



Investigating the Predictive Roles of Affective Responsiveness and Pathological Egocentricity on Cybercrime Awareness

David Okanandu Iloma ^{1*}, Juanida Horne ²

^{1,2} Department of Police Practice, School of Criminal Justice, College of Law,
University of South Africa, Florida Campus, Roodepoort, South Africa.

* Corresponding/lead author: ilomado@unisa.ac.za, vissionanddiscipline@yahoo.com

Second author: hornejs@unisa.ac.za

© Authors

OIDA International Journal of Sustainable Development, Ontario International Development Agency, Canada.
ISSN 1923-6654 (print) ISSN 1923-6662 (online) www.oidaijsd.com

Abstract: The rapid expansion of digital platforms has created new avenues for manipulative and antisocial behaviours, such as defrauding and making life miserable for people. While psychopathic personality traits have been studied in clinical and forensic settings, their digital dimension remains empirically misunderstood. This study aimed to explore the predictive influence of affective responsiveness and pathological egocentricity on cybercrime awareness among university students. Using an analytical cross-sectional survey, 305 participants were purposively recruited from a medium-sized private university in the 'South-South' region of Nigeria. Standardised inventories were employed to measure key study variables. The findings revealed that a sizable proportion of participants, 104 (34.1%), reported having been a cyber-victim, and in specific types of crime, cyber fraud topped the list with 41 (13.4%), followed by money doubling schemes/Ponzi 27 (8.9%), and black-hat hacking/account take-over with 9 (3.0%). To test the study's hypotheses, multiple linear regression was employed, and the study found a significant positive effect of affective responsiveness on cybercrime awareness scores. Additionally, the study found an inverse association between cybercrime awareness and pathological egocentricity when the latter were included in the regression model. This study provides a foundation for enhancing students' awareness of cybercrime on Nigerian university campuses. Integrating cybersecurity education into the curricula which is a key aspect of being intentional about virtual knowledge and continually upgrading, could be the game changer in effectively combating students' vulnerability to cybercrime. This implies enhancing affective responsiveness and reducing egocentricity by incorporating cybercrime awareness programs, such as cyber education and information security awareness, into tertiary institutions' curricula.

Keywords: Affective responsiveness, pathological egocentricity, cybercrime awareness, digital behaviour, mental health and personality

Introduction

In recent times, cybercrime has emerged as one of the most significant threats to Nigeria's digital integrity and socioeconomic status. Cybercrime's primary and most vulnerable targets are Nigeria's tertiary institutions (Ugah et al., 2025). As Nigerian tertiary institutions gravitate towards digitised frameworks, staff and students often find themselves at the mercy of organised, sophisticated cyber threats and the rapid pace of technological advancement (Murad & Qudah, 2025; Pant & Chaubey, 2024). Insofar as institutional technical defences, such as encryption, strong passwords, and firewalls, are in place, the cognitive underpinnings of cybercrime awareness remain largely under-researched in the African tertiary context (Borwell et al., 2021).

The problem appears to be the varying levels of cyber-risk perception among university undergraduates, who, most of the time, are either the main targets or, in some cases, active perpetrators of digital fraud driven by recent interest in the virtual world. Since people downplay or overlook the psychological dispositions that shape how information is

processed and acted upon, most traditional cybercrime awareness campaigns never see the light of day. Specifically, the impacts of personality traits and affective intelligence have been relegated to the background, which has prompted this study to explore and investigate the predictive roles of affective responsiveness (i.e., the emotional component of empathy) and pathological egocentricity (i.e., an extreme focus on self-interest, beliefs, attitudes and a lack of perspective-taking) on the magnitude of cybercrime awareness at a Nigerian university. With a good understanding of these psychological predictors, the study aims to create a more behaviourally informed, effective cybersecurity awareness and policymaking within the Nigerian tertiary institution (Borwell et al., 2021).

People have become so accustomed to using technology (such as mobile phones and iPads) that they now cannot do without it. In fact, they are glued to their phones in the same way that moths are glued to bright light. Research indicates that about 62.5% of the world's population, or 4.95 billion people, use the internet, and this figure is expected to rise to 5.3 billion (von der Ahe, 2022) in the foreseeable future. In 2025 the number of mobile devices in use globally was estimated at around 18.22 billion (Sarkar & Shukla, 2023), indicating that people have engaged with multiple gadgets, which has exposed them to digital fraud, reckless technology use, and several digitally enabled crimes (Pant & Chaubey, 2024). In view of this, it is costly to underestimate the effect of cybercrime on one's well-being.

The psycho-social focus of students allows researchers to assess how these psychopathic traits interact with and influence cybercrime awareness. Selecting tertiary students as the study population (i.e., in their burgeoning phase of life) offers a significant opportunity to understand cybercrime awareness and the psychological factors that shape it and enable educators and policymakers to design effective interventions to prevent cybercrime in educational settings.

Theoretical framework

This study was guided by the cognitive dissonance theory, which provides insight into how individuals deal with conflicts between their self-image (affective component and self-interest) and the disturbing realities of online fraud (Festinger, 1957). Those with a good self-image may experience less dissonance and are more likely to engage in behaviours that protect them from digital fraud, while people with poor self-image may experience more dissonance and more prone to engage in digital behaviours that may compromise their assets and sanity. Developed by Leon Festinger in 1957, cognitive dissonance theory suggests that people feel unease when they hold conflicting beliefs, values, or attitudes. This discomfort or dissonance can prompt them to act to alleviate it. Applied to online crime and cybercrime awareness, this theory helps us understand how individuals interpret their online experiences and make choices in digital spaces (Sharma, 2025). Victims of cybercrime, such as phishing or identity theft, can experience feelings of cognitive dissonance, particularly if they see themselves as well-informed and knowledgeable about digital crime. For instance, people who think they are tech-savvy and yet fall for a scam may feel embarrassed or ashamed. To cope with their uncomfortable feelings, they might minimise the seriousness of the incident, blame it on external factors, such as the cleverness of the scammer, or refuse to admit their mistake or may adopt a nonchalant attitude (Harmon-Jones & Mills, 1999).

Research shows that after being scammed, people often do not take protective measures but instead become emotional (Bai et al., 2026). The pain of recognising their vulnerability can be somewhat overwhelming. This was evident in a study by Urien (2025) who recruited 650 students in a bid to explore the link between cognitive dissonance and cyber-fraud behaviour in Nigeria universities. It was found that several students were depressed and intimidated by classmates who were successful in their online fraud dealings and led lavish lifestyles. Students' cognitive dissonance led to feelings of intimidation, which, in turn, generated psychological embarrassment, prompting significant changes in their attitudes and overt behaviour to suppress the discomfort. On the other hand, when individuals recognise the dangers of cybercrime, they may adjust their behaviours to align with their beliefs. For instance, heightened awareness can lead to improved cybersecurity practices, such as creating strong passwords and exercising caution with personal data and official online activities. This shift in behaviour alleviates dissonance by aligning actions with the beliefs of being informed and careful (O'Sullivan et al., 2019). Understanding the impact of cognitive dissonance on cyber victimisation can enhance educational approaches and empower students.

