



Research Article

Psychological and Demographic Predictors of Phishing Susceptibility: A Survey-Based Study of University Users

Aminu Muhammad Auwal^{1*}  and Sulaiman Shehu² 

¹Department of Natural Sciences, University of Jos, Plateau State, Nigeria

²Department of Software Engineering, Bayero University, Kano State, Nigeria

Article Information

Abstract

Article History

Received: 25 June 2026

Revised: 15 July 2026

Accepted: 18 August 2026

Published online: 10 September 2026

Keywords

Phishing Susceptibility
Social Engineering
Human Factors
Cyber Security Awareness
Personality Traits
Impulsivity
Demographic Analysis
Cybercrime Victimization
Online Behavior
Higher Education Security

Correspondence*

i.elameenu@gmail.com

ORCID

Aminu Muhammad Auwal 
<https://orcid.org/0009-0005-1799-7876>
Sulaiman Shehu 
<https://orcid.org/0009-0002-0056-604X>

Phishing remains one of the most effective forms of cybercrime because it exploits human decision-making rather than technical vulnerabilities. Although organizations invest heavily in technical defenses, phishing attacks continue to succeed due to differences in user behavior, psychological traits, and cybersecurity awareness. However, the combined influence of these factors on phishing susceptibility remains insufficiently understood. This paper investigates the joint contribution of impulsivity, self-reported cyber security knowledge, daily social media use, age group, and gender to phishing click rates among university students and staff, using a purpose-built 30-item phishing identification task administered alongside validated psychological and behavioral measures. A cross-sectional, survey-based empirical study was conducted with 412 volunteer participants recruited from a single university. Participants completed a 30-item phishing email identification instrument comprising 16 phishing and 14 legitimate stimuli drawn from documented campaigns, paired with an 8-item impulsivity scale, a 6-item security knowledge scale, and self-report measures of daily social media use, age, and gender. Multiple linear regression and one-way analysis of variance were used as primary analytical methods. Overall detection accuracy averaged 71.4 percent. Impulsivity (standardized beta = 0.29) and security knowledge (standardized beta = 0.21, negative) were the strongest predictors of phishing click rate, jointly accounting for approximately 24 percent of the observed variance. Participants aged 18 to 24 and those reporting over four hours of daily social media use showed the highest click rates. The full regression model explained 31 percent of total variance ($R^2 = 0.31$, $p < 0.001$). Gender was not a significant predictor once the other variables were controlled. Effective phishing awareness programs should be prioritized toward interventions that interrupt impulsive decision-making and address behavioral patterns associated with heavy social media use, rather than relying on broad demographic targeting by age or gender. Technical controls such as DNS and IP-based phishing detection systems (Islam *et al.*, 2023) complement but cannot replace human-centered training. Ethical governance frameworks for information security practice (Blaise *et al.*, 2024) and sustained cybersecurity education in higher education settings (Ravichandran & Rao, 2022; Yaseen, 2022) are jointly necessary to reduce susceptibility at an institutional level.

© 2026 Centre for Research and Innovation (CRI). This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

I. INTRODUCTION

Phishing is the leading technique for initial access in cyber attacks worldwide, consistently accounting for the majority of data breaches catalogued in annual threat intelligence reports. Unlike exploitation-based attacks that target technical vulnerabilities in software or network infrastructure, phishing targets the human recipient directly, making it effective regardless of the strength of an organization's perimeter defenses. A message that

successfully mimics a trusted sender, conveys apparent urgency, and directs a recipient to a plausible-looking credential-harvesting page can compromise even a well-hardened network within seconds of being clicked. Comprehensive taxonomic reviews of phishing attacks have documented how attackers systematically combine deceptive technical artifacts, including spoofed domains, lookalike logos, and manipulated hyperlinks, with social engineering cues designed to trigger specific psychological responses such as fear, authority compliance, curiosity, and anticipated

reward (Alkhalil *et al.*, 2021). Understanding which individuals are most vulnerable to these combined stimuli, and why, is therefore a central question for both security research and organizational risk management.

Criminological and sociological perspectives on cybercrime victimization add important context to purely psychological accounts of phishing susceptibility. Routine activity theory, originally formulated by Cohen and Felson (1979) to explain offline victimization, posits that victimization results from the convergence of a motivated offender, a suitable target, and the absence of capable guardianship. In the online context, capable guardianship encompasses both technical controls, such as spam filters and multi-factor authentication, and behavioral guardianship, including the habits of vigilance that users develop over time. Auwal and Lazarus (2024) extended the criminological framing of victimization to the cyber domain, proposing a preliminary sociological and criminological categorization that distinguishes between victimization types based on the mechanisms of deception and the socioeconomic vulnerabilities of targets. Their subsequent ethnographic research on victims of socio-economic cybercrimes perpetrated by Nigerian Yahoo Boys (Auwal & Lazarus, 2025) demonstrates how organized offender networks exploit not only technical naivety but also social trust, loneliness, and economic aspiration. Phishing, as a mass-scale variant of these targeted social engineering techniques, operates on similar psychological levers, and understanding which psychological and demographic characteristics make individuals most susceptible to these levers is directly relevant to the design of effective countermeasures. Institutional analysis of Nigerian EFCC conviction records further shows that cybercrime enforcement is concentrated around impersonation-based and cyber-affiliated offences (Auwal, 2026d).

