



Cybercrime as a Threat to Life and Socio-Economic Development: Evidence from Awka South Local Government Area, Anambra State, Nigeria

Agbodike Mmesoma Chinecherem¹ & Okoronta Chibuike Christian²

¹Department of Criminology and Security Studies, Faculty of Social Sciences, Chukwuemeka Odumegwu Ojukwu University, Igbariam, Anambra State, Nigeria. <https://orcid.org/0009-0005-1182-1714>

²Faculty of law, Chukwuemeka Odumegwu Ojukwu University. <https://orcid.org/0009-0007-6287-7675>

Article history:

Received: 17/07/2026

Accepted: 29/08/2026

Published: 09/10/2026

Keywords: cybercrime, socio-economic development, digital fraud, routine activity theory, Awka South, Nigeria

*Corresponding Author:

Agbodike Mmesoma Chinecherem

Abstract

Digital technology expanded rapidly across Awka South Local Government Area, the administrative capital of Anambra State, Nigeria, and with it came a corresponding rise in cybercrime. This paper reported a descriptive survey study of 380 residents that examined the prevalence of cybercrime, the factors that sustained it, and its consequences for personal safety, household finances and local economic development. Data were gathered through a structured questionnaire administered across five communities using multi-stage sampling, and analysed using frequency distributions, mean scores and chi-square tests at the 0.05 level of significance. Online fraud, mobile banking fraud and phishing were found to be the most common offences, sustained chiefly by weak law enforcement, unemployment and low digital literacy. A majority of respondents reported financial loss, business disruption and psychological distress as a result of victimisation, and awareness of protective digital practices remained low despite widespread recognition of the risk. All four hypotheses tested were supported: cybercrime prevalence was significantly related to personal safety ($\chi^2 = 82.47, p < .001$), socio-economic development ($\chi^2 = 73.91, p < .001$) and financial stability ($\chi^2 = 99.34, p < .001$), and digital security awareness was significantly related to victimisation risk ($\chi^2 = 99.76, p < .001$). The paper argued that cybercrime in Awka South was best understood as a structural, not merely technical, problem, and set out recommendations for enforcement, public education and economic intervention accordingly.

Original Research Article

Copyright © 2026 The Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution-Noncommercial 4.0 International License (CC BY-NC 4.0)

How to cite this article: Agbodike Mmesoma Chinecherem & Okoronta Chibuike Christian. (2026). Cybercrime as a threat to life and socio-economic development: Evidence from Awka South Local Government Area, Anambra State, Nigeria. EIRA Journal of Arts, Law and Educational Sciences, 2(5). 38-48.

Introduction

Nigeria's digital economy has grown at a pace that has outstripped the institutional capacity built to protect it. Mobile banking, e-commerce and social media now sit at the centre of everyday economic life for millions of Nigerians, and Awka South, as the seat of Anambra State government and home to Nnamdi Azikiwe University, has absorbed this shift more quickly than most local government areas in the South-East. That shift has not come without cost. The same platforms that allow a trader in Awka to receive payment instantly or a civil servant to manage household finances from a phone also give offenders a route into people's accounts, identities and savings, and the two developments, convenience and exposure, have arrived together rather than one after the other.

The practical value of this kind of localised evidence should not be understated. Policymakers at state level, and the

agencies tasked with enforcing the 2015 Act specifically, generally work from national or, at best, state-level statistics that say little about how cybercrime is actually distributed across a state's constituent local government areas or which forms of it dominate in a given locality. Financial institutions operating branches in Awka South, and the businesses that depend on digital payment for their day-to-day trade, have a similarly practical stake in understanding how far fear of fraud is already shaping customer behaviour in the area. By anchoring its evidence in one clearly defined community rather than aggregating across the state or the country, this study aims to produce findings specific enough to inform decisions, about where enforcement resources are directed, which awareness messages are prioritised, and how digital banking services are marketed and supported, rather than

findings so general that any local actor could take from them whatever conclusion suited their existing plans.

Cybercrime is not a new subject for Nigerian criminology, but most of what has been written about it treats the country, or at best a state, as the unit of analysis. National statistics on fraud losses or reported cases are useful for tracking a general trend, but they say little about what cybercrime actually looks like from inside a specific community: which offences residents encounter most often, what they believe drives the problem, and how far its effects reach into their working lives and sense of safety. Awka South has not, prior to this study, been examined in this closer-grained way, despite the fact that its combination of a young, educated, digitally engaged population and a still-developing enforcement infrastructure makes it a useful case for understanding how cybercrime settles into an urbanising Nigerian community.

The Cybercrimes (Prohibition, Prevention, etc.) Act of 2015 gave Nigeria a legal framework for tackling digital offences that was, at the time, one of the more comprehensive in West Africa. A decade on, the gap between what the Act promises and what residents of a place like Awka South actually experience is worth examining directly. Ibrahim's (2016) early account of Nigerian cybercrime already noted that offenders operate with a fairly accurate sense of how unlikely they are to be caught, and the findings reported below suggest that assessment has aged rather well. Interpol's (2022) regional threat assessment placed Nigeria among the African countries most affected by online fraud and business email compromise, a ranking driven as much by the sophistication of financial technology adoption as by any particular weakness in the country's response.

