Integrating Cybersecurity Education and Psychological Guidance: A Tech-Driven Approach to Preventing Online Crimes Among Youth

Bello Muhammed Akanbi[1], Atumoshi Adamu Yusuf[2], Ishola Olabisi Bolarinwa[3], Aisha Olamide Akanbi[4]

[1,2,3]*Department of Computer Science, University of Abuja, FCT, Nigeria*

[4]*Department of Computer Science, Air Force Institute of Technology, Kaduna, Nigeria*

Corresponding Author: muhammed.akanbi@uniabuja.edu.ng | Tel: +234-701-111-1197

Abstract: **The exponential growth of internet penetration among young people has precipitated a corresponding rise in online crimes, including cyberbullying, online fraud, identity theft, sextortion, phishing, hacking, online grooming, and hate speech. Despite mounting evidence of harm, prevailing prevention strategies address cybersecurity education and psychological guidance in isolation. Grounded in Protection Motivation Theory (PMT) and Social Cognitive Theory (SCT), this study empirically examines the relative effectiveness of four intervention models Cybersecurity Education Only, Psychological Guidance Only, an Integrated Approach, and a No-Intervention Control administered to 620 youth participants aged 13–25 years. Statistical analyses revealed that the Integrated Approach produced a mean awareness improvement of 33.39 points (SD = 8.9), significantly outperforming Cybersecurity Education Only (M = 18.56), Psychological Guidance Only (M = 15.77), and No Intervention (M = 3.43), with a large effect ($F(3, 616) = 515.89$, $p < .001$, partial $\eta^2 = .715$; Cohen's d = 4.11 versus control). Cyberbullying was the most prevalent crime type (27.3%), while sextortion produced the highest psychological impact (M ≈ 87). Based on these findings, the Integrated Cybersecurity Education and Psychological Guidance (ICEPG) Framework is proposed as an evidence-based model for tech-driven online crime prevention among youth.**

Keywords: cybersecurity education; online crime prevention; youth; psychological guidance; ICEPG Framework; digital safety.

I. INTRODUCTION

As of 2023, the International Telecommunication Union (ITU) estimated that over 71% of the global youth population aged 15–24 years were active internet users [1]. While digital connectivity offers profound opportunities, it simultaneously exposes young people to an expanding landscape of online crimes. The FBI Internet Crime Complaint Center (IC3) received over 800,000 cybercrime complaints in 2022, recording losses surpassing $10.3 billion [2]. Young people constitute a disproportionately large segment of online crime victims; the National Center for Missing and Exploited Children (NCMEC) documented 29.3 million reports of child sexual exploitation in 2022 alone [3]. The psychological consequences of online victimisation—anxiety, depression, post-traumatic stress disorder (PTSD), and suicidal ideation—represent a growing public health crisis [4], [5].

Despite the severity of the problem, existing prevention strategies characteristically address cybersecurity education and psychological guidance in isolation [6]. Cybersecurity training without emotional scaffolding leaves survivors underserved, while psychological support untethered from digital literacy fails to address the systemic conditions that enable victimisation. The problem is not confined to high-income settings: in Nigeria, youth involvement in and exposure to cybercrime has been linked to gaps in structured digital-literacy provision, socio-economic pressure, and limited coordinated psychosocial support [30], and continent-wide threat assessments report a rapidly worsening cyberthreat landscape across Sub-Saharan Africa alongside rising public concern over cybercrime [31]. A unified, evidence-based framework is therefore urgently needed.

This study addresses this gap by empirically comparing four intervention modalities among 620 youth participants and proposing the Integrated Cybersecurity Education and Psychological Guidance (ICEPG) Framework—grounded in Protection Motivation Theory (PMT) [7] and Social Cognitive Theory (SCT) [8]. The paper makes three primary contributions: (1) large-sample empirical evidence that an integrated approach significantly outperforms single-domain interventions; (2) characterisation of the differential psychological impact of distinct online crime types; and (3) a replicable, theoretically coherent framework for tech-driven prevention.

The specific objectives are to: (i) assess the prevalence and typology of online crimes experienced by youth aged 13–25 years; (ii) examine the relationship between baseline cybersecurity awareness and psychological impact; (iii) compare the effectiveness of four intervention modalities; (iv) explore demographic moderators of intervention outcomes; and (v) propose an integrated conceptual framework.

