM's card reader to capture card data. Criminals may also use hidden cameras or fake keypads to record PINs (Hassan, Lass & Makinde, 2019) [8].

Automated teller machine (ATM) skimming is also known as theft of bank cards: The theft of bank cards has evolved from the physical theft of the card to simply the theft of the numbers. Today, bank card hackers do not need to be in the same country to steal other people's identities. Fraudsters make use of hidden cameras to record ATM card pins and numbers in distinct places such as an eatery payment using Pos, or at the ATM. According to the Federal Bureau of Investigation (FBI), a method known as ATM skimming can be used and it involves placing an electronic device on an ATM that scoops information from a bank card's magnetic strip whenever a customer uses the machine (FBI, 2021).

Internet other frauds involve fraudster inputting stolen cards numbers on online commercial sites to order goods. Credit card numbers or ATM numbers can be stolen by hackers when users type the credit card number into the Internet page of the seller for online transaction. Different applications can be used to retrieve the information such as key loggers at cybercafés or cloned websites (Ribadu, 2020) [14].

2.2.2 Phishing cybercrime and sustainable Development in DMBs

Phishing is simply the theft of an identity. It involves stealing personal information from unsuspecting users and it is also an act of fraud against the authentic, authorized businesses and financial institutions that are victimized (Wada). Phishing scams are ubiquitous and are exponentially increasing. It has become one of the fastest growing cybercrimes in Nigeria. In this jet age of technology, hoi polloi subscribes to a plethora of sites using their email ad-dresses and are therefore expecting to receive mails of up-dates of their membership or subscription. So, it seems natural when users get regular mails from such organizations. Fraudsters have devised a means to mimic authorized organizations and retrieve confidential information from clients (Kekii, 2023) [9]. In Phishing email messages, the fraudsters find a way to convince and gain the trust of users. An instance of such mail is shown in the figure below showcasing a fraudster trying to build the trust of a client in order to convince them to give up personal banking information. In Nigeria, phishing mails are mostly carried out on bank customers (Ama, Onwubiko, & Nwankwo, 2024) [3].

2.3 Theoretical literature

2.3.1 Theory of Planned Behavior (TPB)

The theory of planned behavior (TPB) is an advancement of the theory of reasoned action (TRA) based on the limitations that were identified with respect to the behavior of people studied. The theory of planned behavior introduced a new element, known as the perceived behavioral control (PBC) (Hardin-Fanning & Ricks, 2017). Perceived behavioral control has to do with determining whether an individual possess the ability to behave in a certain way (Haythornthwaite & Wellman, 2008). The theory of planned behavior is a model that forecasts an intentional behavior because it is believed that behavior may be planned or deliberates (Hughes, 2017). According to the model, the best predictor of behavior is the behavioral intention. The elements that predict the behavioral intention of an individual are attitude, subjective norms and the perceived behavioral control. Furthermore, there are three beliefs that guide the behavioral intention of an individual, which include: behavioral beliefs, normative beliefs and control beliefs (Human Rights Watch, 2018). The behavioral beliefs have to do with the outcome of behavior and the evaluation of behavior. On the other hand, normative beliefs have to do with perceived behavioral expectations from important referral persons around the person, while control beliefs have to do with beliefs on certain factors present that can facilitate the performance of behavior and the power behind these factors.

2.4 Empirical literature

Kekii, (2023) [9] examined cybercrime and economic sustainability of the Financial Institutions in Southeast, Nigeria, the major objectives of the research are: to examine the effect of bank verification number scam on the profitability of the financial institutions and to examine the effect of phishing on the customer base of the financial institutions in the South East. This study adopted survey research design. Frequency distribution table and simple percentages were used to analyze data for this study. Findings show that Bank Verification Number Scam negatively affects the profitability of the financial institutions in the Southeast, Nigeria (76.2%). This is because scammed customers are prone to closing their bank accounts consequent upon the loss, they incurred by means of cybercrime. Phishing negatively affects the customer base of the financial institutions in the Southeast, Nigeria. (76.2%). This is because loss to the financial institution's customer is an indirect loss to the financial institution. In view of the above, the following are recommendations: financial institutions' customers, on their part, should ensure proper security controls and make sure they install the latest security updates on their computer systems and carefully select the sites they visit while the financial institutions should make it a practice to always educate their customers of the ways to avoid cybercrime attacks.

