I J I T I E

INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY INTEGRATION IN EDUCATION

Volume 9, Issue 2, 2026

CYBER ETHICS EDUCATION AS A PROPOSED STRATEGY FOR REDUCING INTERNET FRAUD AMONG UNDERGRADUATES IN UNIVERSITIES IN RIVERS STATE: A CONCEPTUAL FRAMEWORK

Nwankwoala Henry Chinedu Ogbonna, Amadi, Uchechukwu (Ph.D) & Uchechukwu-Amadi, Mabel U. (Ph.D)

Department of Educational Technology, Ignatius Ajuru University of Education, Port Harcourt, Rivers State, Nigeria.

To cite this article:

Ogbonna, N. H. C., Amadi, U. & Uchechukwu-Amadi, M. U. (2026). Cyber ethics education as a proposed strategy for reducing internet fraud among undergraduates in universities in Rivers State: A conceptual framework. *International Journal of Innovative Technology Integration in Education (IJITIE),* 9 (2), 207-228

This article may be used for research, teaching, and private study purposes. Any substantial or systematic reproduction, redistribution, reselling, loan, sub-licensing, systematic supply, or distribution in any form to anyone is expressly forbidden.

Authors alone are responsible for the contents of their articles. The journal owns the copyright of the articles. The publisher shall not be liable for any loss, actions, claims, proceedings, demand, or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of the research material.

I J I T I E

INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY INTEGRATION IN EDUCATION

Volume 9, Issue 2, 2026

CYBER ETHICS EDUCATION AS A PROPOSED STRATEGY FOR REDUCING INTERNET FRAUD AMONG UNDERGRADUATES IN UNIVERSITIES IN RIVERS STATE: A CONCEPTUAL FRAMEWORK

Nwankwoala Henry Chinedu Ogbonna, Amadi, Uchechukwu (Ph.D) & Uchechukwu-Amadi, Mabel U. (Ph.D)

Article Info

Keywords

Cyber ethics education, internet fraud, cybercrime, undergraduates, Rivers State, conceptual paper

Abstract

Internet fraud involving a small subset of undergraduates is a recurring concern in Nigerian higher education, yet preventive responses are often framed around enforcement. This conceptual paper examines whether, and under what conditions, cyber ethics education could help to prevent internet fraud among undergraduates in universities in Rivers State. Using a narrative review of Nigerian and international literature and official sources, the paper clarified key concepts; drew on the Theory of Planned Behaviour, social learning theory, strain theory, techniques of neutralisation and Space Transition Theory to structure the factors associated with student involvement; examined the evidence on whether ethics and awareness education changes behaviour; and proposed a framework that links each factor to a specific educational component, with implementation arrangements, ethical safeguards and an evaluation design. The review found no published prevalence data for universities in Rivers State and no study that tested a cyber ethics course against fraud perpetration among Nigerian undergraduates. Evidence that awareness alone changes behaviour is weak, whereas interactive, case-based and sustained programmes appear more promising. The paper therefore presented cyber ethics education as a proposal to be piloted and evaluated, not as a proven remedy, and recommended that universities Rivers State should test it alongside counselling, employability support and fair enforcement.

INTERNATIONAL JOURNAL OF
INNOVATIVE TECHNOLOGY INTEGRATION IN EDUCATION

IJITIE · VOLUME 9 · ISSUE 2 · 2026

CYBER ETHICS EDUCATION AS A PROPOSED STRATEGY FOR REDUCING INTERNET FRAUD AMONG UNDERGRADUATES IN UNIVERSITIES IN RIVERS STATE: A CONCEPTUAL FRAMEWORK

Nwankwoala Henry Chinedu Ogbonna, Amadi, Uchechukwu (Ph.D) & Uchechukwu-Amadi, Mabel U. (Ph.D)

uchechukwu.amadi@iaue.edu.ng, mabel.uchechukwu-amadi@iaue.edu.ng and uchechukwu.amadi@iaue.edu.ng

Department of Educational Technology, Ignatius Ajuru University of Education, Port Harcourt, Rivers State, Nigeria

Abstract

Internet fraud involving a small subset of undergraduates is a recurring concern in Nigerian higher education, yet preventive responses are often framed around enforcement. This conceptual paper examines whether, and under what conditions, cyber ethics education could help to prevent internet fraud among undergraduates in universities in Rivers State. Using a narrative review of Nigerian and international literature and official sources, the paper clarified key concepts; drew on the Theory of Planned Behaviour, social learning theory, strain theory, techniques of neutralisation and Space Transition Theory to structure the factors associated with student involvement; examined the evidence on whether ethics and awareness education changes behaviour; and proposed a framework that links each factor to a specific educational component, with implementation arrangements, ethical safeguards and an evaluation design. The review found no published prevalence data for universities in Rivers State and no study that tested a cyber ethics course against fraud perpetration among Nigerian undergraduates. Evidence that awareness alone changes behaviour is weak, whereas interactive, case-based and sustained programmes appear more promising. The paper therefore presented cyber ethics education as a proposal to be piloted and evaluated, not as a proven remedy, and recommended that universities Rivers State should test it alongside counselling, employability support and fair enforcement.

Keywords: Cyber ethics education, internet fraud, cybercrime, undergraduates, Rivers State, conceptual paper.

Introduction

Digital technologies are now central to university life. Undergraduates use the internet for research, online classes, communication, banking, entrepreneurship and social networking. The same environment has created new opportunities for misconduct, including internet fraud. In Nigeria, the phenomenon is widely discussed under labels such as "Yahoo-Yahoo", and several studies have

examined its social organization among university students (Tade & Aliyu, 2011; Adeniran, 2008; Egielewa, 2022). Regional and international enforcement activity points to the same concern: INTERPOL's Operation Contender 2.0, announced on 1 October 2024, targeted business email compromise, romance scams and other cyber-enabled financial crimes, primarily in West Africa, with arrests reported in Nigeria and Côte d'Ivoire (INTERPOL, 2024).