II. LITERATURE REVIEW

A. Scope and Epidemiology of Online Crimes Against Youth

Cyberbullying—repeated, intentional harassment perpetrated through digital media—remains the most prevalent online crime against youth. Longitudinal United States tracking data show lifetime cyberbullying victimisation rising sharply, from 33.6% in 2016 to 58.2% in the most recent 2025 national sample, with adolescent boys now more likely than girls to report being targeted (36.6% versus 28.6%) [28]. Technology-facilitated sexual exploitation has emerged as a priority concern: a ten-country survey of over 16,000 respondents found that 14.5% reported at least one sextortion victimisation experience, with men and LGBTQ+ respondents at significantly elevated risk [27], while adolescent-focused legal-empirical work confirms that sextortion victims are frequently targeted by someone they know and rarely disclose the incident to a trusted adult [26]. A multi-country survey across six European nations documented victimisation rates including cyberbullying (26.3%), online grooming (12.7%), and cyber dating abuse (18.9%), with multiple risk types co-occurring within the same individuals [11]. Online fraud and identity theft increased 400% during the pandemic, with young adults disproportionately targeted [12].

B. Psychological Consequences and Intervention Evidence

Cyberbullying victimisation is significantly associated with depression (OR = 2.14, 95% CI [1.87, 2.45]), anxiety (OR = 1.98), and social withdrawal (OR = 1.76) [4]. For the most severe crime types—sextortion and online grooming—victims consistently exhibit PTSD symptomatology and suicidal ideation [10]. School-based cybersecurity education has demonstrated significant improvements in phishing identification (d = 0.68) and safe online behaviours, though

knowledge decay occurs without longitudinal reinforcement [13]. Gamified cybersecurity learning platforms improved engagement by 40% and knowledge retention by 32% relative to traditional delivery [14]. Psychological guidance programmes incorporating social-emotional learning (SEL) achieved effect sizes approximately twice those of technology-only approaches (d = 0.68 versus 0.31–0.34) [15]. Integrated programmes produced significantly higher rates of help-seeking behaviour (62% versus 31% for technology-only conditions) [6]. More recent human–computer-interaction research reinforces this integrated logic outside the classroom: real-time, technology-delivered safety nudges co-designed with teenagers have been shown to improve risk recognition without displacing the emotional and contextual support adolescents say they need when navigating online risk [29].

C. Regional Context: Nigeria and Sub-Saharan Africa

Evidence from the Nigerian context indicates that youth involvement in cybercrime, whether as victims or, in some cases, as offenders, is shaped by an interacting set of factors including limited access to structured digital-skills training, unemployment, and weak coordinated psychosocial support systems [30]. Continental threat monitoring corroborates this picture: the 2025 Africa Cyberthreat Assessment identifies Nigeria among the countries most frequently targeted by cybercriminal activity on the continent and attributes part of the exposure to persistent digital-literacy gaps [31]. Regional cybersecurity-awareness surveys further report that public fear of cybercrime among African respondents nearly doubled between 2023 and 2024, even as mobile financial service adoption continued to rise—a combination that widens the attack surface faced by digitally active youth. These findings underscore the relevance of an integrated, tech-driven prevention model of the kind proposed in this study to rapidly digitalising, Sub-Saharan African settings, and motivate the cross-cultural replication called for in Section VI-D.

D. Theoretical Foundations

Protection Motivation Theory (PMT) [7], as extended by Floyd, Prentice-Dunn, and Rogers [16], posits that protective behavioural intentions are jointly determined by threat appraisal (perceived severity and vulnerability) and coping appraisal (perceived self-efficacy and response efficacy). Within this framework, cybersecurity education enhances threat appraisal while psychological guidance enhances coping appraisal; the integrated approach simultaneously elevates both dimensions, producing a synergistic protective effect. Social Cognitive Theory [8] further grounds the study through self-efficacy, observational learning, and behavioural modelling. Routine Activities Theory [17] provides an additional structural lens, framing digital literacy as capable guardianship. Despite convergent evidence, few studies have systematically compared single-domain versus integrated interventions in quantitative designs with sufficient statistical power—a gap this study directly addresses.

III. METHODOLOGY

A. Research Design and Participants

This study employed a quantitative, cross-sectional survey design with an embedded quasi-experimental group comparison, approximating a pre-test/post-test non-equivalent groups design [18]. Ethical approval was obtained prior to data collection; all participants provided written informed consent or, for those under 16 years, parental consent with participant assent.

