Received: 20.05.2026| Accepted: 29.06.2026 |Published: 30.07.2026
Citation: UDO, U.M, EWA, V.E., & EBANI, E.A. (2026) **PHISHING, BUSINESS E-MAIL COMPROMISE (BEC) AND SOCIO-ECONOMIC ACTIVITIES IN UYO LOCAL GOVERNMENT AREA, AKWA IBOM STATE, NIGERIA**
GAIJASSVol.2.1.2026 pp 91-110 https://globreshub.org/index.php/gaijass/art **DOI:** https://doi.org/10.5281/zenodo.22250321

PHISHING, BUSINESS E-MAIL COMPROMISE (BEC) AND SOCIO-ECONOMIC ACTIVITIES IN UYO LOCAL GOVERNMENT AREA, AKWA IBOM STATE, NIGERIA

[1]Utibeima Monday UDO, [2]Victor Elijah EWA & [3]Anthony Ewa EBANI

[1&3]Department of Sociology and Anthropology, University of Uyo, Nigeria
[2]Department of International Relations, University of Uyo, Nigeria
Corresponding Email: udomacin@gmail.com

Abstract

Background: The rapid expansion of digital communication and online commerce in Uyo, Akwa Ibom State, has increased the exposure of individuals and organizations to cyber threats. Phishing and Business E-mail Compromise (BEC) are deceptive schemes that exploit human trust and email vulnerabilities to extract funds and sensitive information, with potential consequences for socio-economic activities.

Objective: This study assessed the effect of phishing and Business E-mail Compromise on socio-economic activities in Uyo Local Government Area, Akwa Ibom State, Nigeria.
Methods: A descriptive survey design was adopted. Using Taro Yamane's formula, a sample of 400 respondents was drawn from a projected population of 1,393,000 through multi-stage sampling: cluster, stratified, and simple random sampling. Out of 400 questionnaires administered, 384 were retrieved and analyzed, representing a 96.0% response rate. Data were analyzed using SPSS with descriptive statistics and Simple Linear Regression Analysis (SLRA).
Results: Business E-mail Compromise was the most prevalent form of cybercrime victimization reported (Mean = 3.68), while phishing was also substantial (Mean = 3.23). Both victimizations had a statistically significant negative effect on socio-economic activities. BEC most strongly discouraged digital payments (Mean = 3.85), and phishing most strongly reduced business productivity (Mean = 3.45). Regression analysis showed that phishing prevalence significantly predicted the composite socio-economic impact, $F(1, 382) = 1743.397$, $p < .05$. Phishing accounted for 82.0% of the variance in socio-economic activities ($R = .906$, $R^2 = .820$; $\beta = -.906$). Consequently, the null hypothesis was rejected.
Conclusion: The study concludes that phishing and BEC constitute structural, rather than incidental, threats to Uyo's digital economy. It recommends the formation of a Cybersecurity Business Alliance, mandatory multi-factor authentication, and sustained digital-literacy campaigns to mitigate these threats.

Keywords: *Phishing, Business E-Mail Compromise, Socio-Economic Activities, Cybercrime Victimization, Uyo*

1. Introduction

Cybercrime has emerged as a pervasive international menace, fundamentally altering the safety architecture of the contemporary digital world, and Uyo Local Government Area is no exception. As Nigeria experiences a surge in internet penetration, digital connectivity has become a double-edged sword for Uyo's socio-economic development (Smith, 2020). Among the range of cyber threats confronting the city, phishing and business e-mail compromise (BEC) stand out for their reliance on social engineering rather than purely technical exploitation, making them particularly difficult to counter through conventional security measures alone.

Phishing involves cybercriminals attempting to trick users into disclosing personal data, credit card details, passwords, or social security numbers, typically through unsolicited messages designed to resemble legitimate communications from banks or service providers (Akinbobola, 2020). Business e-mail compromise, a related and increasingly prominent scheme, exploits human trust and email vulnerability to defraud businesses, targeting corporations, small enterprises, and government facilities alike (Abdullah, Karim and Zhang, 2023). Unlike conventional malware-based attacks, BEC relies on social engineering to manipulate victims into approving fraudulent transactions, often by impersonating executives, vendors, or trusted employees (Symantec, 2022; Chang and Lee, 2021).

The scale of these threats is considerable. The Anti-Phishing Working Group (2020) estimated that phishing costs the world more than US$50 billion annually, while the FBI (2020) reported that BEC scams cost victims over US$1.7 billion in 2019 alone, and more than US$50 billion cumulatively over the past decade (FBI, 2023). BEC now accounts for roughly half of all financial cybercrime globally (IBM Security, 2023). High-profile cases illustrate the disruptive potential of these schemes: a 2019 BEC attack on a major manufacturer cost approximately US$30 million (FBI, 2020), while the 2017 Maersk cyberattack, which propagated through phishing-adjacent vectors, cost an estimated US$300 million and disrupted global supply chains for weeks (BBC, 2017; Ainsworth, 2017). Zeng et al. (2022) found that organisations victimised by BEC lose an average of 15 percent of shareholder confidence, while the Ponemon Institute (2022) documented an average recovery cost of US$5 million per BEC incident, inclusive of legal fees and forensic investigation. Recent research further highlights the growing role of artificial intelligence in enabling more convincing, harder-to-detect phishing and BEC attempts (Nguyen et al., 2023).

For a fast-growing commercial hub like Uyo, where residents and businesses increasingly rely on digital communication and online

commerce, exposure to phishing and BEC threatens not only individual finances but the broader trust necessary to sustain a digital economy. This study, therefore, assesses the effect of phishing and business e-mail compromise on socio-economic activities in Uyo Local Government Area.