Three theoretical traditions inform how this study approaches the problem. Routine Activity Theory, associated with Cohen and Felson (1979), explains victimisation as a product of motivated offenders meeting suitable targets in the absence of capable guardianship, a framework well suited to a setting where online banking has expanded faster than digital security habits. Social Learning Theory, drawing on Bandura (1977), points to the way cybercrime techniques and the wealth they generate circulate through peer networks, gradually normalising behaviour that would once have been unthinkable. Strain Theory, from Merton (1938) and extended by Agnew (1992), locates the pressure to offend in the gap between culturally endorsed material aspirations and the legitimate means of achieving them, a gap that youth unemployment in South-Eastern Nigeria has widened rather than closed. Read together, these three perspectives suggest that cybercrime in a community like Awka South is unlikely to respond to enforcement measures alone; it is a problem with situational, social and structural roots that a single intervention cannot reach.

A note on terms is useful before proceeding. "Cybercrime" is used throughout this paper in the sense established by the 2015 Act itself and consistent with Holt, Bossler and Seigfried-Spellar's (2018) working definition, criminal

conduct carried out through computer systems, mobile devices or the internet, encompassing offences ranging from financial fraud and identity theft to harassment and unauthorised access. "Socio-economic development" refers here to the material and institutional conditions, income stability, business activity, trust in financial systems, that allow a community's economic life to function and expand; the study treats cybercrime's relationship to development as an empirical question to be tested rather than an assumption, examining specifically whether victimisation correlates with disruption across these dimensions rather than presuming that it must.

Against this background, the study set out to answer four questions: what forms of cybercrime are most prevalent among Awka South residents and what sustains them; how cybercrime threatens personal safety and psychological wellbeing; what effect it has on household financial stability, business activity and broader socio-economic development; and how residents' awareness of digital security practices relates to their risk of victimisation. Answering these questions with facility-level, community-specific evidence is the contribution this paper aims to make.

Literature Review and Theoretical Framework

Forms and Drivers of Cybercrime in Nigeria

Financially motivated offences dominate the pattern of cybercrime reported in Nigeria, and the literature on this point is now fairly settled. Ibrahim (2016) traced the social and economic conditions that gave rise to what is popularly known as "Yahoo Yahoo", arguing that Nigerian cybercrime cannot be understood in isolation from the economic frustration and peer culture that surrounds it. Akinbowale, Klingelhöfer and Zerihun (2020) reached a related conclusion from a forensic accounting perspective, showing that digital fraud in Nigeria increasingly exploits gaps in financial institutions' monitoring systems rather than relying purely on technical sophistication, and that the resulting loss of consumer trust in digital banking carries its own economic cost separate from the fraud itself. More recent Nigerian scholarship has kept pace with the changing shape of the problem. Adewale (2022) traced how social media platforms specifically have become a channel through which cybercrime techniques and justifications circulate among young Nigerians, a finding that complements Ayodele, Oyediji and Badmos's (2022) description of how internet fraud has come to be socially framed among some young Nigerians as a form of entrepreneurial innovation rather than crime, a normalisation process consistent with what Social Learning Theory would predict. Adegbite, Ogunmodede and Olawale (2022) linked unemployment directly to youth involvement in cybercrime using survey evidence from a separate Nigerian state, a finding this study's own data bear out closely.

The digital financial services boom that underlies much of this activity has also drawn scholarly attention in its own

right. Garba, Bala and Muhammad (2023) found that the rapid growth of mobile and internet banking across Nigeria had outpaced public awareness of the risks that come with it, leaving a large proportion of new digital banking users without the basic protective habits, such as recognising phishing attempts or securing login credentials, that might otherwise reduce their exposure. Balogun and Sanni (2024) reported a comparable pattern specifically among younger Nigerian banking customers, concluding that digital literacy interventions had so far reached only a fraction of those who needed them.

Industry-level data help place these community-level patterns in context. The Nigeria Inter-Bank Settlement System's (2024) annual fraud report recorded a sharp year-on-year rise in mobile banking and phishing-related fraud cases across the country, a trend that tracks closely with the growth in mobile payment adoption rather than any single technical vulnerability. The Economic and Financial Crimes Commission's (2023) annual report similarly noted a rising caseload of cyber-enabled financial crime, though prosecution numbers remained modest relative to the scale of reported losses, a gap between offence volume and enforcement capacity that several respondents in this study appeared to sense even without access to the national figures themselves.

Consequences: Financial, Psychological and Developmental

A separate strand of research has examined what cybercrime does to victims and communities once it occurs. Buil-Gil, Miró-Llinares, Moneva, Kemp and Díaz-Castaño (2021), studying opportunity shifts in cybercrime across fourteen countries during the Covid-19 period, found that the psychological consequences of online victimisation, principally anxiety and a diminished sense of personal security, were often reported by victims as more troubling than the financial loss itself. Payne (2020) made a related point in a wider review of cybercrime scholarship, noting that victims frequently withdraw from online activity altogether after an incident, a response that, multiplied across a population, has clear implications for a local economy trying to expand its digital footprint. Stevens, Nurse and Arief (2021), reviewing evidence on cyberstalking and online harassment specifically, documented sustained psychological harm among victims that in some cases persisted well beyond the immediate incident, a pattern echoed in this study's findings on reputational damage and disrupted social activity.

Work focused more directly on reporting behaviour and institutional trust offers a further piece of the picture. Ndubueze (2019), writing on cybercrime and national security in Nigeria, identified stigma and a widespread expectation that little would come of a report as the principal reasons Nigerian victims tend not to approach the police, an expectation this study's respondents shared almost without exception. Guedes, Martins and Cardoso (2023) found, in a study of identity theft victimisation, that perceived risk and

everyday online habits were stronger predictors of both victimisation and the fear of it than any single demographic factor, a finding consistent with the situational logic of Routine Activity Theory discussed below.