Onah, Onodugo and Ugwu, (2023) [13] examined cyber fraud in the Nigeria Banking System in Enugu, Enugu State. Specifically, the study sought to identify the offenders, causes, impacts, and measures of control in Nigeria today. With the help of a survey (questionnaire) and an in-depth interview, primary data was obtained from ten carefully selected banks in Enugu, Enugu State, and the general public who could testify to the issue of cyber fraud in Nigeria. The data was analyzed using a simple percentage comparison and frequency tables. According to the study's findings, educated youngsters (especially males), bank workers, clients, and non-bank customers are the leading culprits of the cyber fraud issue in Nigeria. Several social, cultural, economic, and technological variables contribute to cyber fraud in Nigeria, and the national economy bears the brunt of the consequences (locally and internationally). The study recommended that jobs be created for youths; adequate modern security technology be installed in the banking sector; law enforcement agents be improved; and the public be educated on the implications of cyber fraud in order to reduce cyber fraud in the Nigeria banking system.

Akintoye, Ogunode, Modupe, Abimbola, (2022) [2] examined the impact of cybersecurity in driving the financial innovation of Deposit Money Banks in Nigeria. Specially, the study sought to examine the influence of risk management and bank monitoring on financial innovation in banking industry. The study adopted a survey research design with primary data obtained via a structured questionnaire administered to a sample size of fifty-six (56) Deposit Money Banks Staff purposively selected. The sampled staffs were senior member staff of key impacted departments while the Banks selected accounted for 93% of total market capitalization as on December 31, 2021. The primary data collected were analyzed using descriptive and inferential statistics. The study found that cybersecurity proxied by risk management and bank monitoring had a statistically and positively significant impact on financial innovation of deposit money banks in Nigeria (Adj.R2= 0.447, F(2,55)=23.274, $p< 0.05$). It recommended that deposit money banks should ensure regular review, revision and strengthening of their risk management framework to meet with emerging challenges from the deployment of financial innovative products and services.

Fadairo-Cokers and Ibrahim (2021) [6] examined the impact of cybercrimes on selected Deposit Money Banks (DMBs) in the Federal Capital Territory (FCT). The specific objectives of the study were to identify the influence of banking fraud on performance of deposit money banks in Nigeria. The study used structured questionnaires and the population of the study is the staff and management of the selected Deposit Money Banks (DMBs) in the Federal Capital Territory (FCT). The data analytical technique was descriptive mean analysis. The study also found that there is a high level of banking cybercrime activities in the (FCT), banks online protocols against banking cybercrime activities in (FCT) is adequate, fight against banking cybercrimes in the FCT by the related agencies is below expectation, poor financial literacy and low knowledge of internet operation are the major causes of banking cybercrimes and the awareness creation on banking cybercrimes by all the related agencies are adequate. Therefore, the study recommended that there should be more awareness creation on banking cybercrimes by all the related agencies to reduce the rate of online banking transactions and Automated Teller Machine (ATM) cybercrimes in the Federal Capital Territory (FCT).

Casmir and Oliver (2019) conducted a study to examine the public perceptions on the determinants of youths' involvement in cybercrime in Enugu Urban, Enugu Sate. Specifically, this study aims to examine the public perceptions on the determinants of youth's involvement in cybercrime in Enugu urban, Enugu sate. Survey design was used in which questionnaire and Focus Group Discussions were the major instruments. The questionnaires were distributed to one hundred and forty-four (1475) adults (18 years and above) in Enugu urban. Frequency distribution tables were used in analyzing the data. The findings show that indicated unemployment, poverty and lack of internet security respectively to be the major determinant on involvement of youths in cybercrime. The study recommends that curriculum which will include courses on entrepreneurship and business management be introduced to both tertiary and secondary schools where they are not in existence and where they are in existence that they should be strengthened to take care of the present problem of unemployment identified as the major cause of cybercrime.