Uyo's rapid adoption of digital communication tools and its transition toward a cashless economy have created fertile ground for socially engineered cyber-attacks such as phishing and BEC. While the city functions as a vibrant hub for commerce, education, and public administration, its heavy reliance on digital platforms for financial mediation and record-keeping has made its socio-economic fabric increasingly vulnerable to schemes that exploit trust rather than technical weakness alone (Adesina, 2021; Ibekwe and Okoro, 2021). The absence of specialised cybersecurity professionals and reliance on obsolete systems leave local businesses, particularly small and medium-sized enterprises, susceptible to disruptions that stall long-term growth (PwC, 2020; Ibok, 2024).

Victimization through phishing and BEC manifests not only as direct financial loss but as trauma, social isolation, and erosion of the trust essential for sustainable community cohesion, with lower-income victims often facing reduced economic opportunities as a result (Okon and Bassey, 2023). While existing literature by Okon and Essien (2022) and Akpan and Nnamdi (2023) has extensively explored the general drivers of cybercrime, there remains a significant research gap regarding the specific effects of phishing and BEC victimization on the stability of socio-economic activities in Uyo. Furthermore, the Cybercrime Act 2015 has proven insufficient in curbing the susceptibility of key institutions, such as banks and fintech platforms, to socially engineered fraud (Ekong, 2023), a weakness compounded by inconsistent enforcement and limited technical expertise within law enforcement (Alabi, 2021; Chukwu and Akinyemi, 2023). It is against this backdrop that this study assesses the effect of phishing and business e-mail compromise on socio-economic activities in Uyo Local Government Area.

This paper contributes to the theoretical understanding of socially engineered cybercrime as distinct from purely technical exploitation within a localised Nigerian urban context. Practically, it equips businesses, financial institutions, and policymakers in Uyo with empirical evidence to guide investment in employee training, verification protocols, and collective threat-sharing mechanisms aimed at curbing phishing and BEC victimization.

2. Literature Review

2.1 Conceptual Clarification

2.1.1 Cybercrime. Cybercrime, a term coined by Adeniran (2008), lacks a single universally accepted definition (Holt and

Bossler, 2016), encompassing a dynamic range of illegal activities including phishing, BEC, hacking, and identity theft that can inflict harm on individuals, organisations, and society (Adeyemi, 2021).

2.1.2 Victimization. Victimization refers to the experience of injury or injustice inflicted through criminal or harmful acts (Miers, 2001), and may be economic in nature, as in the case of fraud perpetrated through phishing and BEC schemes.

2.1.3 Phishing. Phishing is a cyber-attack in which criminals attempt to trick users into providing personal data such as credit card details, passwords, or social security information (Akinbobola, 2020), typically through unsolicited messages resembling legitimate communications. Arshad, Khan and Zia (2021), conducting a systematic literature review, identified several phishing variants, email phishing, spear phishing, whaling, clone phishing, vishing, and smishing, and found that individuals with a positive attitude toward sharing personal information online are particularly at risk. Alhaji, Adebayo and Bello (2018) developed a model integrating cognitive, preconscious, and automatic processing to explain phishing victimization, finding that habitual online activity, including frequent social media use, heightens vulnerability. Lain et al. (2021), in a 15-month field study involving 14,000 employees, found that embedded phishing training did not reliably improve resilience and could, in some cases, increase vulnerability, while encouraging simple, low-friction reporting mechanisms proved more effective at building collective vigilance. Robert (2021) examined the psychological tricks phishers use such as fear, curiosity, urgency, and empathy, to provoke uncritical responses from victims, and developed an AI model capable of detecting emotionally manipulative language in phishing emails.

2.1.4 Business E-mail Compromise (BEC). BEC is an advanced scheme that exploits human trust and email vulnerability to defraud businesses, targeting corporations, small enterprises, and government institutions alike (Abdullah, Karim and Zhang, 2023). Attackers typically gain access to corporate email infrastructure through stolen credentials or spear-phishing, sending messages that appear authentic (Chang and Lee, 2021). The FBI (2020) reported that BEC scams cost victims over US$1.7 billion in 2019 alone.

2.1.5 Socio-Economic Activities. Socio-economic activities like employment, entrepreneurship, trade, and digital economic engagement, underpin individual well-being and national development (Zhao and Lee, 2021). Technology adoption has expanded financial inclusion (World Bank, 2023), but this same digital transformation has widened

the scope for phishing- and BEC-related fraud (Mansfield-Devine, 2021).

2.2 Cyber-Phishing and Socio-Economic Activities

Abasi (2022) and Abdullah, Karim and Zhang (2023) both pointed to the growing cyber threat landscape but from different angles: Abasi's analysis of online harassment highlighted gendered barriers to reporting, a pattern also verified by Eze and Obasi (2022) among female cybercrime victims, while Abdullah, Karim and Zhang emphasised phishing's significant financial and operational impact on individuals and organisations, an emphasis echoed by Choo, Smith and Doe (2023), who documented the financial, operational, and reputational losses phishing attacks cause. Adesanya and Akinyele (2023) offered a general analysis of cybercrime victimization in Nigerian cities, later refined by Ajayi's (2020) localised study of Uyo, which identified phishing and romance scams as particularly common in the area, this findings supported by Afolabi's (2023) observation that social media platforms are frequent sites of cybercrime victimization in Uyo, in contrast to the broader, less locally detailed global analysis of Jones and Brown (2020).

The economic burden of phishing on Uyo's SMEs is a recurring theme. Ajayi (2016) found that small and medium-sized enterprises are disproportionately affected by cyber-phishing, a finding reinforced by Akpan and Ekong (2022), who documented the financial losses and elevated business expenses phishing imposes on Uyo SMEs specifically, and by Akpan and Ekanem (2024), who extended this analysis to Uyo's broader economy. Amadi (2022) and Emeka and Amadi (2022) offered a comparative perspective, finding that ransomware and cryptocurrency-related scams pose a similar threat to small businesses in Delta State, suggesting that Uyo's experience reflects a wider regional trend across Nigeria.

