

A Conceptual Model of Digital Behavior and Cybercrime Risk Among Adolescents in Educational Contexts

Anar Javadov¹, Narmina Aliyeva², Intigam Hajiye³, Almaz Aliyeva⁴, Lala Allahverdiyeva⁵

¹Department of Law, National Aviation Academy, Mardakan Avenue 30, Baku, AZ1045, Azerbaijan

²Department of English Language, Baku Engineering University, Hasan Aliyev Street 120, Khirdalan city, AZ0102, Azerbaijan

³Department of Business and Management, Baku Business University, Baku, AZ1122, Azerbaijan

⁴Department of IT Engineering, Mingachevir State University, Mingachevir 4500, Azerbaijan

⁵Department of Pedagogy and Psychology, Nakhchivan State University, Nakhchivan, AZ7000, Azerbaijan

HOW TO CITE:

Anar Javadov, Narmina Aliyeva, Intigam Hajiye, Almaz Aliyeva, Lala Allahverdiyeva (2026). A Conceptual Model of Digital Behavior and Cybercrime Risk Among Adolescents in Educational Contexts. International Journal of Special Education, 41(6s), 613-624.

COPYRIGHT STATEMENT:

Copyright: © 2026 Authors.
Open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).

ABSTRACT:

Adolescents' intensified engagement with networked technologies has reshaped learning, communication, and identity work while simultaneously amplifying exposure to cybercrime-related risks. This article examines the association between digital behavioral patterns and cybercrime risk awareness within educational contexts, with particular emphasis on implications for vocational education. Anchored in contemporary scholarship on digital behavior, online safety, and preventive pedagogy, the study advances a conceptual framework that links everyday online practices—such as social media participation, information sharing, and peer communication—to variations in awareness of privacy threats, data misuse, social engineering, and platform-mediated harms. The analysis argues that deficits in digital literacy and inconsistent school-level guidance create gaps in adolescents' capacity to recognize, appraise, and mitigate online risks. Positioning vocational education as a strategic locus for intervention, the article outlines curriculum-embedded, assessment-aligned approaches that integrate cyber risk awareness, digital ethics, and protective practices into routine instruction. By articulating pedagogically actionable pathways to strengthen students' critical digital competencies, the study contributes to the literature on education-based prevention and offers direction for educators, curriculum designers, and policymakers seeking scalable, context-sensitive strategies to reduce adolescents' vulnerability to cyber-related harm and to foster responsible, informed digital behavior across vocational and secondary settings.

Keywords: digital behavior, cybercrime risk awareness, digital literacy, vocational education, preventive education

1. Introduction

Adolescents' intensified engagement with networked technologies is reshaping learning, communication, and daily routines, while a sizable subset reports "almost constant" platform use that broadens the window of online risk exposure [1]. Across Europe, the EU Kids Online 2020 study documents sharp increases in smartphone-based internet use since 2010 and notes uneven provision of school-based online safety guidance despite rising time online [2]. A global UNICEF evidence review similarly highlights growing participation alongside disparities in digital skills and variability in adult mediation, underscoring the need for preventive and empowering educational responses [3]. Everyday digital behaviors—social media participation, information sharing, and peer-to-peer messaging—are associated with vulnerability to online harms; a cross-national analysis links intense/problematic social media use with both victimization and perpetration of cyberbullying [4]. A systematic mapping confirms negative associations between cyberbullying and youth mental health, while cautioning that the predominance of cross-sectional designs limits causal inference [5]. In privacy literacy, adolescents more readily enact proximal practices (e.g., not sharing passwords) than distal, data-governance actions (e.g., restricting app-level collection), revealing conceptual and procedural gaps for schooling to address [6].

Education frameworks position 21st-century literacy as including critical evaluation of information, recognition of deceptive/phishing content, and responsible online conduct—competencies central to risk mitigation [7].

OECD guidance further emphasizes system-level alignment of teacher capacity, curriculum, and assessment across school, vocational, and higher education to improve quality, equity, and efficiency in digital learning [8].

Comparative policy analyses stress the importance of coherent national digital-education strategies that bridge policy and implementation [9].

Equity-focused work highlights closing gaps in access and skills as a prerequisite for inclusive digital-education outcomes [10].

Within vocational education (VET), studies report heterogeneous self-assessed digital skills and emphasize the role of curriculum-embedded instruction and resources in closing deficits [11].

Research on digital-literacy instruction shows competence gains but uneven standardization and implementation, indicating the value of assessment-aligned designs [12].

VET literature also recommends aligning curricula with labor-market digitalization, strengthening teacher training, and ensuring equitable technology access—priorities that complement prevention of cyber-related harms [13].