Cybercrime's effect on small business activity has received somewhat less attention than its effect on individual victims, despite being of obvious relevance to a commercially active area like Awka South. Okosun and Ilo (2023), tracing the evolution of Nigerian advance-fee fraud into its more contemporary digital forms, observed that the reputational damage cybercrime does to Nigeria's international commercial standing has a domestic mirror: local traders and small business owners increasingly report that customers and suppliers alike approach digital transactions with a caution that slows down otherwise legitimate commerce. Adewale, Bello and Chukwu (2024), studying the effect of cybercrime on local businesses in a neighbouring South-Western state, found that fear of fraud had measurably reduced small business owners' willingness to adopt digital payment tools, a finding this study's evidence on reduced online transaction activity closely parallels.

Theoretical Framework

Three theories, taken together, structure the analysis in this paper. Routine Activity Theory, developed by Cohen and Felson (1979), holds that crime becomes more likely wherever a motivated offender and a suitable target meet in the absence of a capable guardian, whether that guardian is a person, a technology or an institutional safeguard. Leukfeldt and Yar (2016) extended the theory specifically to cybercrime, showing that everyday online routines, internet banking, social media use, online shopping, systematically increase exposure to victimisation once a person's guardianship, meaning their security habits and awareness, fails to keep pace with those routines. Ahmad and Thurasamy's (2022) systematic review of the theory's application to cybercrime broadly confirms this, while also noting that the strength of the relationship varies with the specific offence type, which is one reason this study examines several forms of cybercrime rather than treating the category as a single undifferentiated threat.

Social Learning Theory, associated with Bandura (1977), explains how criminal behaviour, like any other, is acquired through observation, imitation and reinforcement within a person's social environment. Applied to Nigerian cybercrime, the theory helps account for why the practice has spread through particular peer networks and age cohorts rather than appearing at random across the population: where digital fraud is visibly rewarded and only lightly stigmatised within a social circle, the behaviour it produces is, in a straightforward sense, learned.

Strain Theory, originating with Merton (1938) and substantially developed by Agnew (1992), offers the structural half of the explanation. Merton argued that crime tends to emerge where a society instils a shared ambition for

material success while denying a significant portion of its members the legitimate means to achieve it. Agnew's general strain theory broadened this by identifying several sources of strain beyond blocked opportunity alone, including the loss of valued things and exposure to negative circumstances, any of which can generate the frustration that precedes criminal adaptation. Set against the youth unemployment rates the National Bureau of Statistics (2023) has continued to record across South-Eastern Nigeria, and the constrained formal-sector opportunity that accompanies them, the theory offers a plausible account of why cybercrime persists despite the legal and social risks attached to it.

Legislative Framework and Implementation Gaps

The Cybercrimes (Prohibition, Prevention, etc.) Act of 2015 remains the principal legal instrument governing digital offences in Nigeria, criminalising a broad range of conduct from unauthorised access and identity theft to cyberstalking and electronic fraud, and establishing institutional responsibilities across several federal agencies. In principle, the framework is reasonably comprehensive. In practice, a recurring theme across the Nigerian literature is the distance between what the Act permits and what agencies on the ground are equipped to deliver. The National Information Technology Development Agency (2023) has continued to expand digital literacy and cyber security guidance at national level, and Ajayi (2023) has separately documented persistent capacity constraints within Nigerian law enforcement's cybercrime units specifically, yet uptake of national guidance at community level, in schools, in small business associations, in local government awareness programmes, remains uneven, and Awka South's own findings on moderate awareness and low reporting suggest that whatever national guidance exists has not yet reached most residents in a form that changes behaviour. Adesina and Adejumo (2025) have recently argued that closing this gap requires policy attention to implementation and funding rather than further legislative amendment, since the substantive legal tools already exist. This gap between legislative ambition and local implementation forms an important part of the backdrop against which this study's findings on weak enforcement, identified by respondents as the single strongest driver of cybercrime, should be read.

Comparative evidence from outside Nigeria offers a useful check on how far these patterns generalise. Ngo, Piquero, LaPrade and Duong (2020), studying online victimisation more broadly, found that the specific online activities a person engages in, rather than simply the amount of time spent online, were the stronger predictor of victimisation risk, a distinction with practical relevance for awareness campaigns: encouraging residents to spend less time online is a poor substitute for teaching them which specific activities, unverified links, unfamiliar payment requests, carry the greatest risk. Guedes, Martins and Cardoso's (2023) findings on identity theft, mentioned above, point in a similar direction. Taken together with the Nigerian evidence

reviewed in this section, the cross-national literature suggests that the situational logic of Routine Activity Theory travels reasonably well across contexts, even where the specific offences and enforcement environments differ considerably.

A Note on Gendered Vulnerability

One dimension of the cybercrime literature that Nigerian scholarship has only recently begun to address concerns the gendered distribution of certain offence types. Okpako (2023), examining the legal treatment of cybercrimes that specifically target women, argued that forms such as image-based abuse, sextortion and online harassment carry consequences, reputational, social and psychological, that differ in kind from the largely financial offences that dominate the general cybercrime literature, and that Nigerian legislation has been slower to address these forms than it has been to address financial fraud. This study's questionnaire did not disaggregate offence type by gender in sufficient depth to test this distinction directly, and that gap is noted as a limitation below rather than something the present data can resolve, but the broader point, that cybercrime is unlikely to affect all residents in the same way, is one the design of future community-level research in Awka South and comparable areas should take seriously.

