CYBERCRIMES AND CYBER SECURITY AMONG YOUTH IN SOCIAL ENTREPRENEURSHIP VENTURE APPROACH

[1] OVHARHE, ORUGBA HARRY (Ph.D) & [2] ATEDUOBIE WAKAMA (Ph.D)
[1-2] College of Health Science & Technology, UPTH,
Port Harcourt, Rivers State
harryovharhe@yahoo.com

ABSTRACT

This study examined the trend of cybercrime and cyber security in social entrepreneurship venture in Edo State communities, Nigeria. The study adopted longitudinal survey design and digital design because online method and instrumentation scale was employed on the basis of the Cybercrimes in Nigeria: analysis, detection and prevention. Omodunbi (2023) was adopted as systematic review data analysis. Data were generated by quantitative and qualitative method. The study intends to use purposive sampling techniques and digital sampling technique. A total population size of 86648 and sample size of 399 was determined using Taro Yamane's formula at 0.05 level of significance. Also, 399 copies of questionnaire were distributed to the respondents, while 317 copies were completed and retrieved. The instruments were validated with reliability above 0.7 co-efficient, using Cronbach Alpha technique. Three research questions and three hypotheses were raised which was tested with Pearson Product Moment Correlation, Ordinary Least Square Method and Partial Correlation for the moderating variable via SPSS 25 version. From the findings, the concept of cybercrime creates positive outcome cyber editorials, cyber bully and cyber stalking. In conclusion, cyber bully, cyber stalking and cyber editorials have significant influence on the cyber security. Based on the findings and conclusion, this study contributes to the knowledge that computer related fraud, computer related forgery, cyber-pornography and cyber-squatting. It could be recommended among others that cybercrimes management have to ensure that there is effective control of Yahoo-yahoo proxies us social entrepreneurship venture approach because they are fundamental factors to the frame compared with longer-term Cyber stalking among client. Cybercrimes management using social entrepreneurship venture approach should integrate cyber kidnappings in a better manner towards managing cyber stalking.

KEYWORDS: Cyber Kidnapping, Yahoo-Yahoo, Cyber Bully/Stalking, Image Analysis, Criminal Justice, Criminal Investigation, Social Entrepreneurship

1. INTRODUCTION

The social entrepreneurship venture is the merchandizing function that mitigates social vices. Social entrepreneurship venture are models for social innovators that eradicates cybercrimes among youth. Instead of youth to be enshrine as criminal element they are embedded with innovative skills, talent, potentials (2024). They are seen as frugal element in the society (Ovharhe, 2025).

In Nigeria to- day, several internet assisted crimes known as cybercrimes are committed daily in various forms such as fraudulent electronic mails, pornography, identity theft, hacking, cyber harassment, spamming, Automated Teller Machine spoofing, piracy and phishing. Although you have a slight idea of what is cyber kidnapping, here is the proper definition: Cyber kidnapping denotes a cybercrime form where malicious actors employ digital methods to gain control of information, data, or systems for extortion.

Cyber Kidnapping is a kind of crime where the criminals trick their victims into hiding. Later, they get in touch with the victim's family and ask for money. To make it seem real, the victim is made to take pictures that make it look like they are being held against their will, often showing themselves tied up or with their mouths covered. These misleading pictures are sent to the family, making it seem like there's a danger. The victim and their family are made to think that not doing what the kidnappers want could put their loved ones in danger.

Cyber Kidnapping refers to a form of cybercrime where malicious people use digital means to seize control of information, data, or systems with the intent of extortion. It often involves threats to disclose or manipulate data unless a ransom is paid. This can manifest in various forms, such as ransom ware attacks, virtual kidnapping schemes, or the unauthorized seizure of sensitive information. Cyber Kidnapping is a form of extortion scam where victims are deceived into paying a ransom for a supposedly kidnapped loved one. These schemes use threats and deception without actual abductions, often based on information gleaned from social media (Ovharhe, 2025d).

Recently, a Chinese student, who fell victim to 'cyber kidnapping', was discovered safe in rural Utah. Kai Zhuang, aged 17, was reported missing on December 28. When police located him, his parents in China had already paid a ransom of $80,000. Zhuang's parents notified his host school in Riverdale, Utah, about the apparent kidnapping. The school then alerted the police. He was found in a tent approximately 40 kilometers north of Brigham City, where it appears he had chosen to isolate himself. In the Utah boy's case, his parents were sent a picture indicating he had been kidnapped. The police believe the kidnappers have manipulated him since December 20. He was traced by analysing call data and bank records.

According to the FBI's website, although virtual kidnapping takes on many forms, it is always an extortion scheme one that tricks victims into paying a ransom to free a loved one they believe is

being threatened with violence or death. But skills, knowledge and attitude could be a solution (Ovharhe, 2025b). Also, innovation and creativity could be introduce to mitigate crimes (Ovharhe, 2025c)

Unlike traditional abductions, virtual kidnappers have not actually kidnapped anyone. Instead, through deceptions and threats, they coerce victims to pay a quick ransom before the scheme falls apart. Experts believe that with the rise of Cybercrime (AI), such crimes can rise, as scammers can send people voice notes that sound exactly like a loved one in distress. Last year, an Arizona woman testified in the US Senate about receiving just such a call. When Jennifer DeStefano picked up a call from an unknown number, "her 15-year-old daughter", crying, told her some "bad men" had her. A man then threatened her and demanded ransom. After she cut the call, she called up her daughter, and realised she was safe. While there is no clear data yet on how many such case are there.

Cyber crime is probably the crime that pays the best," notes Mr. Steinberg. "With the ability to target people in different languages and from any location, it presents a uniquely global challenge." *BBC* , 2025.