2.5 Literature gaps

There exists research gap between this study and past researches. The research gap covers subject gap, gap on geographical location of the study, gap on the variables and contents of the study, gap on literature and gap on methodology.

Subject gap: The subject matter of this work and some reviewed empirical studies has some differences. There are limited studies that examine the effect of cybercrimes on sustainable development of deposit money banks DMBs in Nigeria. The study is geared to bridge the time gap in literature.

Gap on geographical location of the study: This work covers deposit money banks DMBs in Nigeria and specifically deposit money banks DMBs that operate in South East. None of the past studies used the First Bank of Nigeria, Guaranty Trust Bank, Zenith Bank Nigeria and Access Bank Nigeria as mentioned and most of the past studies were done outside South East Nigeria.

Gap on the variables and contents of the study: The variables used in this study includes Automated teller machine (ATM) skimming and phishing cybercrime (for independent variable) and sustainable development (for dependent variable) were not used by past researches.

Gap on methodology: The data analytical techniques used in this work in some ways differ from what was employed from past researches. The data analytical technique of the study was single regression method. The statistical technique was chosen because of its basic properties of best Linear, unbiased and efficient (BLUE) estimators. It is best for impact analysis.

3.1 Methodology

Study area was Enugu State Nigeria. The research design of the study was descriptive survey design. The study used structured questionnaire to obtain data. The choice of location was based on proximity, effective coverage and cost minimization. The population of the study comprised of 773,000 estimated population of indigenes of Enugu State (2006 Census). The sample size of 371 respondents was drawn from population of the study using Freund and Williams sampling technique. Research questions were answered using frequency, mean and standard deviation. The hypotheses stated were tested using single regression statistic.

3.2 Data presentation and analysis

Table 1: Comprehensive demographic distribution of respondents

Title	Frequency	Percentage
Questionnaire distribution		
Questionnaires Distributed	371	100%
Returned Questionnaires	358	96%
Not Returned Questionnaires	13	4%
Gender		
Female	213	59.5%
Male	145	40.5%
Age bracket		
20-30 Years	153	42.7%
31-40 Years	111	31.0%
41-50 Years	66	18.4%
51Years – above	28	7.8%
Marital status		
Married	223	62.3%
Single	125	34.9%
Widow/widower	7	1.9%
Divorce	3	0.8%

Sources: Field survey, 2025

Three hundred and seventy-one (371) copies of questionnaire were designed and distributed to the respondents. Out of the 371 Questionnaires distributed, 358 (96%) were completed and returned while 13 (4%) were not returned. Therefore, 96 percent respondents were a good representation. The table showed the respondents profile in frequency and percentage distribution of gender, age bracket and marital status.

3.3 Data analysis

Question one: What is the extent to which Automated teller machine (ATM) skimming affects sustainable development of deposit money banks DMBs in Nigeria?

Table 2: Mean rating of respondents on the extent to which Automated teller machine (ATM) skimming affects sustainable development of deposit money banks DMBs in Nigeria