In preventive education, a cluster randomized controlled trial of a school digital-citizenship curriculum found improvements in knowledge and self-efficacy for handling online problems, while broader behavioral outcomes remained limited without stronger systemic support [14].

A randomized trial of a mobile, game-based safety program showed that higher engagement predicted gains in safety knowledge and reductions in unsafe behaviors, underscoring the importance of dosage and design fidelity [15].

Randomized evaluation of a child-safety curriculum covering bullying/cyberbullying also demonstrated knowledge gains over multi-month follow-up [16].

UNICEF's guidance on evaluating online-safety initiatives calls for robust theories of change, outcome alignment, and rigorous monitoring to build cumulative evidence of what works [17].

A critical yet under-addressed vector is social engineering: surveys show low baseline awareness among non-IT student groups [18].

Evidence suggests that game- and scenario-based instruction can raise social-engineering awareness when appropriately designed [19].

Emerging educational work advocates integrating psychological and sociological principles to teach manipulation signals and promote responsible online behavior in age-appropriate ways [20].

This article advances a conceptual model linking adolescents' digital engagement patterns to cybercrime risk awareness through the mediating roles of digital literacy (privacy, authentication, critical evaluation) and the educational ecology (teacher capacity, parental/peer mediation, school

policy), with actionable implications for vocational education and assessment-aligned, scalable implementation [7].

spend between three and six hours a day on digital platforms, primarily for entertainment, gaming, and social media [6, 8]. These platforms promote risky behaviors like excessive self-disclosure, participation in risky challenges, and exposure to inappropriate or unlawful content, even though they also improve peer engagement and information access [7].

Teenagers are more likely to engage in problematic digital activities that could lead to virtual criminality due to the online disinhibition effect, where anonymity and a lack of accountability encourage deviant behaviors [7].

E. Types and Prevalence of Cybercrime

Cyberbullying, illegal content sharing, unauthorized access to digital systems (hacking), and exposure to online drug markets are all considered forms of adolescent virtual criminality [11]. The prevalence of cyberbullying is particularly high, with victimization rates ranging from 14% to more than 50% worldwide [8]. Additionally, studies show that teenagers are becoming more interested in hacking or gaining unauthorized access to accounts, systems, or digital infrastructures [12].

The exposure of teenagers to drug-related content on social media, dark web sites, and encrypted messaging platforms has alarmingly increased, making them more vulnerable to illicit transactions and substance abuse [11].

F. The Function of Education in Cybersecurity

It is widely accepted that cybersecurity education is essential to equipping teenagers with the knowledge, abilities, and moral awareness required for safe online behavior. Effective online safety programs have been shown to reduce participation in cyber aggression, encourage safe online conduct, and curtail risky digital behaviors [5]. However, a lot of current programs frequently struggle with a lack of integration, thorough coverage, and consistency with regard to socio-emotional learning [4]. More and more support is being given to models that enable students to go beyond technical instruction and cultivate critical thinking, digital resilience, and responsible online citizenship [12].

Investigates psychoeducational strategies to increase teenagers' awareness of cyberbullying. The study shows notable improvements in awareness, warning sign recognition, and help-seeking intentions using a

pre/post design with school-based sessions. demonstrates how structured education increases digital resilience and can lessen susceptibility to online aggression, which supports ACRM's prevention pathway [13].

Examines, using survey data and qualitative input, how teenagers deal with bullying in online settings. identifies emotion-focused coping, dependence on peers or adults, and problem-focused strategies (blocking/reporting). draws attention to the gaps that exist between awareness and practical action. strengthens the focus placed by ACRM on developing skills and creating supportive environments in order to convert awareness into protective behavior [14]. Examines the impact of parents on the delinquent online behavior of teenagers. finds that while permissive or inconsistent parenting predicts higher risk, consistent norms, warmth, and quality monitoring correlate with lower cyberdeviance. positions family context as a crucial environmental moderator of risk behaviors, which is consistent with ACRM [15].

Narrative analysis of 17 global initiatives to prevent cyberbullying. Multi-tier design, curriculum integration, bystander training, and whole-school policies are all shared by successful programs. observes inconsistent contextual fit and evaluation rigor. The ACRM education/resilience node is operationalized through the provision of intervention design principles [16]. Suggests deep learning pipelines for social media content detection and filtering of cyberbullying. The paper emphasizes platform-level safeguards that can supplement youth education, despite being technical and dataset-driven. This is a structural control that reduces exposure and prevents escalation toward virtual criminality, according to ACRM [17].