The information security ethics literature provides a complementary vantage point. Blaise *et al.*, (2024) identified significant inconsistencies in the ethical frameworks applied by information security professionals when navigating decisions about monitoring, disclosure, and intervention, inconsistencies that can undermine the effectiveness of technically sound security controls by creating gaps in governance and accountability. In higher education settings, where security culture is often underdeveloped relative to corporate environments, these governance gaps are particularly consequential. Yaseen (2022) documented the growing importance of institutional cybersecurity programs in universities, while recent scholarship has reinforced that cybersecurity education must be treated as a cross-cutting institutional priority rather than a peripheral technical function (Ravichandran & Rao, 2022). Technical interventions such as DNS and IP filtering can substantially reduce the volume of phishing messages that reach end users (Islam *et al.*, 2023), but they cannot eliminate the risk entirely, and their effectiveness depends on timely threat intelligence that is not always available for novel or spear-phishing campaigns.

Within the psychological literature, research has consistently linked phishing susceptibility to individual differences in cognitive style, personality, and information processing habits. Email fraud susceptibility studies have shown that recipients who rely on intuitive, rapid-fire processing of messages are significantly more likely to be deceived than those who adopt careful, analytical evaluation (Jones *et al.*, 2019). Complementary work grounded in information processing theory found that habitual, low-elaboration processing of peripheral email cues, rather than a lack of technical knowledge per se, is the dominant predictor of susceptibility (Wang *et al.*, 2011). Research employing personality frameworks has further identified impulsivity and neuroticism as the traits most strongly predictive of phishing click rates, and has demonstrated that training interventions specifically targeting impulsivity can produce measurable reductions in subsequent susceptibility (Islam *et al.*, 2025). These findings collectively suggest that training programs that fail to address underlying cognitive and personality factors may produce limited and short-lived improvements in behavior. Closely related survey evidence on ransomware social-engineering lures likewise identifies workplace time pressure and neuroticism as important risk factors, while conscientiousness and digital self-efficacy showed protective associations (Auwal & Shehu, 2026b).

Demographic factors present a more complex and contested picture. Age has attracted particular attention, but the relationship between age and phishing susceptibility is nonlinear and heavily moderated by cognitive factors. Gavett *et al.*, (2017) demonstrated that executive functioning, rather than chronological age, is the proximate predictor of phishing suspiciousness, with some older adults showing greater detection accuracy than younger participants once cognitive performance is accounted for. This finding challenges the common assumption that older adults are uniformly more vulnerable, and points toward cognitive profiling rather than age banding as a more precise basis for targeted interventions. Social media use has emerged as a potentially important behavioral predictor, with nationally representative panel data from Finland showing that problematic social media use is associated with elevated cybercrime victimization rates over time, independently of conventional demographic controls (Marttila *et al.*, 2021).

Despite these converging lines of research, few empirical studies have simultaneously measured the full range of psychological, demographic, and behavioral predictors of phishing susceptibility within a single sample, using a common validated task as the outcome measure. Most existing studies test two or three predictors in isolation, leaving the relative weights and interactions of these factors poorly characterized. This limitation is consequential for practitioners, who must allocate limited training and intervention resources toward the factors that matter most. The present study addresses this gap by recruiting 412 university students and staff to complete a purpose-built 30-item phishing identification instrument alongside validated

measures of impulsivity, security knowledge, social media use, age, and gender.

The study makes four principal contributions: (i) the design and validation of a 30-item instrument balanced across phishing and legitimate stimuli and across four social engineering cue categories; (ii) an empirical dataset combining behavioral task performance with self-reported psychological and demographic measures from a single sample; (iii) multivariate regression analyses quantifying the independent and joint contributions of each predictor to click rate; and (iv) actionable recommendations for targeted awareness training grounded in the observed predictor profile.

II. LITERATURE REVIEW

A. *Cybercrime Victimization: Sociological and Criminological Foundations*

The academic study of cybercrime victimization has expanded rapidly, yet the dominant frameworks remain grounded in criminological theories developed for offline contexts. Cohen and Felson's (1979) routine activity theory identifies the convergence of motivated offenders, suitable targets, and absent guardians as the necessary conditions for victimization, and subsequent scholarship has adapted these conditions to the online context by identifying digital equivalents of each element: cybercriminal networks as motivated offenders, users with exploitable behavioral routines as suitable targets, and weak technical and behavioral defenses as absent guardians.

Auwal and Lazarus (2024) advanced this theoretical project by proposing a preliminary sociological and criminological framework for categorizing cybercrime victimization that incorporates the socioeconomic vulnerabilities of victims, the organizational sophistication of offender networks, and the role of platform design in creating or mitigating exposure. Their ethnographic work on victims of Yahoo Boys' socioeconomic cybercrimes in Nigeria (Auwal & Lazarus, 2025) provides granular evidence of how these theoretical mechanisms operate in practice: victims are selected and groomed on the basis of inferred psychological vulnerabilities, and offender networks adapt their techniques continuously in response to user behavior and platform changes.

The concept of ideal victimhood, developed within victimology, is also relevant to understanding phishing susceptibility research. Christie (1986) argued that victims are accorded sympathy and recognition in proportion to how closely they approximate the characteristics of an ideal, blameless victim, a conceptualization that has been applied to the online fraud domain with nuanced implications: victims of phishing who are perceived to have acted naively or impulsively may receive less institutional support than those victimized through more technically sophisticated attacks. This framing matters for survey-based susceptibility

research because it shapes the willingness of participants to honestly report susceptibility and past victimization, a source of bias that the present study attempted to mitigate through strict anonymization and ethics approval.

Lifestyle and exposure theories complement routine activity theory by emphasizing that victimization risk is not uniformly distributed across a population but is concentrated among individuals whose behavioral patterns bring them into regular contact with potential offenders. Social media use represents a behavioral lifestyle factor of particular relevance: platforms that incentivize rapid, impulsive engagement with incoming messages, including direct messages, comment notifications, and sharing prompts, may systematically elevate exposure to social engineering attempts embedded within normal platform interactions. Nationally representative panel data from Finland confirm that problematic social media use, defined as habitual and compulsive platform engagement, is associated with elevated cybercrime victimization risk independently of conventional demographic variables (Marttila *et al.*, 2021).