S/N	Question Items	VGE (5)	GE (4)	ME (3)	LE (2)	VLE (1)	Total	Mean	SD
1	Automated teller machine (ATM) skimming result to providing incorrect information for the purpose of tricking money out of victims reduces customers' bank deposit.	780	496	174	24	8	1475	4.14	0.0029
		156	124	58	12	8	358		
		44%	34%	16%	3%	2%	100%		
2	Internet fraud covers a range of illegal and illicit actions that are committed in cyberspace to obstruct smooth banking transaction	620	624	144	40	10	1438	4.02	0.0027
		124	156	48	20	10	358		
		35%	44%	13%	5%	2%	100%		
3	Cybercrime devices tactics to exploit individuals, steal personal information, and disrupt banks' computer and information security networks.	1065	364	126	18	3	1576	4.40	0.0034
		213	91	42	9	3	358		
		59%	25%	12%	2%	0.8%	100%		
4	Automated Teller Machine (ATM) skimming involves gaining unauthorized access to data in banks' computer or network and steal data ranging from personal information and corporate secrets.	985	416	111	24	8	1544	4.31	0.0032
		197	104	37	12	8	358		
		55%	29%	10%	3%	2%	100%		
	Grand Mean							4.218	0.0031

Source: Field survey, 2025

This table showed the opinion of respondents on the extent to which Automated teller machine (ATM) skimming affects sustainable development of deposit money banks DMBs in Nigeria. The respondents are in agreement with all the items. The research items 1,2,3,4, have mean score of above 4.0 point respectively and it was rated great extent by respondents. Thereby study revealed that Automated teller machine (ATM) skimming has negatively significant effect on sustainable development of deposit money banks DMBs in Nigeria since Automated teller machine (ATM) skimming result to providing incorrect information for the purpose of tricking money out of victims reduces customers' bank deposit. (Grand-mean 4.218 was greater than the cutoff point 3).

Question Two: What is the extent to which phishing scams cybercrime affects sustainable development of deposit money banks DMBs in Nigeria?

Table 3: Mean rating of responses of respondents on the extent to which phishing scams cybercrime affects sustainable development of deposit money banks DMBs in Nigeria

S/N	Question Items	VGE (5)	GE (4)	ME (3)	LE (2)	VLE (1)	Total	Mean	SD
1	The cybercrime involves stealing personal information from unsuspecting users for the purpose of tricking money out of victims thereby reduces customers' bank deposit.	780	496	174	24	8	1475	4.14	0.0029
		156	124	58	12	8	358		
		44%	34%	16%	3%	2%	100%		
2	The phishing scammer uses identity theft to execute clearing fraud, opening fraud and counterfeit securities in DMBs	620	624	144	40	10	1438	4.02	0.0027
		124	156	48	20	10	358		
		35%	44%	13%	5%	2%	100%		
3	The phishing scammer trying to build the trust of a client in order to convince them to give up personal banking information to siphon money from them.	1065	364	126	18	3	1576	4.40	0.0034
		213	91	42	9	3	358		
		59%	25%	12%	2%	0.8%	100%		
4	The cybercrime uses identity theft to perpetuate money transfer fraud, forged cheques and execute cheque kitting in DMBs	985	416	111	24	8	1544	4.31	0.0032
		197	104	37	12	8	358		
		55%	29%	10%	3%	2%	100%		
	Grand Mean							4.218	0.0031

Source: Field survey, 2021

This table showed the opinion of respondents on the extent to which phishing scams cybercrime affects sustainable development of deposit money banks DMBs in Nigeria. The respondents are in agreement with all the items. The research items 1,2,3,4, have mean score of above 4.0 point respectively and it was rated great extent by respondents. Thereby study revealed that phishing scams cybercrime has negatively significant effect on sustainable development of deposit money banks DMBs in Nigeria since phishing scammer trying to build the trust of a client in order to convince them to give up personal banking information to siphon money from them (Grand-mean 4.218 was greater than the cutoff point 3).

3.4 Test of hypotheses

3.4.1 Test of hypothesis one

Automated Teller Machine (ATM) skimming has no significant effect on sustainable development of deposit money banks DMBs in Nigeria.