Examines how educators create chatbots with LLMs to raise awareness of cyberbullying. identifies opportunities for scenario practice and individualized coaching, but also highlights risks (privacy, bias, and misuse). recommends teacher mediation and guardrails. introduces adaptive pedagogies that can effectively increase resilience, thus expanding ACRM [18]. Discusses detection and policy issues while synthesizing the connections between mental health, digital wellbeing, and online harassment. Advocates integrated policy, education, and technical solutions. supports the multi-layered approach of ACRM, which combines the development of psychological skills with exposure management [19].

This article makes the case for adolescent online safety strategies that prioritize autonomy and resilience over models that are solely restrictive. emphasizes using safety tools that respect youth's rights and co-designing with them. conforms to the "empowerment over control" tenet of ACRM in order to reduce susceptibility in a sustainable manner [20]. Discusses teaching digital literacy as a means of combating cyberbullying. advocates for integrating platform navigation, ethical reasoning, and critical consumption into marketing and tourism education contexts—demonstrating the transferability of skills. supports the curriculum-integration suggestion made by ACRM [21].

Measures the frequency of high school students being victims of cyberbullying and connects it to stress and a decline in mental health. identifies risk factors, such as inadequate support networks and excessive screen time. supports early preventive education in ACRM with prevalence and harm data [22]. Examines the relationships between academic self-regulation and time management and exposure to (cyber)bullying. reveals that poorer study management and self-regulatory effort are associated with high exposure. demonstrates the value of resilience training for wider results and downstream academic costs, which extends ACRM [23].

Focuses on the roles of peer norms, self-control, and family climate as psychosocial predictors of cyberdeviance in an Australian cohort. makes recommendations for interventions that focus on parental involvement and socioemotional skills. fits the family-school collaboration and psychological drivers node of ACRM [24]. Policy commentary supporting education on youth sexting and balanced legislation. places a focus on privacy, harm reduction, and practical school solutions. backs ACRM's proposal for frameworks for policies that go beyond punishment alone and instead enhance education [25].

Adolescent digital self-harm has been linked to psychological distress and victimization, according to longitudinal research. Risky online behavior may be mediated by signals that internalize symptoms. As part of resilience building, ACRM recommends psychological screening and support [26]. Examines changes in prevalence, patterns, and demographic subtleties of cyberbullying before and during COVID-19. highlights the importance of culturally sensitive education and the exposure-risk relationship, which is a factor in the implementation of ACRM [27].

Investigates cognitive and affective empathy as protective factors against bias-based cyberbullying.

believes that developing empathy is a good area for interventions. directly contributes to the socio-emotional skill strand of cybersecurity education offered by ACRM [28]. Demonstrates the differential prediction of bullying and cyberbullying offenses by six parenting dimensions. shows that risk is decreased by structured, encouraging parenting. supports the moderator of susceptibility at the family level for ACRM [29].

Links increased suicidality to digital self-harm and calls for combined online safety and mental health solutions. In order to prevent escalation, ACRM advocates integrating mental-health literacy and referral channels into cybersecurity education [30].

G. Research Gaps

There are still a number of research gaps despite the increasing amount of data about teenage cyber risks:

- **Fragmented Focus on Risk Behaviors:** Most research focuses on cyberbullying, with little attention paid to more general forms of virtual criminality, such as hacking, drug exposure, and digital delinquency [11].
- **Limited Integration of Educational Impact:** According to [4], there aren't many empirical studies that assess how formal cybersecurity education affects teenagers' online behaviors and how it affects their participation in or ability to prevent cybercrime.
- **Regional and Cultural Disproportions:** Insufficient attention has been paid to the online behaviors of adolescents in diverse cultural, socio-economic, and developing regions due to the majority of research focusing on Western populations [7].
- **Inadequate Longitudinal Analysis:** Comprehensive longitudinal studies evaluating the long-term effects of cybersecurity efforts in reducing adolescent engagement in online violence or digital criminality are somewhat lacking [5].

The psychological and social factors that contribute to risky online behaviors, such as moral disengagement and online disinhibition, are often overlooked in the literature [7].

By investigating the relationships between teenage digital behaviors, exposure to virtual criminality, and the importance of cybersecurity education, with a focus on early intervention strategies, this study seeks to close these gaps.

2. Methodology

● FRAMEWORK AND METHODOLOGY

In order to clarify the elements that impact teenagers' involvement in online criminal activities, such as digital violence, hacking practices, and exposure to illegal content like online drug advertisements, this study presents the Adolescent Cybercrime Risk Model (ACRM). The model is grounded in empirical data showing that adolescents' susceptibility to cybercrime is influenced by a combination of digital behaviors, exposure to online risks, psychological factors, and educational initiatives [8, 11].