B. *Cognitive and Personality Predictors of Phishing Susceptibility*

The cognitive psychology of phishing susceptibility has been studied through multiple theoretical lenses, all converging on the conclusion that susceptibility is fundamentally a function of information processing style rather than domain knowledge alone. Jones *et al.*, (2019) conducted a controlled experiment in which participants were prompted to evaluate a series of emails under either intuitive or analytical processing conditions, finding that intuitive processing significantly increased susceptibility to deceptive messages while reducing false-positive rates on legitimate messages. This trade-off between susceptibility and selectivity represents a core challenge for training design: interventions that successfully raise analytical processing of incoming email may also produce overly cautious behavior that reduces organizational productivity.

Kleitman *et al.*, (2018) addressed this challenge by developing a 40-item phishing detection task with separate scoring of phishing hits and legitimate false positives, finding that these two outcomes are associated with distinct psychological profiles. High susceptibility to phishing was more strongly predicted by impulsivity and low conscientiousness, while high false-positive rates on legitimate email were more strongly predicted by anxiety and general distrust. This profiling approach enables more targeted training design: impulsive users benefit most from friction-introducing interface modifications that slow the click decision, while overly cautious users benefit from familiarity training on the visual signatures of legitimate institutional communications.

Islam *et al.*, (2025) confirmed the centrality of impulsivity in a more recent study that also identified neuroticism as a significant contributor, and demonstrated that a targeted

psychoeducational intervention addressing impulsivity and emotional reactivity reduced subsequent phishing click rates in a follow-up assessment.

Wang *et al.*, (2011) situated these personality effects within a formal information processing model, showing that habitual low-elaboration processing of peripheral cues, the email equivalent of scanning a message for visual authenticity markers without reading its content carefully, is a stronger predictor of susceptibility than self-assessed computer experience. This finding carries practical implications for training design: programs that emphasize factual knowledge about phishing indicators may have limited impact if they do not also target the processing habits that cause those indicators to be overlooked in the first place. Field evidence from three organizations further indicates that the effectiveness of embedded phishing training varies by lure type and employee engagement (Auwal & Shehu, 2026a).

C. Demographic Factors: Age, Gender, and Social Media Behavior

Age has been studied extensively as a demographic predictor of phishing susceptibility, with inconsistent results. The conventional view that older adults are more vulnerable is not consistently supported by the empirical record. Gavett *et al.*, (2017) demonstrated that executive functioning, which includes working memory capacity, cognitive flexibility, and inhibitory control, mediates the age-susceptibility relationship, with some older participants showing superior detection accuracy relative to younger participants with equivalent cognitive profiles. This finding suggests that age-targeted training programs, which have been widely deployed under the assumption of a simple positive relationship between age and susceptibility, may misallocate resources by ignoring the substantial heterogeneity within age groups. Gender has similarly been examined as a potential predictor, but findings are mixed. Some studies report higher susceptibility among women, others report higher susceptibility among men, and many report no significant gender difference once confounding variables such as role, experience, and information-processing style are controlled. Workplace-based field experiments involving large samples of employees have generally found that organizational role and message framing are more powerful predictors of click behavior than gender (Williams *et al.*, 2018).

This pattern is consistent with the present study's regression findings and with broader critiques in the feminist criminology literature arguing that gender effects on cybercrime vulnerability are often mediated by socioeconomic and contextual factors rather than representing direct effects of gender itself. Social media use has emerged as an important behavioral predictor that complements demographic variables. Chen *et al.*, (2020) examined the effect of prior phishing encounter frequency on subsequent susceptibility, finding a complex pattern in which near-miss experiences, clicks that were detected before credential entry, sometimes reduced subsequent

susceptibility but in other cases produced overconfidence that increased it. The relationship between social media behavioral patterns and phishing susceptibility has been theorized in terms of the habituation effects of rapid-response platform interactions: users who spend extended periods responding quickly to incoming notifications may develop interaction habits that transfer to email, reducing the deliberate evaluation that effective phishing detection requires (Marttila *et al.*, 2021). Evidence on privacy fatigue and ChatGPT adoption among Nigerian higher education users similarly shows how privacy attitudes shape technology use in university populations (Auwal, 2026c).

D. Technical Controls and Ethical Dimensions of Security Practice

Behavioral and psychological interventions do not operate in isolation from the technical environment. DNS and IP filtering systems provide an upstream layer of protection that reduces the volume of phishing messages reaching users, buying time for organizational training programs to achieve behavioral change (Islam *et al.*, 2023). Ontology-based and semantic web approaches to user profiling offer additional possibilities for personalizing security interventions by identifying deviations from established user behavior patterns that may indicate phishing exposure (Ravichandran & Rao, 2022). However, technical detection systems are inherently reactive and depend on accurate, timely threat intelligence that may lag novel or targeted campaigns, particularly those generated using adversarial AI tools that can produce convincing phishing content at unprecedented scale and sophistication (Auwal, 2026b). Analyses of benchmark datasets for cyber attack prediction likewise point to gaps that must be closed before AI-driven defenses can be deployed operationally (Auwal, 2026e). Web application weaknesses such as hidden directories and leaked configuration artifacts add further overlooked pathways that can be combined with phishing-initiated compromise (Auwal, 2025b).

The ethical dimensions of organizational security practice are increasingly recognized as critical determinants of program effectiveness. Blaise *et al.*, (2024) found significant inconsistencies across the ethical frameworks applied by information security professionals, including inconsistencies in how monitoring programs are authorized, how user data collected through simulated phishing campaigns is used, and how disclosure obligations are fulfilled when vulnerabilities are discovered. These inconsistencies undermine the social license that organizations need to conduct simulated phishing campaigns and to deploy monitoring systems that can detect phishing exposure in real time. Research on how students perceive ethical boundaries in AI decision-making also indicates that attitudes toward technology in higher education shift as generative AI adoption grows (Auwal, 2025a).