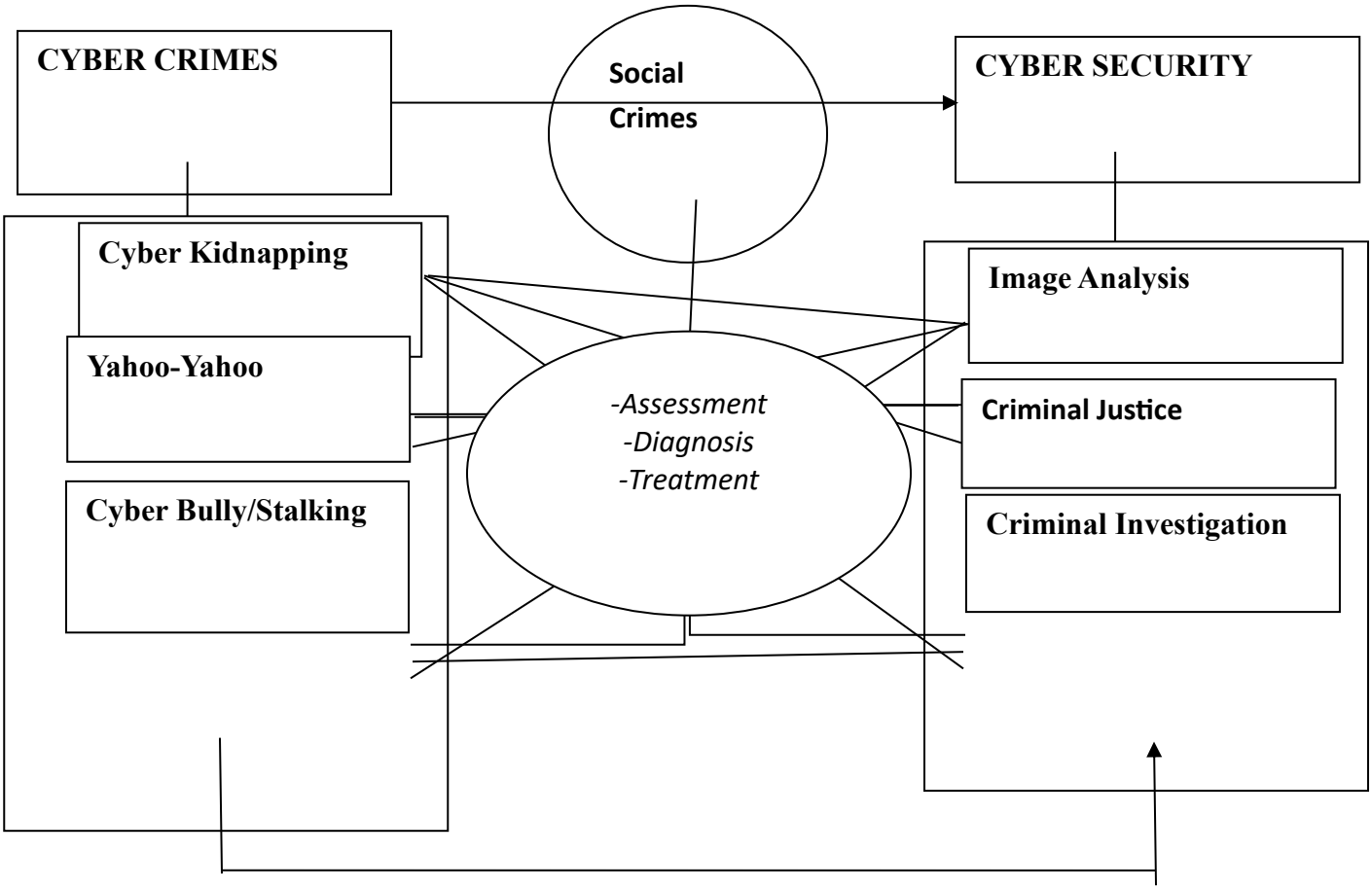
Statement of the Problems

In an era where the digital world blurs the lines between reality and virtuality, '*Cyber Kidnapping*' emerges as a novel and globally significant cyber threat. This sophisticated form of cyber scam, also known as '*Virtual Kidnapping*', involves criminals deceptively claiming to have kidnapped a loved one and demanding ransom. The deceit is often based on information gleaned from social media or through more targeted means, where the criminal has direct sight of the target or knows their whereabouts. Globally, the incidents of cyber kidnappings range between 15,000 to 20,000 annually, a figure that startlingly excludes unreported cases.

In the latest article on www.sdblognation.in, we delve into the alarming trend of 'Cyber Kidnapping, which concise overview highlights key insights from the full piece, offering a glimpse into the evolving landscape of cybercrime and security. Read on for a snapshot of the crucial points covered in our detailed analysis.

Ovharhe (2025) pointed out that frugal innovation is solution to quench all these problems of cyber crimes and cyber security (Ovharhe, 2025a). This is while Ovharhe (2024) anchor on business intelligence as key to boost any issues (Ovharhe & Akandu, 2024).

OPERATIONALIZED FRAMEWORK ON THE VARIABLES OF CYBERCRIME IN THE FUTURE OF CYBER SECURITY



SOURCE: Researcher's Operationalization

The independent variable in this study is cybercrime. Based on the earlier study of Miller (2025), the dimensions in this study are Cyber kidnappings, Yahoo-yahoo and Custom GPT. On the other hand, the dependent variable for this study is cyber security. The measures of Cyber security adopted by Mayo Clinic for this study includes; cyber editorials, cyber bully and cyber stalking.

Hypotheses

The following null hypothetical were raised to buttress the study

Ho$_i$: There is no significant correlation between Cyber kidnapping and cyber security among youth in Edo community

Ho$_{ii}$: There is no significant correlation between Yahoo-yahoo and cyber security among youth in Edo community

Ho$_{iii}$: There is no significant correlation between Cyber bully/stalking and cyber security among youth in Edo community

2. LITRATURE REVIEW

Conceptual Review

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. Ovharhe (2025a) suggested that the business activities should knit with social entrepreneurship venture approach to mitigates cybercrime issues and concerns. While these developments allow for enormous gain in productivity, efficiency and communication they also create a loophole which may totally destroy an enterprise. The term cybercrime can be used to describe any criminal activity which involves the computer or the internet network (Okeshola, 2013). This term is used for crimes such as fraud, theft, blackmail, forgery, and embezzlement, in which computers or networks are used. Technology innovation is needed to activate skills, knowledge and attitude of youth (Ovharhe, 2025b).

In (Maitanmi, 2013) 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. The concept of cybercrime is historical. It was discovered that the first published report of cybercrime occurred on the mainframe computer in the 1960s (Maitanmi, 2013). Ovharhe (2025c) opined that technology consciousness should be the mindfulness of business creation with skills and knowledge instead proliferating crimes (Ovharhe, 2025d).

Since these computers were not connected to the internet or with other computers, the crime was committed by the employers (insider) in the company, hence it was referred to as computer crime rather than cybercrime. According to (Lakshmi, 2015) as at 2003, the United States and South-Korea have the highest cyber-attacks of 35.4%and 12.8% respectively. With the population of Nigeria placed at 160 million from the last census carried out in2006, a recent statistics revealed that about 28.9% have ac-cess to the internet (Hassan, 2012). It was also proven that39.6% African users of internet are actually Nigerian, hence, the high increase in the rate of internet crime in Nigeria (Hassan, 2012). Presently, cybercrimes are performed by people of all ages ranging from young to old, but in most instances the young. Presently, cybercrimes are performed by people of all ages ranging from young to old, but in most instances the young and female in the society (Ovharhe & Odepeli, 2024).