In digital milieus, affective responsiveness manifests as the ability to emotionally internalise the consequences of online breaches or cyberattacks. Individuals with strong affective responsiveness were hypothesised to be more sensitive to the "human cost" of cybercrime, which in turn, drives greater motivation to remain informed and vigilant (Ugah et al., 2025).

Pathological egocentricity is characterised by the inability to draw a line between one's own view and that of others, in addition to a grandiose sense of self-importance and self-centeredness. In a typical university setting, this trait often

manifests as a disregard for institutional security guidelines, which students see as unwanted inconveniences. Egocentric students may reveal “optimism bias”, which is the belief that they cannot be scammed or harmed. This belief reduces their exposure to the latest cybercrime awareness materials. Nigeria occupies a unique position in the global cybercrime landscape because of the localised phenomenon of cyber-enabled fraud, popularly known as yahoo-plus, which is now even ritualised in some cases, popularly known as yahoo-plus (Ajah, et al., 2026). Current studies also indicate that many students only have a superficial awareness of phishing, social engineering, and data privacy laws, yet lack deep knowledge of phishing, social engineering, and data privacy laws (Nzeakor et al., 2022), a phenomenon that is another justification for the current study.

Empirical review

Cybercrime awareness

The rapid evolution of the internet has transformed modern life, enabling unprecedented connectivity, commerce, and communication (Pandey & Kapoor, 2025). Yet, this very pace of technological development has also created fertile ground for cybercriminals who exploit vulnerabilities much faster than lawmakers and institutions can respond to cybercrime (Buono, 2014). As internet usage has become routine for billions of people worldwide, cybercrime has emerged as one of the most pressing challenges of the digital era, affecting individuals, organisations, and governments alike (Sharma, 2025).

Cybercrime refers to unlawful activities perpetrated through computers or digital networks. In cybercrime, the computer may serve as a tool, a target, or both (Mokha, 2017). Traditional crimes, such as fraud, theft, and harassment, have taken on new digital forms, whereas the rate of entirely novel crimes, such as ransomware, phishing, and cyberterrorism, has risen sharply (Mokha, 2017; Sharma, 2025). The anonymity afforded by cyberspace allows perpetrators to operate across borders, making cybercrime more difficult to trace and prosecute than conventional offences (Pandey & Kapoor, 2025).

The scale of cybercrime is staggering. With over 5 billion internet users globally, opportunities for exploitation have multiplied (Bai et al., 2026; Sharma, 2025). Although technological innovations have been beneficial, they have inadvertently facilitated sophisticated attacks. Artificial intelligence and machine learning, for instance, are increasingly weaponised to automate assaults or craft convincing phishing schemes (Pandey & Kapoor, 2025; Sharma, 2025). The COVID-19 pandemic further accelerated digital dependency, leading to a surge in cyber incidents since individuals and organisations relied heavily on online platforms for work, education, and commerce (Pandey & Kapoor, 2025).

According to Mokha (2017), cybercrimes can be classified into four categories, based on their targets and impacts:

- i. **Crimes Against Individuals:** These include hacking, cyberstalking, defamation, email spoofing, phishing, and the dissemination of obscene material. Such offences often cause psychological harm, erode trust, and compromise personal security.
- ii. **Crimes Against Property:** Offences such as intellectual property theft, cyber vandalism, virus transmission, and online financial fraud fall under this category, targeting digital assets and economic resources.
- iii. **Crimes Against Governments or Organisations:** Cyberterrorism, espionage, and unauthorised access to sensitive information threaten national security and institutional stability.
- iv. **Crimes Against Society:** Activities such as online gambling, the sale of illegal goods, and child exploitation via virtual tools affect the social fabric, often with devastating consequences. The consequences of cybercrime extend far beyond financial losses.

According to Cybersecurity Ventures, global damages are projected to reach \$10.5 trillion annually by 2025, encompassing data breaches, ransom payments, sextortion and ripple effects across industries (Pandey & Kapoor, 2025). A single data breach costs businesses an average of \$4.4 million per breach (IBM, 2025). Beyond monetary damage, victims often suffer anxiety, stress, and diminished trust in digital systems (Pandey & Kapoor, 2025). Cyberbullying and online harassment have led to severe mental health issues, particularly among youths and students. In some cases, self-harm was the consequence of cyberbullying and online harassment.

Despite the growing prevalence of cybercrime, public awareness remains limited. Many users recognise threats such as hacking or viruses but remain unaware of phishing, identity theft, or cyberstalking (Mokha, 2017). This knowledge gap exposes individuals to greater risks and underscores the need for comprehensive awareness programs. As Sharma

(2025) notes, users often lack the preparedness to handle security breaches, making education a critical defence mechanism. In view of this, awareness must be continuous rather than episodic. Given the dynamic nature of technology, emerging threats such as AI-driven attacks, quantum computing vulnerabilities, and deepfakes demand ongoing vigilance (Sharma, 2025). Lifelong learning initiatives can ensure that individuals and organisations remain adaptive and resilient (Sharma, 2025).

Affective responsiveness and cybercrime awareness

Empirical evidence suggests that affective responsiveness (that is, the emotional ability to respond to others' experiences) serves as an important cognitive filter in processing cyber-risk information. Gautam and Yadav (2026) investigated the psychological impact of cybercrime on victims, their cognitive inadequacies, and their coping strategies. In time series research from 1998 to 2023, comprising 9 900 empirical papers and 10 online reports, Gautam and Yadav (2026) found that cybercrime has various harmful psychological effects, such as depression, anxiety, stress, and other physical symptoms. Victims of online fraud reported feelings of shame, embarrassment, social isolation, and loss of self-esteem. Their findings indicate that people who can effectively resonate with the outcomes of data breaches (such as the distress caused by identity theft) are more inclined and intrinsically motivated to acquire more knowledge and education on cybercrime.

Catal et al. (2022) investigated the “affective-cognitive gap” in cybersecurity to identify knowledge gaps in cybersecurity graduates. They identified three key knowledge areas with the largest knowledge gaps: Web and Mobile Security, Security Operations and Incident Management, and differences in the perceived importance between less and more experienced personnel. This implies that only participants with a high level of affective responsiveness were able to internalise and translate this knowledge into meaningful protective behaviour from time to time. In other words, cybercrime awareness is not only about knowledge or facts, but also about their emotional salience. Ahmed et al. (2025), after a systematic literature review of 79 research articles from 2015 to 2024, pointed out an important lacuna in understanding how human tasks in extended reality (a broad term for virtual reality), such as interaction modalities and user interface design, influence task performance and other associated cognitive, psychophysiological outcomes. It implies that the emotional gut feeling associated with affective responsiveness may serve as an early warning system against digital fraud. Empirical literature suggests that, in most cases, the impact of cybercrime on victims is either psychological or financial (Borwell et al., 2021).