Internet of Things environments introduce additional ethical and security complexity: Auwal (2025c) documented how IoT deployments in resource-constrained settings create

invisible intrusion pathways and ethical vulnerabilities that compound the risk of phishing-initiated compromise by enabling lateral movement from compromised endpoint devices to connected infrastructure. The intersection of phishing susceptibility research and IoT security is thus not merely theoretical but represents a practical risk escalation pathway that awareness training programs must increasingly address. Experimental work on medical IoT systems has further demonstrated real-time man-in-the-middle attacks against connected devices in low-resource healthcare settings (Auwal, 2025e), and IoT-based telemedicine deployments face technical limitations in remote patient monitoring and secure data transmission (Auwal, 2025d).

III. METHODOLOGY

A. Study Design and Ethical Considerations

This study employed a cross-sectional survey design. Ethical approval was obtained from the university research ethics committee prior to recruitment. All participants provided informed electronic consent and were fully debriefed about the phishing identification nature of the task after completion. Participant data were anonymized at the point of collection and stored on an encrypted, institutional server accessible only to the research team. No personally identifiable information was linked to task performance data. The study complied with the ethical principles governing research involving human participants, including those related to voluntary participation, data protection, and the avoidance of harm. Consistent with the ethical framework literature (Blaise *et al.*, 2024), the design prioritized transparency with participants about the general purpose of the research while preserving the ecological validity of the phishing identification task by not disclosing the specific phishing stimuli in advance.

B. Participants

A total of 412 participants were recruited from a single university through email invitations sent via the institution's mailing lists and through physical posters displayed across university buildings. The sample comprised 256 undergraduate and postgraduate students and 156 members of academic and administrative staff. Participants ranged in age from 18 to 66 years ($M = 29.4$, $SD = 10.8$). Gender distribution was 189 males (45.9 percent), 211 females (51.2 percent), and 12 preferring not to disclose (2.9 percent). All participants reported using email for professional or academic purposes and had internet access at the time of participation. Participants who completed all survey components received a small digital voucher as an incentive.

C. Phishing Detection Instrument

A 30-item phishing email identification instrument was developed following the item profiling methodology introduced by Kleitman *et al.*, (2018). The instrument comprised 16 phishing stimuli and 14 legitimate email

stimuli. Phishing stimuli were adapted from anonymized phishing reports submitted to the university information security office over a 24-month period, supplemented by documented campaigns drawn from publicly available threat intelligence databases, with all organizational identifiers, sender addresses, and logos replaced by neutral placeholder elements. Legitimate stimuli were adapted from real institutional communications, similarly anonymized. Items were deliberately balanced across four social engineering cue categories identified in the phishing attack taxonomy literature (Alkhalil *et al.*, 2021): authority (4 phishing items), urgency (4 phishing items), scarcity (4 phishing items), and curiosity or reward (4 phishing items).

For each item, participants were shown a full-screen screenshot of the email displayed in a standard email client interface and were asked to select one of three actions: (a) click the embedded link or attachment, (b) report the email as suspicious to the IT security desk, or (c) take no action and delete the email. This three-option response format was chosen to capture a richer behavioral profile than binary click or no-click measures, distinguishing between passive avoidance and active reporting, which are treated as qualitatively different security behaviors in organizational security research. The primary outcome variable for regression analyses was phishing click rate, defined as the proportion of the 16 phishing items for which the participant selected action (a).

D. Psychological and Behavioral Measures

Impulsivity was measured using an 8-item self-report scale adapted from established impulsivity measurement instruments in the personality literature. Items assessed tendencies toward rapid decision-making, difficulty resisting immediate impulses, and a preference for acting before thinking, rated on a 5-point Likert scale from strongly disagree to strongly agree. Scale reliability in the present sample was acceptable (Cronbach's $\alpha = 0.81$). Higher total scores indicated greater impulsivity.

Self-reported cyber security knowledge was assessed using a 6-item scale developed for this study covering: recognition of phishing terminology, knowledge of appropriate reporting procedures, familiarity with password hygiene best practices, understanding of software patching, recognition of suspicious email indicators, and awareness of multi-factor authentication. Items were presented as agree or disagree statements. The scale produced a sum score ranging from 0 to 6, with higher scores indicating greater self-reported knowledge. This self-report approach was retained rather than a knowledge test format to capture perceived confidence in security knowledge, which is a distinct behavioral predictor from objectively measured knowledge in the phishing literature (Wang *et al.*, 2011).

Daily social media use was measured by asking participants to estimate the total time they typically spent on social media platforms on an average weekday, entered as a numerical

estimate in hours and minutes and collapsed into three ordinal categories for analysis: low (under 1 hour per day), moderate (1 to 4 hours per day), and high (over 4 hours per day). Age was recorded in years and grouped into four bands (18 to 24, 25 to 34, 35 to 49, and 50 or older) following established groupings in the phishing susceptibility literature (Gavett *et al.*, 2017).

E. Data Analysis

All statistical analyses were conducted using SPSS version 28. Descriptive statistics were computed for all predictor and outcome variables. Pearson correlations were examined among continuous predictors prior to regression to assess multicollinearity; no pair of predictors exceeded $r = 0.41$. Multiple linear regression with simultaneous entry was used to estimate the standardized and unstandardized coefficients for each predictor of phishing click rate. Categorical predictors (social media use category, age group, and gender) were entered as sets of dummy-coded variables. One-way ANOVA with Tukey post hoc tests was used to compare click rates across age groups and social media use categories. The significance threshold was set at $p < 0.05$ for all tests, and effect sizes were reported as partial eta-squared for ANOVA and standardized beta coefficients for regression.