Social Innovation and Social Entrepreneurship

The four primary types of social entrepreneurs are community social entrepreneurs, non-profit social entrepreneurs, transformational social entrepreneurs, and global social entrepreneurs.

From a nonprofit perspective, the stages of social entrepreneurship were defined as follows: Mission statement and opportunity, innovation, product/services and relations, business model definition, social outcomes, social transformation (Perrini and Vurro, 2006) or opportunity identification to Opportunity.

The key elements of a social enterprise are:

- Social mission over financial mission.
- Innovative solution to social problems.
- Self-sustaining business model.
- Impact which could be measured.

Another word for social enterprise

community-oriented organization	**Charity**
grassroots organization	nonprofit organization
public interest organization	public service organization
community benefit organization	community support group
community foundation	charitable company

Characteristics of Social Entrepreneurship

Social awareness, innovation, pragmatism, creative thinking, collaboration and adaptability are all characteristics of social entrepreneurship. The youth are giant of the community that pumps the energy of creation index. Social enterprises can be community-sized where they only work in a particular area, to global where they work to solve problems that affect the whole world (Ovharhe, 2022, 2024).

Youth are social entrepreneurs which boost with strength that include a range of career types and professional backgrounds, ranging from social work and community development to entrepreneurship and environmental science. For this reason, it is difficult to determine who is a social entrepreneur. David Bornstein crave the term "social innovator" interchangeably with social entrepreneur, due to the creative, non-traditional strategies that many social entrepreneurs use. For a clearer definition of what social entrepreneurship entails, it is necessary to set the function of social entrepreneurship apart from other voluntary sector and charity-oriented activities and identify the boundaries within which social entrepreneurs operate. Some scholars have advocated restricting the term to founders of organizations that primarily rely on earned income (meaning income earned directly from paying consumers), rather than income from donations or grants. Others have extended this to include contracted work for public authorities, while still others include grants and donations.

Cyber Kidnapping

Cyber Kidnapping is when criminals use the internet to trick victims into isolating themselves, setting up a situation to demand money from their families. The victim is also forced to send pictures that make it seem like they're being held captive, showing them tied up or with their mouths covered. These pictures are then sent to the family. Both the victim and their family think their loved ones might be harmed if they don't do what the kidnappers want.

- In this crime, attackers trick victims online, making their families think they've been kidnapped and are being held against their will. The scammers then ask for money to let them go.
- In these "cyber kidnapping" situations, the scammers tell victims to be alone and might even force them to make it look like they're being held captive sometimes using webcams or sending voice recordings to the families. To avert crimes of kidnapping, innovation of products, skills and talent is paramount as spell out in Ovharhe & Woko (2024a,2024b), Ovharhe & Chibuike (2024a, 2024b), Ovharhe & Abuda, (2024, 2023), Ovharhe & Akandu (2024).

Cyber kidnapping is a rising concern worldwide, and it's becoming more important for competitive exams like the social enterprising. To look at this problem for the socio-economic status in the entrepreneurship world, you need to know how it could affect the socio-gram setting of communities.

The Tactics of Deception

Human mistakes are a widely recognized weak point in cybersecurity, and they greatly benefit cyber criminals involved in various types of online criminal activities. Deception seeks to alter human perception by taking advantage of psychological weaknesses. Social Engineering depends on manipulating psychology, a highly effective technique used by threat actors to obtain confidential information.

These are the following tactics often used by scammers:

1. **Social Engineering –** Cyber kidnappers exploit trust and vulnerabilities, manipulating emotional triggers like fear and anxiety to control victims and their families.
2. **Phishing and Malware –** They may infiltrate online accounts or devices through fraudulent emails or malware, gaining access to personal information and potentially monitoring communications.
3. **Exploiting Technological Naivety –** Victims unfamiliar with digital safety often prove more susceptible to falling for elaborate deception.

Types of Cyber Kidnapping

Various types of malicious activities used to seize control of information, data, or systems, often with the intent of extortion or harm. Here are several types of cyber kidnapping:

1. **Ransomware Attacks:** In ransomware attacks, cybercriminals encrypt the victim's data or systems and demand a ransom for its release. This type of cyber kidnapping is prevalent and can affect individuals, businesses, and even government entities.
2. **Virtual Kidnapping:** Virtual kidnapping involves manipulating individuals into believing that a family member or loved one has been kidnapped. While no physical abduction occurs, the goal is to extort money from the victim through fear and deception.
3. **Data Kidnapping (Data Hostage Situations):** Data kidnapping involves the unauthorized seizure of sensitive information or intellectual property. Cybercriminals threaten to disclose or manipulate the data unless a ransom is paid.

4. **Credential Kidnapping:** In credential kidnapping, attackers steal or compromise login credentials, gaining unauthorized access to accounts, systems, or networks. This type of cyber kidnapping often leads to identity theft, financial fraud, or unauthorized data access.
5. **Device Kidnapping (Hijacking):** Device kidnapping occurs when cybercriminals take control of a user's device, such as a computer or smartphone. They may lock the device, manipulate its functions, or demand a ransom for its release.
6. **Cloud Kidnapping:** Cloud kidnapping involves compromising cloud-based services or data repositories. Cybercriminals may encrypt or manipulate cloud-stored data, demanding a ransom for its restoration.
7. **Social Media Kidnapping:** In social media kidnapping, attackers compromise or hijack social media accounts. They may use this control for various malicious activities, including spreading misinformation, conducting scams, or demanding ransoms.
8. **IoT Kidnapping:** Internet of Things (IoT) kidnapping involves exploiting vulnerabilities in connected devices. Cybercriminals may take control of IoT devices, disrupting their functionality, and demand a ransom for their release or normal operation.

How To Protect Yourself from Cyber Kidnapping

It is one of many crimes that have emerged in the digital era, such as online scams and phishing. Experts recommend being extra careful with calls from unknown numbers though Cyber Criminals can also make it appear like they are calling from a loved one's number. Scammers can use data you have shared on social media to make their calls more convincing, so be careful of what you share about yourself.