Digital literacy remains a significant predictor of phishing victimization. Akpan, Etim and Nkanta (2022) found that low digital literacy and technological susceptibility are primary drivers of victimization in Uyo, a finding expanded upon by Ekpo and Etim (2021) and Essien (2022), who evaluated the effectiveness of cybersecurity awareness initiatives with somewhat divergent conclusions. Ekpo and Etim express optimism about such campaigns, and Essien offering a more cautious, quantitatively grounded assessment of their limitations. Etim, Akpan and Usen (2022) similarly linked low digital literacy to elevated vulnerability among Uyo youth.

Trust erosion features prominently across the literature. Akpan and Udoh (2024) found that cybercrime, including phishing, directly affects consumer confidence in Uyo's e-commerce and financial stability, a conclusion corroborated by Okon (2023), who attributed a broader pattern of economic

stagnation to declining trust in Uyo's digital economy, a concern that motivates Bassey and Ekong's (2023) proposal for public-private partnerships as a mechanism for restoring trust. Youth unemployment, too, is a fundamental driver: Akpan and Eyo (2021) found a significant correlation between cybercrime and youth unemployment in Uyo, a pattern also identified by Ibekwe and Okoro (2021) and situated within the broader national context by Jelilov and Ndanitsa (2015).

Psychological consequences for victims often overlooked are documented by Inyang and Abasi (2023), who found that digital vulnerability causes considerable stress among business owners, a finding reinforced by Akpan and Inyang's (2023) analysis of the mental-health burden among Uyo entrepreneurs, and by Ayodeji, Olamide and Akinbile's (2018) and Collins's (2021) work on the psychosocial and mental-health effects of cyber-phishing and sextortion respectively. Etim and Akpan (2023) and Ibanga and Ufot (2023) documented the specific role of platforms such as Telegram and social media in facilitating account hijacking and harassment linked to phishing schemes in Uyo.

2.3 E-mail Scam and Socio-Economic Fraud in Business

BEC is widely recognised as a major and increasing threat to socio-economic activities. Abdullah, Karim and Zhang (2023) described BEC as a complex cyber-threat capable of deceiving employees into fraudulently transferring money or information, a characterisation echoed by Choo, Smith and Doe (2023), who highlighted its financial, operational, and reputational effects, and corroborated by the IBM Security (2023) report documenting a sharp rise in both BEC attacks and associated costs. The FBI's Internet Crime Report (2023) confirmed enormous organisational losses attributable to BEC scams internationally, directly connected to the broader economic uncertainty such attacks impose on affected communities.

Methodologically, researchers have examined how BEC techniques are evolving. Nguyen, Wang and Lee (2023) documented cybercriminals' growing use of artificial intelligence to craft more realistic and harder-to-detect BEC messages, a departure from earlier reliance on conventional social engineering, as illustrated by Chang and Lee's (2021) case study of attackers posing as CEOs or vendors, a technique also examined by Copes et al. (2021) in relation to email-based identity theft. The Accenture (2019) Consumer Cybersecurity Confidence report identified a general lack of user awareness as a vulnerability exploited by BEC attackers.

The economic impact of BEC is a repeated theme across the literature. Choo et al. (2023) documented both direct monetary loss and losses associated with incident

response and legal costs, aligning with the BBC's (2017) account of the Maersk cyberattack, which resulted in a US$300 million loss. Abdullah et al. (2023) further highlighted the operational disruption businesses experience following a BEC attack, a pattern the IBM Security (2023) report identified as a significant driver of increased business costs generally.

SMEs are especially vulnerable to BEC. Ajayi (2016) examined how BEC and related cybercrime affect Uyo SMEs, which typically lack resilient cybersecurity frameworks, a finding corroborated by Akpan and Ekong (2022). These conclusions align with Amadi's (2022) findings on the disproportionate impact of ransomware, a related cyber-threat on small businesses, and can be understood through Berkowitz's (1989) frustration-aggression theory, whereby financial hardship-driven frustration may manifest as aggression directed at vulnerable groups such as SMEs.

Beyond direct financial loss, BEC produces substantial reputational damage and erosion of trust. Abasi (2022) documented the obstacles victims face in disclosing online harassment -a dynamic also applicable to BEC, given the shame or embarrassment victims often feel, a pattern corroborated by Ajayi (2020), who found that victimization remains a taboo subject in Uyo, contributing to the crime's continued spread. Calo (2019) argued more broadly that each successful cyberattack further erodes public confidence in digital systems, while Akpan and Udoh (2024) found that BEC attacks specifically undermine consumer confidence in Uyo's e-commerce and financial security.

BEC's spread also constrains digital inclusion, particularly in emerging economies. Essien and Etok (2023) found that cybercrime, including BEC, deters individuals and companies in Uyo from engaging in digital financial processes, a conclusion echoed by Okon and Essien (2021), who identified cybercrime as an obstacle to economic growth and technology adoption in the area , a more pessimistic reading than Ayoob and Suleiman's (2019) view of digital connectivity as a driver of innovation and entrepreneurship, though their optimism does not adequately account for the real risks BEC poses.

Regulatory and enforcement gaps compound the challenge. Adebayo and Mohammed (2021) explained the difficulty of enforcing cybercrime laws in Uyo, a concern echoed by Eze and Obasi (2022), who called for stronger victim-support mechanisms, while Alabi (2021) questioned the effectiveness of the Cybercrime (Prohibition, Prevention) Act 2015 despite ongoing enforcement efforts by agencies such as the EFCC (2023). Collaborative approaches offer a promising counter-response: Bassey, Ekong and Udo (2023) explored the value of public-private partnerships in Uyo's cybercrime prevention efforts, a position shared by Akpan (2023) and consistent with CISA's (2023) emphasis

on post-incident collaboration, though this contrasts with the EU Cybercrime Report's (2023) narrower focus on law-enforcement-led initiatives.