IV. RESULTS

A. Overall Task Performance

Across all 412 participants, mean overall accuracy on the 30-item instrument was 71.4 percent ($SD = 12.3$ percent). Accuracy was higher for legitimate email items ($M = 80.1$ percent, $SD = 14.7$ percent) than for phishing items ($M = 64.2$ percent, $SD = 16.9$ percent), indicating a systematic tendency toward false negatives (failing to detect phishing) rather than false positives (incorrectly flagging legitimate email). The

mean phishing click rate was 0.36 ($SD = 0.21$), indicating that participants clicked approximately 5.8 of the 16 phishing items on average. Reporting rate, the proportion of phishing items for which participants selected the report option, was 0.21 ($SD = 0.14$), and passive avoidance (delete without click or report) accounted for the remaining 0.43 of phishing item responses on average.

B. Click Rate by Demographic and Behavioral Group

Table 1 presents click rates disaggregated by age group, social media use category, and gender. The 18-to-24 age group recorded the highest mean click rate ($M = 0.44$, $SD = 0.20$), followed by a monotonic decline through the 25-to-34 and 35-to-49 groups before a modest increase among participants aged 50 or older ($M = 0.33$, $SD = 0.22$). One-way ANOVA confirmed a significant overall effect of age group on click rate, $F(3, 408) = 6.82$, $p < 0.001$, partial eta-squared = 0.048. Tukey post hoc comparisons revealed that the 18-to-24 group differed significantly from the 35-to-49 group ($p < 0.001$) but not from the 50-or-older group ($p = 0.214$), consistent with the nonlinear age-susceptibility relationship predicted by executive-functioning accounts (Gavett *et al.*, 2017).

Social media use category showed a clear monotonic relationship with click rate, with high-use participants recording nearly twice the click rate of low-use participants. One-way ANOVA confirmed a significant effect, $F(2, 409) = 11.94$, $p < 0.001$, partial eta-squared = 0.055. All pairwise differences between use categories were statistically significant at $p < 0.05$ by Tukey post hoc comparison. Gender differences were in the expected direction (males higher) but did not reach statistical significance ($p = 0.178$), consistent with prior evidence that gender effects on phishing susceptibility are generally weak and may be explained by confounding variables such as social media use patterns and role-based exposure.

TABLE 1 CLICK RATE (PROPORTION OF PHISHING ITEMS CLICKED) BY GROUP

Group	n	M click rate	SD	ANOVA F	p
Age 18 to 24	148	0.44	0.20		
Age 25 to 34	121	0.35	0.19	6.82	< 0.001
Age 35 to 49	97	0.29	0.18		
Age 50 or older	46	0.33	0.22		
Social media: Low (<1 h)	84	0.27	0.17		
Social media: Moderate (1-4 h)	201	0.36	0.20	11.94	< 0.001
Social media: High (>4 h)	127	0.45	0.21		
Male	189	0.38	0.21	1.82	0.178
Female	211	0.34	0.20		

C. Regression Model

The full regression model accounted for 31 percent of the variance in phishing click rate, $R^2 = 0.31$, adjusted $R^2 = 0.30$, $F(7, 404) = 26.0$, $p < 0.001$. Impulsivity was the strongest

individual predictor, with a standardized beta of 0.29 ($p < 0.001$), indicating that a one standard deviation increase in impulsivity score was associated with a 0.041 increase in click rate, equivalent to clicking approximately 0.66 additional phishing items out of 16.

TABLE II MULTIPLE REGRESSION PREDICTING PHISHING CLICK RATE (N = 412)

Predictor	Std. beta	B	SE	t	p	Part. R ²
Impulsivity	0.29	0.041	0.007	5.86	< 0.001	0.078
Security knowledge (neg.)	0.21	0.038	0.009	4.22	< 0.001	0.042
Social media: High vs Low	0.18	0.082	0.023	3.57	0.002	0.030
Social media: Mod vs Low	0.09	0.039	0.021	1.86	0.064	0.008
Age: 18-24 vs 35-49	0.11	0.048	0.023	2.09	0.041	0.011
Age: 50+ vs 35-49	0.07	0.033	0.024	1.38	0.169	0.005
Gender: Male vs Female	0.05	0.022	0.019	1.16	0.247	0.003

Security knowledge showed a comparable effect in the opposite direction, with a standardized beta of 0.21 ($p < 0.001$), indicating that higher self-reported knowledge was associated with meaningfully lower click rates. Together, impulsivity and security knowledge accounted for approximately 24 percent of the total explained variance, roughly double the combined contribution of age group and social media use. The high social media use category (more than 4 hours per day) was a significant predictor relative to the low-use reference category ($p = 0.002$), while the moderate-use category did not reach significance ($p = 0.064$), suggesting a threshold effect in the social media use relationship. Gender and older age groups did not reach significance after controlling for the other predictors.

D. Cue-Level Analysis

Click rates varied across the four social engineering cue categories embedded in the phishing stimuli. Authority-themed items produced the highest mean click rate ($M = 0.48$, $SD = 0.24$), followed by urgency items ($M = 0.38$, $SD = 0.21$), curiosity or reward items ($M = 0.33$, $SD = 0.20$), and scarcity items ($M = 0.28$, $SD = 0.19$). One-way ANOVA confirmed a significant cue-type effect, $F(3, 1644) = 14.7$, $p < 0.001$. Impulsivity scores showed the strongest correlation with authority-cue click rates ($r = 0.39$, $p < 0.001$) and the weakest correlation with scarcity-cue click rates ($r = 0.22$, $p < 0.001$), suggesting that authority-framed messages engage the impulsive processing pathway more effectively than other cue types. Security knowledge scores showed approximately equal negative correlations with click rates across all four cue categories (range $r = 0.24$ to 0.28).