Evidence on how many students are involved is limited. National enforcement statistics show that advance fee fraud, money laundering and cybercrime were among the most prevalent offences handled by the Economic and Financial Crimes Commission (EFCC) in 2024, when it reported 4,111 convictions nationally, 185 of them in its Port Harcourt zone (Ayodele, 2025; Igbintade, 2025). These figures do not separate students from other offenders, and they say nothing about the proportion of Rivers State undergraduates involved. Court records offer only illustrations. In July 2023 the Federal High Court in Port Harcourt convicted a University of Calabar undergraduate on a guilty plea to charges including impersonation and obtaining money by false pretense (EFCC, 2023). In October 2024 the same court sentenced a final-year University of Port Harcourt student, who also pleaded guilty, to two years on each of seven counts, an aggregate widely reported as 14 years, with an option of a fine on each count (EFCC, 2024). Two cases cannot establish a pattern. They are cited here only to show that the issue reaches the courts in Port Harcourt, and Section 5 discusses what the available evidence does and does not show.

It is important to be precise about whom this paper concerns. The great majority of undergraduates do not commit fraud, and many are themselves targets of it. The paper is concerned with a small subset of students who may be drawn into fraud, and with the wider student population who may be victims, bystanders or influencers of peers. Nothing in it should be read as a generalization about undergraduates.

Policy responses to student involvement in internet fraud have centred on arrests and prosecution. Enforcement is necessary, but a complementary preventive argument is that students need the judgement, values and social skills to resist fraud, in addition to knowing it is illegal. Cyber ethics education is one way of attempting this. Whether it works, however, is an empirical question that the literature has not yet answered for Nigerian undergraduates, and this paper treats it as such.

Purpose, objectives and guiding questions

The purpose of this paper is to develop and critically examine a conceptual case for cyber ethics education as a strategy for reducing internet fraud among undergraduates in Rivers State universities, and to propose a framework that can be tested. The objectives are to: (1) clarify the key concepts; (2) establish a theoretical basis for how education could influence fraud-related behaviour; (3) review the evidence on the scale of the problem and its associated factors; (4) assess what the literature says about whether ethics and awareness education changes behaviour; and (5) propose an implementation and evaluation framework with appropriate safeguards. The paper is guided by four questions:

RQ1. What evidence exists on the scale of, and factors associated with, internet fraud among Nigerian undergraduates, and what is known specifically about Rivers State?

RQ2. Which theories explain why education in ethics might, or might not, change fraud-related behaviour?

RQ3. What does the available evidence say about the effects of ethics, awareness and digital-literacy education on behaviour, and under what conditions?

RQ4. If a cyber ethics programme is introduced, how should it be designed, delivered, safeguarded and evaluated in universities in Rivers State?

Scope

The paper focuses on undergraduates in universities in Rivers State, including the University of Port Harcourt, Rivers State University and Ignatius Ajuru University of Education. Where evidence from Rivers State is unavailable, the paper draws on Nigerian studies from other states and on international literature, and says so explicitly. The term "undergraduate" here refers to first-degree students, most of whom are adults; Section 3.4 explains why this matters for the theory and evidence used.

Methodology

This is a conceptual paper. It combines conceptual analysis with a narrative review. The approach was chosen because the aim is to build and examine an argument and a framework, not to estimate

an effect, and because the empirical literature on the specific question is too small and too varied for a systematic review or meta-analysis.

Literature was identified through searches of Google Scholar, African Journals Online, publisher and institutional repositories, and the websites of the EFCC, INTERPOL and the National Universities Commission, using combinations of the terms "cyber ethics", "internet fraud", "Yahoo-Yahoo", "cybercrime", "undergraduates", "Nigeria", "digital citizenship", "ethics instruction" and "moral education". Google Scholar and African Journals Online databases were searched for peer-reviewed articles on cyber ethics education published in English between 2020 and 2025. Sources were included if they (a) addressed internet fraud, cybercrime or online deviance among students or young people, (b) addressed ethics, moral, digital-literacy or awareness education and its outcomes, (c) supplied theory used in the framework, or (d) were official statistics, court records, press releases or legislation. Peer-reviewed sources were preferred; preprints, press releases and news reports were used only where no peer-reviewed alternative existed and are identified as such. Nigerian studies were given priority for context, and established international literature was used for theory and for evidence on the effects of ethics instruction. Because the review is narrative, it is subject to selection bias, and no formal quality appraisal was applied. The paper tried to reduce this risk by reporting studies that found limited effects alongside those that found positive effects, and by stating the strength of evidence for each claim (Table 1). Conclusions are framed as propositions to be tested.

Conceptual Clarification

Cyber ethics

Cyber ethics refers to the moral principles and standards that guide behaviour when using digital technologies and communicating online. It is closely related to computer ethics, which Moor (1985) describes as the analysis of the nature and social impact of computer technology and the policies needed for its ethical use. Tavani (2016) adds that new technological possibilities create new responsibilities. Put simply, cyber ethics distinguishes between what a person can do with technology and what the person ought to do.