Three main dimensions are included in the ACRM:

- *Digital Exposure:* How frequently and for how long people use high-risk online platforms (such as social media, online gaming communities, and encrypted applications)
- *Risk Behaviours and Psychological Drivers:* Online disinhibition (less accountability because of anonymity), Moral disengagement, or the defense of destructive online behavior, and Peer pressure and interest in hacking or illicit content
- *Preventive Moderators:* Cybersecurity education, Capabilities for digital resilience, and Recognizing the consequences of using the internet

According to the model, peer pressure and psychological vulnerabilities further moderate the likelihood of engaging in online criminal activity, even though increased digital exposure raises the likelihood of risk. Nonetheless, the presence of proactive moderators, particularly structured cybersecurity training, reduces the probability of participating in detrimental online activities.

A. Important Theories of Behavior and Criminology

The proposed model is based on established theories that explain how teenage cybercrime behaviors develop:

1. *Disinhibition Effect of the Internet:* According to this theory, the asynchronous nature of digital communication, anonymity, and invisibility reduce self-regulation and encourage behaviors that people might otherwise refrain from in-person interactions. This effect contributes to aggressive remarks, hacking attempts, cyberbullying, and the use of illegal online content among teenagers [7, 9].

2. *Social Learning Theory:* Teenagers often imitate actions they see in their peers, role models, or online groups. Imitation is encouraged by exposure to normalized online aggression, hacking showcases, or drug-related content, especially in the absence of robust digital ethics education [1, 12].

3. *Moral Disengagement Theory:* This framework clarifies how people minimize the effects, dehumanize victims, or shift blame in order to defend harmful actions. Higher rates of cyberbullying, hacking, and online deviance among youth have been repeatedly linked to moral disengagement [2, 7].

4. *Routine Activity Theory:* According to this criminological theory, crime happens when three factors come together: an appropriate target, a motivated offender, and the lack of capable guardianship. The importance of preventative education as a type of digital guardianship is highlighted by the fact that adolescents' unsupervised online activities increase their risk of becoming victims and committing cybercrimes [3, 11].

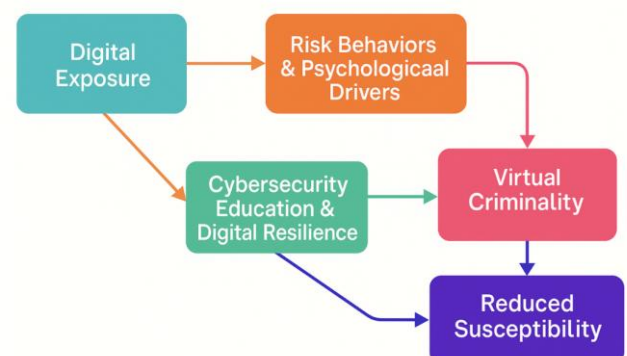


Fig. 1 Adolescent Cybercrime Risk Model

The Fig. 1 framework recognizes the complex and multifaceted nature of teenage cybercrime behaviors and emphasizes the value of proactive, focused educational initiatives to encourage safer online conduct.

B. Algorithm: Adolescent Cybercrime Risk Model (ACRM)

Step 1: Digital Exposure for Input

- Get information about how much time adolescents spend online, what platforms they use, and what kinds of activities they engage in.
- Determine the exposure level (low, moderate, or high).

Step 2: Assess Psychological Drivers and Risky Behaviors

- Look for indications of anonymity-driven behavior, or online disinhibition.
- Evaluate moral disengagement (justifying destructive online behavior).
- Keep track of dangerous online conduct, such as excessive sharing, peer pressure, and hacker curiosity.

Step 3: Assess the Possibility of Cybercrime

- Adolescence is extremely vulnerable if risky behaviors surpass the threshold.
- Otherwise, the adolescent is considered moderately vulnerable if risk behaviors fall below the threshold.
- Otherwise, adolescents pose little risk.

Step 4: Use Digital Resilience & Cybersecurity Education (Moderating Factor)

- Verify whether the teenager has participated in workshops or school curricula that offer formal cybersecurity training.
- Improve your digital resilience score if you're trained.
- Mark as a high-priority intervention if not trained.

Step 5: Modify the Virtual Criminality Risk

- Add the education/resilience score to the risk behaviors score.
- A high level of resilience reduces the likelihood of being involved in cybercrime.
- The likelihood rises if resilience is low.

Step 6: Susceptibility Level Output

- If (high risk + lack of education) = High Susceptibility.
- If (partial education + moderate risk) = Moderate Susceptibility.
- Reduced Susceptibility if (low risk + strong education).

Step 7: Feedback loop

- Suggest focused interventions:
 - Adolescents at high risk should receive rigorous instruction,

guidance, and parental/educational support.