- Cyber criminals can also make it appear like they are calling from a loved one's number.
- Scammers can use data you have shared on social media to make their calls more convincing.
- It's important to be careful of what you share about yourself and your children online, especially names, specific locations, and pictures of your home, neighborhood, or children's school.
- Experts also recommend checking up on your loved ones before making payments and approaching the police.
- There are other measures as well to keep oneself safe i.e., Turn on multi-factor authentication, Think before you click, Use strong passwords, Social media privacy, etc.

Importance of Cybercrime Awareness

To combat the rising tide of cyber snatching, fostering cybercrime awareness is paramount. Educating oneself and one's team on the nuances of online security can significantly reduce the risk of falling prey to virtual extortion.

Collaborative Efforts for Security

Ensuring cybercrime and security is a collective responsibility. Businesses, individuals, and government bodies must collaborate to create a robust cybersecurity framework that safeguards against cyber snatching and other digital threats.

Preventive Measures: Safeguarding Your Digital Domain

Implementing Strong Password Policies

One of the foundational steps in fortifying against cyber-Snatching is implementing strong password policies. Using a combination of uppercase and lowercase letters, numbers, and special characters can significantly enhance the security of digital accounts.

Regular Software Updates

Staying one step ahead of cybercriminals involves regularly updating software and applications. This simple yet effective measure patches vulnerabilities that could be exploited by virtual kidnappers.

Employing Encryption Technologies

Encrypting sensitive data adds an extra layer of protection, making it challenging for cybercriminals to access and exploit confidential information. Utilizing encryption technologies is a strategic move in safeguarding digital assets.

Conducting Employee Training Programs

Human error is often a gateway for cyber kidnappers. Conducting regular cybersecurity training programs for employees can create a vigilant workforce that can identify and mitigate potential threats effectively.

The threat of cyber-Snatching looms large in our interconnected world. Understanding the tactics employed by virtual kidnappers, staying abreast of cyber cases in India and worldwide, and adopting proactive measures are crucial steps toward fortifying our digital domains. By prioritizing cybercrime awareness and implementing robust preventive measures, we can collectively create a more secure online environment.

Overview of Cybercrime

Cybercrime is a new trend that is gradually growing as the internet continues to penetrate every sector of our society and no one can predict its future. The crime usually requires a hectic task to trace. Generally, cybercrime may be divided into one of two types of categories:

1. Crimes that affects computer networks and devices directly. Examples are malicious code, computing viruses, mal-ware etc.

2. Crimes facilitated by computer networks or devices, the primary target of which is independent of the computer networks or device. Examples include Cyber Stalking, Fraud and identity theft, phishing scams and information warfare.

Causes of Cybercrimes in Nigeria

The following are some of the identified causes of cyber-crime (Hassan, 2012)

a. Unemployment is one of the major causes of Cybercrime in Nigeria. It is a known fact that over 20 million graduates in the country do not have gainful employment. This has automatically increased the rate at which they take part in criminal activities for their survival.
b. Quest for Wealth is another cause of cybercrime in Nigeria. Youths of nowadays are very greedy, they are not ready to start small hence they strive to level up with their rich counterparts by engaging in cybercrimes.
c. Lack of strong Cyber Crime Laws also encourages the perpetrators to commit more crime knowing that they can always go uncaught. There is need for our government to come up with stronger laws and be able to enforce such laws so that criminals will not go unpunished.
d. Incompetent security on personal computers. Some personal computers do not have proper or competent security controls, it is prone to criminal activities hence the information on it can be stolen. Though, lean entrepreneurship and therapeutic entrepreneurship are profane means of tackling cybercrimes (Ovharhe, 2022a, Ovharhe, 2022b). Ovharhe and Okolo (2022) and Ovharhe et al (2019) pursue lean and remote working as possible alternative of managing cybercrimes (Ovharhe, Woko & Ezeocha, 2021; Ovharhe & Igbokwe, 2021).

Cybercrimes in the e-Commerce Sector

The Nigerian economy, including the enormous amount ofe- businesses, is greatly threatened by the rapid increase of e-crimes could be determine by artificial intelligence and business innovation (Ovharhe, 2024). Also, Ovharhe (2025a) argues on frugal innovation as a possible remedy to reduce crimes and poverty. E-commerce refers to the use of technology, particularly the Internet, to buy, sell and market goods and ser-vices to customers (Michael, 2014). Very few e-crimes are discovered in this sector because most businesses fear the loss from negative publicity than the crimes involved. In arecent article by This Day and Vanguard, Senator Iroegbuestimated the annual

cost of cybercrime to Nigeria at about0.08% of the county's Gross Domestic products (GDP) whichamounts to approximately 127 billion Naira (Ewepu, 2016). Software Piracy (Intellectual Property Theft): The term"Copyright" means little or nothing to the average Nigerian.Piracy involves the unlawful reproduction and sharing ofapplications software, games, movies/videos and audios. Cybercriminals make money from the illegal sales of pirated copies of software and even go as far as providing cracks for pirated software. The internet has created a platform for almost anonymous, free and illegal distribution of pirated materials in Nigeria. Sales Fraud & Forgery: In our society today, fraudulent sales of products that do not exist or that are replicas are increasingly common. The purchase of an item before actu-ally seeing it has created ways for fraudsters to make money via the sale of unoriginal products or in some cases, the total absence of the product. Many persons have fallen victim of these particular crimes on popular e-commerce websites. Data and Airtime Time (DAT) theft from service providers: This is a very rampant scam among the youths of today. They illegally gain access to "Cheat codes" and unlawfully use them to gain thousands of mobile data and unlimited airtime without making the necessary payment. Also, cybercafes have developed means of connecting to the network of internet service providers. However, consignment inventory system, lean accounting, lean entrepreneurship and light entrepreneurship and customer funded business are modern business approach to pursuit on remedies to criminality on cyber issues (Ovharhe, Ahunanya & Woko, 2022; Ovharhe, Chibuike & Abada, 2023; Ovharhe, Okolo, Woko & Igbokwe, 2022; Ovharhe, Woko & Ogolo, 2021). Crimes affect entrepreneurship entry and exist decision in the business (Ovharhe & Abada, 2023).

3. METHODOLOGY

This is a scientific method that deals with observable social reality and measurable facts. "Positivist focus strictly on scientific empiricist method designed to yield pure data and facts uninfluenced by human interpretation" (Saunders et al, 2019). O'Leary, 2004 (cited by Mackenzie and Kinpe, 2006) suggested that the sole aim of a positivist is to test a theory or describe an experience through observation and measurement to control the situation/forces around them. Most time positivism is used in quantitative research because it is based on reality in research work and most time the stance used by the researcher is objective (Saunders, 2019).