V. DISCUSSION

A. Impulsivity and Security Knowledge as Central Predictors

The dominant role of impulsivity in the regression model is consistent with the broader cognitive science literature on decision-making under uncertainty, which identifies impulsivity as a predisposition to act on the first response generated rather than to evaluate it against alternatives (Jones *et al.*, 2019; Wang *et al.*, 2011). In the phishing context, this means that impulsive users are more likely to click on a message that generates an immediate sense of legitimacy, even when a more careful evaluation would reveal inconsistencies in the sender address, message phrasing, or

embedded link destination. The finding that impulsivity was particularly strongly correlated with authority-cue click rates is theoretically coherent: authority-framed messages activate a well-established compliance heuristic that generates a rapid sense of obligation to act, which impulsive individuals are less likely to override through deliberate evaluation. Prior experimental work supports this interpretation: when participants were prompted to adopt an analytical processing orientation before viewing phishing stimuli, susceptibility to authority-framed messages declined more than susceptibility to other cue types (Jones *et al.*, 2019).

The significant negative effect of security knowledge on click rates, while expected, is noteworthy in its magnitude: a one-unit increase in the knowledge scale (equivalent to correctly endorsing one additional security knowledge item) was associated with a 0.038 reduction in click rate, or approximately 0.6 fewer clicks across the 16 phishing items. However, the relatively moderate correlation between security knowledge and click rate ($r = 0.34$ before regression adjustment), and the fact that knowledge accounted for less variance than impulsivity, caution against relying on knowledge-based training alone. Wang *et al.*, (2011) demonstrated that low-elaboration processing habits can override factual knowledge about phishing indicators: a user who knows intellectually that emails requesting urgent action may be phishing attempts may still click such an email if habitual rapid processing prevents that knowledge from being applied in time. These findings support a training design that combines factual instruction with behavioral friction mechanisms, such as mandatory delays before link clicks or interface prompts that cue analytical review.

B. Social Media Use: A Behavioral Lifestyle Risk Factor

The significant monotonic relationship between social media use category and click rate, and the threshold effect apparent in the regression (high use significant, moderate use not), suggest that the behavioral habits associated with heavy social media use constitute a distinct risk factor rather than a mere correlate of other demographic predictors. This finding is consistent with panel evidence from Finland linking problematic social media use to elevated cybercrime victimization rates over time (Marttila *et al.*, 2021), and extends that finding to the specific mechanism of phishing click behavior in a controlled task setting. The theoretical explanation is plausible: social media platforms are designed

to reward rapid, high-volume engagement with incoming content, including messages from semi-known contacts, promotional content, and unsolicited direct messages. Users who spend more than four hours per day in this interaction regime may develop habitual response patterns that generalize to email, reducing the deliberate processing that phishing detection requires.

For awareness training design, this finding suggests that programs targeting younger students or employees should explicitly address the behavioral patterns associated with heavy platform use rather than treating age as a proxy. Heavy social media users may benefit from specific training on the differences between the interaction norms of social platforms (where clicking links from unknown sources is normalized) and the higher-risk environment of institutional email, where the consequences of a single click can be organizational-level. Cybercrime victimization research has documented that individual embedded in high-exposure online lifestyles face compounding risks across multiple victimization categories (Auwal & Lazarus, 2024, 2025), and phishing susceptibility is likely to be one component of a broader vulnerability profile that training programs should aim to address holistically.

C. Nonlinear Age Effects and Demographic Profiling

The nonlinear age pattern observed in Table I, with the highest click rates among the 18-to-24 group, a nadir in the 35-to-49 group, and a slight rebound among the 50-or-older group, is consistent with the executive-functioning account of age and phishing susceptibility (Gavett *et al.*, 2017). The youngest group likely combines high social media use, lower accumulated institutional experience with suspicious email patterns, and cognitive styles not yet fully matured in executive control. The oldest group's slightly elevated rates relative to the 35-to-49 nadir may reflect age-related changes in inhibitory control, as documented in the neuropsychological literature on aging and decision-making. However, the failure of the 50-or-older versus 35-to-49 contrast to reach significance in regression, and the nonsignificance of the older group relative to the overall model, caution against strong conclusions about older-adult vulnerability in this sample, which may have been insufficiently powered for age-group comparisons at the oldest band ($n = 46$).

D. Technical Controls, Ethical Governance, and Institutional Recommendations

The predictor pattern observed in this study implies a layered response strategy that combines behavioral training with technical controls and institutional governance reform. Technical defenses including DNS and IP filtering (Islam *et al.*, 2023) and ontology-based behavioral monitoring (Ravichandran & Rao, 2022) reduce the volume of phishing stimuli reaching users and provide detection signals when user behavior deviates from established patterns, but they cannot eliminate the residual risk posed by novel, AI-generated, or highly personalized phishing messages (Auwal,

2026b). Awareness training that explicitly targets impulsivity and social media behavioral habits represents the human-layer complement to these technical defenses. The ethical governance of both technical monitoring systems and awareness training programs requires the kind of principled professional framework that Blaise *et al.*, (2024) found to be inconsistently applied in practice. Institutions that deploy phishing simulation campaigns or behavioral monitoring systems without transparent governance risk eroding the institutional trust that makes training programs effective in the first place. Organizational survey evidence on ransomware shows that data exfiltration was the strongest predictor of ransom payment (Auwal & Shehu, 2026c), underscoring the cost of a single successful click, and resource-constrained organizations such as Nigerian SMEs face particular difficulty prioritizing vulnerability management under financial limitations (Auwal & Abiodun, 2025).