Pathological egocentricity and cybercrime awareness

Some empirical studies have identified pathological egocentricity as a primary psychological barrier to cybercrime awareness. Warren Buffet believes that cybercrime is the number one problem with mankind and poses real risks to humans (Mahesh et al., 2022). Mazzeo et al. (2025), who enrolled 202 undergraduate students, found that narcissism was consistently related to cyberbullying and trolling behaviour; they also found that narcissists exhibited trolling behaviour when they had high levels of revenge drivers and were less likely to engage in online bullying if they had lower levels of revenge. A possible explanation is that undergraduate students with high levels of egocentricity were prone to belittle and dismiss cybercrime awareness programs and campaigns at the institution, assuming that they could not be scammed and were immune to scams because of their perceived superior intelligence. Similarly, Naga et al. (2024) enrolled 311 undergraduate students and, in a quantitative survey, found a significant relationship, highlighting the roles of neuroticism and extraversion in increasing susceptibility to online security risks and information security behaviours.

Nzeakor et al. (2022) examined the current trend in cybercrime awareness and its impact on cybercrime vulnerability by recruiting 1104 internet users. They found that awareness of information security was high, and about 2 in 3 participants demonstrated a favourable level of awareness of information security and cybercrime. Further, Nzeakor et al. (2022) found that although most internet users demonstrated awareness of e-theft, hacking, and ATM theft, they were rarely aware of sexually related offences (for instance, sextortion), cyberterrorism, malware attacks, spam emails, and identity theft. To escape from their virtual trauma, victims of cybercrime employed negative coping techniques, such as passivity, alcohol use, and avoidance, which jeopardised their psychological well-being (Pant & Chaubey, 2024).

In synthesising these recent findings, the authors identified a “psychological tug-of-war”: affective responsiveness that drives cybercrime awareness and prosocial digital behaviour, whereas pathological egocentricity acts as a significant impediment (Hudon et al., 2025). In contemporary Nigeria, these traits are further shaped by the socially perceived normalisation of cybercrime, thereby ensuring that the predictive role of these psychological factors is more pronounced in influencing who remains active or vigilant, on the one hand, and who becomes a cyber-victim or an

unmindful accomplice, on the other. Given the varied psychological impact, the researchers investigated the predictive roles of affective responsiveness and pathological egocentricity on cybercrime awareness, as this objective understanding is paramount for navigating and negotiating the complexity of the virtual world. Based on the foregoing, the study proposes that (i) affective responsiveness will significantly predict cybercrime awareness among students to such an extent that those with high levels of affective traits will report high levels of cybercrime awareness, and (ii) pathological egocentricity will significantly predict cybercrime awareness among students to such a degree that students with high levels of pathological egocentricity will exhibit low levels of cybercrime awareness.

Methods

Research design and area of study

The analytical cross-sectional survey design focused on investigating the predictive roles of affective responsiveness and pathological egocentricity on cybercrime awareness. This strategic choice facilitates efficient data collection, enabling a comprehensive understanding of the factors contributing to students' cybercrime awareness. Numerous studies have highlighted the benefits of surveys because they can effectively capture students' perceptions and attitudes toward cyber-related issues and psychological factors (Saunders et al., 2019; Tella & Owolabi, 2017). The purpose of the survey design was to compare outcomes between students with high levels of pathological egocentricity and those with low levels; as well as those with high levels of affective responsiveness and students with low levels in order to identify potential risk factors on cybercrime awareness. At the same time, data were collected at one particular point in time, offering a "snapshot" of the population sampled. Furthermore, the measures of association were examined using the prevalence ratio (PR), and the probability of the outcome between groups affective responsiveness group alone was found to be significant using the generalised linear models of the Poisson distribution and log link function with exponents of the coefficients ($\exp(B)$) of $-.08, p = .049$; implying an outcome prevalence of 0.923. This means the outcome variable in the study (cybercrime awareness) is approximately 7.7 per cent less prevalent in the exposed group (high level of affective responsiveness) compared to the unexposed group (low level of affective responsiveness).

This study, being a quantitative study, was conducted at Topfaith University in Mkpatak in the Essien Udim Local Government Area (LGA) of Akwa Ibom State, South-South Nigeria. Topfaith University was licensed on April 8, 2021. As a private university, it provides a structured academic environment that facilitates research, learning, and socio-cultural interactions. It currently operates with five faculties and 25 programs or departments, and has about 779 students (Records of Topfaith University Matriculation Ceremony Magazine, Vice Chancellor's Address) as at the time of data collection for this study (May, 2025).

The students were largely adolescents or teenagers and are regular internet users. Certain psychological, social and cognitive factors tend to influence their behaviours and decision-making (Ajah et al., 2026; Arnett, 2000). This age group engages with digital technology for academic, social and recreational purposes, which tends to expose them to potential cyber risks. Studies show that young people often have limited awareness of cyber risks and may engage in risky online behaviour due to impulsiveness, naivety, lack of empathy, and manipulateness (Ajah et al., 2026; Bai et al., 2026). Such traits are prevalent among adolescents and young adults (Anderson & Jiang, 2018).

Sample, sampling techniques and eligibility criteria

A total of three hundred and five (305) undergraduate students were recruited in this study, which approximates 50% of the total students in the research area. The sample size (n) would be the unit that makes up the population with an assumed error of 0.05 and within the confidence interval of 95% accuracy. This was realized by utilizing Taro Yamane formula below: $n = \frac{N}{1+N(e)^2}$

Where: n = sample size; N = Population size (779) at the time of the study; e = Sampling error (0.05); using Taro Yamane formula, the sample size was obtained below:

$$n = \frac{779}{1 + 779(0.05)^2}, n = \frac{779}{3.79} = 205.54$$

From the computation above, the overall sample size was 205 participants; however, we overestimated and distributed 320 copies for better generalisation of study findings. Non-probability sampling, specifically purposive sampling, was used to deliberately select participants who met predefined inclusion criteria and who were considered information-rich and appropriate for addressing the research objectives (Maree et al., 2025). In other words, only participants who

met the eligibility requirements were included in the study. The participants were required to meet the following conditions:

University enrollment: respondents had to be undergraduate students of Topfaith University to ensure relevance to the academic setting being studied.

Age range: only students aged 18 years and above were included, as they are legally recognised as adults capable of providing informed consent for research participation. Those under the legal age were required to obtain their parents' or guardians' consent.

Active internet users: respondents were required to be active internet users, particularly those who engage in online interactions, as cybercrime awareness is closely tied to digital activity (Ekong, 2020).

Willingness to participate: only students who voluntarily agreed to participate after they had been informed of the study's purpose and who had signed the informed-consent form were recruited.