The philosophical underpinned was orchestrated on positivism because it's embedded on scientific facts been applicable to triangulation techniques on research.

The study integrated the ex post facto and correlation research design. Ex post facto research is systematic empirical inquiry in which the scientist does not have direct control of independent variables because their manifestations have already occurred or because they are inherently not manipulated.

The targeted population was centered on digitalization clients that familiarized themselves with computer related fraud, computer related forgery, cyber-pornography, cyber-stalking and cyber-

squatting. Evidence from Ninja News 2025 revealed that over 97448 clients of social works are simultaneously interfacing online with computer related fraud, computer related forgery, cyber-pornography, cyber-stalking and cyber-squatting.

Convenience sampling technique was used to select only those that have interest on cybercrimes. Additionally, proportionate stratified random sampling technique was used to select reasonable percentages from each of the categories of personnel from each of the computer related fraud, computer related forgery, cyber-pornography, cyber-stalking and cyber-squatting. While simple random sampling technique without replacement was used to select the potential respondents.

However, because it was not possible to cover the entire Cybercrimes management, an accessible population was estimated to the total number of 85678 from the available records and there is a 95 % chance that the sample was distributed in the same way as the population (i.e. 0.05) confidence level.

We can determine the sample size by using Taro Yamane's (1967) formula as shown below:

$$n = \frac{N}{1 + N(e)^2}$$

Where, n = sample size sought

e = level of significance or (acceptable sampling error)

N = population

Applying the above formula:

$$n = \frac{86648}{1 + 86648\ (0.05)^2}$$

$$= \frac{86648}{1 + 86648\ (0.0025)}$$

$$= \frac{86648}{1 + 214}$$

$$= \frac{86648}{215}$$

Therefore n = 399 respondents

A test re-test method was used to establish the reliability of the questionnaire. Twenty stakeholders comprising of twenty employees knowledgeable in cybercrime and cyber security others being familiar in the computer related fraud, computer related forgery, cyber-pornography, cyber-stalking and cyber-squatting were used to establish the reliability of the questionnaire. They were used since they share similar characteristics with the potential respondents of the study. Twenty copies of the questionnaire were administered to them, and after two weeks, the same questionnaire was re-administered to the same respondents. The responses on the questionnaire from the first administration was correlated with the responses from the second administration using Pearson Product Moment Correlation for reliability of the entire instrument. Again, Cronbach alpha was used to establish the inter-item and inter-scale reliability of the questionnaire. These statistical tools (i.e. Pearson Product Moment Correlation and Cronbach alpha) in the Statistical Package for Social Science (SPSS) version IBM 25 was used. Questionnaire with reliability co-efficient should be at least 0.70 above could be considered reliable and used for the study, but the study alpha mean was 0.870. However, the reliability coefficient analysis was Cyber kidnappings (α =.882), Yahoo-yahoo (α=878), Cyber stalking (α=866), cyber editorials (α=884), cyber bully (α=870), cyber stalking (α=882) and mental health (α=887).

The researcher assembled all the returned copies of the questionnaire, sort out the ones that are properly filled and separate them from the ones not properly filled (if any). The copies of questionnaire were coded for analysis using SPSS version IBM 25, and item-by-item, while sub-scale and overall analysis was implored in this study.

4. DATA PRESENTATION, ANALYSIS, RESULTS AND DISCUSSIONS

Presentation of Data

The study deploys both descriptive and inferential statistics in evaluating the underlying relationships of outlined predictors and criterion variables. The study clearly outline evidences and results in tables and charts. The hypothesis where tested and findings discussed in later part of the chapter.

Questionnaire distribution

	Frequency	**Percentage (%)**
Sample Size	399	-
Questionnaire copies distributed	399	100
Questionnaires Retrieved	378	93.71
Incomplete/Wrongly Filled	10	7.35
Valid Questionnaire	317	74.54

Source: *Author's Field Survey*

The study in previous section deduced the suitability of a minimum sample size of 399. But due to exigencies and vagaries in the field, the author mobilized 399 (100%) questionnaire to the sample areas. While only 378 (93.71%) questionnaire were retrieved, the authors observed that 10 (7.35%) questionnaire were either wrongly filled or incomplete thereby making them invalid to the study. This owes largely to non-adherence to stipulated instructions by respondents, honest omission by respondents and selections of multiple options in a single item which actively invalidates the questionnaire. Only 317 (74.54%) of mobilized questionnaire were considered valid and admissible and therefore utilized in the study. To further confirm the validity and reliability of the admitted questionnaire, the study employed the reliability test using the Cronbach alpha reliability statistics.

Reliability statistics

Variables	Dimensions/Measures	Alpha Value
Cybercrimes management(Predictor)	Cyber kidnappings	**0.882**
	Yahoo-yahoo	**0.878**
	Cyber stalking	**0.866**
Cyber security(Criterion)	Cyber editorials	**0.884**
	Cyber bully	**0.870**
	Cyber stalking	**0.882**
Moderating	Mental health	**0.887**
	Average Reliability Statistics	**0.870**

Source: *Author's Field Survey - SPSS version 25 output extracts*

Using the Cronbach alpha statistics to scale the variables, it can be easily observed that there is convergence in the responses given by respondents. This shows clarity and understanding of the questionnaire (items). This is linked to the fact that all item showed an Alpha values greater than 0.70 (70%) as prescribed by Nunally (1978) thereby showing reliability of the study variables.

It should be further identified that the study utilized dimension reduction, as all items under each dimension/measures were statistically collapsed into a single principal component using factor analysis, it is therefore relevant to similarly show how well captured these items are in their respective using the confirmatory factor analysis.

Confirmatory Factor analysis test using the KMO

Variables	Determinant	KMO of Sampling Adequacy	Sig
Cyber kidnappings	0.1586013	0.929	0.000
Yahoo-yahoo	0.5450900	0.907	0.000
Cyber stalking	0.2847291	0.672	0.000
Cyber editorials	0.4651321	0.840	0.000
Cyber bully	0.9762009	0.904	0.000
Cyber stalking	0.7682308	0.892	0.000
Mental health	0.8210008	0.890	0.000

Source: *Author's Field Survey - SPSS version 25 output extracts*

The output above shows all determinant statistics to be above 0.0001. A threshold before which showed multicollinearity and autocorrelation between items of the same predictor/criterion. The KMO (Kaiser-Meyer-Olkin) of sampling size is greater than 50%(0.5) in all employed dimension and measures further showing that each principal component deduced from the myriad of items in the questionnaires are true representative of the questionnaire items and are therefore very reliable. The significance levels are all below 0.05(5%) which leads to the rejection of the null hypothesis of no structure detected. Therefore, Cybercrimes management suitability of our proxies shows that the variables viability and eligibility for subsequent tests.

