CYBERCRIME ACTIVITIES AND ITS IMPLICATIONS ON BANKS PERFORMANCE IN OYO STATE NIGERIA.

[1]IBRAHIM Majeed AJibola ,[2]SAHEED Daud Omotosho,
[3]JAJI Lateef Kayode and [4]EKPE Abraham Uwaifo

[1]ajibolamagaji@gmail.com, [2]oshoprint@gmail.com,
[3]lateef.0mo@gmail.com and [4]abrahamekpeu@gmail.com
[1]Corresponding Author:ajibolamagaji@gmail.com, +2347032873780
[1,3&4] Department of Banking and Finance, Federal Corporative College, Ibadan, Nigeria.
[2]Department of Accounting and Finance, Kwara State University, Malete, Nigeria.

Abstract

The rendition of products and services by banks given electronic banking has exposed financial service operators to cybercrime activities of different natures posing a serious threat to their financial performance. This paper empirically examined Cybercrime activities and their implications on banks' Performance in Oyo state Nigeria. The basis of this paper is to establish the effect of mail hacking, card fraud and identity theft on banks' performance in Nigeria. A qualitative design approach was used, and 50 respondents from each of the five topmost deposit money Banks that serve as a sample of the study were chosen. A total of 250 questionnaires were administered, and 200 of them received responses. Data were gathered from answers to questionnaires. The degree of the association between the dependent and independent variables was assessed using regression and correlation analysis, and the data's normality was checked using the Komolgorov-Smirnov and Shapiro-Wilk preliminary tests. The outcome of this study shows a negative and significant relationship between cybercrime activities and banks' performance. The study recommends that to enhance the performance of banks, cyber-risk must be integrated into the risk management framework of banks as this will ensure public confidence in Bank E-product platforms usage.

Keywords: Banks Performance, Cybercrime Activities

Jel code: G20, G21,C51,M15,M29

1. INTRODUCTION

Over the past decades, the banking sector has been operating in a very volatile and competitive environment which is strongly driven by high-powered technology that enables it to serve its numerous customers electronically via different channels which gave birth to the incidence of sophisticated and complex Cyber Crime due to the persistent usage of online banking channels to conduct diverse banking transactions by individual and corporate bodies. Raghavan and Latha (2014) opined that the development of cyber Technology has birthed numerous unintended consequences concerning cybercrimes. The banking service rendition has experienced divergent nature of cybercrime-related activities in the form of identity theft, Denial of Service, ATM frauds and Mail Phishing.

Fred et al. (2014) cited by Ajibola (2021) posited that between 2006 and 2013, account takeovers through the activities of cybercriminals have grown proportionately by over 150% and Cybercrime has jumped to the second most reported economic and financial crimes globally. Perpetrators of cybercrime-related activities have succeeded in developing high-powered technology purposely for customer account takeover which exposes banks' customers' databases to operational risk thereby becoming a serious concern among bank service operators, academics, regulators and policymakers on the need to have control mechanisms for the prevalence of cybercrime due to the risk it poses to the survival of deposit money banks as public saving repositories (CBN, 2015).

The Economic and Financial Crime Commission in 2021 revealed that over #6.28billion (about $ 40 million) was stolen from a Nigerian bank by a group of cybercriminals in connivance with an employee of the bank. This corroborates the fact that the prevalence of cybercrime has become worrisome, hence, calling for the need for banks to institute dynamic and sophisticated control measures against cybercrimes to prevent the monumental losses and operational risks exposure due to the nefarious activities of cybercriminals and equally to maintain public confidence in the deposit money banks as this will promote usage of online banking platform among the bank customers (Adeyemi, 2021).