Technical skill and ethical judgement are separate. A student who knows how to create anonymous accounts or manipulate digital information may use that knowledge legitimately or fraudulently,

and the difference lies largely in the person's ethical judgement and sense of responsibility. Three strands of cyber ethics bear directly on fraud: honesty and integrity in digital interaction, including the use of false identities; respect for the privacy and personal data of others, since unauthorised use of personal data underlies identity theft and payment fraud (Floridi, 2013); and accountability for the harm that online actions cause, which anonymity can obscure. Other strands, such as intellectual property and responsible disclosure of security vulnerabilities, are part of the wider field but are only indirectly related to fraud and are therefore treated briefly in the proposed course (Section 9.2).

Cyber ethics education

Cyber ethics education is the planned teaching and learning of ethical principles, legal obligations and decision-making skills for the use of digital technologies. In this paper it is distinguished from three neighbouring concepts. Cybersecurity awareness aims to protect users from attack. Digital literacy concerns the skills to find, evaluate and use information. Digital citizenship concerns responsible, safe and ethical participation in digital society. Cyber ethics education overlaps with all three, but its distinctive focus is moral reasoning and the choices that people make as potential actors online, including the choice not to defraud. It should prepare students both to protect themselves from fraud and to refuse to take part in it.

Internet fraud

Following Tade and Aliyu (2011), internet fraud is defined in this paper as any fraud scheme that uses one or more components of the internet to commit a crime. In Nigeria, such conduct is prosecuted mainly under the Advance Fee Fraud and Other Fraud Related Offences Act 2006 and the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, as amended in 2024, which are the statutes cited in the charges in the court cases discussed above (EFCC, 2023, 2024; Federal Republic of Nigeria, 2006, 2015, 2024). Common forms include phishing, online impersonation, romance scams, fraudulent investment schemes, business email compromise and other social-engineering schemes. The paper uses this single definition throughout.

Undergraduates and the relevance of age

Undergraduates are students enrolled in first-degree programmes. The paper does not treat them as adolescents. Many Nigerian undergraduates are aged 18 or above, and developmental research

increasingly describes the late teens and twenties as a distinct period of "emerging adulthood" marked by identity exploration and instability (Arnett, 2000). Evidence from younger adolescents, such as the Hong Kong study of 14-year-olds by Ng (2020), is therefore used only as indicative evidence on teaching methods and is not applied to undergraduates without qualification. Claims about undergraduate attitudes and behaviour are supported wherever possible by studies of university students.

Theoretical Framework

Arguing that education should reduce fraud requires an account of why people commit fraud and how education could alter the process. No single theory supplies this, so the paper draws on five complementary perspectives, each of which maps to a component of the proposed framework (Table 2).

Theory of Planned Behaviour. Ajzen (1991) proposes that behaviour follows from intention, which is shaped by attitude towards the behaviour, subjective norms (perceived approval from important others) and perceived behavioural control. This theory gives a direct role for education, which can shift attitudes and norm perceptions, but it also predicts that information alone will not change behaviour unless attitudes, norms and control change too. It is the paper's organising framework.

Social learning theory. Akers (2009) argues that criminal behaviour is learned through association with others, imitation, definitions favourable to crime, and differential reinforcement. Where peer groups reward fraud, students learn techniques and justifications from them. Education can supply competing definitions and alternative models, but it competes with peers who have more influence over daily life.

Techniques of neutralisation. Sykes and Matza (1957) suggest that offenders often hold conventional values but use rationalisations, such as denying the victim or the harm, to suspend them. Fraud rationalised as "the victims are rich and foreign" is an example. This is the main reason that teaching that fraud is wrong is not enough; education needs to confront the rationalisations themselves.

Strain theory. Merton (1938) holds that deviance can arise when culturally valued goals, such as wealth, are emphasised but legitimate means of reaching them are blocked. Applied to Nigerian students, this links fraud to economic pressure and visible displays of wealth. It implies that ethics education alone cannot succeed unless legitimate opportunities exist.

Space Transition Theory and online disinhibition. Jaishankar (2008) argues that people may behave online in ways they would not in physical space, owing to anonymity, identity flexibility and weaker deterrence. Suler (2004) describes a related online disinhibition effect. These ideas bear on perceived low risk and on the sense that online victims are distant. Education can address them by making consequences, traceability and victims' harm concrete.

Kohlberg's (1981) account of moral development, in which moral reasoning matures through stages that can be stimulated by dilemma discussion, also underpins the case-based approach proposed in Section 9. Taken together, these theories predict that cyber ethics education could change behaviour only under particular conditions: when it targets attitudes, norms and rationalisations as well as knowledge; when it is interactive; and when it is accompanied by legitimate opportunities and credible, fair enforcement.

Internet Fraud among Undergraduates: What the Evidence Shows

National, regional and institutional evidence

Evidence on the scale of student involvement is patchy. At the national level, EFCC statistics show high volumes of advance fee fraud and cybercrime cases but do not identify students (Ayodele, 2025; Igbintade, 2025). Several Nigerian studies have examined undergraduates directly. Tade and Aliyu (2011) described the social organisation of internet fraud among university undergraduates, and Okeshola and Adeta (2013) examined its nature, causes and consequences in tertiary institutions in Zaria. Egielewa (2022) surveyed 372 undergraduates from two institutions in Edo State to examine the temptation to engage in fraud and attitudes to hard work. Balogun et al. (2024) studied the prevalence of internet crimes among undergraduates at the University of Ilorin, and Igwe (2024) examined students' involvement in social media fraud at Lagos State University. These studies come from other states, and most are cross-sectional surveys that rely on self-report, which is subject to social-desirability bias on a sensitive topic.

For Rivers State, the review found no published prevalence or incidence data on student involvement in internet fraud, whether from EFCC records, university disciplinary files or student surveys. This is a limitation of the evidence base, and it means that claims about the extent of the problem in Rivers State universities cannot be made with confidence. The first recommendation in Section 15 is therefore to establish baseline data.