- Peer-group discussions and ongoing awareness workshops are recommended for adolescents at moderate risk.
- Adolescents at low risk should be encouraged to practice safe online conduct and digital resilience.

Later on, this algorithm can be used in adolescent cybersecurity education programs as a risk assessment model or decision support tool.

C. Methodology

A quantitative, cross-sectional survey methodology was used in this study to investigate the relationship between the exposure of adolescents to virtual criminality, their digital activities, and the moderating effect of cybersecurity education. Teenagers were asked to self-report their online habits, experiences with cybercrime, and opinions on online safety education using a structured questionnaire.

1. An Example of a Description: Teenagers aged 12 and up were part of the study's target population. They were chosen to guarantee a varied representation of the key age groups related to adolescent development and trends in online behavior. There were 101 valid answers in all.

Breakdown of Demographics:

Gender: 44 men (43.6%), 56 women (55.4%), and 1 person (1%) who wished to remain anonymous

Groups by Age:

- 31 respondents (30.7%) were between the ages of 12 and 13.
- 12 respondents (11.9%) were between the ages of 14 and 15.
- Ages 16–17: 2 responders (2%)
- 56 responders (55.4%) were 18 years of age or older.

The participants' varied internet usage habits provided insights into differing degrees of digital exposure and experiences with cyberthreats.

2. Details of the Survey Instrument: Based on previous research on teenage digital behaviors, cybercrime tendencies, and cybersecurity awareness, an anonymous,

self-administered online questionnaire was developed [8, 11].

Both closed-ended and Likert-scale questions were included in the survey to address:

- The amount of time spent online each day
- Using social media platforms
- Experiences with or observations of cyberbullying
- Interest in or participation in hacking
- exposure to internet content about drugs
- Prior involvement in cybersecurity education
- Perceived need to incorporate cybersecurity into school curricula

To confirm the questionnaire's face validity, reliability, and clarity, a pilot test was conducted with a small sample of respondents.

3. Data Gathering Methods: To improve accessibility and convenience for teenage participants, data was collected via an online survey platform. Over the course of two weeks, the survey link was disseminated through youth organizations, social media, and educational networks.

The survey had clear instructions and eligibility requirements at the outset, and participation was entirely voluntary. Based on average completion times noted during data collection, respondents completed the questionnaire in about 4 to 7 minutes.

4. Moral Points to Remember: All aspects of this study were guided by ethical principles, particularly in light of the participation of adolescents:

- All participants gave their informed consent, and in accordance with ethical guidelines for research involving minors, those under the age of 18 required additional parental consent.
- Confidentiality and anonymity were maintained during the entire data collection and reporting procedure. No information that could be used to identify the individual was gathered.
- Participants were informed that they could leave the study at any moment without suffering any repercussions.
- The study adhered to the rules set forth by the institutional research ethics committee in question.

- In order to minimize possible distress, sensitive subjects like cyberbullying and online drug exposure were handled carefully, and support resources were made available when required.

This methodology ensures thorough, morally sound data collection that advances knowledge of teenage cybercrime behaviors and aids in the development of preventative measures.

3. Results

A. Profile of Demographics

The demographic information for the final group, there were 101 teenagers in the sample. Of these, one participant (1%) wished to remain anonymous, and 56 participants (55.4%) were female and 44 participants (43.6%) were male. 31 participants (30.7%) were between the ages of 12 and 13, 12 participants (11.9%) were between the ages of 14 and 15, and 2 participants (2%) were between the ages of 16 and 17. 56 participants (55.4%) who were at least 18 years old made up the largest group.

Although a sizable portion (55.4%) of the sample is 18 years of age or older, the age distribution shows a diverse sample of adolescents, providing insights from early to late adolescence and early adulthood.

B. Patterns of Online Behavior

According to the study, teenagers had higher levels of digital engagement (Table 1). Nearly 46% of respondents reported spending more than four hours a day online, with 27.7% reporting four to six hours and 17.8% reporting more than six hours. Just 11.9% of respondents said they spent less than an hour online each day, whereas the majority (42.6%) said they used the internet for one to three hours every day. The majority of respondents actively used social media sites like Facebook, Instagram, TikTok, and Snapchat, indicating a high level of daily exposure to online environments.

TABLE 1
AVERAGE DAILY ONLINE ACTIVITY

Online Time per Day	Frequency	Percentage (%)
Less than 1 hour	12	11.9
1–3 hours	43	42.6
4–6 hours	28	27.7
More than 6 hours	18	17.8
Total	101	100

Remarkably, 45.5% of respondents said they use the internet for more than four hours every day, indicating a high degree of digital exposure. Social media was widely used, and the majority of people were active users of Facebook, Instagram, TikTok, and Snapchat.