Awareness of cybercrime issues: only students who had some prior cybercrime knowledge were enrolled (Bassey & Udoh, 2022).

The study excluded individuals who met the following conditions: mentally unstable to participate and unwilling to participate, as well as students with clinically diagnosed severe mental health conditions or those experiencing adverse life events, particularly those affecting cognitive function, to ensure data validity and ethical research conduct (Bassey & Udoh, 2022).

Procedure

Data collection was conducted between April and May 2025 using self-administered questionnaires distributed to students. Data coding and cleansing were conducted in October 2025. In aiding to mitigate internal biases for the data collected, this survey approach allowed respondents to complete the questionnaires anonymously, promoting honest responses and increasing the response rate. The distribution occurred physically (hard copies) within classrooms or study halls to expand reach and convenience for respondents; thereby ensuring standardised procedure of data collection. In fact, data collectors were unaware of study's outcome status to prevent them from influencing the result by suggesting likely responses to participants. This approach ensures inclusivity and access for all students (Maree et al., 2025; Maree, 2025). Students were informed about the study's purpose, and formally informed consent was obtained to ensure ethical compliance. The researchers also implemented representative sampling by ensuring that virtually all levels of students were recruited in the study. The researchers, with the aid of two research assistants sought the lecturers' permission to administer the questionnaires later, and students were awarded two bonus marks in a particular course in the Beta semester as an incentive to respond to the questionnaires, thereby reducing attrition. A total of three hundred and twenty (320) copies of the questionnaire were distributed; 310 were recovered after a three-week data gathering process. After the data had been collated, coded and cleansed, five unusable copies were discarded. No less than 305 copies were used for data analysis, yielding a return rate of 95.31 per cent.

Measures

The instruments consisted of three sections designed to measure sociodemographic factors, psychopathic personality traits (affective responsiveness and pathological egocentricity), and cybercrime awareness.

Sociodemographics

The sociodemographic section (section A) collected information on age, gender, educational level, socioeconomic background, ever being a victim of cybercrime, frequency of internet use, hours spent online, marital status, and types of cybercrime experienced. This section provides data to explore how demographic factors influence cybercrime awareness.

Affective responsiveness and pathological egocentricity

As to section B, affective responsiveness and pathological egocentricity were measured using the Psychopathic Personality Traits Scale (PPTS) of Boduszek et al. (2016). The PPTS is a self-reported 20-item measure designed to assess psychopathic traits in forensic and non-forensic populations. The scale measures four factors: affective responsiveness (Factor 1), cognitive responsiveness (Factor 2), interpersonal manipulation (Factor 3), and egocentricity (Factor 4). Each subscale consists of five items using *agree* (1) and *disagree* (0) likert scale format (i.e., a trait is either present or absent). Scores range from 0 to 20, and high scores indicate elevated levels of psychopathic personality traits.

The affective responsiveness and pathological egocentricity subscales were used in the present study. The affective responsiveness subscale is made up of items concerning characteristics of low empathy and emotional shallowness, whereas the egocentricity subscale assesses an individual's tendency to focus on their own interests, beliefs, and attitudes. In the present study, Cronbach's alpha value $\alpha = 0.76$ was obtained, indicating very good internal consistency, with a norm score of 34.81. This implied that students with scores of 34.81 and higher were regarded as having psychopathic personalities, and students who scored below the norm were categorized as those with little or no psychopathic personality problems.

Cybercrime awareness

To measure cybercrime awareness, the Cybercrime Awareness Scale (CAS) developed by Arpaci and Ates (2022) was adopted in section C. The CAS is a Likert-type scale that measures individuals' cybercrime awareness. The CAS consists of three dimensions (namely "information systems crimes", "personal data crimes", and "privacy and security") and having a total of 41 items. The first sub-dimension contains items related to the illegal control of an information system. The second sub-dimension includes items related to crimes involving personal data, and the third sub-dimension concerns crimes that violate privacy and security. All items are scored on a five-point scale between "strongly disagree (1)" and "strongly agree (5)". However, for the present study, the 17-item personal data offences dimension of the CAS was utilised, encompassing crimes such as theft, fraud, cyberbullying, privacy violations, and seizure of personal information. These crimes can be committed without being in the same place as the victim. Scale scores ranged from 17 to 85, with higher scores indicating greater cybercrime awareness. Again, a Cronbach's alpha value in the present study was reported as $\alpha = 0.88$ with a norm score of 70.13, implying that scores up to 70.13 and above were categorised as students with a high level of cybercrime awareness, and those below 70.13 were categorized as students with a low level of cybercrime awareness.

Data analysis

The study employed quantitative data analysis to assess the predictive relationships between affective responsiveness, pathological egocentricity, and cybercrime awareness. The analysis, which was conducted in November 2025, also included descriptive statistics (such as means, standard deviations, frequencies, and percentages) and multiple regression, with statistical tests selected to accurately test each research hypothesis. Significance levels (typically $p < 0.05$ - two-tailed) were applied to determine if the hypotheses were to be accepted or not confirmed. Data were analysed with the Statistical Package for the Social Sciences (SPSS) version 25.0 (IBM Corp., Armonk, NY, USA).

Results

The following section presents the data and the results of the data analysis. To test the proposed hypotheses, multiple linear regressions were employed. Detailed results are presented in the data analysis section below.

Table 1 below provides an overview of the demographic features of the recruited respondents, capturing descriptive indices for variables such as age, gender, level of study, socio-economic status, marital status, and so on.

Demographic factors were measured using means, minimums, maximums, frequencies, percentages, and standard deviation from the mean. Further analysis using t-test and one-way ANOVA revealed that no demographic variables reached statistical significance with cybercrime awareness ($p > 0.05$) and were not utilized as covariates.

Table 1. Summary of demographic factors among participants (n = 305)

Demographics	N	(%)
Have you ever been a cyber victim?		
Yes	104	34.1
No	201	65.9
Gender		
Male	123	40.3
Female	182	59.7
Age Mean age = 18.68 (SD: 1.96) Minimum age = 15 Maximum age = 30	305	100
Level of study		
Year 1	107	35.1
Year 2	60	19.7
Year 3	98	32.1
Year 4	40	13.1
Socio-economic status		
Low income (N70,000 and below)	20	6.6
Middle income (N71,000 to N199,000)	34	11.1
High income (N200,000 and above)	251	82.3
Marital Status		
Single	260	85.2
In a relationship	38	12.5
Married	7	2.3
Average Daily Hours Spent online (ADHS)		
Less than 1 hour spent	28	9.2
1-3 hours	108	35.4
4-6 hours	94	30.8
7 hours plus	95	24.6
Total = 305		100%

(Source: Field data, 2025)

The descriptive results in Table 1 indicate that the ages of the 305 undergraduates ranged from 15 to 30 years with a mean age of 18.68 years (SD = 1.96). The gender of respondents indicated that males accounted for 123 (40.3%) and females for 182 (59.7%). When respondents were quizzed on their level of study, descriptive results revealed that 107 (35.1%) were in year one, 60 (19.7%) in year two, 98 (32.1%) in year three, and 40 (13.1%) in year four. The socioeconomic status of respondents' parents was measured, and the results indicated that 251 (82.3%) were from high-income homes, 34 (11.1%) from medium-income homes, and 20 (6.6%) from low-income homes. As to their average daily hours spent online, 108 (35.4%) spent between 1 and 3 hours a day online; 94 (30.8%) spent between 4 and 6 hours a day online; 75 (24.6%) spent 7 hours or more a day online. Only 28 (9.2%) spent less than 1 hour a day online.