Digital literacy campaigns remain a widely cited coping strategy. Ekpo and Etim (2021) and Essien (2022) both found that digital-literacy campaigns meaningfully improve cybersecurity awareness in Uyo, aligning with ENISA's (2021) emphasis on post-incident education and Lain et al.'s (2021) findings on the value of employee-led phishing detection, a useful counter to Afolabi's (2023) and Okon and Ekpenyong's (2021) findings that technological vulnerability and low digital literacy continue to expose residents to scams.

Finally, socio-economic drivers of BEC deserve particular attention. Okon and Essien (2022) linked high unemployment rates in Uyo to cybercrime engagement, an expression of the economic theory of crime and General Strain Theory as articulated by Becker (1968) and Agnew (1992), whereby social and economic strain precipitates criminal coping. Nwachukwu and Ekanem (2022) similarly attributed the rise of online scams to socio-economic inequality, a pattern substantiated by National Bureau of Statistics (2022) unemployment data. Collectively, this literature demonstrates that BEC is not merely a technological problem but a complex socio-economic concern rooted in inequality and economic desperation.

2.4 Theoretical Framework

2.4.1 Routine Activity Theory (RAT). Cohen and Felson's (1979) RAT explains crime as a function of the convergence of a motivated offender, a suitable target, and the absence of a capable guardian. Applied to phishing and BEC, the routine use of email and online business communication in Uyo generates an abundant supply of suitable targets, while an easy supply of motivated offenders exploits gaps in verification protocols and employee vigilance, the absence of capable guardianship.

2.4.2 General Strain Theory (GST). Agnew's (1992) GST holds that economic and social strain can precipitate criminal coping behaviour. Financially strained individuals may turn to phishing or BEC as a means of achieving material success through illegitimate channels, while victims experience a further form of strain, financial loss, reputational damage, and diminished trust, that can suppress future digital economic participation.

2.4.3 Space Transition Theory (STT). Jaishankar's STT holds that the anonymity and disinhibition of cyberspace convert real-world strain into online offending patterns distinct from physical-world crime. Applied to phishing and BEC, STT explains why offenders favour impersonation and deception over direct confrontation,

exploiting the psychological distance the digital medium affords.

3. Materials and Methods

This study adopted a descriptive survey design suited to investigating the prevalence and socio-economic impact of phishing and BEC in Uyo Local Government Area, the capital of Akwa Ibom State, with a population of approximately 1,393,000 as of mid-2024 (NPC, 2024). The population of the study comprised internet-using individuals and business operators in Uyo engaged in online banking, e-commerce, and digital communication, and therefore exposed to phishing and BEC risk.

Using Taro Yamane's (1966) finite-population formula ($n = N/(1+N(e)^2)$, with N = 1,393,000 and e = 0.05), a sample size of 400 was derived. A multi-stage sampling technique combined cluster sampling across Uyo's three political wards, stratified sampling by age, socio-economic status and occupation, and simple random sampling within strata.

Data were collected using the Cybercrime Victimization and Socioeconomic Impact Questionnaire (CVSIQ), a structured, closed-ended instrument covering demographic characteristics, cybercrime victimization (including phishing- and BEC-specific items), and perceived socio-economic impact on a 4-point Likert scale. The instrument was validated by the supervisor and the Post Graduate Board of the Department of Sociology and Anthropology, University of Uyo, and tested for reliability via test–re-test with 20 respondents (10 excluded from the main study), yielding a Cronbach's alpha of 0.80 or above.

Of 400 questionnaires administered, 384 (96.0%) were retrieved and analysed using SPSS. Descriptive statistics summarised respondents' experiences of phishing and BEC and their perceived socio-economic impact, while Simple Linear Regression Analysis (SLRA) tested the effect of phishing victimization (independent variable) on socio-economic activities (dependent variable). Ethical safeguards included informed consent, voluntary participation, and guaranteed confidentiality and anonymity.

4. Results and Discussion

4.1 Socio-Demographic Profile of Respondents

Out of the 400 questionnaires administered, 384 (96.0%) were returned while 16 (4.0%) were not returned, reflecting strong participation and enhancing the reliability of the collected data. Male respondents made up 63.54% of the sample against 36.46% female. Respondents below 30 years made up 42.7%, those aged 31–45 made up 34.4%, those aged 46–60 made up 17.2%, and those above 60 made up 5.7%. In terms of education, 48.2% held the SSCE, 37.5% held a Bachelor's degree, and 14.3% held a postgraduate degree. Single respondents comprised 52% of the sample, married

respondents 39.1%, and divorced respondents 8.9%. By occupation, 39.84% were tech experts, 38.02% were engaged in trading/digital investment, 13.02% were students, 5.21% were civil servants, and 3.91% were artisans.

4.2 Prevalence of Phishing and Business E-mail Compromise in Uyo Local Government Area

Among the four cybercrime types assessed, e-mail compromise was the most commonly experienced (mean = 3.68, SD = 0.80), while phishing scams recorded a mean of 3.23 (SD = 0.88), on a par with cyber-hacking. On the proliferation scale, "Business E-mail compromise is very common" recorded a mean of 3.47 (SD = 0.68), while "cybercrime via phishing is very common" recorded a mean of 3.17 (SD = 1.04), the latter showing greater dispersion of opinion, suggesting more varied individual experiences of phishing exposure across the sample. Both means fell above the scale midpoint, indicating widespread experience of both crime types in Uyo.

4.3 Impact of Phishing on Socio-Economic Activities

Table 1: Respondents' Rating of the Impact of Phishing on Socio-Economic Activities (N = 384)

Effect of Phishing	Mean ($\bar{X}$)	Standard Deviation
Negatively affects financial transaction	2.79	1.24
Discourages digital payment	3.03	0.71
Reduces business productivity	3.45	0.93
Loss of customers	3.01	1.02

Source: Fieldwork (2025)

Respondents' ratings indicated that phishing most strongly reduced business productivity (mean = 3.45), followed by discouragement of digital payment (mean = 3.03), loss of customers (mean = 3.01), and negative effect on financial transactions (mean = 2.79, the least-rated item, though with a standard deviation greater than one, indicating divergent respondent experience likely reflecting differing causes and spread of phishing attacks across businesses in the area). All means fell above the midpoint of the 4-point Likert scale, indicating a widespread and significant experience of phishing's socio-economic impact in Uyo.