Parametric checks

Due to the nature of the Pearson Product Moment and Regression analysis, this study observes the internal parameter of study variables by carrying out the normality test.

Table A: Summarized Parametric test check output

	Std. Dev.	Skewness	Kurtosis	Jarque-Bera	Probability	Observations
Cyber kidnappings	0.999999	-1.51292	3.584707	2.091734	0.3826	317
Yahoo-yahoo	1.000001	-1.42873	3.177840	1.704938	0.4651	317
Cyber stalking	1.000000	-1.24595	1.698484	8.846257	0.2018	317
Cyber editorials	0.999998	-1.42631	2.932714	1.568203	0.5100	317
Cyber bully	1.000000	-1.76142	3.362805	3.132865	0.3514	317
Networking	1.000000	-1.66542	2.765447	2.876546	0.4372	317
Mental health	0.999999	-0.94253	1.251630	4.777134	0.3098	317

Source: *Author's Field Survey: - SPSS version 25 output extracts*

Based on the above table, it can be easily identified that the standard deviation of all variables are largely close to one. The rule of thumb for a normally distributed data in light of the standard deviation is that the statistics or deviation must lie between 1 or be close to one. This is easily the case as seen from Table, which therefore shows good parametric tendencies in the study variables as deduced from the deployed questionnaires.

As a rule of thumb, a skewness should be between -1 and -0.5 or 0.5 and 1. Any skewness less than -1 or greater than 1 shows that the distribution is highly skewed. Of all employed variables, only mental health as the moderating variable and cyber stalking as the medicating variable are observed to be of a moderate skewness. The average responses associated to these variables must most likely be evenly distributed over the five-point Likert scale. While for other dimensions and measures, their respective responses must most likely be "highly" skewed negatively. Similarly, a skewness close to zero shows a non-normally distributed data which is not the case with our study variables.

The kurtosis which shows the sharpness and height of the central peak is meant to be with the range of -2 and 2 and in some cases -3 and 3. It can be seen that majority of the variables fall between these bracket and are therefore seen as normally distributed.

The jarque-bera probability level of shows that all variables have probability level greater than 0.05(5%), this therefore Cybercrimes management the evidence of normal distribution in the sample as the null hypothesis of normal distribution is highly upheld in the model.

Data Analysis

-Univariate Analysis

To further understand the nature of the questionnaire responses by respondents, the study employs a univariate evaluation of the responses. The study capitalizes on the central tendencies of these responses as it shows the major direction of response of the respondents' choices. This analysis is majorly descriptive with undertones of inferences drawn from the observed responses.

The adopted mean threshold of the study is 3, which using the 5 point Likert scale adopted is the realm of indecision. This therefore aids with the cyber editorials of responses as values greater than 3 ($x > 3$) are observed to be affirmative. While values less than 2 ($x < 3$) are seen as non-affirmative to the questionnaire item. The decision rule is tied to the interpretation by Narling (2010) which prescribes the identification of the response categories based on a grand mean as linked to a threshold. This will reinforce the study conclusion as it will contribute to building the manifestation of the study variables. The study presents the univariate distributions as follows.

Universal Model Evaluation

To observe how fitted the employed variables are, the study starts by evaluating the interplay of the employed dimensions and measures of the study variables as follows

Model 1 (Cyber editorials)

Model Evaluation of Cyber editorials as influenced by Cyber kidnappings, Cyber stalking, Yahoo-yahoo.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.787[a]	.773	.773	.16434941

a. Predictors: (Constant), Cyber kidnappings, Cyber stalking, YAHOO-YAHOO

ANOVA[a]

Model		F	Sig.
1	Regression	2846.764	.000[b]
	Residual		
	Total		

a. Dependent Variable: Cyber editorials

b. Predictors: (Constant), Cyber kidnappings, Cyber stalking, YAHOO-YAHOO

Source: *Author's Field Survey- SPSS version 25 output.*

The Study observes from the R-square value of 0.783 that all employed dimensions (Cyber kidnappings, Cyber stalking, Yahoo-yahoo) jointly account for up to 77.3 percent of variation in the criterion variable as captured in the model (model 1) by cyber editorials. This shows that the variables used to predict the behavior of efficiency of the firm are adequate predictors of the variables. As such, this shows that the variables are well selected. The F-statistics value of 2846.764 at a significance level of 0.000 which is lower than the 0.05 significance shows that the model is well fitted. This means that the employed variables go hand-in-hand and as such are well blended.

Model 2 (Cyber bully)

Table 4.14 Model Evaluation of Cyber bully as influenced by Cyber kidnappings, Cyber stalking, Yahoo-yahoo.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.882[a]	.864	.864	.18971415

a. Predictors: (Constant), Cyber kidnappings, Cyber stalking, YAHOO-YAHOO

ANOVA[a]

Model		F	Sig.
1	Regression	2116.965	.000[b]
	Residual		
	Total		

a. Dependent Variable: Cyber bully

b. Predictors: (Constant), Cyber kidnappings, Cyber stalking, YAHOO-YAHOO

Source: *Author's Field Survey (2025)- SPSS version 25 output.*

The Study observes from the R-square value of 0.864 that all employed dimensions (Cyber kidnappings, Cyber stalking, Yahoo-yahoo) jointly account for up to 86.4 percent of variation in the criterion variable as captured in the model (model 2) by cyber bully. This shows that the variables used to predict the behavior of efficiency of the firm are adequate predictors of the variables. As such, this shows that the variables are well selected. The F-statistics value of 2116.965 at a significance level of 0.000 which is lower than the 0.05 significance shows that the model is well fitted. This means that the employed variables go hand-in-hand and as such are well blended.