Regarding respondents' marital status, 260 (85.2%) were single; 38 (12.5%) were in a relationship but not married; and only 7 (2.3%) were married. When asked whether they had ever been a cyber-victim, 104 (34.1%) responded yes, and 201 (65.9%) said no. Next, the types of crime they were victims of were assessed. The results revealed that cyber fraud topped the list with 41 victims (13.4%), followed by money-doubling schemes/Ponzi with 27 victims (8.9%), black-hat hacking/account take-over with 9 victims (3.0%), and cyber bullying with 8 victims (2.6%). Other crimes included ATM fraud or theft, identity theft/defamation, phishing/vishing, banking fraud/scam, video framing, App savings fraud, and cyber threat.

Test of hypotheses

Table 2 illustrates the regression model for the independent variables (affective responsiveness and pathological egocentricity) and shows how they model the criterion variable (cybercrime awareness) independently and collectively.

Table 2. Summary of regression based on the predictive outcome of affective responsiveness and pathological egocentricity on cybercrime awareness among respondents

Predictors	Cybercrime awareness				
	Model β	t	β eta	P	95% CI
Constant	58.19	16.89	-	.00	[51.41, 64.97]
Affective responsiveness	1.01	5.13	.30	.00	[0.62, 1.40]
Pathological egocentricity	-.31	-2.11	-.12	.00	[-.60, -.02]
R^2	0.081				
F	13.38				
AR^2	0.075				
Sig.	<0.05				

Note: $n = 305$, CI = Confidence Interval; *Significant at the 0.05 level; $R = 0.285$

(Field Data, 2025)

Hypothesis one: Affective responsiveness will significantly predict cybercrime awareness among students, such that those with high levels of affective traits will report high levels of cybercrime awareness.

Table 2 explains the regression model used to examine the empirical and predictive connection between affective responsiveness and pathological egocentricity on cybercrime awareness among selected respondents in this study. To assess the first hypothesis, multiple linear regressions were used to assess the predictive role of affective responsiveness on cybercrime awareness among undergraduate students. Table 2 above shows that affective responsiveness independently predicted cybercrime awareness among respondents ($\beta = .30$; $t = 5.13$; $p < 0.05$). The regression direction showed a direct connection, indicating that higher levels of affective responsiveness were associated with greater cybercrime awareness among respondents. Therefore, the first hypothesis – affective responsiveness will significantly predict cybercrime awareness among students, such that those with high levels of affective traits will report high levels of cybercrime awareness – was confirmed.

Hypothesis two: Pathological egocentricity will significantly predict cybercrime awareness among students; in other words, students with high levels of pathological egocentricity will exhibit low levels of cybercrime awareness.

Table 2 also revealed that pathological egocentricity independently predicted cybercrime awareness among respondents ($\beta = -.12$; $t = -2.11$; $p < 0.05$). The regression direction indicated an inverse connection, suggesting that higher levels of pathological egocentricity are associated with lower levels of cybercrime awareness. Hence, the second hypothesis – pathological egocentricity will significantly predict cybercrime awareness among students; students with a high level of pathological egocentricity will exhibit low levels of cybercrime awareness – was also confirmed. In addition, the results indicated that affective responsiveness and pathological egocentricity yielded a coefficient of multiple correlation (R) of 0.285 and multiple correlation square (R^2) of 0.081, meaning that 8.1% of the variance in cybercrime awareness can be explained by the merged influence of affective responsiveness and pathological egocentricity. Looking at the interplay of predictor variables, a significant joint prediction of cybercrime awareness was observed due to the influence of affective responsiveness and pathological egocentricity, $F(2, 304) = 13.38$, $p < 0.05$ level of significance.

Discussion

Building on existing research on cybercrime awareness and affective egocentrism, this study examined the predictive impact of affective responsiveness and pathological egocentrism on cybercrime awareness among students at a Nigerian university. Because digital evidence on the internet, cloud services and social media platforms can be vast and diverse, and because it provides valuable insights into online activities and communications that are important in tackling cybercrime in the criminal justice system, there was a need to theoretically justify the importance of this study (Jordaan, 2024). The study was grounded in the cognitive dissonance theory (Festinger, 1957), which suggests that people feel uneasy when they hold conflicting beliefs, values, or attitudes. Their dissonance can prompt them to act to alleviate it, which helps us understand how individuals interpret their online experiences and make choices in digital spaces. The study's findings largely support the validity of this theoretical framework.

Affective responsiveness significantly predicted cybercrime awareness among students: those with high levels of affective traits reported higher levels of cybercrime awareness, and vice versa. This finding aligned with a previous study that found that undergraduates who scored high in affective responsiveness were more likely to follow MFA protocols. In other words, students who can effectively resonate with the outcomes of cyber fraud or identity theft are intrinsically motivated to educate themselves on cybercrime (Gautam & Yadav, 2026; Naga et al., 2024). This finding was also consistent with those of Catal et al. (2022), who discovered that cybersecurity graduates with a high level of affective responsiveness could internalise cybersecurity knowledge and translate it into meaningful protective online behaviour.

The following factors may explain the significant difference in cybercrime awareness scores between students with high and low affective components. First, the emotional shallowness and low empathy of those reporting affective responsiveness might have made them feel pressured and overwhelmed, thereby showing the ripple effects in superficial feelings and their inability to connect with others due to past or ongoing identity crises and insecurities. In this state, they may impulsively feel an urgent need to expand their knowledge base on existential matters that are in vogue in their environment, so as not to experience further abuse, neglect, or harm that cybercrime may inflict on its victims. Second, this finding suggests that the emotional component of empathy is enough to promote one's mental readiness to safeguard oneself from cybercrime, thereby supporting the cognitive dissonance theory and previous studies that demonstrate the positive effects of the relationship between university students' affective responsiveness and cybercrime awareness of (Ahmed et al., 2025; Borwell et al., 2021).