4.5 Impact of Business E-mail Compromise on Socio-Economic Activities

Table 2: Respondents' Rating of the Impact of Business E-mail Compromise on Socio-Economic Activities (N = 384)

Effect of Business E-mail Compromise	Mean ($\bar{X}$)	Standard Deviation
Negatively affects financial transaction	3.10	0.85
Discourages digital payment	3.85	0.41
Reduces business productivity	3.15	0.77
Loss of customers	3.20	0.83

Source: Fieldwork (2025)

Business e-mail compromise most strongly discouraged digital payment (mean = 3.85, the highest mean recorded across all cybercrime-impact items in the study, with a comparatively low standard deviation of 0.41 indicating strong respondent consensus), followed by loss of customers (mean = 3.20), reduced business productivity (mean = 3.15), and negative effect on financial transactions (mean = 3.10, the least-rated item though still well above the scale midpoint). All means indicated a widespread and significant impact of BEC on socio-economic activities in the study area.

A Simple Linear Regression Analysis was conducted, regressing respondents' rating of the socio-economic impact of phishing (dependent variable) on their rating of phishing prevalence (independent variable).

Table 3: Simple Linear Regression Analysis of the Effect of Phishing on Socio-Economic Activities in Uyo Local Government Area (N = 384)

Statistic	Value
R	.906
R^2	.820
Adjusted R^2	.820
Std. Error	.43488
F (1, 382)	1743.397
Sig. (F)	.000

Statistic	Value
Constant (B)	-0.031
Phishing coefficient (B)	-.887
Beta (β)	-.906
t	41.754
Sig. (t)	.001

Dependent Variable: Socio-economic activities

The relationship between phishing and socio-economic activities was strong and positive in magnitude (R = .906), with phishing accounting for 82.0% of the variance in socio-economic activities (R^2 = .820). The regression model was statistically significant, $F(1, 382) = 1743.397$, $p < .05$, indicating that despite the positive correlation coefficient, a significant causative difference exists between phishing victimization and socio-economic outcomes. The beta coefficient for phishing was negative (β = -.906, t = 41.754, $p < .05$), indicating that a unit increase in phishing activity is associated with a 0.887-unit decrease in socio-economic activities in Uyo, consistent with the descriptive findings on financial transaction, digital payment, business productivity, and customer loss reported above. The null hypothesis of no relationship was therefore rejected, confirming a significant relationship between phishing/BEC victimization and the disruption of socio-economic activities in Uyo Local Government Area.

4.7 Discussion of Findings

Phishing and business e-mail compromise exert a highly influential impact on socio-economic activities in Uyo, a finding well explained through the lens of Routine Activity Theory. Cohen and Felson (1979) contend that crime occurs when a motivated offender, an appropriate target, and the absence of an effective guardian converge in time and space. In Uyo, the routine online business operations and personal digital lives of enterprises and individuals including e-commerce and electronic communication, inadvertently generate an overwhelming array of appropriate targets, while an easily available supply of motivated cybercriminals stands ready to exploit these opportunities. The elevated operational costs documented by Nse and Ekong (2022) reflect a direct consequence of this convergence, as businesses must devote substantial resources to offsetting ineffective guardianship, resources that would otherwise support productive, growth-oriented activity.

This impact also highlights how a cycle of financial instability and social erosion is sustained by the continuous vulnerability created by the absence of competent guardianship. Businesses with limited financial means, common in digitally emerging areas such as Uyo, are especially exposed to these attacks (Udoh and Ekanem, 2024), representing a significant and accessible target pool. The resulting successful attacks cause both direct financial damage and an often-irreparable loss of trust among consumers and businesses alike. This ongoing cycle of aggression and defence can discourage the adoption of new technologies and online platforms, ultimately constraining socio-economic development. The findings of this study provide robust empirical support for the conclusion that phishing and BEC are actively interfering with Uyo's economic environment through the mechanisms identified by Routine Activity Theory, confirming that these are not isolated incidents but structural impediments to digital and economic advancement in the study area.

5.0 Conclusion and Recommendations

This study concludes that phishing and business e-mail compromise are prevalent and statistically significant threats to socio-economic activities in Uyo Local Government Area, with phishing alone accounting for over 82% of the variance in reported socio-economic disruption among respondents, and BEC emerging as the single most commonly experienced form of cybercrime victimization overall. Both schemes undermine business productivity, discourage digital payment adoption, and erode customer trust, functioning as structural rather than merely incidental impediments to Uyo's digital and economic development.

Based on these findings, it is recommended that: the Uyo business community establish a collaborative Cybersecurity Business Alliance to support regular workshops, real-time threat-sharing, and a group defence mechanism against evolving phishing and BEC tactics, financial institutions and digital service providers operating in Uyo be required to implement multi-factor authentication (MFA) as a default security measure and to provide accessible educational resources on its use, businesses in Uyo institute verification protocols such as callback confirmation for payment or vendor-detail changes requested by email to counter the social-engineering tactics central to BEC. Also, Government and non-profit organisations in Uyo should mount sustained, city-wide public awareness campaigns on phishing recognition and safe digital communication practices, delivered through radio, community centres, and social media, and law enforcement agencies strengthen the enforcement of the Cybercrime (Prohibition, Prevention) Act 2015 in Uyo through improved training and collaboration with financial institutions and telecommunications providers.

References

Abasi, A., (2022). Barriers to reporting online harassment: A gender perspective. *Cyber Safety Review,* 7(2), 65-78.