The Gap This Study Addresses

Odunayo's (2024) recent review of the Nigerian cybercrime literature reaches a similar conclusion, noting that most existing work remains either narrowly technical or too broad in geographic scope to inform local policy directly. What the existing literature has not done, and what this study sets out to do, is bring these three explanatory strands together within a single Nigerian community and test them against survey evidence gathered specifically for that purpose. National and cross-national studies establish that cybercrime is widespread and costly; Nigerian studies establish that unemployment, peer influence and weak enforcement all play a part. What has been missing is a community-level account that measures the prevalence of specific offences, tests the statistical relationship between victimisation and its various consequences, and does so in a locality, Awka South, whose rapid urbanisation and digital growth make it a useful indicator of where similar Nigerian communities may be heading.

Methodology

The study adopted a descriptive survey design, chosen because the research questions called for systematic description of residents' experiences, perceptions and reported outcomes rather than experimental manipulation of variables (Bryman, 2016; Creswell and Creswell, 2018). Fieldwork was carried out in Awka South Local Government Area, Anambra State, an area comprising several communities, including Awka, Amawbia, Okpuno, Nibo and Nise, and selected for its high level of internet penetration and its concentration of economically active, digitally engaged residents.

The target population comprised adult residents aged eighteen and above who were economically active within the area, estimated at approximately 120,000 people once students, traders, civil servants and business owners were taken into account. This population estimate, though necessarily approximate given the absence of a recent, community-specific census for Awka South, was derived from local government administrative figures and cross-checked against university and state civil service enrolment data, and is consistent with the population bases used in comparable Nigerian community-level surveys. Sample size was calculated using Yamane's (1967) formula at a 5 per cent margin of error, giving a required minimum of approximately 399; the target was set at 420 to allow for non-response. Of the 420 questionnaires distributed, 392 were returned and 380 were found complete and usable, a response rate of 90.5 per cent. A three-stage sampling procedure was used: the local government area was first divided into its constituent communities, with proportional representation across Awka, Amawbia, Okpuno, Nibo and Nise; respondents within each community were then stratified by occupation, covering students, civil servants, traders and small business owners; and simple random sampling, using a table of random numbers, was applied within each stratum to select individual respondents.

The primary instrument was a structured questionnaire comprising a biographical section and a series of closed-ended items addressing the study's four research questions, including five-point Likert-scale statements covering the prevalence and drivers of cybercrime, its effects on personal safety and psychological wellbeing, its socio-economic and financial consequences, and residents' awareness and preventive practices. The instrument was reviewed by departmental colleagues for content validity and revised accordingly before administration. Reliability was not formally piloted with a separate sample, and this is acknowledged as a limitation below; internal consistency across the Likert-scale sections was, however, monitored during data cleaning, and items that produced markedly inconsistent response patterns were flagged and reviewed.

Data collection took place through direct, in-person administration by the researcher across the selected communities, with respondents given a brief verbal

explanation of the study's purpose and an assurance of anonymity before completing the questionnaire. Completed instruments were checked for completeness at the point of collection, which contributed to the high proportion of usable returns. Participation was voluntary throughout, respondents were free to decline or to stop at any point without consequence, and no identifying information was collected on the questionnaire itself, in keeping with standard ethical practice for social survey research of this kind (Bryman, 2016).

Quantitative data were processed and analysed using descriptive statistics, frequency distributions, percentages and mean scores, with a decision rule of a mean score of 3.00 or above on the five-point scale taken to indicate general agreement with a given statement. Chi-square tests of independence were used to test all four hypotheses, comparing victimisation status or awareness level against the relevant outcome variable, with statistical significance set at $p < .05$ throughout.

Results

Respondent Profile

Table 1 summarises the characteristics of the 380 respondents. Men made up 57.4 per cent of the sample and women 42.6 per cent, a near-even split that helped ensure the study captured cybercrime experiences across both groups rather than skewing toward one. Respondents aged 35 and below accounted for 66.8 per cent of the sample, reflecting the youthful profile of Awka South's population and, not incidentally, the demographic most exposed to digital platforms in daily life. Students formed the largest single occupational group (27.9 per cent), followed by civil servants (25.0 per cent) and traders (21.8 per cent), and 67.1 per cent of respondents held a tertiary qualification, consistent with the area's status as home to a major university and a concentration of government institutions. This educational profile matters for how the findings below should be read: a population this well-schooled cannot easily be assumed to lack general awareness of online risk, which makes the gap this study finds between awareness and protective behaviour, discussed in section 4.5, more a matter of practice than of ignorance.

Table 1: Respondent Characteristics (N = 380)

Variable	Category	n	%
Sex	Male	218	57.4
	Female	162	42.6
Age group	18–25 years	133	35.0
	26–35 years	121	31.8
	36–45 years	79	20.8
	46 years and above	47	12.4

Variable	Category	n	%
Occupation	Student	106	27.9
	Civil servant	95	25.0
	Trader	83	21.8
	Small business owner	57	15.0
	Professional (private sector)	39	10.3
Education	Secondary school (WAEC/NECO/SSCE)	57	15.0
	OND/NCE	68	17.9
	HND/B.Sc.	160	42.1
	Master's/PhD	95	25.0

Source: Field survey, 2026.