What the court cases do and do not show

The two cases summarised in Section 1.1 illustrate that students in the Port Harcourt area have been prosecuted. They do not show how common this is. They are also not fully representative: the 2023 case involved a student of an institution outside Rivers State, and both defendants pleaded guilty, so no contested facts were tested. Sentencing outcomes in individual cases are not evidence about prevention. In this paper the cases are used neutrally and only to motivate the question.

Factors Associated with Student Involvement in Internet Fraud

The factors commonly proposed are summarised in Table 1, together with the evidence found for each and a judgement of its strength. The factors are described as "associated with" involvement, not as established causes, because most of the evidence is correlational or self-reported, and because none of it comes from Rivers State.

Table 1. Factors associated with student involvement in internet fraud: evidence and strength

Factor	Guiding theory	Illustrative evidence	Evidence strength
Peer influence and normalisation	Social learning; Planned Behaviour (subjective norms)	Ajake et al. (2024) studied moral values, peer influence and cybercrime tendencies among undergraduates in Cross River State. Akinroye and Lawal (2025) reported that peer norms and media portrayals of cybercrime were associated with Nigerian undergraduates' attitudes and involvement. Tade and Aliyu (2011) described fraud networks among students.	Moderate: several Nigerian survey studies; no Rivers State data
Economic pressure and unemployment	Strain	Tade and Aliyu (2011) and Okeshola and Adeta (2013) identified economic motives in their studies of students and	Moderate for association; causal

fears		tertiary institutions. The EFCC attributed high caseloads partly to youth unemployment and the quest for quick wealth (Ayodele, 2025), although this is an agency statement, not a research finding.	direction unclear
Materialism and the culture of quick wealth	Strain; social learning	Egielewa (2022) linked students' attraction to fraud with narrow-mindedness, laziness and a weak valuation of hard work, using a survey of 372 undergraduates in Edo State. Adeniran (2008) described a "Yahoo boys" subculture that celebrates conspicuous consumption.	Limited to moderate: survey and descriptive work
Weak moral formation and rationalisation	Neutralisation; Kohlberg	Ajake et al. (2024) reported a relationship between moral values and cybercrime tendencies. No Nigerian study reviewed measured moral reasoning or neutralisation directly in relation to fraud.	Limited: largely theoretical for this population
Anonymity and perceived low risk	Space Transition Theory; online disinhibition	Supported mainly by theory (Jaishankar, 2008; Suler, 2004). Nigerian studies describe offenders' use of anonymity but do not test perceived risk as a predictor.	Limited: theoretical
Limited cybersecurity knowledge	Planned Behaviour (perceived control)	Ugwu et al. (2021), in a preprint, found that only about half of students and staff at one Nigerian university had good cyber-hygiene knowledge or behaviour, and that age and level of education did not differ significantly. This concerns vulnerability to attack, not engagement in fraud.	Limited, and relevant mainly to victimisation

Three points follow from the table. First, the evidence is strongest for peer influence and economic pressure, both of which are largely outside the direct reach of a classroom course. Second, "weak moral formation" and "inadequate cybersecurity knowledge" are often presented as causes of offending but have little direct supporting data; cybersecurity knowledge, in particular, bears more on victimisation than on perpetration. Third, because the factors are interrelated, no single intervention is likely to address all of them, which is why the framework in Section 9 combines

education with other measures. For completeness, Tade (2013) documented a distinct ritual dimension ("Yahoo Plus") in some fraud networks; it is outside the scope of this paper because it is not a mainstream student factor in the studies reviewed. Ebere et al. (2025), who studied delinquency patterns and academic performance among undergraduates at Rivers State University, provide a related and locally situated source on student misconduct and counselling, although it does not address fraud specifically.

Does Education Change Behaviour? The Knowledge–Behaviour Gap and the Evidence on Interventions

The knowledge–behaviour gap

The paper's central assumption, that cyber ethics education can reduce fraud, is challenged by a gap between knowing and doing. Eke (2024), in a study of Nigerian youths generally, reported high awareness of internet fraud as a problem, and the study recommended further awareness campaigns. High awareness of a problem does not imply low participation; a person can know that fraud is illegal and harmful and still take part, particularly if neutralising beliefs, peer approval and financial pressure are present (Sykes & Matza, 1957; Akers, 2009). More generally, intentions explain only part of behaviour, and the evidence on the "intention–behaviour gap" shows that even people who intend to act in a certain way frequently fail to do so (Sheeran & Webb, 2016). Awareness is therefore at best a necessary condition for behaviour change, not a sufficient one.

Evidence on the effects of ethics and literacy interventions

Meta-analytic evidence from other fields is cautious. A meta-analysis of 25 business ethics instructional programmes concluded that, overall, they had a minimal impact on ethical perceptions, behaviour or awareness, although effects varied with content and method (Waples et al., 2009). A meta-analysis of 26 evaluations of ethics instruction in the sciences found overall effects that were modest; more effective programmes were case-based and interactive, gave participants the chance to practise ethical decision-making, and were run as seminars separate from the standard curriculum, not embedded in existing courses (Antes et al., 2009). These fields differ from cyber ethics and from the Nigerian setting, so the findings are indicative, but they establish that ethics instruction does not automatically change behaviour and that design matters.