Abdullah, H., Karim, A. and Zhang, T. (2023). Business email compromise: A growing cyber threat to organizations. *Journal of Cybersecurity,* 8(3), 115-129.

Accenture. (2019). *Consumer Cybersecurity Confidence Index.*

Adebayo, T. O., and Mohammed, S. J. (2021). The challenges of enforcing cybercrime laws in Nigeria: A case study of Uyo. *Journal of Nigerian Law and Technology,* 19(4), 72-88.

Adegbola, O. I. and Fadara, A. (2022). *The impact of digital infrastructure growth on cybercrime in Nigeria: The case of Uyo Local Government Area. Journal of Cybersecurity Studies,* 8(3), 45-62.

Adeniran, M. A. (2008). *Cybercrime and its impact on Nigeria's development*. *Nigerian Journal of Criminology and Sociology,* 9(1), 45-60.

Adesanya, A. and Akinyele, J. (2023). Cybercrime victimization in Nigeria's urban areas: An examination. *Journal of Digital Security Studies,* 15(2), 45-67.

Adesina, O. (2021). *Trends in cybercrime and the Nigerian youth*. Abuja: Nigerian Cybersecurity Review.

Adeyemi, O. (2021). Cybercrime trends in Nigerian states with high economic activity. *Nigerian Cybersecurity Review,* 7(2), 112-129.

Afolabi, K. (2023). Social media platforms as hubs for cybercrime victimization: A case study in Uyo. *African Journal of Social Media Research,* 6(3), 101-118.

Agnew, R. (1992). *Foundation for a general strain theory of crime and delinquency*. *Criminology,* 30(1), 47-88.

Ajayi, O. A. (2016). *Cybercrime and its impact on small and medium-sized enterprises in Nigeria: A study of Uyo Local Government Area. Journal of Information Security and Privacy,* 5(2), 45-61.

Ajayi, S. (2020). *Evolving patterns of cybercrime in Nigeria: A case study of Uyo Local Government Area*. *Journal of Cybercrime and Law,* 7(2), 98-110.

Akinbobola, A. (2020). A rise in cybercrime victimization at the University of Uyo: An analysis of phishing-related account hacking. *African Journal of Cyber Studies,* 8(3), 203-220.

Akpan, I. M., and Eyo, B. I. (2021). The relationship between youth unemployment and cybercrime in Uyo Local Government Area. *Journal of Social Sciences,* 34(2), 55-68.

Akpan, I., and Nnamdi, O. (2023). Factors influencing youth engagement in cybercrime in Akwa Ibom. *Nigerian Journal of Criminology,* 8 (4), 123-145.

Akpan, J. and Nnamdi, T. (2023). Challenges in quantifying cybercrime victimization in Nigeria. *Journal of Cybersecurity Studies,* 15(3), 45-62.

Akpan, O. E. and Udoh, M. (2024). Cybercrime and consumer trust in Uyo's digital economy: Impacts on e-commerce and financial stability. *Journal of Digital Economy and Security,* 9(1), 101-116.

Akpan, O. E., and Ekanem, U. (2024). The economic consequences of cybercrime in Uyo Local Government Area: A focus on SMEs. *Business and Technology Journal,* 11(1), 58-72.

Akpan, O. E., and Ekong, S. (2022). Cybercrime and its economic implications for SMEs in Uyo Local Government Area. *Journal of Nigerian Business and Economics,* 14(2), 134-148.

Akpan, O. E., and Inyang, I. (2023). The psychological impact of cybercrime on Uyo's entrepreneurs: The stress of digital vulnerability. *Journal of Entrepreneurship and Digital Economy,* 4(2), 22-38.

Akpan, O., Etim, I., and Nkanta, M. (2022). Cybercrime victimization in Uyo: Technological vulnerabilities and limited digital literacy. *Journal of Cybersecurity and Law*, 5(2), 112-129.

Alabi, A. (2021). The effectiveness of the Cybercrime Act 2015 in Nigeria. Lagos: University of Lagos Press.

Alhaji, I., Adebayo, O. and Bello, T. (2018). Factors leading to phishing victimization: A comprehensive model integrating cognitive, preconscious, and automatic processes. *Journal of Cybersecurity and Privacy Studies, 12*(4), 230-247.

Amadi, S. (2022). Ransomware and cryptocurrency: A growing threat to small businesses in Delta State. *Journal of Digital Crime and Security,* 5(4), 112-128.

Anti-Phishing Working Group (APWG). (2020). *Phishing Activity Trends Report:* Q1 2020.

Arshad, A., Khan, R. A. and Zia, M. S. (2021). A systematic literature review on phishing attacks: Evolution, techniques, and countermeasures. *Journal of Cybersecurity and Privacy*, *7*(4), 215-232.

Ayodeji, I. A., Olamide, T., and Akinbile, A. (2018). Psychosocial consequences of cyberstalking on victims in Nigeria. *International Journal of Cybersecurity and Digital Forensics,* 7(3), 46-62.

Ayoob, O. and Suleiman, F. (2019). The role of digital connectivity in fostering innovation and entrepreneurship in Uyo. *Journal of Innovation and Digital Literacy*, 7(3), 142-155.

Bassey, J., Ekong, E. and Udo, P. (2023). Public-private partnerships in cybercrime prevention: A case study

of Uyo, Nigeria. *Journal of Digital Security*, 8(3), 145-160.

BBC. (2014). Sony Pictures Hack Cost Company Over US$100 Million. BBC News.

BBC. (2017). Maersk Cyberattack Cost US$300 Million. BBC News.

Becker, G. S. (1968). *Crime and punishment: An economic approach*. *Journal of Political Economy,* 76(2), 169-217.

Berkman Klein Center for Internet and Society. (2023). Cybercrime's impact on innovation: A necessary evil? *Harvard Law Review,* 37(2), 145-163.