Prevalence and Drivers of Cybercrime

Online fraud was the most commonly reported offence, experienced by 74.5 per cent of respondents, followed by mobile banking fraud (68.2 per cent) and phishing (61.3 per cent). Social media impersonation (55.8 per cent), identity theft (48.7 per cent), cyber harassment (39.5 per cent) and digital extortion (28.4 per cent) were also reported at levels too high to dismiss as marginal. The dominance of financially motivated offences fits comfortably within the pattern Ibrahim (2016) and Akinbowale and colleagues (2020) describe nationally, and the particular weight of mobile banking fraud tracks the rapid uptake of mobile payment platforms that the Nigeria Inter-Bank Settlement System (2024) has documented across Nigeria more broadly.

Asked what sustains cybercrime locally, respondents pointed overwhelmingly to institutional and economic failure rather than to any deficiency on the part of victims. Weak law enforcement and a low perceived risk of punishment drew the strongest agreement of any statement in this section (mean = 4.20), ahead of unemployment and economic pressure (mean = 4.09) and low digital literacy (mean = 4.02). Peer influence and the social normalisation of cybercrime (mean = 3.95), easy access to digital technology (mean = 3.80) and the visible display of fraud-derived wealth (mean = 3.71) were also rated as significant, consistent with the social learning mechanism Ayodele and colleagues (2022) describe among Nigerian youth. Respondents were, in effect, offering a structural rather than an individual explanation for cybercrime: none of the six factors tested placed responsibility on victims' own conduct, and the two highest-rated items, weak enforcement and economic pressure, point squarely at institutions and the wider economy rather than at the technology itself.

Financial and Business Impact

Direct financial loss was reported by 67.4 per cent of respondents. Among those who lost money, 35.2 per cent lost between ₦10,001 and ₦50,000 and 14.8 per cent lost more than ₦200,000, sums that, for a trader or small business

owner in a commercial area like Awka South, can represent a meaningful share of working capital rather than a trivial inconvenience. Business-related consequences followed a similar pattern: respondents agreed that cybercrime had disrupted their business operations (mean = 3.75), reduced customer numbers or sales (mean = 3.42) and affected household income (mean = 3.62). The finding that 72.1 per cent of respondents agreed or strongly agreed that fear of fraud had made them cut back on online transactions (mean = 3.83) is, on its own, one of the more consequential figures in the study, since it points to cybercrime suppressing exactly the kind of digital economic activity that Awka South's growth depends on.

4.4 Personal Safety, Psychological Wellbeing and Development

Respondents linked cybercrime to psychological harm almost as consistently as to financial loss. Stress and anxiety following victimisation (mean = 3.79) and a reduced sense of safety in subsequent online activity (mean = 3.79) were the most strongly endorsed items, with reputational damage (mean = 3.17) and disruption to daily social life (mean = 3.43) also drawing agreement. These findings sit closely alongside Buil-Gil and colleagues' (2021) cross-national evidence that psychological harm is often the more persistent legacy of cyber victimisation, and Stevens, Nurse and Arief's (2021) findings on the lasting effects of online harassment specifically.

At the community level, respondents agreed that cybercrime undermines trust in digital financial systems (mean = 3.97), discourages investment in digital business (mean = 3.88), threatens the livelihoods of small enterprises (mean = 3.88) and slows local economic growth more generally (mean = 3.74). Read alongside the finding on reduced online transaction activity above, this suggests cybercrime operates in Awka South not only as a source of individual loss but as a drag on the area's broader digital economic development.

Awareness and Preventive Practices

Awareness of common fraud tactics was moderate (mean = 3.46), as was the use of basic protective habits such as strong passwords (mean = 3.27). Respondents were considerably less confident about what to do if victimised (mean = 3.03), and disagreed both that they had reported an incident to the authorities (mean = 2.44) and that law enforcement handles cybercrime cases effectively (mean = 2.35). This pattern of awareness without reporting matches Ndubueze's (2019) account of the stigma and scepticism that keep Nigerian victims away from formal channels. The gap between the two lowest-rated items and everything above them is fairly sharp: residents are willing to say they know something about fraud tactics and generally use a password, but confidence collapses once the question turns to what happens after victimisation, whether that means knowing the right steps to take or trusting that a report will lead anywhere. That collapse, more than the moderate awareness scores on their own, is probably the more informative finding for anyone designing a response.

Hypothesis Testing

Table 2 summarises the four chi-square tests. For each hypothesis, victimisation status or awareness level was cross-tabulated against the relevant outcome. Cybercrime prevalence was significantly related to personal safety ($\chi^2 = 82.47$, $df = 1$, $p < .001$): 72.7 per cent of those who had experienced cybercrime reported that their personal safety felt threatened, against 25.8 per cent of those who had not. It was significantly related to socio-economic development ($\chi^2 = 73.91$, $df = 1$, $p < .001$), with 86.3 per cent of victims reporting negative socio-economic consequences against 46.8 per cent of non-victims, and to financial stability ($\chi^2 = 99.34$, $df = 1$, $p < .001$), with 79.3 per cent of victims reporting disrupted financial stability against 25.0 per cent of non-victims. Finally, awareness of digital security practices was significantly related to victimisation risk ($\chi^2 = 99.76$, $df = 1$, $p < .001$): residents with low awareness were victimised at a rate of 89.4 per cent, compared with 43.1 per cent among those with high awareness, a gap that offers about as direct a piece of evidence for the protective value of digital literacy as a single cross-tabulation can provide. All four null hypotheses were therefore rejected.

Table 2: Summary of Chi-Square Hypothesis Tests (N = 380)

Hypothesis	Relationship tested	χ^2	df	p	Decision
H1	Cybercrime prevalence and personal safety	82.47	1	< .001	Null rejected
H2	Cybercrime prevalence and socio-economic development	73.91	1	< .001	Null rejected
H3	Cybercrime prevalence and financial stability	99.34	1	< .001	Null rejected
H4	Digital security awareness and victimisation risk	99.76	1	< .001	Null rejected

Source: Field survey, 2026. Significance level = 0.05.