Additional results revealed an inverse predictive relationship between cybercrime awareness scores and pathological egocentricity. Hence, the second hypothesis, which stated that pathological egocentricity will significantly predict cybercrime awareness among students, such that students with a high level of pathological egocentricity will exhibit low levels of cybercrime awareness, was supported. Similarly, the second outcome of this study mirrored the study of Naga et al. (2024), who proved significant relationships highlighting the roles of neuroticism and extraversion in increasing susceptibility to security risks and information security behaviour, implying that students with egocentric traits may view security rules and regulations as unnecessary instead of imbibing and applying protective measures.

A probable explanation of this finding stems from the fact that when young people focus more on things pertaining to their self-interest and belief system and exhibit a lack of perspective-taking with work and life in general, they tend to be blind to the red flags that would have alerted them to the schemes fraudsters and online schemers resort to. Conversely, when they focus less on subjective matters and think more about others, they will inevitably have access to information that will aid them and eventually protect them from falling victim to cybercrime prevalent in cyberspace today. As emotion-focused coping strategies, these traits play a crucial role in adaptive coping, helping individuals maintain a positive outlook amid the heightened cybercrime threat. Previous research on university students has shown

that planning for the unknown and being hopeful about the best possible outcome not only enable individuals to adapt to adversity (Laranjeira & Querido, 2022) but also enhance their mental well-being (Counted et al., 2022; Tsai & Morissette, 2022). Interactively, the results indicated that affective responsiveness and pathological egocentricity jointly predicted cybercrime awareness, accounting for 8.1 per cent of the variance in cybercrime awareness.

Implications for practice

This article's findings have significant implications for educators, mental health professionals, and researchers. For educators in criminal justice and psychology departments, the results suggest that intentionally integrating psychopathic traits improves affective responsiveness. Secondly, reducing egocentricity in cybercrime awareness efforts will go a long way in addressing the cybercrime problem. These traits can be integrated into educational and research intervention programs, and, if mastered, can help students identify and apply innate psychological traits to reduce their proneness to becoming victims of cybercrime and to promote personal growth and well-being. Such programs can foster a healthier and more resilient mindset by encouraging students to focus on their cognitive strengths rather than their perceived weaknesses and inherent vulnerabilities.

For mental health professionals, this study highlights the importance of incorporating skills to enhance affective responsiveness and reduce egocentric tendencies in counselling sessions. Encouraging clients to create an affective-egocentric inventory to prevent cybercrime, overcome life cybercrime challenges, and improve their overall well-being. This approach could help them break free from depressive dissonance after being scammed or defrauded, form positive thought patterns, and develop key personality traits, ultimately boosting their confidence for future virtual engagements.

The article's results highlighted the psychopathic personality traits that expose and, at the same time, can help Nigerian university students navigate online challenges, foster relational growth, and enhance their academic pursuits and overall well-being. As a result, researchers can develop activities to raise students' cybercrime awareness on university campuses, as well as interventions targeting these psychopathic personality traits in future studies to improve students' cognitive abilities and overall psychological well-being. This study also adds to existing literature by providing additional insights into the psychopathic impact of cybercrime on people's well-being. Therefore, our article's findings suggest that curriculum should include the grooming of personality traits linked to affective responsiveness and egocentricity among university students. Additionally, researchers are encouraged to gain a more comprehensive and up-to-date understanding of other constructs that may predict cybercrime awareness, protect university students from fast-evolving online scams and cyber-fraud, and help them achieve their personal, academic, and mental health goals.

Limitations and opportunities for future studies

This study has two limitations. First, because it is a cross-sectional survey (though analytical in nature) and because it was conducted at a single university, the generalisability of the findings to a broader population of Nigerian university students may be problematic. Future studies should employ a qualitative or longitudinal design and recruit participants from other universities (public universities or those from different religions) in other geopolitical zones of Nigeria such as South-east, South-west and Northern regions to obtain more diverse and reliable results. Second, because cybercrime is a sensitive topic that can make people hide their feelings (Ajah et al., 2026), the possibility of social desirability bias cannot be ruled out. Since people want to make a good impression on others, they may under- or over-report their experiences in surveys. Future research should consider administering reverse-phrased questions, using more online surveys, building more rapport, and utilising forced-choice items to gather data.

Conclusion

To the best of the researchers' knowledge, this study is the first to investigate the predictive impact of affective responsiveness and pathological egocentricity on cybercrime awareness in a Nigerian university. Affective responsiveness had a significant effect on cybercrime awareness scores. Additionally, the study highlights an inverse relationship of pathological egocentricity in the regression model. It lays the foundation for enhancing students' cybercrime awareness at Nigerian university campuses, emphasising the urgent need for support systems, such as social support, tailored counselling, and mentoring, to help undergraduate students cope with the affective-egocentric impacts of cybercrime.

The reason for this is that the rapid evolution of the internet has transformed modern life, enabling unprecedented connectivity, commerce, and communication. Yet, the rapid pace of technological development has also created fertile ground for cybercriminals, who exploit vulnerabilities faster than lawmakers, institutions and individuals, including

vulnerable students, can foresee. Regrettably, as internet usage has become routine for billions of people worldwide, cybercrime has also emerged as one of the most pressing challenges of the digital era, affecting students, individuals, organisations, and governments alike. Hence, cybercrime is an evolving and multifaceted threat that mirrors the rapid expansion of digital technologies. Its financial, psychological, and societal impacts are profound, and its global nature makes it challenging to combat. Therefore, in the digital age, cybercrime awareness is not only a defensive measure but also a necessity for safeguarding individuals, organisations, and nations. In order to mitigate internal biases of data collected which served as the vehicle of study findings, the researchers employed some empirical steps namely, gathering data from varied demographic backgrounds, working with the data without knowing the source or expected results (blind data processing), properly training of research assistants who helped in collecting data (standardised data collection), and in ensuring that every participant had an equal chance of being selected in the sampling technique employed.

Declarations

Funding: The authors received publication grant for this work from the University of South Africa but received no financial support from any institution for conducting the survey in this study.

Ethical Approval: Ethical approval was obtained from the Research and Ethics Committee (REC) of Topfaith University, Akwa Ibom State, Nigeria, with certificate reference number TUM25-RECNO-IN001 in accordance with the Belmont Report of 1979 and Declaration of Helsinki (DoH) by the World Medical Association of 1964.

Informed Consent: Informed consent was signed by respondents and obtained through a formal letter attached to the first page of the administered instruments.

Statement Regarding Research Involving Human Participants and/or Animals: Participants were properly briefed about the nature of the study and informed that there would be no consequences for not having to participate or for withdrawing at any point during the survey.

Consent to Publish: The authors affirm that research participants provided informed consent for publication of the information in Table(s) 1, and 2 which were produced in aggregate and showing no individualised data.

Author's Contribution: David Okanandu Iloma (DOI): Study conceptualization, methodology, and theoretical framework, reliability of instruments, data gathering, references, data analysis and interpretation. Juanida Horne (JH): General overview, discussion, supervision, proofreading and organization of the study. All authors duly read and approved the final version of the manuscript for publication.