Regression Coefficient Model 1 (Cyber editorials)

Multiple regression coefficient and significance

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.002E-013	.009		.000	1.000
	Yahoo-yahoo	.431	.040	.431	10.760	.000
	Cyber kidnappings	.439	.040	.439	10.873	.000
	Cyber stalking	.073	.031	.073	2.346	.020

a. Dependent Variable: Cyber editorials

Source: *Author's Field Survey- SPSS version 25 output*

In light of cyber editorials, the study observes that all dimensions (Cyber kidnappings, Cyber stalking, and Yahoo-yahoo) exhibit positive coefficient with the measure of the criterion variable. This shows that increase of one standard deviation in the Cyber kidnappings, Cyber stalking, and Yahoo-yahoo will make for 0.431, 0.49, and 0.073 increase in cyber editorials. This therefore shows that a firm engaged in cybercrime is likely to strongly increase the level of innovativeness in its operations, products or services. This agrees with theoretical underpinnings that predicts higher resource efficiency in the wake of cybercrime overtime.

5. SUMMARY, CONCLUSIONS, RECOMMENDATIONS AND CONTRIBUTION TO SCHOLARSHIP

Summary of the Study

The study sought to establish the relationship between cybercrime and cyber security of computer related fraud, computer related forgery, cyber-pornography, cyber-stalking and cyber-squatting in Edo State. The selected predictor proxies included Yahoo-yahoo, Cyber stalkings and Cyber kidnappings, while the criterion proxies are cyber editorials, cyber stalking and cyber bully, while the mental health was adopted as moderating variable. Three research questions and three hypotheses were raised. The study employed several theories to advanced and explain the link between cybercrime and cyber security. These include AI theory. The study followed cross sectional survey and ex-post facto design was used. Multiple regression analysis was utilized to test the hypotheses. The findings revealed the null hypotheses were rejected and alternate hypotheses accepted.

Conclusions

Cybercrime is a menace that should be eradicated or reduced to a very minimal level for our great nation to break even. Several prominent cybercrimes and causes have been discussed in this study. The study conducted in tertiary institutions to determine students' participation in cybercrimes shows that majority of the crimes conducted are carried out by the youths in our society majorly through phishing. Numerous ways have been proposed to prevent future occurrence of this crime, how-ever much can still be done by government and individuals to reduce it.

Recommendations

Based on the findings and conclusions the following recommendations were made

1. Cybercrimes management have to ensure that there is effective control of Yahoo-yahoo proxies because they are fundamental factors to the frame compared with longer-term Cyber stalking among client.

2. The Cybercrimes management using social entrepreneurship venture approach should integrate cyber kidnappings in a better manner towards managing cyber stalking.

3. Cyber stalking should be implemented and demonstrated by strict restrictions be regulatory bodings.

Contribution to Knowledge

To sum up the main ideas, preventing and dealing with cyber kidnapping needs a full social entrepreneurship venture approach. This includes using good cybersecurity habits, using technology to protect, and working together between industries and governments. Everyone individuals, businesses, and policymakers' needs to focus on learning about cybersecurity, using advanced technologies, and cooperating globally. Only by working together we can make our digital world stronger and avoid the harmful effects of cyber kidnapping in the future

The decision was part of a wider initiative to try to convince enterprises that their data is safe with computer related fraud, computer related forgery, cyber-pornography, cyber-stalking and cyber-squatting.

REFERENCES

Hassan, A. B. Lass F. D., & Makinde J. (2012) Cybercrime in Nigeria: Causes, Effects and the Way Out, ARPN Journal of Science and Technology, vol. VOL. 2(7), 626 – 631.

Lakshmi P. and Ishwarya M. (2015), Cyber Crime: Prevention & Detection," International Journal of Advanced Research in Computerand Communication Engineering, vol. Vol. 4(3).

Maitanmi, O. Ogunlere, S. andAyinde S. (2013), Impact of Cybercrimeson Nigerian Economy, The International Journal of Engineering andScience (IJES, vol. vol 2(4), 45–51.

Michael, A.,Boniface., A. and Olumide, A. (2014) Mitigating Cybercrime and Online Social Networks Threats in Nigeria, Proceedings of the World Congress on Engineering and Computer Science Adu Michael Kz,vol. Vol I WCECS 2014, 22–24.

Ndible N., (2016) Practical Application of Cyber Crime Issues Retrieved onMay 6, 2016 availableat:http://ijma3.org/Admin/Additionals/Cybercrime/Nibal%20Idlebi%20Presentation.pdfShandilya A. (2011) Online Banking: Security Issues for Onlinepayment,from www.buzzle.com/articles.

Okeshola F.B. and Adeta A.K, (2013) The Nature, Causes and Consequencesof Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, NigeriaAmerican International Journal of Contemporary Research, vol. 3(9),98-114.

Ovharhe, O. H. (2022a). Sustainable development goals: Multicollinearity between therapeutic entrepreneurship and rehabilitation therapy among African nations. *International Journal of Small Business and Entrepreneurship Research*, 10(3), 1-59. DOI: https://doi.org/10.37745/ijsber.2013/vol10n3157

Ovharhe, O. H., Woko, E. B., & Ezeocha, V. U. (2021). Remote working: Entrepreneurial risk and entrepreneurial survival in the micro firms in Niger-Delta, Nigeria (COVID-19 Pandemic Prospects). *International Journal of Small Business and Entrepreneurship Research*, 9(4), 11-28. DOI: https://doi.org/10.37745/ijsber.2013/vol9n11-28

Ovharhe, O. H., & Chukwuemeka, S. P. (2023). Sustainable Development Goals: Therapeutic Entrepreneurship and Mental Health Conditions. *British Journal of Multidisciplinary and Advanced Studies*, *4*(1), 81–119. https://doi.org/10.37745/bjmas.2022.0107

Ovharhe, O. H., & Igbokwe, E. L. (2021). Analytical intervention of remote working correlates on risk culture and entrepreneurial adaptability in South-South Geopolitical Zone, Nigeria: Covid-19 Perspective. *Journal of Education and Practice, IISTE*, 12(3), 34-44, DOI: 10.7176/JEP/12-34-05

Ovharhe, O. H., & Okolo, B. S. (2022). Sustainable development goals: Lean entrepreneurship and Green entrepreneurship. *International Journal of Research and Scientific Innovation, 9(10), 59-71. ISSN: 2321-2705*

Ovharhe, O. H., Ahunanya, V., & Woko, E. B. (2022). Consignment inventory system and entrepreneurial survival in Lagos State. *International Journal of Social Science & Management Research*, 8(5), 29-42. DOI: 10.56201/ijssmr.v8.no5.2022.pg29.42

Ovharhe, O. H., Chibuike, C. U., & Abada, A. M. (2023). Lean Accounting And Lean Entrepreneurship. *American Journal of Social Development and Entrepreneurship*,. 2(2) 1-8, DOI: https://doi.org/10.54536/ajsde.v2i2.1578