C. Cyberthreat Exposure a. Cyberbullying Experience

According to the study, 16.8% of teenagers had personally been the victim of cyberbullying, and 22.8% said they had witnessed such incidents. According to Table 2, more than half of the respondents (51.5%) said they had no experience with cyberbullying, and 8.9% were unsure. As shown in Table 3, nearly 60% of participants considered cyberbullying to be a very serious threat, despite the wide range of exposure levels. This indicates that adolescents are highly aware of the negative effects of cyberbullying.

TABLE 2
EXPERIENCE WITH CYBERBULLYING

Response	Frequency	Percentage (%)
Victim of cyberbullying	17	16.8
Witnessed cyberbullying	23	22.8
Not experienced or witnessed	52	51.5
Unsure	9	8.9
Total	101	100

TABLE 3
PERCEPTION OF CYBERBULLYING SEVERITY

Severity Rating	Frequency	Percentage (%)
Very serious	60	59.4
Moderately serious	24	23.8
Not serious	10	9.9
Don't know	7	6.9
Total	101	100

The results indicate that cyberbullying is quite common and that young people strongly recognize how serious it is.

Propensities for Hacking: According to the data, a significant 40.6% of teenagers showed curiosity or involvement in hacking, whereas 59.4% expressed no interest or involvement in the activity. In particular, Table 4 shows that 10.9% attempted hacking, 3% succeeded in gaining access to a system, and 26.7% were interested but did not act. These findings demonstrate that teenagers are very interested in hacking, underscoring the significance of launching cybersecurity education programs at a young age.

TABLE 4
HACKING CURIOSITY AND INVOLVEMENT

Response	Frequency	Percentage (%)
Never been curious or attempted hacking	60	59.4
Curious but never acted on it	27	26.7
Attempted hacking	11	10.9
Successfully hacked something	3	3
Total	101	100

The need for targeted preventive education is highlighted by the fact that over 40% of youth expressed interest in or involvement in hacking-related activities.

2. Coming Across Drug-Related Content Online: According to the study, 28% of teenagers had encountered drug-related content online, with 21.8% having done so once or twice and 5.9% reporting frequent exposure. Furthermore, Table 5 reveals that 59.4% of respondents said they had never seen such content, while 12.9% were unsure about their exposure. These findings demonstrate growing concerns regarding teenagers' vulnerability to the promotion of illicit substances online.

TABLE 5
ENCOUNTER WITH ONLINE DRUG-RELATED
CONTENT

Response	Frequency	Percentage (%)
Never encountered drug offers	60	59.4
Encountered once or twice	22	21.8
Frequently encountered	6	5.9
Unsure	13	12.9
Total	101	100

Concerns over the promotion of illegal substances online are growing, as evidenced by the 28% of teenagers who reported seeing drug-related content online.

D. Awareness and Education Levels

The findings showed that teens' formal cybersecurity education was noticeably lacking. Just 39.6% of respondents said they had received organized education, of which 16.8% had come from particular workshops or projects and 22.8% had come from the regular school curriculum. Furthermore, Table 6 indicates that 31.7% of respondents said they had never received any cybersecurity education, while 28.7% said they had learned about online safety on their own. However, participants gave cybersecurity topics a high importance rating of 3.53 out of 5, indicating a strong desire for better instruction on digital safety.

TABLE 6
CYBERSECURITY EDUCATION EXPOSURE

Response	Frequency	Percentage (%)
Received as part of regular school curriculum	23	22.8
Attended special workshops or projects	17	16.8
Never received formal education	32	31.7
Self-taught through personal exploration	29	28.7
Total	101	100

Overall, only 39.6% of respondents said they had formal cybersecurity education, indicating significant gaps in structured preventative strategies. The importance of including topics like cybercrime prevention, ethical behavior in the digital sphere, and online safety in school curricula was also asked of the participants. Teenagers strongly support the inclusion of

cybersecurity education in formal academic programs, as evidenced by the average rating of 3.53 out of 5 for the importance of these topics.

E. Discussion

1. Examination of the Principal Findings

According to the proposed Adolescent Cybercrime Risk Model (ACRM), the study's findings show different ways that teenage digital behaviors could result in virtual criminality. The algorithm identifies this amount of digital exposure as the first input condition that results in increased susceptibility to cyber risks, and nearly 46% of teenagers reported spending more than four hours a day online. This bolsters concerns around the world that extended use of digital devices is closely linked to negative behaviors [6].