Evidence on cyber ethics and fraud specifically is thin. Ng (2020) tested a self-assessment teaching method with 28 students aged about 14 in a Hong Kong secondary school; students reported greater self-awareness of cyberethics, but the study measured self-reported reflection, had a very small sample, and did not measure behaviour. Ugwuanyi et al. (2025) studied a social-media-based digital literacy intervention among Economics Education undergraduates in South East Nigeria and reported reduced vulnerability to online fraud; this single study concerns susceptibility to fraud rather than perpetration, involved a specific student group, and may not be comparable with students in Rivers State. Afolabi and Wahab (2025) used a quasi-experimental design with 650 students in five Colleges of Education in South West Nigeria to test two interventions on involvement in "Yahoo-Yahoo" and recommended integrating cyber-ethics education, financial literacy and mentoring into curricula; as a recent study it needs replication, and it did not test a cyber ethics course as proposed here. Finally, the finding by Ugwu et al. (2021) that level of education was not significantly associated with cyber-hygiene knowledge or behaviour suggests that simply being in higher education does not confer safe or ethical online practice.

Implications

Three implications follow. First, no study located tests whether a cyber ethics course reduces fraud perpetration among Nigerian undergraduates, so the claim in the title is a proposition and is presented as such. Second, the better evidence points to conditions under which education may help: interactive and case-based methods, practice in decision-making, attention to rationalisations and peer norms, and duration beyond a single event. Third, because education is unlikely to be sufficient, it should be combined with legitimate economic opportunities, supportive counselling and consistent enforcement, and its effects should be evaluated.

Existing Curricula and the Gap That Cyber Ethics Would Fill

It is sometimes assumed that students receive technical training without ethical education. This assumption needs qualification. Nigerian universities already teach General Studies (GST) courses and other content with ethical or digital components. The National Universities Commission (NUC) replaced its Benchmark Minimum Academic Standards (BMAS) with the Core Curriculum and Minimum Academic Standards (CCMAS), implemented from September 2023, which reduced General Studies from 36 to 12 credit units across six courses and allows universities to

determine 30% of each programme (BusinessDay, 2023; NUC, 2022). University GST listings seen during the review include communication, philosophy and logic, Nigerian peoples and culture (with outcomes that include identifying and proposing solutions to social and moral problems), peace and conflict resolution, and entrepreneurship, and some CCMAS course descriptions include practical use of computers and the internet.

On the basis of these sources, the content that exists is general ethics, civic values and basic ICT skills. The review did not find evidence that the standard GST content addresses internet fraud, cybercrime law, online rationalisations or digital decision-making directly. This is a provisional finding, since the review examined published course descriptions and not what is taught in practice at each Rivers State university. The first step should therefore be a curriculum audit to establish what each institution covers, so that the specific gap is documented before any course is introduced (Section 15). The tight GST credit limit also matters: a new compulsory GST course may be difficult, whereas the 30% university-determined portion offers a possible route.

Proposed Framework: Linking Factors to Interventions

The framework

Table 2 links each factor in Table 1 to the mechanism through which education could act, the proposed component, and an indicator by which effects could be assessed. The framework is a proposal to be tested.

Table 2. Framework linking factors, mechanisms, interventions and indicators

Factor	Mechanism (theory)	Proposed component	Indicator
Peer influence	Change perceived norms and refusal skills (Planned Behaviour; social learning)	Scenario-based refusal and bystander exercises; peer-led discussion; correcting the misperception that "everyone does it"	Perceived peer approval of fraud; refusal self-efficacy
Economic pressure and materialism	Provide legitimate means and reframe success (strain)	Linkage with entrepreneurship, freelancing and digital-skills training; careers and financial-literacy sessions; counselling referral	Participation in skills programmes; attitudes to quick wealth
Rationalisation	Challenge	Dilemma discussions; victim-	Acceptance of

and weak moral reasoning	neutralisations; stimulate moral reasoning (Sykes & Matza; Kohlberg)	impact cases; structured rebuttal of common justifications	neutralising statements; moral-reasoning score
Anonymity and perceived low risk	Make traceability and harm concrete (Space Transition; disinhibition)	Sessions on digital evidence, the Cybercrimes Act and victims' accounts	Perceived risk of detection; empathy with victims
Limited cyber knowledge	Build perceived control and protective skills (Planned Behaviour)	Practical modules on spotting and reporting scams, privacy and data protection	Scam-recognition test; reporting intentions
Weak institutional credibility	Strengthen deterrence perceptions through fair rules	Clear, communicated acceptable-use policy and disciplinary procedures	Student awareness and perceived fairness of policy

Course design

Table 3 sets out an illustrative course. It is a model for piloting, not a finished curriculum. The design draws on the evidence in Section 7: it is case-based and interactive, it gives students practice at decisions, and it deals only briefly with intellectual property and vulnerability disclosure, which relate less directly to fraud.

Table 3. Illustrative outline of a two-unit cyber ethics course

Weeks	**Module**	**Content and methods**
1–2	Digital life, rights and responsibilities	Concepts of cyber ethics, digital citizenship and anonymity; class discussion of students' own online experiences
3–4	Ethical reasoning	Consequence-, duty- and virtue-based reasoning; structured dilemmas on impersonation, shared passwords and misleading offers
5–6	Internet fraud, victims and the law	Forms of fraud; the Cybercrimes Act and the Advance Fee Fraud Act; victim-impact accounts; digital evidence and traceability
7–8	Why people take part: rationalisations, peers and money	Neutralisations and how to rebut them; peer norms; strain and the pressure of visible wealth; role-play of refusal
9	Privacy and data protection	Personal data, the Nigeria Data Protection Act 2023

		(Federal Republic of Nigeria, 2023), and the link between data misuse and identity fraud
10	Protecting self and others	Spotting, verifying and reporting scams; responsible sharing of messages; brief treatment of intellectual property and responsible disclosure of vulnerabilities
11	Legitimate digital livelihoods	Freelancing, digital marketing, software and data work; joint session with entrepreneurship and careers units
12	Emerging risks	AI-enabled impersonation, deepfakes and cryptocurrency schemes
13–14	Case clinic and capstone	Group analysis of an anonymised case; presentation of a decision and its justification

Learning outcomes. By the end of the course students should be able to (a) explain the main forms of internet fraud, their harms and the legal consequences; (b) analyse an ethical dilemma using more than one ethical framework and justify a decision; (c) identify and rebut common rationalisations for fraud; (d) recognise and report scams and protect personal data; and (e) describe legitimate digital routes to income.