In higher education settings specifically, the underdevelopment of security culture noted by Yaseen (2022) and Ravichandran and Rao (2022) implies that institutional investment in cybersecurity awareness must be sustained and systematic rather than episodic. A single training campaign, even if well-designed, is unlikely to produce lasting change in impulsivity-mediated processing habits or in the behavioral patterns associated with heavy social media use. Longitudinal, multi-session programs that track individual progress and adapt content to measured susceptibility profiles are better aligned with the predictor pattern observed in this study than one-off awareness campaigns delivered to an undifferentiated audience. Work on adversarial AI vulnerability in secondary education has likewise identified gaps in cybersecurity competencies and proposed a framework integrating threat recognition, behavioral resilience, critical authentication, and institutional response literacy (Auwal, 2026a).

E. Limitations and Future Work

This study has several limitations that qualify the generalizability of its findings. First, self-reported measures of impulsivity, security knowledge, and social media use may be subject to social desirability bias, particularly in a university setting where participants may be aware of the socially desirable direction of responses on security-related scales. Future work should supplement self-report with objective measures, such as reaction time-based impulsivity assessment and platform-sourced social media usage logs. Second, the sample was drawn from a single university, which limits generalizability to other organizational contexts including corporate, healthcare, and government settings with different role structures and security cultures. Third, the phishing detection task was administered outside participants' normal email environment, which may underestimate in situ susceptibility by removing time pressure, notification distractions, and the multitasking conditions typical of real email processing. Fourth, the cross-sectional design precludes causal inference about the

temporal ordering of predictors and outcomes. Future longitudinal studies that track changes in impulsivity, knowledge, social media use, and phishing click behavior over time would enable stronger causal conclusions and would allow researchers to evaluate the durability of training-induced behavior change. The emergence of adversarial AI tools capable of generating convincing personalized phishing messages at scale (Auwal, 2026b) represents a further challenge for future research: susceptibility instruments calibrated against known phishing templates may systematically underestimate vulnerability to AI-generated campaigns that closely mimic trusted correspondents and institutional communications.

VI. CONCLUSION

This paper presented a survey-based study of 412 university participants combining a purpose-built 30-item phishing detection task with validated measures of impulsivity, security knowledge, daily social media use, age, and gender. The principal findings are that impulsivity and security knowledge are the strongest predictors of phishing click rate, jointly accounting for approximately 24 percent of the observed variance, that heavy social media use (over 4 hours per day) is an independent behavioral risk factor, and that age shows a nonlinear relationship with susceptibility that is better explained by underlying cognitive factors than by chronological age per se. Gender does not significantly predict click rates once these other factors are controlled. These findings imply that effective phishing awareness programs should prioritize behavioral and cognitive interventions targeting impulsive decision-making and heavy platform exposure, rather than relying on broad demographic targeting by age or gender alone. Technical defenses including DNS and IP filtering (Islam *et al.*, 2023) and ontology-based profiling (Ravichandran & Rao, 2022) should be deployed alongside behavioral training, and the ethical governance of organizational security programs should conform to principled professional frameworks (Blaise *et al.*, 2024) that maintain institutional trust and transparency. Sustained cybersecurity education in higher education institutions (Ravichandran & Rao, 2022; Yaseen, 2022) is a prerequisite for any training program to achieve lasting population-level reductions in phishing susceptibility. Future research should extend this design to longitudinal and organizational field settings, incorporate objective behavioral measures, and examine susceptibility to AI-generated phishing stimuli, which represent the next frontier of social engineering risk (Auwal, 2025c, 2026b).

ACKNOWLEDGEMENT

The authors thank the university information security office for providing anonymized phishing report samples used in constructing the detection instrument, and all student and staff volunteers who participated in and pilot-tested the survey.

Declaration of Conflicting Interests

The authors declare no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

Use of Artificial Intelligence (AI)-Assisted Technology for Manuscript Preparation

The author(s) utilised generative AI technologies solely to improve language clarity and refine grammar. No images were generated, manipulated, or altered using AI-assisted technologies