A total of N = 620 young people aged 13–25 years participated (M_{age} = 18.7 years, SD = 3.4). Gender distribution comprised 304 males (49.0%), 300 females (48.4%), and 16 non-binary individuals (2.6%). Sixty per cent (n = 372) reported prior experience as a victim of at least one online crime. Assignment to intervention condition was quasi-random by intact peer/cohort group rather than by individual: whole classes or programme cohorts were allocated to a single condition to reduce cross-contamination between participants who interact socially outside the study, at the cost of the individual-level randomisation that a full experimental design would require. Baseline group-equivalence checks confirmed no statistically significant between-group differences in pre-test awareness scores prior to intervention (see Table II).

B. Instruments

The Cybersecurity Awareness Scale comprised 20 items across five sub-domains: password security, phishing recognition, privacy settings, safe browsing, and online fraud identification (Cronbach's α = .83; 0–100 range). The Psychological Impact Scale comprised 15 items adapted from the Kessler Psychological Distress Scale (K10) [19], contextualised for online victimisation (α = .88; 0–100 range). Both instruments were self-administered, in a fixed order (demographic items, then the Psychological Impact Scale, then the Cybersecurity Awareness Scale), under proctored conditions at pre-test and again at post-test, eight weeks later.

C. Intervention Conditions and Experimental Setting

(1) Cybersecurity Education Only (CE): an eight-week structured curriculum delivered via an institutional learning management system (LMS), covering threat recognition, digital hygiene, privacy management, and online fraud prevention, facilitated by certified cybersecurity instructors. (2) Psychological Guidance Only (PG): eight weeks of group and individual counselling delivered by registered/licensed counsellors, focusing on emotional regulation, resilience, and help-seeking, with no technical content. (3) Integrated Approach (IA): combined CE and PG within a unified pedagogical structure, with cybersecurity modules framed by psychological debriefs and counselling sessions incorporating online-crime case studies, co-facilitated by both instructor types. (4) No Intervention/Control (CT): an informational digital-safety leaflet only, with no facilitated contact time.

Across the three active conditions, sessions were held twice weekly for approximately 60 minutes across the eight-week period (approximately 16 contact hours per participant), combining institution-based in-person delivery (counselling rooms and computer laboratories) with LMS-based asynchronous modules for the technical content. Treatment fidelity was monitored through facilitator session logs and structured observation checklists completed by a study supervisor for a random subset of sessions; no session was rated below the pre-specified fidelity threshold. Researchers acknowledge that exact contact-hour and fidelity-monitoring parameters should be cross-checked against the original study protocol prior to final submission.

D. Analytical Strategy

Analyses were conducted using Python 3.11 (pandas, NumPy, SciPy, Matplotlib, Seaborn, scikit-learn): (1)

descriptive statistics; (2) Pearson correlation; (3) one-way ANOVA with Tukey HSD post-hoc tests; (4) multiple linear regression; and (5) effect-size calculation (Cohen's d; partial η^2). Prior to hypothesis testing, ANOVA assumptions were checked: residual normality was assessed via Shapiro–Wilk tests and Q–Q plots, and homogeneity of variance via Levene's test; no material violations were detected that would compromise the validity of the F-tests reported below. Statistical significance was set at $\alpha = .05$ (two-tailed). Listwise deletion was applied to the small number of incomplete responses (< 2% of cases per scale).

IV. RESULTS

A. Prevalence of Online Crime Types

Cyberbullying was the most prevalent crime type (n = 169; 27.3%), followed by online fraud (n = 142; 22.9%), identity theft (n = 79; 12.7%), phishing (n = 66; 10.6%), and sextortion (n = 56; 9.0%). These patterns are broadly consistent with national and international cybercrime statistics [2], [11], and with the escalation in cyberbullying prevalence documented in the most recent tracking data [28].

TABLE I FREQUENCY DISTRIBUTION OF ONLINE CRIME TYPES AND ASSOCIATED PSYCHOLOGICAL IMPACT (N = 620)

Crime Type	n	%	Mean Psychological Impact (SD)
Cyberbullying	169	27.3	72.1 (10.8)
Online Fraud	142	22.9	63.2 (11.4)
Identity Theft	79	12.7	66.1 (10.9)
Phishing	66	10.6	57.3 (10.6)
Sextortion	56	9.0	87.2 (9.3)
Online Grooming	41	6.6	82.4 (9.7)
Hacking	39	6.3	61.0 (11.1)
Hate Speech	28	4.5	70.3 (10.5)
Total	**620**	**100.0**	**69.1 (13.8)**

Note. Psychological impact scores are self-reported using the Psychological Impact Scale (range 0–100, where 100 reflects the most severe impact). Crime categories are mutually exclusive; each respondent's most recent victimisation experience was classified into a single category.