Competing Interests: The authors do not have any conflicts of interest to report.

Data Availability: The data supporting the findings are presented in quantitative form, do not contain participants' personal details, and authors affirm that the data guiding the outcome of this study will be made available from the lead author in a software spreadsheet format upon reasonable demand.

Use of AI Services: Artificial intelligence (AI) was not used in this study. However, the manuscript underwent language editing which utilises an aspect of AI. This does not in any change the original contextual idea of the authors but rather helped in enhancing the grammatical structure of the manuscript (assistive AI use).

Acknowledgments

We express our appreciation to the Department of Police Practice, University of South Africa, for their support with the space and conducive environment provided the lead author to collate, analyse and interpret the data which produced this manuscript as well as thanking the University of South Africa for providing the funding that enabled the article processing charge (APC) for this work. We would also like to express our gratitude to Mr. Enwongo-Abasi Ita Ana for formally permitting his project supervisor at Topfaith University (Dr. David Okanandu Iloma, 2024/2025 academic session) to make use of the project data in the current study.

References

1. Ajah, B. O., Onyejebu, D. C., Isife, C. T., Enweonwu, O. A., Chinweze, U. C., Anyadike, N. O., Ilo, K. O., Omaliko, J. C., Asadu, N., Ugwu, C. C. O., Okemini, O. O., Chukwuemeka, L. K., Ohabuenyi, J., Uzoigwe, C. O., Iloma, D. O., Madubuko, J. C., & Ngwu, G. E. (2026). Narrative accounts, feelings, and perceptions of yahoo-plus offenders in Enugu and Abakaliki correctional centers, Nigeria. *International Journal of Law, Crime and Justice*, 84, 100823, 1-12. <https://doi.org/10.1016/j.ijlcj.2025.100823>
2. Ahmed, N., Wu, P., Huang, K., Jung, S., Rheem, H., Tan, G., Imani, M., & Islam, R. (2025). Human task performance and associated internal states in extended reality: A systematic review of cognitive, psychophysiological, and physiological dimensions. *Frontiers in Virtual Reality*, 6:1589256, 1-18. <https://doi: 10.3389/frvir.2025.1589256>
3. Anderson, M., & Jiang, J. (2018). Teens, Social Media & Technology. Pew Research Center. <https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018>
4. Arnett, J. J. (2000). Emerging adulthood: A theory of development from the late teens through the twenties. *American Psychologist*, 55(5), 469-480.
5. Arpaci, I., & Ates, E. (2022). Development of the cybercrime awareness scale (CAS): A validity and reliability study in a Turkish sample. *Online Information Review*, 1-12. <https://doi 10.1108/OIR-01-2022-0023>
6. Bai, J., Ho, M-H., Sung, H-T., Hung, C-S., & Tsai, J-H. (2026). Mental health and psychosocial sequelae of fraud victimization: A systematic review. *Frontiers in Psychology*, 17:1805536. <https://doi: 10.3389/fpsyg.2026.1805536>
7. Bassey, E. A., & Udoh, I. M. (2022). Cybersecurity awareness and risk perception among Nigerian university students. *Journal of Digital Society Studies*, 14(2), 77-92.
8. Boduszek, D., Debowska, A., Dhingra, K., & DeLisi, M. (2016). Introduction and validation of the Psychopathic Personality Traits Scale (PPTS) in a large prison sample. *Journal of Criminal Justice*, 46(3), 9-17. <https://doi:10.1016/j.jcrimjus.2016.02.004>
9. Borwell, J., Jansen, J., & Stol, W. (2021). The psychological and financial impact of cybercrime victimization: A novel application of the Shattered Assumptions Theory. *Social Science Computer Review*, 40(4), 933-954. <https://doi:10.1177/0894439320983828>
10. Buono, L., 2014, June. Fighting cybercrime through prevention, outreach and awareness raising. In *ERA Forum* (Vol. 15, No. 1, pp. 1-8). Berlin/Heidelberg: Springer Berlin Heidelberg.
11. Catal, C., Ozcan, A., Donmez, E., & Kasif, A. (2022). Analysis of cyber security knowledge gaps based on cyber security body of knowledge. *Education and Information Technologies*, 28, 1809-1831. <https://doi.org/10.1007/s10639-022-11261-8>
12. Counted, V., Pargament, K. I., Bechara, A. O., Joynt, S., & Cowden, R. G. (2022). Hope and well-being in vulnerable contexts during the COVID-19 pandemic: Does religious coping matter? *The Journal of Positive Psychology*, 17(1), 70-81. <https://doi.org/10.1080/17439760.2020.1832247>
13. Ekong, U. J. (2020). Internet penetration and digital literacy among students in Nigerian tertiary institutions. *West African Technology Review*, 11(3), 101-118.
14. Festinger, L. (1957). *A Theory of Cognitive Dissonance*. Stanford University Press.
15. Garbaa, A. A., Sirajb, M. M., Othman, S. H., & Zogaan, W. A. (2021). Cybersecurity awareness of university students in Nigeria: Analysis approach. *Turkish Journal of Computer and Mathematics Education*, 12(12), 3739-3752.
16. Gautam, R., & Yadav, S. (2026). Psychological impact of cyber-crime on victims. *Current Psychology*, 45(3), 24-36. <https://doi.org/10.1007/s12144-025-08873-x>
17. Harmon-Jones, E., & Mills, J. (1999). An introduction to cognitive dissonance theory: A review of the influences on attitudes and beliefs. *Psychological Bulletin*.
18. Hudon, A., Harvey, E., Nicolas, S., Dufour, M., Guerin-Therriault, C., Berube-Fortin, J., Combey, I., Yue, Y. C., Perreault, A., Borduas Page, S., & MacDermott, V. (2025). Cyberpsychopathy: A multidimensional framework for understanding psychopathic traits in digital environments. *European Journal of Investigation in Health, Psychology and Education*, 15(6), 107-126. <https://doi.org/10.3390/ejihpe15060107>
19. IBM. 2025. Cost of Data Breach Report 2025. Available at: <https://www.ibm.com/reports/data-breach>. (Accessed 18 February 2026).