A consistent pattern runs through all four tests: in every case, the gap between victimised and non-victimised respondents, or between high- and low-awareness respondents, was large enough that a chance explanation can be ruled out with a fair degree of confidence. The smallest of the four chi-square values, for the relationship between cybercrime and socio-economic development, was still large enough to produce a p-value below .001, and the largest, for the relationship between digital security awareness and victimisation, points to one of the clearer protective effects reported anywhere in this dataset. Read together, these results support the study's underlying premise that cybercrime in Awka South is not a series of unconnected individual misfortunes but a phenomenon whose consequences are statistically predictable once victimisation status or awareness level is known.

Discussion

The picture that emerges from this study is one in which cybercrime has become an ordinary feature of economic life in Awka South rather than an occasional shock. Nearly

three-quarters of respondents had experienced online fraud, and the four hypotheses tested all confirmed statistically significant relationships between victimisation and its various consequences at levels well beyond conventional thresholds. Taken together, these findings support a reading of cybercrime not as an isolated criminal justice problem but as a structural feature of how a rapidly digitising community is currently organised, one that touches personal safety, household income and the pace of local economic development at once.

The dominance of financially motivated offences, online fraud, mobile banking fraud and phishing, fits the pattern documented by Ibrahim (2016) and by Akinbowale and colleagues (2020), and it also makes practical sense given how quickly mobile payment platforms have spread through Awka South's trading and student population. What this study adds to that picture is a clearer sense of what residents believe sustains the problem: not, in the main, technological sophistication on the part of offenders, but weak enforcement and economic pressure on the part

of the system around them. When a community rates the low risk of punishment as the single strongest driver of cybercrime, ahead even of unemployment, that is a fairly direct statement about where residents think the solution has to start.

The financial and business findings deserve particular attention given Awka South's commercial character. A loss of ₦50,000 to ₦200,000 might be recoverable for a salaried civil servant; for a trader whose working capital sits in that same range, it can mean the difference between staying open and closing down. The finding that 72.1 per cent of respondents had reduced their online transactions out of fear of fraud is, in some ways, the most consequential figure in the study, because it describes cybercrime actively working against the digital economic growth that Awka South's development depends on. This is consistent with Garba, Bala and Muhammad's (2023) observation that Nigeria's digital banking expansion has, in places, outpaced the public confidence needed to sustain it, and with Akinbowale and colleagues' (2020) argument that fraud erodes institutional trust in ways that persist well after any individual incident is resolved.

The psychological findings extend this argument in a direction that Nigerian cybercrime research has, until fairly recently, given less attention than it deserves. Stress, anxiety and a reduced sense of online safety were reported almost as consistently as financial loss, aligning with Buil-Gil and colleagues' (2021) cross-national evidence, Stevens, Nurse and Arief's (2021) findings on the durability of harm from online harassment, and Kim's (2023) synthesis of research linking online victimisation to sustained anxiety and diminished wellbeing. If victims are, in effect, withdrawing from digital platforms partly out of financial caution and partly out of a diminished sense of safety, then interventions aimed only at reducing financial loss, better fraud detection, faster reimbursement, are unlikely on their own to restore the confidence needed for genuine digital economic participation.

The awareness findings raise a question that this study can identify but not fully resolve: why does a well-educated population, two-thirds of whom hold a tertiary qualification, report only moderate familiarity with basic protective practices and very low confidence in what to do after victimisation? One plausible explanation is that general education and specific digital security literacy are simply different skills, and that Awka South's schools and university have not, so far, treated the second as part of their responsibility. Another, not mutually exclusive, explanation is that low reporting reflects a rational response to weak enforcement rather than ignorance of the option to report at all: if 89 per cent of residents doubt that law enforcement handles cybercrime effectively, choosing

not to report is arguably a reasonable inference from available evidence rather than a gap in awareness. The sharp statistical relationship between low awareness and victimisation risk, residents with low awareness were victimised at more than double the rate of those with high awareness, suggests that whichever explanation carries more weight, the practical response is the same: awareness-focused intervention has a clear, testable payoff.

Placed alongside regional evidence, the Awka South findings look less like a local anomaly than a fairly typical instance of a wider West African pattern. Interpol's (2022) African cyberthreat assessment identified Nigeria as one of the region's most heavily affected countries for both online fraud and business email compromise, driven in large part by the same combination this study documents locally: rapid financial technology adoption running ahead of public protective habits and formal enforcement capacity. What this study adds to that regional picture is not a different diagnosis but a more precise one, showing what that national-level pattern actually looks like once it is traced down to a single, fast-growing local government area, and confirming that the statistical relationships regional analyses imply do, in fact, hold up when tested directly against residents' own reported experience.

Reading the findings through the three theories set out earlier, each receives fairly direct support. Routine Activity Theory's logic, that victimisation follows from the combination of exposure and weak guardianship, is visible in the strong statistical link between low digital security awareness and victimisation risk. Social Learning Theory's account of behaviour spreading through peer networks is reflected in respondents' identification of peer influence and the social display of cybercrime wealth as meaningful drivers, echoing Ayodele and colleagues' (2022) account of fraud being reframed as entrepreneurial success among some young Nigerians. Strain Theory's structural argument is supported most directly by the high rating given to unemployment and economic pressure, consistent with Adegbite, Ogunmodede and Olawale's (2022) Nigerian evidence linking joblessness to cybercrime involvement. None of the three theories, on this evidence, is sufficient on its own; the pattern of findings instead supports treating them as complementary explanations of a single, multi-layered problem.