However, most of the earlier research work on Cyber Crime and Banks performance which include Wada and Odulaja (2012), Shewangu (2015), Seema (2016), Inês and Alexandra (2017), Akanji (2020) and Ajibola (2021) out of several authors that researched on cybercrime activities and banks performance in Nigeria and outside the shore of Nigeria focused mainly on cybercrime threats and challenges on the operations of financial institutions without given credence to the nature and types of cybercrime that financial service operators are confronted with. To the best of the researcher's knowledge, there has been little or no research done regarding how cybercrime activities affect the performance of financial service operators specifically in Nigeria context. Perhaps, the impact of cybercrime activities concerning the performance of bank service operators in Nigeria has not been fully researched. Therefore, in an attempt to fill this gap, it is imperative to take a look at how cybercrime activities have influenced

the performance of banks in Nigeria. To guide the thrust of this research work, the following questions were asked:

i. To what extent does mail hacking by cybercriminals affects the performance of deposit money banks in Nigeria?
ii. In what way does card fraud by cybercriminals affects the performance of deposit money banks in Nigeria?
iii. What is the relationship between identity theft by cybercriminals and the performance of deposit money banks in Nigeria?

2.0 LITERATURE REVIEW

2.1 Conceptual Review

Cybercrime has been conceptualized by various researchers such as Wada and Odulaja (2012), Shewangu (2015), Seema (2016), Inês and Alexandra (2017), Akanji (2020) and Ajibola (2021) and many others:

Wada and Odulaja (2012) cited by Ibrahim (2020) opined that cybercrime is mostly associated with Electronic banking given the fact that cybercrime is usually committed in the process of opening a deposit account, paying bills online, making transfers and withdrawals online, as well as any other online banking transaction, using the internet as a delivery method for these services. In the same vein, Ajibola (2021) posited that cybercrime is all about all forms of irregularities being perpetrated in cyberspace to gain an undue advantage over other cyberspace users. Similarly, Akanji (2020) maintained that cybercrime is all about all forms of crime being carried out with the use of the Internet. The opinion, Inês and Alexandra (2017) cited by Adeyemi (2021) opined that cybercrime has to do with any form of illegal and illicit computerised mediation aimed at gaining undue advantage over other users of electronic networks. Therefore, in the opinion of Sanchi (2016) the nature of Cyber-crime related to the banking sector includes the following:

Mail Hacking: Mail hacking is when a person obtains unauthorized access to a system intending to manoeuvre security measures by compromising the customer database with a view of obtaining confidential information that will enable them to divert account information (Adeyem,2021).

Card Fraud: This is all about a process whereby cybercriminal uses customers' credit card for all sort of payment without the authorization of the card owner (Shewnagu, 2015). In the same vein, Akanji (2020) posit that Cybercriminals now use complex techniques aimed at hacking unsuspecting bank customers' card details with a view of defrauding credit card owner.

Identity Theft: Identity theft is now one of the common ways that perpetrators of cyberspace crime adopt to have full-blown customers' account details through deception (Saleh, 2013). Different methods can be used to steal someone's identity. Popular among

all is Skimming. Ajibola (2021) opined that Skimming is all about the process of obtaining personal data from a credit card while making a valid purchase through an electronic gadget that captures all the data on a magnetic strip.

2.2 Theoretical Background

2.21 Learning Theory

For this study, the theory proposed by Beatson in 1991 which is popularly referred to as the least possible privilege theory was adopted as the theoretical framework considering its connectivity to cybercrime activities and the performance of banks with a view of drawing inference from the experience of banks customers concerning banks electronic platforms usage concerning losses suffered as a result of cybercriminals activities and how it influences their disposition to the usage of banks electronic platforms. The theory suggests that new users are more vulnerable to security breaches when using information systems (IS). Denning (1999) theorizes about defensive information warfare and proposes that security policy training and awareness will better equip users against threats. Other proponents theorized about ethical awareness and culture as factors that influence IT security. Kabay (2002) theorized about using social psychology as a tool to improve user security conduct. The importance of the interest of senior management and integrating security issues as part of the corporate asset protection model was highlighted by Katsikas (2000), Kovacich and Halibozek (2003) and Perry 1985) also modelled an Information System security awareness program to address end-users, IT personnel and management executives (Wada and Odulaja, 2012). In this instance, it is believed that cybercrime occurs as a result of opportunities, which allows cybercriminals to exploit bank customers and consequently resulting declining profitability. It then posits that cybercrimes can however be prevented through security training, ethical awareness and culture to ensure there is the least opportunity for cybercriminals to perpetrate internet frauds.