Model summary

Model	R	R square	Adjusted R square	Std. error of the estimate
1	.917[a]	.840	.840	.40781

a. Predictors: (Constant), Automated teller machine (ATM) skimming

ANOVA[a]

	Model	Sum of squares	Df	Mean square	F	Sig.
1	Regression	34.556	1	34.556	15.954	.000[b]
	Residual	773.262	357	2.166		
	Total	807.818	358			

a. Dependent Variable: Sustainable Development

b. Predictors: (Constant), Automated teller machine (ATM) skimming

Coefficients[a]

	Model	Unstandardized coefficients		Standardized coefficients	t	Sig.
		B	Std. error	Beta		
1	(Constant)	.640	.113		5.645	.000
	Automated Teller Machine (ATM) skimming	-.208	.025	.917	-8.312	.000

a. Dependent Variable: Sustainable Development

In testing this hypothesis, Automated teller machine (ATM) skimming was regressed against sustainable development. The result of the single-regression analysis showed the model to examine the effect of Automated teller machine (ATM) skimming on sustainable development of deposit money banks DMBs in Nigeria

Sustainable development = 0.640 - 0.208 Automated Teller Machine (ATM) skimming

The empirical result showed that the coefficient of Automated teller machine (ATM) skimming has negative effect on sustainable development; it means that Automated teller machine (ATM) skimming had negative and indirect effect on sustainable development. The result of the t – statistics denotes that the coefficient of Automated teller machine (ATM) skimming was statistically significance because the observed values of t – statistics (-8.312) is greater than its P-values (0.000). The result of the F – statistical test showed that the overall regression of the hypothesis one was statistically significance because the observed value of the F – statistics (15.954) was great than its P-value (0.000). Again, our empirical result showed that the Pearson product moment correlation analysis (r) was 0.917. The strength of relationship between the two variables was high. However, we rejected the null hypothesis and conclude that Automated teller machine (ATM) skimming had negatively significant effect on sustainable development of deposit money banks DMBs in Nigeria.

3.4.2 Test of hypothesis two

Phishing scams cybercrime has no significant effect on sustainable development of deposit money banks DMBs in Nigeria.

Model summary

Model	R	R square	Adjusted R square	Std. error of the estimate
1	.932[a]	.869	.868	.37028

a. Predictors: (Constant), Phishing scams cybercrime

ANOVA[a]

	Model	Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	24.229	1	24.229	11.338	.000[b]
	Residual	762.909	357	2.137		
	Total	787.138	358			

a. Dependent Variable: Sustainable Development

b. Predictors: (Constant), Phishing scams cybercrime

Coefficients[a]

Model		Unstandardized coefficients		Standardized coefficients	t	Sig.
		B	Std. error	Beta		
1	(Constant)	.650	.102		6.401	.000
	Phishing scams cybercrime	-.409	.063	.932	-6.491	.000

a. Dependent Variable: Sustainable Development

In testing this hypothesis, phishing scams cybercrime was regressed against sustainable development. The result of the single-regression analysis shows the model to examine the effect of phishing scams cybercrime on sustainable development of deposit money banks DMBs in Nigeria.

Sustainable development = 0.640 - 0.409 phishing scams cybercrime

The empirical result showed that the coefficient of phishing scams cybercrime had positive effect on sustainable development; it means that phishing scams cybercrime has negative and inverse effect on sustainable development. The result of the t – statistics denotes that the coefficient of phishing scams cybercrime was statistically significance because the observed values of t – statistics (6.491) was greater than its P-values (0.000). The result of the F – statistical test showed that the overall regression of the hypothesis one was statistically significance because the observed value of the F – statistics (11.338) was great than its P-value (0.000). Again, our empirical result showed that the Pearson product moment correlation analysis (r) was 0.932. The strength of relationship between the two variables was high. However, we rejected the null hypothesis and concluded that phishing scams cybercrime had negatively significant effect on sustainable development of deposit money banks DMBs in Nigeria.

4.3 Discussion of the findings

4.3.1 Effect of Automated Teller Machine (ATM) skimming on sustainable development of deposit money banks DMBs in Nigeria

The findings of the study revealed that that Automated teller machine (ATM) skimming has negatively significant effect on sustainable development of deposit money banks DMBs in Nigeria since Automated teller machine (ATM) skimming result to providing incorrect information for the purpose of tricking money out of victims reduces customers' bank deposit (t-statistic; -8.954; *p*-value; 0.000 < Sig-value; 0.05).