Berkowitz, L. (1989). *Frustration-aggression hypothesis: Examination and reformulation*. *Psychological Bulletin,* 106(1), 59-73.

Brennan, M., (2022). Gender differences in romance scams: An empirical study in Europe. *International Journal of Cybersecurity,* 13(2), 150-163.

Broadhurst, R., Grabosky, P., Alazab, M., and Chon, S. (2013). *Cybercrime: The transformation of crime in the information age*. London: Routledge.

Burgess, M. (2019). The Equifax Breach Settlement: *What You Need to Know.* Consumer Reports. https://www.consumerreports.org

Calo, R. (2019). Privacy and the Future of Identity Protection. *Stanford Law Review.* https://www.stanfordlawreview.org

Campbell, J., and Nichols, M. (2024). The economic implications of cybercrime in developing economies: A digital economy perspective. *Journal of Cybercrime Research,* 21(1), 54-67.

Choo, K. K. R., Smith, R. and Doe, J. (2023). The economic impact of business email compromise (BEC) attacks: Financial, operational, and reputational consequences. *Journal of Cybersecurity,* 45(2), 115-134.

Chukwu, A. and Akinyemi, B. (2023). Cybercrime and digital safety in Nigerian urban centers. *Journal of Cybersecurity Studies*, *12*(1), 45–60.

Cohen, L. E., and Felson, M. (1979). *Social change and crime rate trends: A routine activity approach*. *American Sociological Review*, 44(4), 588-608.

Collins, J. (2021). Sextortion: The silent killer of self-esteem and mental health. *Journal of Cyber Victimology,* 8(2), 124-139.

Copes, H., Doss, M. and Levenson, J. (2021). The rise of email-based identity theft scams: An analysis of social engineering techniques in fraudulent communications. *Journal of Cybercrime and Digital Fraud, 7*(2), 45-62.

EFCC (2023). *Annual report on cybercrime cases in Nigeria*. Abuja: EFCC Press.

Ekong, P. (2023). Cybersecurity infrastructure and its challenges in

Uyo. *African Journal of Information Technology*, 11(3), 300-322.

Ekpo, E. and Etim, I. (2021). The impact of digital literacy campaigns on cybersecurity awareness in Uyo. *Cybersecurity Education Journal*, 6(1), 56-70.

Emeka, C., and Amadi, S. (2022). Cryptocurrency-related scams in Delta State: A growing trend in cybercrime. *African Journal of Cyber Fraud,* 6(2), 23-34.

ENISA. (2023). *ENISA threat landscape 2023*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

Essien, P. (2022). Effectiveness of cybersecurity awareness campaigns in Uyo: A quantitative assessment. *Journal of Information Security Education*, 4(2), 134-147.

Essien, S. and Etok, E. (2023). The digital divide in Uyo Local Government Area: cybercrime as a barrier to financial inclusion. *Journal of Financial Technology,* 5(4), 45-59.

Etim, E. and Akpan, U. (2023). Telegram as a platform for cybercrime: account hijacking and scams in Uyo. *Digital Fraud Journal,* 8(1), 56-72.

Etim, J. O., Akpan, M. B. and Usen, S. F. (2022). Digital literacy and susceptibility to cybercrime among youth in Uyo Local Government Area. *International Journal of Information Technology,* 22(3), 91-103.

Etim, M., Ufot, J., and Abasi, E. (2022). *The impact of digital infrastructure on socio-economic activities in Uyo*. *Journal of Social Science and Technology,* 17(1), 78-94.

Etukudo, U., and Ekpe, E. (2020). Romance scams and digital vulnerabilities in Uyo Local Government Area: A case study. *Journal of Online Fraud Prevention,* 9(1), 56-73.

Eze, D. and Obasi, A. (2022). *Challenges in addressing cybercrime in Nigeria: The need for effective support systems. Nigerian Journal of Crime Prevention,* 14(1), 18-32.

Eze, P. and Obasi, T. (2022). Silence and impunity in cases of female cybercrime victimization. *Women and Cybercrime*, 9(1), 112-126.

FBI (2023). *Internet crime report 2023*. Washington, DC: Federal Bureau of Investigation Press.

FBI. (2020). *Internet Crime Report 2019: Business Email Compromise*. California: Federal Bureau of Investigation Press.

Federal Trade Commission Report (2019). *Equifax Data Breach Settlement.* Washington DC: Federal Trade Commission.

Funke, D. (2021). Gendered perspectives on cybercrime victimization in Uyo Local

Government Area. *Gender and Cyber Safety,* 7(3), 200-215.

Halder, D. and Jaishankar, K. (2011). *Cybercrimes against women in India: Problems and solutions*. *Crime, Law and Social Change,* 55(1), 23-45.

Harrell, E. (2016). *Victims of identity theft, 2016*. Bureau of Justice Statistics.

Holt, T. J. and Bossler, A. M. (2016). *Cybercrime victimization in the age of the internet: A comprehensive review. Journal of Digital Crime and Digital Forensics,* 4(2), 28-42.

Hoofnagle, C. J. (2012). *Identity theft: New account fraud and account takeover. The Journal of Criminal Law and Criminology,* 102(2), 411–448.

Ibanga, P. and Ufot, I. (2023). Social media as a tool for targeted harassment and online fraud in Uyo. *Cyber Awareness Journal,* 16(1), 45-58.

Ibekwe, A., and Okoro, M. (2021). Cybercrime and youth involvement in Uyo. *Nigerian Journal of Youth Studies,* 5(2), 55-90.

Ibok, E. (2024). Security challenges in digital economies. *Journal of Information Technology in Africa,* 19(1), 134-167.

Identity Theft Resource Center. (2020). *2020 data breach report: The impact of data breaches on identity theft*. Identity Theft Resource Center.

Identity Theft Resource Center. (2021). *The Psychological Effects of Identity Theft:* A Report. https://www.idtheftcenter.org

Inyang, P. and Abasi, P. (2023). Psychological consequences of cybercrime victimization on business owners in Uyo. *Journal of Psychological Impact and Business*, 11(1), 42-55.