2.3 Empirical Review

Evidence at International Level

Siam (2010) examined the implication of cyber-related fraud activities on the profitability of selected license banks in Jordan between 1999 and 2009. A questionnaire was employed as the instrument of data collection from the selected target audience that serves as the sample size for the study using regression analysis. The regression result of the study shows that there is a bidirectional statistically significant relationship between cyber-related fraud activities and the profitability of the selected banks in Jordan. Imran and Sana (2011) investigated the impact of electronic crime on the performance of the Indian banking sector. Using multiple regression analysis, data for the study were collected through a questionnaire from the purposively selected sample size that represents the totality of the population under study. The regression result of the finding exhibits a negative relationship between the dependent and independent variables. This indicates that electronic-related crime has a voracious adverse effect on the performance of Indian Banks which must be controlled to prevent a systemic collapse by developing high-powered technology security as well the incorporation of cyberspace risk management to check cybercrime activities such as mail hacking, mail pharming, mail phishing as well as Identity thefts.

Inês and Alexandra (2017) in their paper titled “financial institutions and Cybercrime: threats, challenges and Opportunities" submitted that recent high-profile cases of financial institutions being targeted by cybercriminals, such as the attack on the Bangladesh Central Bank in February 2016 that resulted in a loss of $81 million, illustrate the dangers posed by cybercrime to the international financial system. Using regression and correlation for the content analysis. Their study revealed that Threats to financial institutions include two types of cybercrime. ‘Cyberdependent' crimes, such as hacking and Document and file virus attacks, are not possible without the use of the internet. Cyber-enabled (or 'cyber-assisted') crimes, by contrast, are 'traditional' crimes – such as fraud, robbery and extortion – which are facilitated and made easier by technology, but would still take place if the technology were not available. Financial institutions need to have strategies in place that allow them to respond to and understand both types of threats. Nair and Nair. (2022) examined the impact of cyber policies on customer satisfaction in the banking sector. Using multiple regressions for the content analysis. They use a qualitative research approach to analyze data from a survey of customers in the banking sector in India. The authors found that cyber policies have a significant impact on customer satisfaction and that customers are more likely to be satisfied with their banking services when they perceive that the cyber policies are fair and transparent. The authors also suggest that banks should focus on improving customer service and providing more information about cyber policies to ensure customer satisfaction.

Evidence at Africa Level

Shewangu (2015) looked into the impact of electronic fraud on the performance of banks in Zimbabwe. Data were collected with a questionnaire from 22 selected bank customers and a descriptive method was adopted to make a content analysis of the data. The result of the finding shows that most of the cyber-related crimes in Zimbabwe were due to poor technology facilities and inadequate public awareness of the subject matter. Ishmael, et al. (2016) studied Cybercrime as an emerging threat to the financial services sector in Zimbabwe. Data for the study was collected from 48 customers that were purposively selected from the four selected commercial banks that represent the totality of all the banks in Zimbabwe. The analysis of the collected data was done through regression and correlation and the result revealed among others that cybercrime has caused the untimely death of some banks in Zimbabwe because of its huge implications on the operating profit of Banks. Common among the cybercrime in Zimbabwe is identity theft, and malware.

Ogbadu and Usman (2022) in their study examined the impact of cyber fraud on customer loyalty and banks' profitability Keyan. Using multiple regressions for the analysis, these study findings revealed that there is a negative relationship between cyber fraud and customer loyalty as well as a bank's profitability. However, it can be deduced from their study that cybercrime management is a viable competitive tool to enhance customer loyalty and also to attain desired profitability.

Evidence at the Local Level

Madueme (2010) examined the impact of ICT on banking efficiency in Nigeria using 13 banks as a sample size. CAMEL rating and transcendental logarithmic function of banks were used as a barometer for drawing inference and it was discovered that the adoption of CAMEL rating and transcendental logarithmic function of banks induce efficiency values by 1% concerning ICT financial products usage. Maiyaki and Mokhtar (2010) empirically examined the effect of electronic banking facilities on customer satisfaction in Kano State Nigeria. A total of 407 bank customers were selected to serve as a fair representation of the population under study. Data were collected primarily through the use of a questionnaire. Using regression and correlation for the analysis and the result of the findings indicated that customer usage of electronic banking facilities such as ATMs, online banking and telephone banking has no significant effect on customer satisfaction.