With 40% of respondents reporting either direct or indirect experiences, cyberbullying has emerged as a crucial form of online aggression. Crucially, 83% of respondents identified it as a moderate to very serious problem, indicating that although adolescents are aware of how serious it is, they continue to be at risk because of ongoing exposure. Regarding risk behaviors, 28% of participants reported coming across online content about drugs, and over 40% of participants indicated interest in or participation in hacking. According to the ACRM framework, these actions are moral disengagement and psychological drivers that increase the probability of moving from virtual exposure to actual virtual criminality.

The algorithm's weak moderating factor was highlighted by the startling finding that only 39.6% of teenagers had formal cybersecurity education. Teenagers are still at a higher risk of developing into online criminals if they do not receive structured instruction to improve their digital resilience.

2. Assessment in Light of Recent Research

These results are consistent with international research that indicates a positive relationship between increased exposure to cyberthreats and extensive internet use [7, 8]. The prevalence of cyberbullying in this study is consistent with victimization rates that range from 14% to 58% worldwide, indicating that it continues to be a problem among adolescents worldwide [8].

The percentage of teenagers who are interested in hacking is consistent with studies that show peer pressure and online disinhibition contribute to the normalization of such dangerous behaviors [7, 12]. In a similar vein, exposure to drug-related content supports

[11] worries about the increasing convergence of teenagers and illegal online marketplaces.

The dearth of official cybersecurity education is in line with the recommendations made by [4, 5], who emphasize the value of empowerment-based training as opposed to control-based limitations. This missing component increases susceptibility by undermining the preventive moderation loop in the algorithmic model.

3. Implications for Policy and Adolescent Internet Safety

The urgent need for early preventive interventions that improve digital resilience and block the path to criminal exposure is highlighted by the ACRM algorithm. The following legislative and instructional actions are suggested in light of this framework:

- Include required cybersecurity instruction in school curricula, covering not only technical understanding but also empathy, ethical reasoning, and responsible digital citizenship.
- To strengthen practical cybersecurity skills, use experiential learning techniques like workshops, role-playing, and peer-learning exercises [4].
- Social-emotional learning programs that foster empathy, accountability, and critical reflection can help address psychological drivers such as moral disengagement and online disinhibition [7].
- Create focused interventions for teenagers who exhibit high-risk behaviors, especially a propensity for hacking or frequent exposure to drug-related content.
- To maintain a balance between parental guidance and adolescent autonomy, parents, educators, and legislators should collaborate across multiple stakeholder groups [12].

The algorithmic interpretation of the results demonstrates that education and resilience act as

mediators rather than being the sole cause of adolescents' transition from digital exposure to virtual criminality. Reducing cyber aggression, online drug exposure, and hacking tendencies requires enhancing cybersecurity education and encouraging responsible digital behavior. Stakeholders can change outcomes toward decreased susceptibility and safer online environments for teenagers by integrating preventive education into the ACRM framework.

5. Conclusion

- This study looked at the relationship between teenagers' online activity, their exposure to online dangers, and the value of cybersecurity education. According to the findings, teens use the internet extensively, are exposed to a lot of content about drugs and cyberbullying, and are either curious about or involved in hacking activities. Despite these risks, only roughly 40% of participants have access to formal cybersecurity training. Teenagers' susceptibility to online criminal activity is shaped by a combination of digital exposure, psychological factors, and preventive education, as demonstrated by the proposed Adolescent Cybercrime Risk Model (ACRM). The results highlight the need for early, thorough, and hands-on cybersecurity education to reduce online risks and foster safer digital environments for youth. Despite the fact that the study provides insightful information, its limitations include a cross-sectional design, a small sample size, and reliance on self-reported data. To improve knowledge and evaluate the efficacy of particular interventions, future research should employ mixed-methods and longitudinal approaches. Reducing teenage involvement in cybercrime requires enhancing cybersecurity education in schools and encouraging digital resilience.

References

- A. Bandura, *Social Learning Theory*. Prentice Hall, Englewood Cliffs, NJ, 1977.
- A. Bandura, "Moral disengagement in the perpetration of inhumanities". *Personality and Social Psychology Review*, 3(3), pp. 193–209, 1999.
- M. Felson and L.E. Cohen, "A routine activity approach to social change and crime rates". *American Sociological Review*, 44(4), pp. 588–608, 1979.
- P. Hernández, S. Park and R. Dominguez, "Increasing adolescent cybersecurity resilience: A model for preventive education". *Journal of Adolescent Online Safety*, 16(2), pp. 115–132, 2024.