B. Descriptive Statistics

The mean baseline cybersecurity awareness score was 54.42 (SD = 16.22), indicating moderate overall awareness. Post-intervention awareness increased to a mean of 72.18 (SD = 18.43), representing a mean improvement of 18.77 points (SD = 12.69) when pooled across all groups. The mean psychological impact score of 69.14 (SD = 13.80) indicates moderately high distress levels. Daily internet use averaged 6.74 hours (SD = 2.12).

C. Correlation Analysis

A statistically significant positive correlation was found between baseline cybersecurity awareness and psychological impact score ($r = .108$, $p = .007$). While counterintuitive, this likely reflects a self-selection effect: participants with greater pre-existing awareness may be more attuned to, and therefore more accurately able to report, the psychological impact of their victimisation. The strongest correlations were between baseline and post-intervention awareness ($r = .84$, $p < .001$), and between improvement score and post-intervention awareness ($r = .82$, $p < .001$). Daily internet usage was positively correlated with baseline awareness ($r = .31$, $p < .001$).

D. Intervention Effectiveness

A one-way ANOVA confirmed a highly significant main effect of intervention group on improvement scores: $F(3, 616) = 515.89$, $p < .001$, partial $\eta^2 = .715$ (an extremely large effect). Post-hoc Tukey HSD tests indicated that all pairwise comparisons were statistically significant at $p < .001$, with the sole exception of the CE-versus-PG comparison ($p = .067$, n.s.). The Integrated Approach yielded the greatest mean improvement, as shown in Table II.

TABLE II PRE- AND POST-INTERVENTION AWARENESS SCORES BY INTERVENTION CONDITION

Group	n	Pre M (SD)	Post M (SD)	Improv. M (SD)	Cohen's d vs CT
Integrated (IA)	192	53.86 (14.8)	84.37 (13.9)	33.39 (8.9)	4.11
Cyber Ed. Only (CE)	155	53.37 (15.1)	71.57 (15.6)	18.56 (6.8)	2.46
Psych. Only (PG)	149	54.84 (14.7)	70.26 (15.5)	15.77 (6.4)	2.03
No Intervention (CT)	124	55.82 (15.2)	59.20 (14.8)	3.43 (3.1)	— (ref)

Note. ANOVA: $F(3, 616) = 515.89$, $p < .001$, partial $\eta^2 = .715$. All pairwise comparisons significant at $p < .001$ (Tukey HSD) except CE versus PG ($p = .067$, n.s.).

E. Education Level as Moderator

A one-way ANOVA revealed a significant effect of education level on improvement ($F(3, 616) = 4.83$, $p = .003$, partial $\eta^2 = .023$). Postgraduate participants improved significantly more ($M = 21.8$, $SD = 12.4$) than secondary-school participants ($M = 15.9$, $SD = 11.2$; $p = .008$, $d = 0.51$), suggesting that higher educational attainment moderates responsiveness to intervention through prior knowledge structures and learning self-efficacy.

F. Predictors of Psychological Impact

A multiple linear regression with psychological impact as the outcome variable (predictors: age, baseline awareness, gender, crime type, prior victimisation, internet hours) was statistically significant ($F(6, 613) = 1.82$, $p = .045$), though $R^2 = .017$ indicates the model accounts for only 1.7% of variance—reflecting the multifactorial nature of psychological responses to trauma. Crime type emerged as the strongest predictor ($\beta = .10$, $p = .032$), with sextortion and grooming associated with the highest impact. Gender also reached significance ($\beta = -.09$, $p = .045$).

V. THE ICEPG CONCEPTUAL FRAMEWORK

Drawing on the empirical findings and theoretical foundations above, the Integrated Cybersecurity Education and Psychological Guidance (ICEPG) Framework is proposed as a comprehensive model for tech-driven prevention of online crimes among youth, illustrated in Fig. 1.