Ishola, S., Akanbi, M., Olumuyiwa, A. and Aransi, D. (2024). Female participation in cybercrime: A gendered analysis of online fraud in Nigeria. *African Journal of Cybercrime Studies*, 18(3), 132-146.

Jelilov, G., and Ndanitsa, R. (2015). Socioeconomic challenges of cybercrime in Nigeria. *West African Economic Review,* 10(3), 321-350.

Johnson, S., (2022). Gender, cyberbullying, and online harassment: A comparative analysis of Uyo and Europe. *Journal of Gender and Technology,* 14(1), 91-108.

Jones, R. (2021). Challenges in tracing cybercriminals. *Journal of International Security,* 15(3), 250-272.

Kamini, V. (2011). *Cybercrime: A growing global concern. Cybersecurity Review*, 2(3), 52-59.

Lain, T., Smith, J. and Brown, R. (2021). *The effectiveness of embedded training and employee-driven phishing detection: A 15-month longitudinal study of 14,000 employees. Journal of*

Cybersecurity Education, 14(3), 45-67.

Lazarus, S. (2024). A critical review of the roles of male and female offenders in Nigerian cybercrime. *Journal of Criminal Justice Studies*, 19(1), 77-91.

Mansfield-Devine, S. (2021). Cybercrime and digital fraud: The challenges of protecting online transactions. *Computer Fraud and Security*, 2021(5), 9-13.

McQuade, S. C. (2006). *Cybercrime: A guide to the technology, laws, and human impact*. Accura: Pearson Education Press.

Microsoft Threat Intelligence. (2023). *Adversary-in-the-middle (AiTM) and MFA fatigue attacks*. https://www.microsoft.com/security

Miers, D. (2001). *Understanding victimization: A critical introduction*. London: Palgrave Macmillan.

National Bureau of Statistics (2022). Unemployment and underemployment in Nigeria: 2022 Annual Report. *National Bureau of Statistics*, 5(19): 45-67.

National Population Commission (NPC), 2004). Nigeria Demographic and Health Survey 2003. Abuja: NPC and ORC Macro.

Newman, L. H. (2015). *The Emotional Toll of Identity Theft.* The New York Times.

Ngo, F. T., and Paternoster, R. (2011). *The routine activities of individuals and the risk of victimization: A situational explanation of personal crime victimization. Journal of Research in Crime and Delinquency,* 48(4), 513-545.

Nguyen, T., Wang, S. and Lee, H. (2023). Leveraging AI for business email compromise: How cybercriminals are adapting to new technologies. *Cybersecurity Advances*, 7(1), 22-40.

Nse, E. (2023). The rise of cybersecurity investments and costs in Uyo's small businesses. *Journal of Business Security,* 10(3), 110-124.

Nwachukwu, C. I. and Ekanem, F. S. (2022). Socio-economic inequality and the proliferation of online scams in Uyo. *African Journal of Cybersecurity,* 8(1), 27-39.

Nwankwo, E. and Eze, P. (2022). Economic disparities and the vulnerability of women to online scams. *Journal of Digital Poverty Studies,* 5(4), 82-98.

OECD (2022). The intersection of cybercrime and legislation: Policy responses across nations. *International Journal of Policy and Governance,* 8(4), 120-135.

Ogunleye, A., Ojedokun, A. and Eraye, T. (2019). Male dominance in cybercrime: A review of offender profiles and networks. *Cybercrime Review*, 7(1), 51-63.

Okon, I. (2023). The trust erosion in Uyo's digital economy due to cybercrime. *Journal of Economic Development,* 12(1), 34-48.

Okon, M. and Bassey, E. (2023). Cybercrime victimization and its effects in Uyo Local Government Area. *African Journal of Criminal Justice,* 13(1), 34-67.

Okon, M. and Essien, J. (2022). Economic drivers of cybercrime in Uyo Local Government Area. *Journal of Nigerian Studies,* 11(4), 200-233.

Ponemon Institute (2022). The business of cybersecurity: How organizations invest in protection. *Journal of Information Protection,* 6(3), 103-120.

PWC Global Economic Crime Survey. (2020). *Nigeria Cybercrime report*. PWC.

Robert, A. (2021). *Factors enhancing phishing effectiveness: Psychological tactics and emotional manipulation in phishing attacks. Journal of Cybersecurity and Behavioral Psychology,* 10(3), 45-59.

Smith, J. and Doe, A. (2023). *Identity theft and its growing impact on digital security. Cybercrime Journal,* 15(3), 234-245.

Smith, T. (2020). Cybercrime dynamics in Nigeria. *African Information Studies,* 5(3), 123-156.

Symantec. (2022). The rise of Business Email Compromise (BEC) attacks: Trends and prevention strategies. *Symantec Cybersecurity Report*, 15(2), 56-72.

Udoh, M. and Ekanem, S. (2024). Cybercrime costs and the financial strain on SMEs in Uyo. *Small Business Economics,* 8(4), 56-71.

Walklate, S. (2015). *Criminology: The basics*. London: Routledge Press.

World Bank. (2023). *Digital economy and financial inclusion: Global trends and emerging challenges*. Zealand: World Bank Publications.

Yamane, T. (1967). *Statistics: An introductory analysis* (2nd ed.). New York: Harper and Row.

Zeng, X., Chen, Q. and Zhou, X. (2022). Impact of business email compromise on shareholder confidence: A study of the corporate fallout. *International Journal of Business and Economics*, 41(3), 255-272.

Zetter, K. (2014). JPMorgan Chase Data Breach Affected 76 Million Households. Wired. https://www.wired.com

Zhao, L. and Lee, C. (2021). The role of socio-economic activities in global economic development. *Journal of Global Economic Studies*, 32(2), 123-145.