The outcome of the study was in line with the study of Kekii, (2023) [9] that examined cybercrime and economic sustainability of the Financial Institutions in Southeast, Nigeria, the major objectives of the research are: to examine the effect of bank verification number scam on the profitability of the financial institutions and to examine the effect of phishing on the customer base of the financial institutions in the South East. This study adopted survey research design. Frequency distribution table and simple percentages were used to analyze data for this study. Findings show that Bank Verification Number Scam negatively affects the profitability of the financial institutions in the Southeast, Nigeria (76.2%). This is because scammed customers are prone to closing their bank accounts consequent upon the loss, they incurred by means of cybercrime. Phishing negatively affects the customer base of the financial institutions in the Southeast, Nigeria. (76.2%). This is because loss to the financial institution's customer is an indirect loss to the financial institution.

4.3.2 Effect of phishing cybercrime on sustainable development of deposit money banks DMBs in Nigeria

The findings of the study revealed that phishing scams cybercrime has negatively significant effect on sustainable development of deposit money banks DMBs in Nigeria since phishing scammer trying to build the trust of a client in order to convince them to give up personal banking information to siphon money from them (t-statistic; -6.491; P-value; 0.000 < Sig-value; 0.05).

The outcome of the study was in line with the study of Onah, Onodugo and Ugwu, (2023) [13] that examined cyber fraud in the Nigeria Banking System in Enugu, Enugu State. Specifically, the study sought to identify the offenders, causes, impacts, and measures of control in Nigeria today. With the help of a survey (questionnaire) and an in-depth interview, primary data was obtained from ten carefully selected banks in Enugu, Enugu State, and the general public who could testify to the issue of cyber fraud in Nigeria. The data was analyzed using a simple percentage comparison and frequency tables. According to the study's findings, educated youngsters (especially males), bank workers, clients, and non-bank customers are the leading culprits of the cyber fraud issue in Nigeria. Several social, cultural, economic, and technological variables contribute to cyber fraud in Nigeria, and the national economy bears the brunt of the consequences (locally and internationally).

5.1 Summary of findings

The following are the major findings of the study**:**

- The study revealed that Automated teller machine (ATM) skimming has negatively significant effect on sustainable development of deposit money banks DMBs in Nigeria since Automated teller machine (ATM) skimming result to providing incorrect information for the purpose of tricking money out of victims reduces customers' bank deposit (t-statistic; -8.954; *p*-value; 0.000 < Sig-value; 0.05).
- The study revealed that phishing scams cybercrime has negatively significant effect on sustainable development

of deposit money banks DMBs in Nigeria since phishing scammer trying to build the trust of a client in order to convince them to give up personal banking information to siphon money from them (t-statistic; -6.491; *p*-value; 0.000 < Sig-value; 0.05).

5.2 Conclusion

The study concluded that cybercrime has negatively significant effect on sustainable development of deposit money banks DMBs in Nigeria. According to the findings of the study, unemployment is a key contributor to cyber fraud in Nigeria. And a corrupted recruitment system is a contributing element, as is the idea of embezzlement (getting rich quick syndrome) by non – intrinsically motivated job applicants. Peer group influence plays a significant role in the rising tides of cyber fraud in the Nigerian financial system among youths.

In addition, weak internal control and monitoring were revealed to facilitate cyber fraud in the Nigeria financial sector. It was discovered that Nigerian banks lack internal control and proper monitoring, making them vulnerable to cyber fraud criminals. In terms of the impact of cyber fraud in Nigeria, it was discovered that cyber fraud has wrecked several individuals' businesses in Nigeria. Aside from the issue of individuals, cyber fraud has harmed Nigeria's image around the world.