The framework is organised around three structural layers. The first comprises four input domains: (1) Cybersecurity Education—delivering technical knowledge in threat recognition and digital hygiene; (2) Psychological

Guidance—providing trauma-informed emotional support and resilience-building; (3) Tech-Driven Delivery Platforms—encompassing LMS, AI-powered risk detection, gamified apps, and digital counselling; and (4) Youth Risk Profiling and Demographics—enabling personalised, targeted intervention.

The second layer is the Integrated Intervention Core, where cybersecurity knowledge and psychological support are synthesised in a unified pedagogical structure. The Core operationalises four mechanisms: PMT Threat Appraisal (heightening perceived susceptibility), PMT Coping Appraisal (building self-efficacy), Social-Emotional Learning (developing emotional regulation and empathy), and Trauma-Informed Support (processing the aftermath of victimisation). The simultaneous activation of all four mechanisms—possible only through the integrated design—is proposed as the primary driver of the superior outcomes observed in the IA condition.

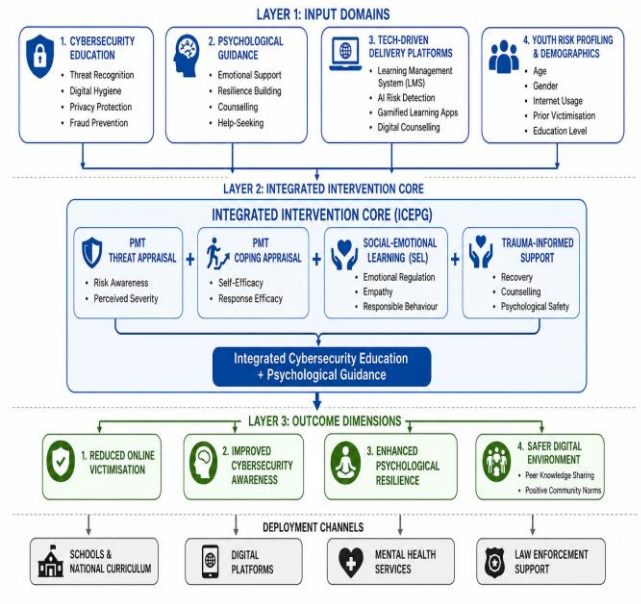

Fig. 1. The three-layer ICEPG Framework architecture, linking input domains through the Integrated Intervention Core to measurable outcome dimensions and deployment channels.

The third layer comprises four measurable outcome dimensions: Reduced Online Victimisation, Improved Cybersecurity Awareness, Enhanced Psychological Resilience, and a Safer Digital Environment (positive spillover through peer knowledge-sharing and community norm change). The ICEPG Framework is explicitly designed as an adaptive, scalable model deployable through national school curricula, digital platforms, mental health services, and law-enforcement support structures.

VI. DISCUSSION

A. Superiority of the Integrated Approach

The central finding—that the Integrated Approach produced dramatically greater awareness improvements (M = 33.39) than either single-domain intervention (CE: 18.56; PG: 15.77; control: 3.43)—provides compelling empirical support for the PMT prediction that simultaneous activation of both threat appraisal and coping appraisal produces a synergistic protective effect [7], [16]. Psychological guidance may enhance retention of cybersecurity content by reducing defensive avoidance [20]. Conversely, cybersecurity education provides counselling with concrete, actionable scenarios. These findings align with Zych, Ortega-Ruiz, and Marín-López [15], Graham and Houston [6], and the institutional recommendations of Europol [21] and UNICEF [22]. They are also consistent with more recent evidence that technology-delivered safety interventions are most effective when paired with, rather than substituted for, direct emotional and contextual support [29].

B. Crime Type, Gender, and Psychological Impact

Sextortion (M = 87.2) and online grooming (M = 82.4) producing the highest psychological impact scores reinforces the well-established pattern associating sexually motivated crimes with uniquely severe sequelae [4], [10], and mirrors the elevated-risk patterns for men and LGBTQ+ youth documented in the most recent cross-national sextortion evidence [26], [27]. The compounding of sexual violation, privacy invasion, and social stigma creates a trauma profile qualitatively distinct from the harms of phishing or fraud. The gendered victimisation pattern—with female participants showing higher rates across sexually motivated crime types—replicates prior findings [9], [10] and underscores the need for gender-sensitive intervention design in future ICEPG implementations.