These theoretical conclusions carry a practical implication that is easy to state but not always easy to act on: because the drivers of cybercrime in Awka South are situational, social and economic at once, a response built around any single lever, more arrests, more awareness campaigns, more job schemes, is likely to under-deliver relative to what a coordinated response across all three could achieve.

Enforcement without economic opportunity leaves the underlying pressure to offend largely intact; awareness campaigns without improved reporting mechanisms ask residents to trust a system many of them already doubt; and economic intervention alone does nothing to address the specific digital vulnerabilities that Routine Activity Theory identifies. The recommendations that follow are framed with this interdependence in mind, rather than as a menu from which a single option might be selected.

A further point worth drawing out concerns the relationship between the business findings and the psychological ones. Respondents who had cut back on online transactions after being defrauded were not, on the whole, describing a purely rational risk calculation; the same group also reported elevated stress and a reduced sense of safety, suggesting that withdrawal from digital commerce is as much an emotional response to victimisation as a considered one. This matters for how recommendations aimed at restoring digital economic confidence should be framed. A campaign that addresses only the practical mechanics of fraud prevention, stronger passwords, two-factor authentication, is likely to miss a significant part of what is keeping victims away from digital platforms if it does not also address the anxiety and diminished trust that victimisation leaves behind. Financial institutions and public awareness campaigns alike would do well to treat reassurance and psychological support as part of fraud response, not as an optional addition to it.

6. Conclusion and Recommendations

This study set out to establish how cybercrime is experienced, sustained and felt within one rapidly digitising Nigerian community, and the evidence gathered points to a consistent conclusion: cybercrime in Awka South is pervasive, structurally rooted, and already exacting a measurable cost on personal safety, household finances and local economic development. All four hypotheses tested were supported, and the three theoretical perspectives drawn on, Routine Activity Theory, Social Learning Theory and Strain Theory, each found support in the pattern of results, suggesting that no single explanation, and by extension no single category of response, is likely to be sufficient on its own.

Four recommendations follow from the findings. First, law enforcement agencies, working with the Economic and Financial Crimes Commission, should treat improved local enforcement capacity as a priority rather than a background concern, since weak enforcement was the single most strongly endorsed driver of cybercrime identified in this study; this means dedicated, adequately trained cybercrime response capacity at state command level, and visible follow-through on reported cases, since

residents' scepticism about enforcement appears to be shaping their willingness to report in the first place. Second, government agencies, educational institutions and civil society organisations should expand digital literacy and cyber security awareness programmes specifically targeted at practical protective behaviour, recognising secure banking habits, knowing what to do after victimisation, rather than general digital literacy alone, given that this study found awareness of basic risks to be only moderate even among a well-educated population. Third, state and local authorities should treat youth unemployment and economic exclusion as part of the cybercrime problem rather than a separate policy area, since economic pressure was rated as the second-strongest driver of cybercrime in this study; vocational training, entrepreneurship support and job creation targeted at young people are, on this evidence, a legitimate component of crime prevention rather than a tangential social programme. Fourth, financial institutions and mobile money operators should strengthen fraud detection and, just as importantly, simplify the process by which victims report and recover from fraud, since the finding that most victims do not report incidents to authorities at all suggests that formal channels are currently seen as more trouble than they are worth. None of these four measures is likely to succeed as a standalone initiative; the interdependence noted in the discussion above applies just as much to implementation as it does to theory, and a coordinating body bringing law enforcement, educational institutions, financial regulators and local government together would give the four recommendations a far better chance of reinforcing rather than duplicating one another.

Some limitations should be acknowledged. The cross-sectional design captures a single point in time and cannot, on its own, establish that cybercrime prevalence causes the outcomes with which it is statistically associated, even though the theoretical framework and the consistency of the findings make that interpretation the more plausible one. The absence of a separate reliability pilot, noted in the methodology section, means that internal consistency statistics for the Likert-scale sections cannot be reported with the same confidence a formally piloted instrument would allow, although the consistency of response patterns during data cleaning offers some reassurance on this point. The study also relies entirely on self-reported data, which is standard practice in victimisation research but always carries some risk of recall or social desirability bias, particularly on sensitive questions such as whether a respondent reported an incident to the police.

These limitations suggest useful directions for further work. A longitudinal design tracking cybercrime prevalence and awareness in Awka South over several years would allow a clearer test of whether the awareness

campaigns and enforcement measures recommended here actually shift outcomes once implemented. Comparative research across several Anambra State local government areas, or between Awka South and a less urbanised comparison site, would help establish how much of what this study found is specific to a rapidly digitising commercial and administrative centre, as opposed to reflecting a wider Nigerian pattern. Research that includes the perspectives of offenders themselves, an angle this victim-focused study could not accommodate, would also usefully complement the account given here. What the present study can say with reasonable confidence is that, for the residents of Awka South, cybercrime is no longer a marginal risk attached to digital participation; it is, for a majority of them, part of what digital participation in the area now means, and addressing it will require treating enforcement, education and economic opportunity as parts of a single response rather than separate agendas.