Ovharhe, O. H., Okolo, B. S., Woko, E. B.,, & Igbokwe, L. (2022). Light entrepreneurship and customer funded business model. *International Journal of Social Sciences and Management Research*, 8(5), 87-106.DOI: 10.56201/ijssmr.v8.no5.2022.pg87.106

Ovharhe, O. H., Woko, E. B., & Ogolo, T. M. (2021). Competitive risk strategy and entrepreneurial satisfaction among fast moving consuming goods in Nigeria during covid-19 pandemic using confirmatory factor analysis. *International Journal of Multidisciplinary Research and Growth Evaluation*, 2(6), 267-272.https://doi.org/10.54660/anfo.2021.3.1.14

Ovharhe, O. H.., & Abada, A. M. (2023). IFRS adoptions on entrepreneurship entry and entrepreneurship exit: The Nigeria experience from 2006-2017. 2**(** 2**),** *American Journal of Social Development and Entrepreneurship*. DOI: https://doi.org/10.54536/ajsde.v2i2

Ovharhe, O.H. (2022b). Sustainable development goals: Therapeutic entrepreneurship and entrepreneurship Injelititis among West Africa Countries. World Journal of Entrepreneurial Development Studies (WJEDS) 7(1), 87-113. DOI: 10.56201/wjeds.v7.no1.2022.pg87.113

Ovharhe, O. H., & Odepeli, S. (2024). Environmental pollution and maternal mortality among female entrepreneurs. *International Journal of Geography and Environmental Management* (IJGEM), 10(2), 172-197.D.O.I: 10.56201/ijgem.v10.no3.2024.pg172.197

Ovharhe, O. H., & Woko, B. E. (2024a). Environmental pollution and life expectancy among Intrepreneurs. *International Journal of Medical Evaluation and Physical Report* (IJMEPR), 10(2), 9-32. DOI: 10.56201/ijmepr.v8.no3.2024.pg9.32

Ovharhe, O. H. & Woko, B. E. (2024b). Environmental pollution and infant mortality on entrepreneurial opportunities: A champiopreneurship approach. *International Journal of Geography & Environmental Management (IJGEM),* 10 (3), 144-171. D.O.I: 10.56201/ijgem.v10.no3.2024.pg144.171

Ovharhe, O. H. & Chibuike, C. U (2024a). Creative Accounting and Creative Entrepreneurship. *Journal of Accounting and Financial Management (JAFM)*, 10(7), 157-174. DOI: https://doi.org/10.56201/jafm.v10.no5.2024.pg157.174

Ovharhe, O. H., & Chibuike, C. U. (2024b). Innovation Accounting and Frugal Innovation. *World Journal of Innovation and Modern Technology* (WJIMT), 8(2), 50-70.DOI: 10.56201/wjimt.v8.no2.2024.pg50.70

Ovharhe, O. H., & Akandu, C. J.(2024). Innovation Accounting and Innovation Entrepreneurship. *World Journal of Innovation and Modern Technology* (WJIMT). 8(2), 31-49 DOI: 10.56201/wjimt.v8.no2.2024.pg31.49

Ovharhe, O. H., & Abada, A. M. (2024). Creative Accounting and Entrepreneurship Opportunities. Journal of Accounting and Financial Management (JAFM) 10(5) 175-190. DOI: 10.56201/jafm.v10.no5.2024.pg175.190

Ovharhe, O.H. (2024). *Business intelligence and innovation moderating roles on entrepreneurship and management using champiopreneurship approach*. In K. Kankaew, P. Nakpathom, A. Chnitphattana, K. Pitchayadejanant, & S. Kunnapapdeelert (Eds.), *Applying business intelligence and innovation to entrepreneurship advances in business strategy and competitive advantage* (p. 171-223). IGI Global.com .https://doi.org/10.4018/979-8-3693-1846-1.ch009.

Ovharhe, O. H. (2025a). *Frugal Innovation and Social Entrepreneurship with Social Extrapreneurs and Ultrapreneurs*. In R. Manna., A. Singh., & K, Dixit. (Eds.). (2025). *Frugal Innovation in Entrepreneurship*. IGI Global. https://doi.org/10.4018/979-8-3693-4050-9

Ovharhe, O. H. (2025b). KSA and Entrepreneurship Growth Strategies. *Management and Human Resource Research Journal*, *14*(12), 1–22. Retrieved from https://cirdjournals.com/index.php/mhrrj/article/view/1387

Ovharhe, O. H. (2025c). Leveraging Technology Innovation and Creativity in Entrepreneurship Opportunities. *Business Management and Entrepreneurship Academic Journal*, *7*(12), 18–35. Retrieved from https://cirdjournals.com/index.php/bmeaj/article/view/138

Ovharhe, O. H. (2025d). Entrepreneurship Spirituality and Light Entrepreneurship. *Business Management and Entrepreneurship Academic Journal*, *7*(12), 1–17. Retrieved from https://cirdjournals.com/index.php/bmeaj/article/view/1386

Parthiban L, & Raghavan A. R. (2014), The effect of cybercrime on aBank's finances, International journal of Current Research andAcademic Review, vol. Volume-2(2), no. ISSN: 2347-3215, 173–178,Retrieved Feb. 2014 from www.ijcrar.com

Wada F. and Odulaja G. O. (2014), "Electronic Banking and Cyber CrimeIn Nigeria - A Theoretical Policy Perspective on Causation," Afr J Comp& ICT, Vol 4(3), no. Issue 2.A Summary of the Legislation on Cybercrime in Nigeria, Legislative &Government Relations Unit, Public Affairs Deparment,

FederalBureau of Investigation (2016), ATM skimming,Retrieved June 8,2016available online:https://www.fbi.gov/news/stories/2011/july/atm_071411.

Ewepu G, (2016) Nigeria loses N127bn annually to cyber-crime — NSAavailable at:http://www.vanguardngr.com/2016/04/nigeria-loses-n127bn-annually-cyber-crime-nsa/Retrieved Jun. 9, 2016.

Iroegbu, E "Cyber-security: Nigeria loses over N127bn annually throughCybercrime," available at:http://www.thisdaylive.com/index.php/2016/04/18/cyber-security-nigeria-loses-over-n127bn-annually-through-cybercrime/ RetievedJun. 9, 2016.

Omodunbi, B. (2023). Cybercrimes in Nigeria: analysis, detection and prevention. FUOYE Journal of Engineering and Technology, 1(1),:37-42