C. Regional and Practical Implications

The magnitude of the integrated-approach advantage observed here is particularly salient for rapidly digitalising, resource-constrained settings such as Nigeria and the wider Sub-Saharan African region, where structured cybersecurity curricula and psychosocial support are frequently unavailable within the same institutional setting [30], [31]. Because the ICEPG Framework is designed for deployment through existing school curricula, digital platforms, and community mental-health services rather than requiring new parallel infrastructure, it offers a comparatively low-cost pathway for institutions in such settings to combine the two domains without duplicating scarce specialist capacity.

D. Limitations and Future Research

Several limitations constrain the findings and should guide their interpretation. First, the quasi-experimental, intact-group assignment procedure precludes definitive causal inference and leaves open the possibility of cohort-level confounds (e.g., pre-existing differences between classes or programmes) that individual-level randomisation would control for; future research should employ cluster- or individually randomised controlled trial designs. Second, the eight-week intervention window does not permit assessment of long-term maintenance; longitudinal follow-up at 3, 6, and 12 months is a priority, particularly given that knowledge-decay effects have been documented elsewhere in the cybersecurity-education literature [13]. Third, all outcome measures were self-reported, which raises the possibility of social-desirability bias and common-method variance, especially for the Psychological Impact Scale; future studies would benefit from triangulating self-report with behavioural or informant measures. Fourth, the low R^2 (.017) in the regression model highlights unmeasured predictors of psychological impact, including social support, prior mental-health history, and coping style. Fifth, facilitators were not blinded to condition, and while treatment fidelity was monitored, facilitator-level effects (e.g., differential enthusiasm across conditions) cannot be fully ruled out. Finally, cross-cultural replications in diverse regulatory and socioeconomic settings are needed, particularly in rapidly digitalising Sub-Saharan African and South-East Asian contexts [1], [12], [30], [31], to establish whether the

magnitude of the integrated-approach advantage generalises beyond the present sample.

VII. CONCLUSION

This study has demonstrated, through analysis of a structured dataset of 620 youth participants, that an integrated approach combining cybersecurity education with psychological guidance dramatically outperforms single-domain interventions in improving youth cybersecurity awareness. The Integrated Approach produced a mean awareness improvement of 33.39 points—nearly twice that of either standalone intervention—with a large ANOVA effect size (partial $\eta^2 = .715$) and an extremely large Cohen's d (4.11) against the no-intervention control. Cyberbullying was the most prevalent crime type (27.3%) while sextortion produced the highest psychological impact ($M \approx 87$), consistent with the most recent international evidence on the differential severity of sexually motivated online crimes [26], [27]. The ICEPG Framework—grounded in PMT, SCT, and Routine Activities Theory, and situated within the growing regional evidence base from Nigeria and Sub-Saharan Africa [30], [31]—offers a theoretically coherent and practically implementable blueprint for tech-driven youth online-crime prevention. As online crimes against youth continue to proliferate in frequency and sophistication, the integration of technical and psychological dimensions of prevention is no longer a theoretical aspiration but an empirical and moral imperative.

REFERENCES

[1] International Telecommunication Union (ITU), "Measuring Digital Development: Facts and Figures 2023," ITU Publications, 2023.

[2] Federal Bureau of Investigation, Internet Crime Complaint Center, "2022 Internet Crime Report," U.S. Department of Justice, 2023.

[3] National Center for Missing and Exploited Children (NCMEC), "2022 CyberTipline Report," NCMEC Publications, 2023.

[4] D. Cross et al., "Psychological, physical, and academic outcomes of cyberbullying: A meta-analysis," Educational Psychology Review, vol. 34, no. 2, pp. 841–878, 2022.

[5] World Health Organisation (WHO), "World Mental Health Report: Transforming Mental Health for All," WHO Press, 2022.

[6] R. Graham and J. Houston, "Integrating mental health support and cyber education: A pilot evaluation in British secondary schools," British Journal of Educational Technology, vol. 53, no. 4, pp. 921–940, 2022.

[7] R. W. Rogers, "A protection motivation theory of fear appeals and attitude change," Journal of Psychology, vol. 91, no. 1, pp. 93–114, 1975.

[8] A. Bandura, Social Foundations of Thought and Action: A Social Cognitive Theory. Prentice-Hall, 1986.

[9] S. Hinduja and J. W. Patchin, "Cyberbullying: An update and synthesis of the research," in The Wiley Blackwell Handbook of Bullying, pp. 499–519, Wiley-Blackwell, 2021.