20. Jordaan, J. (2024). Digital forensics. In Benson, B., Cooper, A., Naidoo, Y., Dintwe, S., Horne, J., Jones, G., Jordaan, J., Labuschangne, G., Lochner, H., Manamela, M., Mokwena, R., Schmitz, P., Smith, J., Stanley, B., van der Watt, M., van Graan, J., van Niekerk, T., & R. Zinn (Eds.), *Forensic Investigation: Legislative principles and investigative practice* (pp. 501–553). Juta and Company (Pty) Ltd. ISBN: 978 1 48515 261 3.
21. Laranjeira, C., & Querido, A. (2022). Hope and optimism as an opportunity to improve the “positive mental health” demand. *Frontiers in Psychology*, 13, 827320. <https://doi.org/10.3389/fpsyg.2022.827320>
22. Mahesh, K. M., Aithal, P. S., & Sharma, K. R. S. (2022). Open Network for Digital Commerce -ONDC (E-Commerce) Infrastructure: To Promote SME/ MSME Sector for Inclusive and Sustainable Digital Economic Growth. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, 7(2), 320-340. <https://doi.org/10.5281/zenodo.7141841>
23. Maree, K., Rajab & Pietersen, J. (2025). Surveys and the use of questionnaires (pp. 242-255). In Maree, K. (Ed.). *First steps in research*. 4th edition. Pretoria: Van Schaik Publishers. (Page 222).
24. Maree, K. (2025). *First steps in research*. 4th edition. Pretoria: Van Schaik Publishers.
25. Mazzeo, O., La Selva, G., Longo, M., & Monacis, L. (2025). Narcissism between cold-blooded and hot-headed characters in toxic online behaviors: The moderating role of the R4 functional drivers. *Frontiers in Psychology*, 16:1562635. <https://doi.org/10.3389/fpsyg.2025.1562635>
26. Mokha, A. K. (2017). A study on awareness of cybercrime and security. *Research Journal of Humanities and Social Sciences*, 8(4):459-464. <https://doi.org/10.5958/2321-5828.2017.00067.5>
27. Murad, H. A., & Qudah, M. (2025). The attitudes of communicators toward cybersecurity concerning security, safety in national institutions. *Frontiers in Communication*, 1–22, 10:1552520. <https://doi.org/10.3389/fcomm.2025.1552520>
28. Naga, J. F., Tinam-isan, M. A. C., Maluya, M. M. O., Panal, K. A. D., & Tupac, M. T. A. (2024). Investigating the relationship between personality traits and information security awareness. *International Journal of Computing and Digital Systems*, 16(1), 1233-1246. <http://dx.doi.org/10.12785/ijcds/160191>
29. Nzeakor, O. F., Nwokeoma, B. N., Hassan, I., Ajah, B. O., & Okpa, J. T. (2022). Emerging Trends in Cybercrime Awareness in Nigeria. *International Journal of Cybersecurity Intelligence & Cybercrime*: 5(3), 41-67. <https://doi.org/10.52306/2578-3289.1098>
30. O'Sullivan, L., McEwan, T. E., & O'Reilly, N. (2019). Behavioural changes in response to cyber threats: The role of awareness and dissonance. *Cyberpsychology: Journal of Psychosocial Research*, 1-14.
31. Pandey, P., & Kapoor, A. (2025). Cybercrime in the digital era: Impacts, awareness, and strategic solutions for a secure future. *Sachetas*, 4(1), 32-37. <https://doi.org/10.55955/410004>
32. Pant, R. & Chaubey, U. (2024). Protecting Minds in the Digital Age: A Review Based Study on Psychological Impact of Cybercrime. *International Journal of Indian Psychology*, 12(3), 2240-2247. <https://doi.org/10.25215/1203.220>
33. Sarkar, G., & Shukla, S. K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology*, 2, 12-23.
34. Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research Methods for Business Students*. 8th ed. Pearson Education.
35. Sharma, J. (2025). Evaluating the impact of cybercrime awareness: A case study. *International Journal of Innovations in Science Engineering and Management*, 4(3), 59-65. <https://doi.org/10.69968/ijisem.2025v4i359-65>
36. Tella, A., & Owolabi, A. (2017). Cybercrime Awareness among University Students in Nigeria: A Survey. *Journal of Information Technology Policy*, 1, 1-13.
37. Tsai, J., & Morissette, S. B. (2022). Introduction to the special issue: Resilience and perseverance for human flourishing. *Psychological Trauma: Theory, Research, Practice, and Policy*, 14(1), 1-3. <https://doi.org/10.1037/tra0001215>
38. Ugah, J. O., Sunday, O., Obidinma, A., & Ene, O. S. (2025). Cybercrime in developing countries: Negative effects and panacea. *Open Access Library Journal*, 12, 1-19. e13218. <https://doi.org/10.4236/oalib.1113218>
39. Urien, J. (2025). Cognitive dissonance and cyber-fraud behaviour among university students in Nigeria. *Journal of Social Sciences and Humanities*, 10(1), 86-94.
40. Von der Ahe, L. (2022). Mental wellbeing and cybercrime: The psychological impact of cybercrime on the victim. pp. 1-45. (Bachelor's thesis, University of Twente).

Author Biography

Dr David Okanandu Iloma (BSc, MSc, PhD), graduated from Nnamdi Azikiwe University, Awka, where he obtained his bachelor's degree in psychology. He proceeded to Nasarawa State University, Keffi where he earned his master's degree in Forensic and Correctional Psychology. Furthermore, he bagged his PhD in Clinical Psychology at the University of Uyo. Dr. Iloma is also proficient in cyber-security and has taught in the Department of Sociology/Criminology and Security Studies at Topfaith University, Psychology Department at University of Uyo, and is currently a postdoctoral research fellow at the Department of Police Practice, University of South Africa. Dr. Iloma's research interest is in psychological distress and crime prevention, with subspecialty in substance use/abuse, suicidal ideation, social change, LGBTIQ+ community, behavioural addiction, and AI/social media disorders amongst others. Dr. Iloma is also interested in crimes against women and young children (girls and boys alike). He has participated in several local and international conferences, local and international grants, as well as mentoring/coaching programs and community development projects. As a scholar/researcher of multidisciplinary background, licensed clinical psychologist, forensic expert, prolific writer, and seasoned statistical analyst, Dr. Iloma has to his credit, dozens of publications in learned journals or indexed/abstracted in Clarivate Analytics and Scopus/Scimago.

Prof Juanida Horne is a distinguished senior lecturer specialising in Forensic Investigation of Crime within the Department of Police Practice at Unisa. With a remarkable 17-year career in the former South African Air Force Police, she demonstrated exceptional leadership as an officer commander at multiple police stations, amassing extensive expertise in law enforcement and investigative techniques. As a lieutenant colonel, her final assignment was at SO1 System Management, where she held the position of second-in-command in the Northern Military Police Region. Prof Horne's unwavering commitment to education and professional growth is reflected in her qualifications, which encompass a National Diploma in Police Administration, BTech in Policing, MTech in Forensic Investigation, and a DLitt et Phil in Police Science.

In 2011, Prof Horne was honoured with Unisa's Developing Researcher Award. Her body of work includes published articles and co-authorship of a chapter in the book "Forensic Investigation – Legislative Principles and Investigation Practice", co-authorship and editor of the 2nd edition of Forensic Investigation – Legislative Principles and Investigation Practice." Additionally, she has co-authored the books "Investigation: A Comprehensive Guide to the Basic Principles, Procedures and Forensic Processes" and "Forensic Document Examination Techniques Supporting Investigations and Judicial Procedures" which have been published by Juta.