REFERENCES

- Auwal, A. M. (2025a). Autonomy versus algorithm: A replication study of student perspectives on AI ethical boundaries. *International Journal of Educational Technology in Higher Education*, 22, Article 72. <https://doi.org/10.1186/s41239-025-00570-w>.
- Auwal, A. M. (2025b). Directory brute-forcing and artifact exposure: Qualitative insight into underestimated threats to web application security. *Asian Journal of Engineering and Applied Technology*, 14(1), 24–32. <https://doi.org/10.70112/ajeat-2025.14.1.4296>.
- Auwal, A. M. (2025c). Invisible intrusions, internal threats and ethical vulnerabilities in Nigeria's Internet of Things. *Discover Internet of Things*, 5, Article 128. <https://doi.org/10.1007/s43926-025-00251-0>.
- Auwal, A. M. (2025d). IoT integration in telemedicine: Investigating remote patient monitoring and data transmission reliability [Preprint]. *Research Square*. <https://doi.org/10.21203/rs.3.rs-3419693/v1>.
- Auwal, A. M. (2025e). Smart medical IoT security vulnerabilities: Real-time MITM attack analysis and lightweight encryption deployment [Preprint]. *arXiv*. <https://doi.org/10.48550/arXiv.2510.09629>.
- Auwal, A. M. (2026a). Adversarial AI vulnerability in secondary education: Threats and cybersecurity competencies. In *Secondary education: Contemporary issues, practices, and future directions*. IntechOpen. <https://doi.org/10.5772/intechopen.1016684>.
- Auwal, A. M. (2026b). Adversarial threat modeling in generative AI: A systematic mapping of attack vectors to defense mechanisms. *AI Ethics*, 6, Article 284. <https://doi.org/10.1007/s43681-026-01154-8>.
- Auwal, A. M. (2026c). A cross cultural extension study on privacy fatigue and AI adoption behavioral model. *Discover Education*. <https://doi.org/10.1007/s44217-026-01903-1>.
- Auwal, A. M. (2026d). Institutional typology of cybercrime enforcement in Nigeria using EFCC conviction records. *Discover Data*, 4, Article 19. <https://doi.org/10.1007/s44248-026-00115-0>.
- Auwal, A. M. (2026e). Operationalizing cyber attack prediction: A gap-prioritized framework with dataset and model selection guidelines [Preprint]. *arXiv*. <https://doi.org/10.48550/arXiv.2606.03386>.
- Auwal, A. M., & Abiodun, J. O. (2025). A sectoral study of cyber threats and vulnerability management in resource-constrained Nigerian SMEs. *Asian Journal of Engineering and Applied Technology*, 14(1), 33–38. <https://doi.org/10.70112/ajeat-2025.14.1.4297>.
- Auwal, A. M., & Lazarus, S. (2024). Sociological and criminological research of victimization issues: Preliminary stage and new sphere of cybercrime categorization. *Journal of Digital Technologies and Law*, 2(4), 915–942. <https://doi.org/10.21202/jdtl.2024.44>.
- Auwal, A. M., & Lazarus, S. (2025). Experiences of local victims of Yahoo Boys' socio-economic cybercrimes in Nigeria. *Discover Psychology*, 5, Article 161. <https://doi.org/10.1007/s44202-025-00479-5>.
- Auwal, A. M., & Shehu, S. (2026a). Measuring the impact of embedded phishing training on ransomware-lure click behavior: A field study across three organizations. *Asian Journal of Science and Applied Technology*, 15(1), 47–54. <https://doi.org/10.70112/ajsat-2026.15.1.4350>.
- Auwal, A. M., & Shehu, S. (2026b). Psychological, situational, and demographic predictors of susceptibility to ransomware social-engineering lures: A survey study. *NeuroData*, 3. <https://doi.org/10.63688/neurodata2026305>.
- Auwal, A. M., & Shehu, S. (2026c). To pay or not to pay: An organizational survey of ransom payment decision drivers, data exfiltration, and the role of cyber insurance among mid sized organizations. *NeuroData*, 3. <https://doi.org/10.63688/neurodata2026306>.

- Blaise, O. O., Aaron, I., Alfred, U., & Amusa, A. (2024). Evaluating the ethical frameworks of information security professionals: A comparative analysis. *Asian Journal of Computer Science and Technology*, 13(2), 61–66. <https://doi.org/10.70112/ajcst-2024.13.2.4289>.
- Chen, R., Gaia, J., & Rao, H. R. (2020). An examination of the effect of recent phishing encounters on phishing susceptibility. *Decision Support Systems*, 133, Article 113287. <https://doi.org/10.1016/j.dss.2020.113287>.
- Christie, N. (1986). The ideal victim. In E. A. Fattah (Ed.), *From crime policy to victim policy* (pp. 17–30). Palgrave Macmillan.
- Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588–608.
- Gavett, B. E., Zhao, R., John, S. E., Bussell, C. A., Roberts, J. R., & Yue, C. (2017). Phishing suspiciousness in older and younger adults: The role of executive functioning. *PLOS ONE*, 12(2), Article e0171620. <https://doi.org/10.1371/journal.pone.0171620>.
- Islam, A., Rashid, M. M., & Othman, F. (2025). Identifying personality traits associated with phishing susceptibility. *Security Journal*, 38, Article 18. <https://doi.org/10.1057/s41284-025-00466-4>.
- Islam, M. S., Sajjad, M., Hasan, M. M., & Mazumder, M. S. I. (2023). Phishing attack detecting system using DNS and IP filtering. *Asian Journal of Computer Science and Technology*, 12(1), 16–20. <https://doi.org/10.51983/ajcst-2023.12.1.3552>.
- Jones, H. S., Towse, J. N., Race, N., & Harrison, T. (2019). Email fraud: The search for psychological predictors of susceptibility. *PLOS ONE* 14(1), Article e0209684. <https://doi.org/10.1371/journal.pone.0209684>.
- Kleitman, S., Law, M. K. H., & Kay, J. (2018). It's the deceiver and the receiver: Individual differences in phishing susceptibility and false positives with item profiling. *PLOS ONE*, 13(10), Article e0205089. <https://doi.org/10.1371/journal.pone.0205089>.
- Marttila, E., Koivula, A., & Räsänen, P. (2022). Cybercrime victimization and problematic social media use: Findings from a nationally representative panel study. *American Journal of Criminal Justice*, 47(1), 108–128. <https://doi.org/10.1007/s12103-021-09665-2>.
- Ravichandran, S., & Rao, K. L. N. (2022). Design and development of an advancing web information stockpiling for engraved ontology in user contours. *Asian Journal of Computer Science and Technology*, 11(2), 11–15. <https://doi.org/10.51983/ajcst-2022.11.2.3379>.
- Wang, J., Li, Y., & Rao, H. R. (2011). Testing individual differences in phishing vulnerability within an integrated information processing model. *Decision Support Systems*, 51(3), 576–586. <https://doi.org/10.1016/j.dss.2011.03.002>.
- Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, 120, 1–13. <https://doi.org/10.1016/j.ijhcs.2018.06.004>.
- Yaseen, K. A. Y. (2022). Importance of cybersecurity in the higher education sector. *Asian Journal of Computer Science and Technology*, 11(2), 20–24. <https://doi.org/10.51983/ajcst-2022.11.2.3448>.