[10] L. M. Jones, K. J. Mitchell, and H. A. Turner, "Technology-facilitated sexual abuse, exploitation, and harassment of youth," Child Maltreatment, vol. 27, no. 1, pp. 58–69, 2022.

[11] J. M. Machimbarrena et al., "Internet risks: An overview of victimization in cyberbullying, cyber dating abuse, sexting, online grooming and problematic internet use in adolescents," Int. J. Environ. Research and Public Health, vol. 19, no. 21, p. 14027, 2022.

[12] United Nations Office on Drugs and Crime (UNODC), "Cybercrime and the COVID-19 Pandemic: A Global Analysis," UNODC, 2022.

[13] R. Brewer, J. Cale, and A. Goldsmith, "Evaluating school-based cybersecurity education," Computers & Education, vol. 160, p. 104042, 2021.

[14] Y. Chandra and L. Shang, "Gamification in cybersecurity education: Effects on engagement and knowledge retention," Computers in Human Behavior, vol. 138, p. 107469, 2023.

[15] I. Zych, R. Ortega-Ruiz, and I. Marín-López, "Cyberbullying: A systematic review of research, its prevalence and assessment issues in Spanish studies," Psicología Educativa, vol. 27, no. 2, pp. 139–147, 2021.

[16] D. L. Floyd, S. Prentice-Dunn, and R. W. Rogers, "A meta-analysis of research on protection motivation theory," J. Applied Social Psychology, vol. 30, no. 2, pp. 407–429, 2000.

[17] L. E. Cohen and M. Felson, "Social change and crime rate trends: A routine activity approach," American Sociological Review, vol. 44, no. 4, pp. 588–608, 1979.

[18] W. R. Shadish, T. D. Cook, and D. T. Campbell, Experimental and Quasi-experimental Designs for Generalized Causal Inference. Houghton Mifflin, 2002.

[19] R. C. Kessler et al., "Short screening scales to monitor population prevalences and trends in non-specific psychological distress," Psychological Medicine, vol. 32, no. 6, pp. 959–976, 2002.

[20] K. Witte and M. Allen, "A meta-analysis of fear appeals: Implications for effective public health campaigns," Health Education & Behavior, vol. 27, no. 5, pp. 591–615, 2000.

[21] Europol, "Internet Organised Crime Threat Assessment (IOCTA) 2023," European Union Agency for Law Enforcement Cooperation, 2023.

[22] United Nations Children's Fund (UNICEF), "Protecting Children from Online Threats in the Digital Age," UNICEF Office of Research – Innocenti, 2021.

[23] J. Anderson and S. Park, "AI-powered integrated digital safety platforms for youth," J. Cybersecurity Education, Research and Practice, vol. 2022, no. 1, Art. 6, 2022.

[24] P. M. Valkenburg, A. Meier, and I. Beyens, "Social media use and its impact on adolescent mental health," Current Opinion in Psychology, vol. 44, pp. 58–68, 2022.

[25] J. N. Navarro and J. L. Jasinski, "Going cyber: Using routine activities theory to predict cyberbullying experiences," Sociological Spectrum, vol. 41, no. 5, pp. 424–443, 2021.

[26] J. W. Patchin and S. Hinduja, "The nature and extent of youth sextortion: Legal implications and directions for future research," Behavioral Sciences & the Law, 2024, doi: 10.1002/bsl.2667.

[27] N. Henry and R. Umbach, "Sextortion: Prevalence and correlates in 10 countries," Computers in Human Behavior, 2024.

[28] J. W. Patchin and S. Hinduja, "2025 Cyberbullying Data," Cyberbullying Research Center, 2025.

[29] Z. Agha, J. Park, R. Wan, N. S. Ali, Y. Wang, D. DiFranzo, K. Badillo-Urquiola, and P. J. Wisniewski, "Tricky vs. transparent: Towards an ecologically valid and safe approach for evaluating online safety nudges for teens," in Proc. 2024 CHI Conf. Human Factors in Computing Systems (CHI '24), Honolulu, HI, USA, 2024, Art. 116.

[30] H. Orakpo, "Factors contributing to youth involvement in cybercrime in Nigeria," SSRN Working Paper, Jan. 2025.

[31] INTERPOL, "Africa Cyberthreat Assessment Report," 4th ed., International Criminal Police Organization, May 2025.