Credit load, methods and assessment. A two-credit-unit course, consistent with the 30-hour contact load of two-unit courses in the CCMAS, delivered through short inputs followed by case discussion, role-play and group work. Assessment would combine continuous assessment (40%), comprising case analyses, a reflective journal and a group presentation, with an end-of-course examination (60%) that uses applied scenarios, not recall of definitions.

Who would teach it. A teaching team is preferable to a single lecturer, because the course draws on technology, law, ethics and counselling. A lead lecturer from Educational Technology, Computer Science or Philosophy could coordinate, with contributions from a legal practitioner, a counsellor and, where appropriate, guest speakers, with the safeguards in Section 10. Staff would need short preparatory training, which is itself a cost to plan for.

Delivery routes

Two routes are possible. Route A is a stand-alone two-unit course within the university-determined 30% of the curriculum, which the evidence in Section 7.2 suggests is preferable, since seminar-style programmes separate from the standard curriculum tended to be more effective than

embedded ones (Antes et al., 2009). Route B, for universities with no available credit space, is a shorter module of about ten hours embedded in an existing GST course such as the ICT or philosophy course. The shorter route is a fallback and its effects are likely to be smaller. Orientation sessions for new students can reinforce either route but should not be the only component.

Complementary components

Counselling, mentoring and employability support address the economic and social pressures that a course cannot remove; their role is to offer help, as described in Section 10. Digital citizenship campaigns can reinforce messages but should be assessed as a supplement to, and not a substitute for, structured teaching. Institutional acceptable-use policies and fair, consistent disciplinary procedures give the course credibility, since ethical teaching is undermined when policy exists only on paper.

Evaluation

The programme should be evaluated for its effect on fraud-related attitudes and behaviour, not only on satisfaction or knowledge. A feasible design is a pilot at one or more Rivers State universities with a comparison group, such as students in a cohort or institution not yet offered the course, using pre-course, post-course and 6- to 12-month follow-up measures. Outcome measures would include acceptance of neutralising statements, perceived peer norms, intentions, scam-recognition and, with ethical approval, anonymous self-reported involvement using methods that reduce social-desirability bias. Institutional records, such as the number of referrals for misconduct, can supplement these measures but should not be used to identify individuals. The evaluation should report null and negative findings as well as positive ones.

Ethical and Practical Safeguards

Two of the proposals commonly made for cyber ethics programmes raise concerns that need explicit safeguards.

Collaboration with the EFCC and other agencies. Partnerships can provide expertise and realistic information on consequences, but if students see the programme as policing it may produce distrust and resistance, and a reluctance to seek help. Recommended safeguards are: the

course remains academically led, with agency staff taking part only as invited guest speakers; no student information is shared with any agency; agency participation is governed by a written agreement that preserves the educational purpose; and students are told clearly what the agency's role is. A university may choose to use cybersecurity professionals or legal academics instead, if agency involvement would undermine trust.

Counselling and the identification of students "at risk". An earlier formulation of this proposal asked counselling units to identify students at risk of engaging in fraud. Doing so raises serious problems of privacy, profiling and stigma, because the predictors involved (such as financial hardship or peer group) are shared by many students who will never commit fraud, and a label of "at risk" can harm students and discourage help-seeking. This paper therefore recommends a universal, voluntary approach: all students have access to financial-stress, career and wellbeing support; counsellors are trained in these topics and in referral; no risk lists are kept; confidentiality follows professional counselling standards and the Nigeria Data Protection Act 2023 (Federal Republic of Nigeria, 2023); and counselling records are never used for discipline or reported to enforcement agencies.

Language and fairness. Course materials and campaign messages should avoid portraying students as presumptive offenders. Cases should be anonymised, and discussion should be framed as exploring pressures and choices, not accusing participants.

Challenges and Proposed Responses

The challenges below are assumptions that should be tested during piloting, not established findings. Each is paired with a response.

Table 4. Anticipated challenges, evidence status and responses

Challenge	Evidence status	Response
Limited credit space	Supported by the CCMAS reduction of GST to 12 credit units (BusinessDay, 2023)	Use the 30% university-determined portion (Route A) or an embedded module (Route B); begin with a pilot
Shortage of qualified instructors	Assumption; no staffing data for Rivers State were found	Audit staff expertise; use team teaching; provide short training; involve law and counselling staff

Rapid technological change	Well documented for fraud generally (for example, AI-enabled impersonation) but not for course update cycles	Keep the course principle-based; review case material annually
Student resistance or perception of control	Assumption; plausible given the policing concern in Section 10	Use participatory methods, student input and the safeguards in Section 10
Economic and social pressures	Supported by the evidence in Table 1	Link with entrepreneurship, careers and counselling; set realistic expectations of what a course can achieve
Weak institutional enforcement	Assumption; no Rivers State evidence was found	Publish clear acceptable-use and disciplinary procedures and apply them consistently; include them in the audit

Implications for Policy and Practice

For university management, the review implies that investment in cyber ethics education should be staged: audit, pilot, evaluate, then scale. For the NUC and university senates, it indicates that the university-determined portion of the CCMAS is a practical space for such a course. For counselling and student affairs units, it points to universal support in place of risk profiling. For researchers and funders, it highlights an evidence gap that a modest evaluation study could fill. For enforcement agencies, it suggests that a supportive, non-policing role in education is likely to be more productive than one that blurs education with investigation.