Ajibola (2021) examine the impact of cybercrime on customer brand loyalty in Nigeria: Evidence from selected deposit money Banks. A total of 100 respondents drawn from four topmost-rated banks in Nigeria were selected to serve a fair representation of the population under study using purposive sampling techniques. A questionnaire was adopted as the main research instrument. The content analysis based on the regression result revealed that identity theft and malware are the main types of cybercrime in banks.

Research gap

This paper aims to empirically examine how cybercrime activities affect the Performance of banks in Oyo State, Nigeria. It was discovered most of the previous research works on cybercrime were conducted outside the study Area (Oyo state, Nigeria) leaving a geographical gap. Hence, this paper attempt to address the identified gap as related to the subject matter.

2.4 Conceptual Framework

Different studies on the impact of cybercrime activities on the performance of Banks present mixed results as to the effect of each of these variables on the Banks' performance. Most studies present a significant negative relationship between the dependent and independent variables. This framework Figure 1 indicates how cybercrime activities are likely to voraciously affect the banks' performance in varying dimensions as related to mail hacking, card fraud and identity theft.

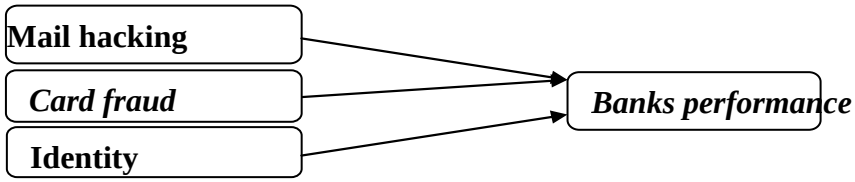

Figure 1. The schematic link between Cybercrime activities and Banks' Performance.

Source: Authors (2023)

3.0 METHODOLOGY

Because the target audience has a fairly broad population, this work uses survey research. All the commercial banks in Oyo State make up the population for this study. It is imperative to state clearly that there are several licensed financial service operators performing a specific range of financial services; based on this fact, this study was specifically restricted to all the operating commercial banks in Oyo state. Because commercial banks are the main targets of cybercrimes since commercial banks are public repository institutions with the largest amount of public savings and deposits. Likewise, Oyo State was chosen for the study because it was close to the researchers. As a result, the study adopts a stratified random sampling technique. The method entails grouping respondents into strata on the bases of common characteristics which in this case is the industrial affiliation. After the grouping, the simple random sampling technique is then applied to select the required sample size for the fair representation of the population under study. Therefore, to create a sample size, the researchers choose fifty (50) clients from each of the five topmost-rated banks, to make a total of two hundred and fifty (250) Customers who subsequently participate in the study as respondents. A closed-ended questionnaire was the main tool used to collect data. The questionnaire was in a close-ended format that allowed the respondents to offer their views according to the Lickert scale of responses as follows;

Sa = 5 = Strongly Agreed, A = 4 = Agreed, I = 3 = Indifference, D = 2 = Disagree, Sd = 1 = Strongly Disagreed.

The data collected using the questionnaires were edited, coded and tabulated for completeness, efficiency and accuracy. First raw data gathered were analysed using the latest version of the Statistical Package for Social Scientists (SPSS) program. Descriptive statistics such as tables were used in the presentation of the data and qualitative data was collected which requires a descriptive and content analysis. Correlation and Linear Regression models were also used to proffered answers to the research questions.

3.1 Model Specification

This study was modelled in line with the study of Ishmael, et al. (2016) which studied Cybercrime as an emerging threat to the financial services sector in Zimbabwe.