5.3 Recommendations

Based on the study's findings, the following recommendations were made to address the threat of cyber fraud in Nigeria's banking system:

- Government should provide digital national identification card for each Nigerian, as well as a centralized national database of citizens and immigrants, should be provided. To detect fraudsters, there is a requirement for centralized processing of bio – data and thumb – printing of all citizens in a database. Advanced technological security systems, such as using Interactive Voice Response (IVR), terminals advanced tracking devices, and upgrading existing ones when new technology is introduced, should be implemented in Nigeria's financial sector.
- Management of deposit money banks should provide effective security system that uses cutting-edge technology to protect bank information. In other words, some valuable information should be restricted from clients, and strong passwords should be used to secure web links, as well as effective internal control, supervision, and monitoring in computerized banking operations (inbuilt software and devices). Again, raise awareness among youths about the dangers of cybercrime and promote literacy at all levels. Every individual should be informed and trained on how to keep their bank account PIN safe. The entire population should be educated about cyber-fraud. Individuals and businesses should constantly take precautions to safeguard their bank accounts and other sensitive information.

References

1. Adewumi W. Fraud in Banks. Lagos: Nigeria Institute of Bankers, 2021.
2. Akintoye R, Ogunode O, Modupe A, Abimbola AJ. Cyber Security and Financial Innovation of Selected Deposit Money Banks in Nigeria. Univ J Account Finance. 2022;10(3):643-52. doi:10.13189/ujaf.2022.100302
3. Ama GAN, Onwubiko CO, Nwankwo HA. Cybersecurity Challenge in Nigeria Deposit Money Banks. J Inf Secur. 2024;15:494-523.
4. Central Bank of Nigeria. List of deposit money banks and Financial holding companies operating in Nigeria as of September 30th, 2018 [Internet]. Abuja: CBN, 2018 [cited 2025 Mar 10]. Available from: https://www.cbn.gov.ng
5. Chukwu PO. Fraud in the Nigerian Banking Systems, Problems and Prospects (A Case Study of First Bank of Nigeria Plc, and Oceanic Bank Plc, Abakaliki Branch Offices) [Postgraduate thesis]. Enugu: University of Nigeria, 2021.
6. Fadairo-Cokers OA, Ibrahim GU. Impact of Cybercrime on Selected Deposit Money Banks (DMBs) in the Federal Capital Territory (FCT). Int J Adv Res Stat Manag Finance. 2021;8(1):12-23.
7. Godswill E. Causes of Frauds and Forgeries in Banking. Cash and Tellers Refresher Course. Abuja: Nigeria, 2017.
8. Hassan AB, Lass FD, Makinde J. Cybercrime in Nigeria: Causes, Effects and the Way Out. ARPN J Sci Technol. 2019;2(7):22-7.
9. Kekii TL. Cybercrime and Economic Sustainability of the Financial Institutions in Southeast, Nigeria. Glob J Finance Bus Rev. 2023;6(3):63-77.
10. Kuna M, Willson P. Computer Crime and Computer Fraud. Maryland: Dept. of Technology and Criminal Justice, 2021.
11. Okonkwo ON, Emayomi D, Akamike OJ. Impact of Fraud and Financial Crimes on the Growth and Development of the Nigerian Economy. Direct Res J Soc Sci Educ Stud. 2023;11(5):80-7.
12. Olalekan OO, Rakiya A, Ayanwuyi J. The Effect of Cyber-Crimes on Depositors Funds in Deposit Money Banks in Nigeria. J Afr Res Adv Res. 2024;5(2):167-72.
13. Onah VC, Onodugo IC, Ugwu J. Deposit taking banks and cyber fraud among the public in Enugu Urban, Enugu State Nigeria. Int J Adv Res Stat Manag Finance. 2023;8(1):12-23.
14. Ribadu N. Cyber Crime and Commercial Fraud: A Nigeria perspective. Paper presented at: 4th Annual Session of UNCITRAL, 2020 Jul 9-12.