Limitations

This paper has some limitations. It is a narrative, conceptual review and not a systematic review, so some relevant studies may have been missed and no formal quality appraisal was applied. No Rivers State prevalence data were found, and much of the evidence comes from other Nigerian states and from other fields. Many of the cited studies are cross-sectional and self-reported. Some sources are recent, unreplicated or published in outlets whose indexing was not verified, and some information, such as court outcomes, is taken from agency press releases and news reports. The proposed framework and course are untested. The paper also examines curriculum documents and not classroom practice. These limitations mean the paper's conclusions should be read as propositions.

Conclusion and Directions for Future Research

Internet fraud involving a small subset of undergraduates is a concern for Nigerian higher education, and enforcement alone is unlikely to be the whole answer. This paper has made a conceptual case that cyber ethics education could play a preventive role in Rivers State universities, and has contributed a theory-based framework that links factors associated with fraud to specific educational components, together with a course outline, safeguards and an evaluation design. It has also shown that the case is not yet proven: there are no Rivers State prevalence data, no study tests a cyber ethics course against fraud perpetration among Nigerian undergraduates, and the evidence from ethics instruction more generally suggests that effects are modest and depend heavily on design.

Future research should therefore (1) establish baseline prevalence and attitudes in Rivers State universities through anonymous surveys and institutional data; (2) audit what existing curricula teach; (3) pilot the proposed course and evaluate it with a comparison group and follow-up, measuring attitudes, norms and, ethically, behaviour; (4) test which components, such as case-based discussion or refusal training, contribute most; and (5) examine unintended effects, including stigma and changes in help-seeking. Until such evidence exists, cyber ethics education should be introduced as a tested, well-safeguarded complement to, not a replacement for, economic opportunity, counselling and fair enforcement.

Suggestions

The suggestions below are specific about responsibility and timing. Timelines assume approval at the start of an academic session.

Table 5. Recommendations, responsible bodies and timelines

S/N	Recommendation	Responsible body	Timeline
1	Collect baseline data on student attitudes to, and exposure to, internet fraud through an anonymous survey, and analyse anonymised disciplinary records	Directorate of Academic Planning with Educational Technology and Counselling departments; ethics committee approval	First semester
2	Audit existing GST, ICT and ethics content to document what is taught about	Directorate of General Studies and Senate	First semester

	fraud, cybercrime law and digital decision-making	curriculum committee	
3	Approve a two-unit pilot cyber ethics course within the university-determined portion of the curriculum, based on Table 3	University Senate; Directorate of General Studies	Second semester approval; pilot in the following session
4	Train a teaching team (technology, law, ethics, counselling) and prepare anonymised case materials	Faculty of Education and Directorate of General Studies	Before the pilot
5	Provide universal, voluntary counselling and career support, with confidentiality protocols and no risk lists	University Counselling Unit; Student Affairs; Data Protection Officer	Begin in the first session and continue
6	Set up a written protocol for any agency participation limiting it to guest education and prohibiting sharing of student data	Vice-Chancellor's office; Legal Unit	Before any agency session
7	Publish and consistently apply an acceptable-use policy and disciplinary procedure	University Management; ICT Directorate	Within the first session
8	Evaluate the pilot with a comparison group and a 6- to 12-month follow-up, and publish results, including null findings	Research team with Directorate of Academic Planning	End of the pilot session; follow-up within the next session

References

Adeniran, A. I. (2008). The Internet and emergence of Yahooboys sub-culture in Nigeria. *International Journal of Cyber Criminology, 2*(2), 368–381.

Afolabi, A. A., & Wahab, I. (2025). Involvement in Yahoo-Yahoo and learning outcomes among students in colleges of education South Western, Nigeria. *African Journal of Educational Management, 26*(1), 478–496. https://journals.ui.edu.ng/index.php/ajem/article/view/2202

Ajake, U. E., Kalu, G. U., & Ugwu, S. C. (2024). Moral value, peer influence and tendencies to cybercrime involvement among undergraduates in public universities in Cross River State. *Global Journal of Educational Research, 23*, 137–147.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Akers, R. L. (2009). *Social learning and social structure: A general theory of crime and deviance*. Transaction Publishers.

Akinroye, A. O., & Lawal, A. A. (2025). Assessing the impact of media exposure and subjective norms on cybercrime-related internet behaviour among Nigerian undergraduates. *International Journal of Research and Innovation in Social Science, 9*(7), 2489–2515. https://rsisinternational.org/journals/ijriss/articles/assessing-the-impact-of-media-exposure-and-subjective-norms-on-cybercrime-related-internet-behavior-among-nigerian-undergraduates/

Uchechukwu, A., & Onah, L. C. (2026). Digital Citizenship and Ethical Technology Use Among University Students in Rivers State: Legal, Wellness, and Security Perspectives. *International Journal of Innovative Technology Integration in Education*, *9*(1), 250-268.

Antes, A. L., Murphy, S. T., Waples, E. P., Mumford, M. D., Brown, R. P., Connelly, S., & Devenport, L. D. (2009). A meta-analysis of ethics instruction effectiveness in the sciences. *Ethics & Behavior*, *19*(5), 379–402.

Arnett, J. J. (2000). Emerging adulthood: A theory of development from the late teens through the twenties. *American Psychologist, 55*(5), 469–480.