The functional model of the equation is presented as:

BP= *f*(CBA)……..3.1

Where: BP = Banks Performance

CBA = Cyber Crime Activities

Where: Banks Performance = Financial performance of selected banks

: Cyber Crime Activities = MH; CF and IT

MH= Mail hacking

CF = Card fraud

IT = Identity theft

It then follows as;

BP= *f*(MH;CF;IT)……3.2

To arrive at a multivariate relationship we then substitute equation 3.2 into 3.1 as follows;

$$\mathbf{BP=\beta_0+B_1MH+\beta_2CF+\beta_3IT+\varepsilon_i}\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\mathbf{3.3}$$

Where:

β_0 = Intercept of the model.

β_1 = Coefficient of each independent variable in the model.

ε_i**=** Error term

The adopted surrogates for cybercrime activities and the performance of Banks proxies are expected to relate negatively, based on the *a priori expectation* from the model discussed above.

3.2 Validity and Reliability Test for the Research Instrument

To ascertain the suitability of the research instrument expert opinion was adopted while the evaluation of the reliability of the instrument was done with Cronbach's Alpha.

4.0 Data Presentation, Analysis and Interpretation

Response Rate of the returned questionnaire

Table 1

		No of Questionnaires	Percentage%
a.	Questionnaire administered	250	100
b.	Questionnaire Returned complete	200	80%
c.	Questionnaire Returned incomplete	30	12%
d.	Questionnaire not returned	20	8%

Source: Authors Survey, 2023.

A total of 250 questionnaires were distributed to study participants, who were selected from the top five deposit money banks in Oyo State. Of these, 200 questionnaires, or 80% of the total, were returned and completed correctly, 30 questionnaires, or 12% of the total, were returned but incomplete and thus invalid, and 20 questionnaires, or 20% of the total, were returned but not properly completed. Analyses were based on feedback suggestions from the respondents to questionnaires.

4.1 Preliminary Analysis

Table 2

Tests of Normality

	Kolmogorov-Smirnov[a]			**Shapiro-Wilk**		
	Statistic	Df	Sig.	Statistic	Df	Sig.
Mail hacking	.274	200	.140	.762	200	.341
Card Fraud	.270	200	.135	.714	200	.316
Identity theft	.272	200	.138	.738	200	.327

a. Lilliefors Significance Correction

Source: Authors, 2023.

According to Table 2, the data for each of the adopted variables were normally distributed based on the results affirmation of the Komolgorov-Smirnov and Shapiro-Wilk tests which were not significant at 0.05 (p = 0.140, 0.135, 0.138, and, respectively,

0.341, 0.316, and 0.327). This conclusion led to the consideration and eventual selection of parametric statistical analysis for this study.

Table 3: Reliability Test Using Cronbach's Alpha

Variable	**Cronbach's Alpha**	**N**
Mail hacking	0.75	4
Card Fraud	0.78	4
Identity theft	0.74	4
Overall	**0.76**	**12**

Source: Authors Computation, 2023.

The aforementioned Table 3, shows that the coefficients for each of the adopted surrogates stood at 0.75%, 0.78%, and 0.74 respectively which are relatively high and the overall Cronbach's Alpha coefficient stood at 0.76%, which is higher than the expected margin of 0.70. Given the credibility of the aforementioned Cronbach's Alpha result, one may therefore infer that the scale is thought to be credible.

4.2 Correlation Coefficient Matrix among Variables

Table 4: Correlation Matrix

		MH	CF	IT
MH	Pearson Correlation	1	.576**	.586**
	Sig. (2-tailed)		.000	.000
	N	200	200	200
CF	Pearson Correlation	.576**	1	.610**
	Sig. (2-tailed)	.000		.000
	N	200	200	200
IT	Pearson Correlation	.586**	.610**	1
	Sig. (2-tailed)	.000	.000	
	N	200	200	200

**. Correlation is significant at the 0.01 level (2-tailed).

Source: Authors Computation, 2023.