- M. Stoilova, S. Livingstone and A. Kelly, "Cybersecurity, safety and digital literacy education: A systematic review of the international evidence". *Computers & Education*, 182, 104497, 2022.
- B. Priego-Parra and T. López-Castro, "A worldwide view of teenage digital behavior and mental health". *International Journal of Environmental Research and Public Health*, 20(1), pp. 22–38, 2023.
- D. Moreno, B. Martínez-Ferrer and G. Musitu, "A systematic review of teenage online aggression and moral disengagement". *Children and Youth Services Review*, 150, 106994, 2023.
- J.M. Machimbarrena, J. Ortega-Barón and J. González-Cabrera, "Cyberbullying's prevalence and psychological effects on teenagers". *Journal of Adolescent Health*, 72(4), pp. 562–570, 2023.
- J. Suler, "The online disinhibition effect". *CyberPsychology & Behavior*, 7(3), pp. 321–326, 2004.
- A. Slater and M. Tiggemann, "Teenage digital behavior and online harm during the COVID-19 pandemic: A systematic review". *Cyberpsychology, Behavior, and Social Networking*, 26(1), pp. 23–32, 2023.
- S. Yubero, R. Navarro and E. Larrañaga, "Trends and prevention of risky online behavior in teenagers". *Youth & Society*, 56(1), pp. 110–127, 2024.
- X. Li, L. Wang and Y. Zhou, "Techniques for lowering teenage involvement in cybercrime: Empowerment versus control". *Computers in Human Behavior*, 139, 107531, 2023.
- F. I. Rosyidah, S. Purwati and N. Muzayyanah, "Improving adolescent knowledge to prevent cyberbullying through psychoeducation". *International Journal of Research and Innovation in Social Science*, pp. 399–408, 2023.
- B. Paryente, "Adolescents' perspectives on coping with bullying in the digital environment". *Adolescents*, 4(2), pp. 248–262, 2024.
- I. B. Wissink, J. J. Asscher and G. J. Stams, "Online delinquent behaviors of adolescents: Parents as potential 'influencers'?" *International Journal of Offender Therapy and Comparative Criminology*, 2023.
- S. Siddiqui and A. Schultze-Krumbholz, "Successful and emerging cyberbullying prevention programs: A narrative review of seventeen interventions applied worldwide". *Societies*, 13(9), 212, 2023.
- B. Rohan, K. Ganguly, A. Das and D. Saha, "Securing social spaces: Harnessing deep learning to eradicate cyberbullying". *arXiv*, 2024.
- M. A. Hedderich, et al., "A piece of theatre: Investigating how teachers design LLM chatbots to assist adolescent cyberbullying education". *arXiv*, 2024.
- M. Kulkarni, S. Durve and B. Jia, "Cyberbully and online harassment: Issues associated with digital wellbeing". *arXiv*, 2024.
- J. Park, et al., "Towards resilience and autonomy-based approaches for adolescents online safety". *arXiv*, 2025.
- "Digital literacy education and cyberbullying combat: Scope and perspectives". In: *Strategic Innovative Marketing and Tourism (ICSIMAT)*, SpringerLink, 2024.
- O. M. E. Ramadan, et al., "Digital dilemma of cyberbullying victimization among high school students: Prevalence, risk factors, and associations with stress and mental well-being". *Children*, 11(6), 634, 2024.
- J. L. Solas-Martínez, et al., "Association of high levels of bullying and cyberbullying with study time management and effort self-regulation in adolescent boys and girls". *Education Sciences*, 15(5), 563, 2025.
- [Anonymous], "Link between psychosocial factors and cyberdeviance: Contact author and family study, Australian context". *SpringerLink*, 2023.
- S. Hinduja and J. W. Patchin, "Addressing youth sexting through rational legislation and education". *Journal of Adolescent Health*, 74(4), pp. 530–532, 2024.
- S. Hinduja and J. W. Patchin, "Adolescent digital self-harm over time: Prevalence and perspectives". *Journal of School Violence*, 23(4), pp. 542–554, 2024.
- S. Hinduja and J. W. Patchin, "Cyberbullying among Asian American youth before and during the COVID-19 pandemic". *Journal of School Health*, 93(1), pp. 82–87, 2023.

- S. Hinduja and J. W. Patchin, "Bias-based cyberbullying among early adolescents: Associations with cognitive and affective empathy". *Journal of Early Adolescence*, 42(9), pp. 1204–1235, 2022.
- S. Hinduja and J. W. Patchin, "Bullying and cyberbullying offending: The influence of six parenting dimensions among US youth". *Journal of Child and Family Studies*, 31, pp. 1454–1473, 2022.
- J. W. Patchin, S. Hinduja and R. C. Meldrum, "Digital self-harm and suicidality among adolescents". *Child and Adolescent Mental Health*, 28(1), pp. 52–59, 2023.