References

1. Adebite, E., Ogunmodede, A., & Olawale, A. (2022). Unemployment and youth engagement in cybercrime: A Nigerian perspective. *Nigerian Journal of Criminology*, 14(3), 231–245.
2. Adesina, O., & Adejumo, L. (2025). Enhancing cybersecurity policies in Nigeria: Challenges and policy recommendations. *Nigerian Journal of Digital Security*, 8(3), 98–115.
3. Adewale, K., Bello, T., & Chukwu, F. (2024). Cybercrime and its impact on local businesses in Osun State. *Nigerian Journal of Social Sciences*, 18(2), 45–60.
4. Adewale, S. (2022). Social media influence and cybercrime involvement among Nigerian youths: A cultural perspective. *International Journal of Cyber Studies*, 6(3), 101–119.
5. Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. *Criminology*, 30(1), 47–87. <https://doi.org/10.1111/j.1745-9125.1992.tb01093.x>
6. Ahmad, R., & Thurasamy, R. (2022). A systematic literature review of routine activity theory's applicability in cybercrimes. *Journal of Cyber Security and Mobility*, 11(3), 405–432.
7. Ajayi, K. (2023). Law enforcement and cybercrime: Challenges and prospects in Nigeria. *Journal of Criminal Justice and Security Studies*, 10(4), 59–77.
8. Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020). An innovative approach in combating economic crime using forensic accounting techniques. *Journal of Financial Crime*, 27(4), 1253–1271. <https://doi.org/10.1108/JFC-04-2020-0065>
9. Ayodele, A., Oyedele, J. K., & Badmos, H. O. (2022). Social construction of internet fraud as innovation among youths in Nigeria. *International Journal of Cybersecurity Intelligence & Cybercrime*, 5(1), 23–42. <https://doi.org/10.52306/BUVC2778>
10. Balogun, S., & Sanni, M. (2024). Cyber fraud and digital literacy: A Nigerian perspective. *Journal of Cybersecurity Studies*, 18(2), 45–67.
11. Bandura, A. (1977). *Social learning theory*. Prentice-Hall.
12. Bryman, A. (2016). *Social research methods* (5th ed.). Oxford University Press.
13. Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during COVID-19: A criminological analysis of findings from 14 countries. *European Societies*, 23(S1), S170–S195. <https://doi.org/10.1080/14616696.2020.1804973>
14. Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588–608. <https://doi.org/10.2307/2094589>
15. Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.
16. Cybercrimes (Prohibition, Prevention, etc.) Act, No. 9. (2015). Federal Republic of Nigeria Official Gazette.
17. Economic and Financial Crimes Commission. (2023). *Annual report 2023: Cybercrime prosecutions and financial crimes enforcement*. EFCC.
18. Garba, A. A., Bala, S., & Muhammad, U. (2023). Digital banking growth and public awareness of cybercrime risks in Nigeria. *Journal of Financial Technology and Security*, 6(1), 33–48.
19. Guedes, I., Martins, M., & Cardoso, C. S. (2023). Exploring the determinants of victimization and fear of online identity theft: An empirical study. *Security Journal*, 36(3), 472–497. <https://doi.org/10.1057/s41284-022-00350-5>
20. Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). Cybercrime and digital forensics: An

introduction (2nd ed.). Routledge.

21. Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, 47, 94–107. <https://doi.org/10.1016/j.ijlcj.2016.07.002>
22. Interpol. (2022). African cyberthreat assessment report 2022. INTERPOL General Secretariat. <https://www.interpol.int/>
23. Kim, B. (2023). Cyberstalking research: A synthesis of factors associated with perpetration and victimization. *Journal of Interpersonal Violence*, 38(15–16), 9021–9045. <https://doi.org/10.1177/08862605231166396>
24. Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, 37(3), 263–280. <https://doi.org/10.1080/01639625.2015.1012409>
25. Merton, R. K. (1938). Social structure and anomie. *American Sociological Review*, 3(5), 672–682. <https://doi.org/10.2307/2084686>
26. National Information Technology Development Agency. (2023). National digital literacy and cybersecurity report. NITDA. <https://www.nitda.gov.ng/>
27. National Bureau of Statistics. (2023). Unemployment and underemployment report, Nigeria. NBS. <https://nigerianstat.gov.ng/>
28. Ndubueze, P. N. (2019). Cybercrime and national security challenges in Nigeria. Ahmadu Bello University Press.
29. Ngo, F. T., Piquero, A. R., LaPrade, J., & Duong, B. (2020). Victimization in cyberspace: Is it how long we spend online, what we do online, or what we post online? *Criminal Justice Review*, 45(4), 430–451. <https://doi.org/10.1177/0734016820934175>
30. Nigeria Inter-Bank Settlement System. (2024). Industry fraud and electronic payment report 2024. NIBSS. <https://nibss-plc.com.ng/>
31. Odunayo, A. (2024). A literature review on emerging cybercrime in Nigeria. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4814920>
32. Okosun, I. K., & Ilo, C. (2023). Tracing the evolution of the Nigerian prince scam: From advance fee fraud to digital romance fraud. *African Journal of Criminology and Justice Studies*, 9(1), 1–19.
33. Okpako, E. (2023). Cybercrimes and the victimization of women: Laws, rights and regulation. *Covenant Journal of Politics and International Affairs*, 7(3), 1–18.
34. Payne, B. K. (2020). Defining cybercrime. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 3–25). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-78440-3_1
35. Stevens, F., Nurse, J. R. C., & Arief, B. (2021). Cyber stalking, cyber harassment, and adult mental health: A systematic review. *Cyberpsychology, Behavior, and Social Networking*, 24(6), 367–376. <https://doi.org/10.1089/cyber.2020.0253>
36. Yamane, T. (1967). *Statistics: An introductory analysis* (2nd ed.). Harper and Row.