The multi-collinearity at the level among the used variables was displayed in Table 4. The outcome suggests that the series are free of multi-collinearity when taking into account the negligible correlation of individual coefficients, which was below 0.70 per cent. The logic behind the assumption of no multicollinearity is that if the value of the correlation coefficient between two variables is greater than 0.70, it could be interpreted and concluded that the variables are having a multicollinearity problem (Gujarati, 2015)

Table 5: Regression coefficient

Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	-.807	.314		-2.570	.004
	Mail Hacking (MH)	-.253	.094	.108	-.269	.004
	Card Fraud (CF)	-.223	.075	.187	-.297	.000
	Identity Theft. (IT)	-.709	.065	.688	-10.907	.005

a. Dependent Variable: performance of the selected banks.

Source: Authors Computation, 2023.

Table 5 summarizes the regression result of the model which specifically looked into the effect of cybercrime activities on the performance of Banks. The coefficient of Mail Hacking stood at-.253, which is statistically significant at 5% implying that for every percentage change in Mail Hacking, the performance of the selected banks will decline by over 25%. The coefficient of Card Fraud stood at -.223, which is statistically significant at 1% implying that for every percentage change in Card Fraud, the performance of the selected banks will decline by over 22%. The coefficient of Identity Theft stood at -.709, which is statistically significant at 0.5% implying that for every percentage change in Identity Theft, the performance of the selected banks will decline by over 70%. The adopted variables are jointly significant in explaining the dependent variables at a 5% level of significance giving credence to the reported coefficient for constant.

4.3 Model Summary

Table 6: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.884[a]	.758	.755	.289

a. Predictors: (Constant), cybercrime activities

Source: Authors Computation, 2023.

A summary of the model's goodness of fit was provided in Table 6. The set of predictors as a whole and the financial health were suggested to be strongly correlated by multiple correlation coefficients (R) of 0.884. According to the coefficient of (R^2), which was 0.758, the adopted surrogate for the independent variables can account for 75.8% of the variation in the financial health of the chosen banks, which is the dependent variable, while the remaining 24.2% represents the stochastic component of the model which represent the error term.

Table 7: ANOVA

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	73.106	3	30.137	320.120	.000[a]
	Residual	32.102	197	.075		
	Total	105.208	200			

a. Predictors: (Constant), mail hacking, card fraud, identity theft

b. Dependent Variable: performance of the selected banks.

Source: Authors Computation, 2023.

Table 7 indicates that the result shows a general p-value of 0.000 which is less than the level of significance at 0.05. This implies that the regression model is statistically significant and predicts the outcome variable. This was further affirmed by the result of the F-Statistics which stood at 320.120 significant at 1%.

5.0 Conclusion and Recommendations

Based on the empirical outcome of this study, it was revealed that a bidirectional relationship exists between the adopted surrogates (mail hacking, card fraud and identity theft) for cybercrime activities and the performance of the selected banks in Oyo State Nigeria. Therefore, a percentage increase in mail hacking, card fraud and identity theft will no doubt erode public confidence in the usage of bank E- products voraciously, thereby inducing the financial performance of banks adversely considering the negative relationship that exists between mail hacking, card fraud and identity theft as proxies for the performance of the selected banks. By implication, the revenue (bank charges) that should accrue to the banks from e-banking services will insatiably decline due to loss of public confidence as a result of cybercrime activities thereby posing some threat to the financial health of banks. The following recommendations were made in light of the information above: The Government should promote awareness for the masses regarding cyber security on the various antics of cyber criminals as a way to ensure a sound and credible banking system.

REFERENCES

Adeyemi, I (2021). Impact of ICT tools for Combating Cyber Crime in Nigeria Online Banking: A Conceptual Review. *International Journal of Finance,* 3(6),180-188.

Ajibola, O (2021). Impact of cybercrime on customer brand loyalty in Nigeria. *Journal of Policy and Development Studies.* 9 (1), 179-193.

Akanji, O. O. (2020): The role of microfinance in empowering women in Africa. *International Journal of Business,* 2(.2), 159-178.

Central Bank of Nigeria, (2015), *Improving and Securing the Cyber-Environment. Nigerian e-Fraud Forum (NeFF) Annual Report, 2015.*

Cohen, L. & Felson M. (1979) Social Change and Crime Rate Trends: A Routine Activity Approach*, American Sociological Review,* 44 (4), 588-608

Daily Post News, (03/08/2017), Senate: Nigeria Losses N127billion Annually to Cybercrime. Online at the *daily post. ng/2017/03/08.* Retrieved on 22/10/2017.