Ayodele, A. (2025). *EFCC sets record with 4,111 convictions, biggest asset recovery in 2024*. News Agency of Nigeria. https://nannews.ng/efcc-sets-record-with-4111-convictions-biggest-asset-recovery-in-2024/

Balogun, N. A., Abdulrahaman, M. D., & Aka, K. (2024). Exploring the prevalence of internet crimes among undergraduate students in a Nigerian university: A case study of the University of Ilorin. *Nigerian Journal of Technology*, *43*(1).

BusinessDay. (2023, August 25). *What to know about new varsity curriculum taking off September*. https://businessday.ng/news/article/what-to-know-about-new-varsity-curriculum-taking-off-september

Ebere, S. W., Egwurugwu, N. A., & Elijah, M. N. (2025). Exploring the relationship between delinquency patterns and academic performance of undergraduates' students in Rivers State University: Implication for counselling. *International Journal of Research and Innovation in Social Science, 9*(8), e 3955 – 3961.

Economic and Financial Crimes Commission. (2023). *Court jails undergraduate three years for internet fraud in Port Harcourt* [Press release]. https://efccnigeria.org/efcc/news-and-information/news-release/9357-court-jails-undergraduate-three-years-for-internet-fraud-in-port-harcourt

Economic and Financial Crimes Commission. (2024, October 30). *Undergraduate bags 14 years jail term in Port Harcourt* [Press release]. https://www.efcc.gov.ng/news-and-information/news-release/10484-undergraduate-bags-14-years-jail-term-in-port-harcourt

Egielewa, P. E. (2022). Yahooism or internet fraud in the Nigerian higher education system. *Journal of Ethics in Higher Education, 1*, 75–101. https://doi.org/10.26034/fr.jehe.2022.3378

Eke, C. (2024). Awareness and perception of internet fraud epidemics among Nigerian youths. *African Journal of Social and Behavioural Sciences, 14*(3).

Federal Republic of Nigeria. (2006). *Advance Fee Fraud and Other Fraud Related Offences Act, 2006*.

Federal Republic of Nigeria. (2015). *Cybercrimes (Prohibition, Prevention, etc.) Act, 2015*.

Federal Republic of Nigeria. (2023). *Nigeria Data Protection Act, 2023*.

Federal Republic of Nigeria. (2024). *Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024*. Policy and Legal Advocacy Centre.

Floridi, L. (2013). *The ethics of information*. Oxford University Press.

Igbintade, W. (2025, March 10). EFCC announces recovery of over N364bn, secures 4,111 convictions. *ThisDay*. https://www.thisdaylive.com/2025/03/10/efcc-announces-recovery-of-over-n364bn-secures-4111-convictions/

Igwe, D. O. (2024). Students' involvement in social media fraud: A case study of Lagos State University. *African Journal of Social and Behavioural Sciences, 13*(2).

INTERPOL. (2024, October 1). *Arrests in international operation targeting cybercriminals in West Africa* [Press release]. https://www.interpol.int/en/News-and-Events/News/2024/Arrests-in-international-operation-targeting-cybercriminals-in-West-Africa

Jaishankar, K. (2008). Space transition theory of cybercrimes. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283–301). Prentice Hall.

Kohlberg, L. (1981). *Essays on moral development: Vol. 1. The philosophy of moral development*. Harper & Row.

Merton, R. K. (1938). Social structure and anomie. *American Sociological Review, 3*(5), 672–682.

Moor, J. H. (1985). What is computer ethics? *Metaphilosophy, 16*(4), 266–275.

National Universities Commission. (2022). *Core curriculum and minimum academic standards (CCMAS) for the Nigerian university system*.

Ng, W. S. (2020). A self-assessment approach to adolescents' cyberethics education. *Journal of Information Technology Education: Research, 19*, 555–570. https://doi.org/10.28945/4623

Okeshola, F. B., & Adeta, A. K. (2013). The nature, causes and consequences of cyber-crime in tertiary institutions in Zaria-Kaduna State, Nigeria. *American International Journal of Contemporary Research, 3*(9), 98–114.

Sheeran, P., & Webb, T. L. (2016). The intention–behavior gap. *Social and Personality Psychology Compass, 10*(9), 503–518. https://doi.org/10.1111/spc3.12265

Suler, J. (2004). The online disinhibition effect. *CyberPsychology & Behavior, 7*(3), 321–326.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review, 22*(6), 664–670.

Tade, O. (2013). A spiritual dimension to cybercrime in Nigeria: The "Yahoo Plus" phenomenon. *Human Affairs, 23*(4), 689–705.

Tade, O., & Aliyu, I. (2011). Social organization of internet fraud among university undergraduates in Nigeria. *International Journal of Cyber Criminology, 5*(2), 860–875.

Tavani, H. T. (2016). *Ethics and technology: Ethical issues in an age of information and communication technology* (5th ed.). Wiley.

Ugwu, C., Ani, C., Ezema, M., Asogwa, C., Ome, U., Obayi, A., Ebem, D., Atanda, A., & Ukwandu, E. (2021). *Towards determining the effect of age and educational level on cyber-hygiene* (arXiv:2103.06621). arXiv. https://doi.org/10.48550/arXiv.2103.06621

Ugwuanyi, C. K., Onuoha, J. C., Eneogu, N. D., & Ugwonna, G. (2025). Impact of social media based-digital literacy on reduction of internet fraud among Economics Education undergraduates in South East, Nigeria. *Journal of Educational Research on Children, Parents and Teacher, 6*(2), 157–167.

Waples, E. P., Antes, A. L., Murphy, S. T., Connelly, S., & Mumford, M. D. (2009). A meta-analytic investigation of business ethics instruction. *Journal of Business Ethics, 87*(1), 133–151.