Florêncio, D., & Herley, C. (2010). *Phishing and money mules. In Information Forensics and Security WIFS, IEEE International Workshop on pp*. 1-5.IEEE.

Fred, B.Brian, B. &Gene, L. (2014) Organized Cyber Crime and Bank Account Takeovers. *International Journal of Finance,* 2(2),609-630.

Imran, M. & Sana, R. (2011) Impact of Electronic crime in Indian Banking Sector – An Overview. *International Journal of Business & Information Technology.* 1(2), 401-424.

Inês, S. & Alexandra, S. (2017) Financial Institutions and Cybercrime: Threats, Challenges and Opportunities. *International Journal of Business* 1(4), 304-321.

Ishmael, M. Shingirai, G. Martin, M. & Rufaro, C. (2016), Cybercrime - The Emerging Threat to the Financial Services Sector in Zimbabwe. *Mediterranean Journal of Social Sciences,* 7(3), 500-522.

Nair, O.S., & Nair, E.G. (2022). Impact of cyber policies on customer satisfaction in India. *Journal of Research in International Business Management*. 1(4), 251-257.

Ogbabu, T. & Usman, A. (2022). Impact cyber fraud on customer loyalty and banks profitability Keyan. *Journal of Business Theory and Practice.* 3(1), 202-225.

Raghavan1, R & Latha, P. (2014), The effect of cybercrime on a Bank's finances. *International Journal of Current Research and Academic Review,* 2 (2), 173-178.

Sanchi, A. (2016), Cyber Crime in Banking Sector. *Research Journal of Management Sciences.* 3(4), 140-152.

Seema, G. (2016), Cyber-crime: A Growing Threat to Indian Banking Sector. *International Journal of Science Technology and Management*, 5 (12), 200-220.

Shewangu, D. (2015), Cyber-banking Fraud Risk Mitigation; Conceptual Model. *Banks and Bank Systems*, 10(2), 2015. 180-201.

Wada, F. & Odulaja, O. (2012), Electronic Banking and Cyber Crime In Nigeria - A Theoretical Policy Perspective on Causation. *African Journal of Computing & ICT,* 4(3),130-146.

Index

QUESTIONNAIRE INSTRUCTION: Please tick (√) against your responses in the space provided.

SECTION A: DEMOGRAPHIC DATA

1. Age (tick appropriately) 18-29 ( ) 30 - 49 ( ) 50 and Above ( )
2. Gender: Male ( ) Female ( )
3. Marital status: Single ( ) Married ( )
4. Occupation: Civil servant ( ) Corporate employee ( ) Entrepreneur ( ) Student ( )

NB; from the next section, kindly tick appropriately,

SA = 5 = STRONGLY AGREED
A = 4 = AGREED
I = 3 = INDIFFERENCE
D = 2 = DISAGREE
SD = 1 = STRONGLY DISAGREED

Section B

Operational Information

I. Establish the relationship between mail hacking (MH) and the performance of banks s

S/N	**STATEMENT**	**SA**	**A**	**I**	**D**	**SD**
1.	MH reduce e-banking service revenue					
2.	MH discourage e-banking service usage by the customer					
3.	MH influence customers' disposition to banking culture.					
4.	MH is a major form of cybercrime					

II. Analyze the effect of card fraud (CF) on the performance of banks

S/N	**STATEMENT**	**SA**	**A**	**I**	**D**	**SD**
5.	CF is part of cybercrime activities					

6.	CF is a setback for digital banking					
7.	CF induces customer loyalty.					
8.	CF is the most reported cybercrime.					

III. identify the effects of identity theft (IT) on the performance of banks

S/N	**STATEMENT**	**SA**	**A**	**I**	**D**	**SD**
9.	IT induce public confidence in e-banking service					
10.	IT affects the credibility of digital banking					
11.	It increases the fear of cybercriminals among the bank customers					
12.	IT has led to a loss of money for the users and the providers of e-banking service					