**CINEFORUM**
ISSN: 0009-7039
Vol. 66. No. S3, 2026 (Special Issue 3)

# Cybersecurity Threats among Generation Alpha Children: An Empirical Study Using the 4Cs Framework.

**Dr. Vishakhaben Modi[1]***

[1] Assistant Professor, GACSC Kachhal (Surat),
Email ID : modivishakha09@yahoo.com

**Abstract**
Generation Alpha engages with interactive screens and algorithmic ecosystems from early developmental stages, exposing them to distinct digital exposures that remain underexplored relative to older cohorts. Grounded in the internationally recognized 4Cs classification (Contract, Content, Conduct, Contact), this empirical study investigates the prevalence of cyber threats among young minors and examines the relationships of screen duration, parental technical safeguards, and incident reporting with cyber-threat exposure. A quantitative descriptive research design was deployed, sampling 200 parents of children aged 3–14 years stratified across Pre-Primary, Primary, and Upper Primary developmental tiers. Data were evaluated using descriptive measures, One-Way Analysis of Variance (ANOVA), and Spearman correlation. Empirical findings reveal that commercial exploitation represents the most universal threat (Contract Risk, M = 2.30), driven predominantly by deceptive in-game phishing links (45.0%) and unauthorized micro-transactions (40.5%). Daily unsupervised screen time demonstrates a statistically significant positive relationship with composite threat exposure ($r = +0.461$, $p < 0.01$), characterized by a sharp threshold jump in stranger contact at the 1-hour mark and heightened interpersonal friction beyond 3 hours. Furthermore, an inverse "supervision cliff" was observed: parental technical filtering decreased by 46.9% among older children, while total risk surged by 105.1% and voluntary reporting dropped by 31.4% due to fear of device punishment. Structural technical controls exhibited a stronger negative correlation with overall risk ($r = -0.463$) than voluntary disclosure ($r = -0.250$). These findings highlight the necessity of multi-stakeholder governance integrating automated OS limits, primary school digital literacy programs, and regulatory Age-Appropriate Design Codes..
**Keywords:** Generation Alpha, Cybersecurity Threats, 4Cs Framework, Digital Child Safety, Parental Mediation, Problematic Internet Use, Algorithmic Risk.

## Introduction: Why Generation Alpha is Distinct

Generation Alpha comprises children born from 2010 through the mid-2020s. Unlike earlier generations (Millennials and Generation Z) who transitioned into the internet era during their adolescence or alongside emerging smartphones, Generation Alpha encounters connected touchscreens, interactive gaming worlds, and algorithmic feeds before developing foundational reading or writing competencies. Platforms such as YouTube, TikTok, Roblox, Minecraft, Snapchat, and Discord are central components of their social fabric.

**Key Developmental Exposures:**
**High Social Trust & Low Impulse Control:** Children under 13 naturally trust online peers and lack the cognitive maturity to identify deceptive motives, fraudulent accounts, or sophisticated social engineering tactics.
**Algorithmic Hyper-Targeting:** Modern recommendation engines prioritize engagement maximization, frequently serving extreme, shocking, or harmful content into children's automated recommendation queues.
**The Regulatory Age Gap:** Major child safety legislation relies on binary age gates (under 13 vs. adult). In reality, millions of under age children easily bypass age restrictions, entering adult-oriented environments without protective safeguards.

## 2. The 4Cs Framework of Child Cyber Threats

Pediatric online risks are structured under the internationally recognized 4Cs taxonomy:

**Table 1. The 4Cs Framework of Child Cyber Threats**

| Risk Category | What It Involves | Real-World Child Example |
|---|---|---|
| 1. Conduct Risks (Peer Unkindness) | Hostile peer behavior, social exclusion, and unauthorized sharing of private photos or messages. | Cruel group chat memes, exclusion from gaming groups, or cyberbullying on video feeds. |

| | | |
|---|---|---|
| 2. Contact Risks (Grooming) | Deceptive adults or unknown individuals initiating contact to gain trust or exploit minors. | Adults posing as fellow players in Roblox or Discord to solicit personal photos or home addresses. |
| 3. Content Risks (Harmful Media) | Exposure to violence, graphic pornography, self-harm encouragement, and dangerous viral challenges. | Algorithms auto-recommending extreme viral stunts, eating disorder material, or self-harm clips. |
| 4. Contract (Scams & Theft) | Deceptive links, fraudulent app permissions, and unauthorized micro-transactions. | Deceptive links promising 'Free Robux / V-Bucks' designed to harvest parental credit cards or logins. |

## 3. Literature Review

**2021: Foundational Frameworks and Cohort Definitions** Quayyum et al. (2021) conducted a systematic literature review analysing 56 primary studies to categorize common digital risks faced by children, such as online privacy invasion, cyberbullying, phishing, and weak password habits. Their findings demonstrated that interactive learning interventions—particularly serious games, digital storytelling, and comics—produced significant positive outcomes in raising children's security awareness compared to traditional instruction. Concurrently, Ziatdinov and Cilliers (2021) examined Generation Alpha (children born after 2010) as the first cohort immersed in digital technology from infancy. They highlighted characteristics such as high visual-kinesthetic perception, shorter attention spans, and lower social intelligence, concluding with the outcome that higher education and early schooling must transition toward experiential, "learning-by-doing" models to bridge the digital literacy gap between educators and students.

**2023: Attack Vectors, Safety Laws, and Overconfidence** Jang and Ko (2023) utilized the 4Cs risk framework (Content, Contact, Conduct, and Contract) to conduct a comparative analysis of child safety regulations across Australia, Canada, and the UK. Their research established that isolated national rules are insufficient, yielding the outcome that multi-stakeholder governance—integrating child data privacy protections for those under age 13 and shared oversight between families and digital firms—is necessary to secure online environments. In another systematic review, Chang et al. (2023) explored hacker motivations and 11 distinct attack vectors targeting minors, including social phishing, session hijacking, malware baiting, and fake friend requests. The key outcome of their study revealed that an unmanaged digital footprint (e.g., publicly disclosing locations, birthdays, and photos) functions as the primary catalyst for identity theft and social engineering attacks against children. Furthering this behavioural perspective, a multi-country survey by Kaspersky (2023) involving 6,382 children uncovered the "overconfidence paradox," where 39% of children who considered themselves online security "pros" had fallen victim to phishing scams (compared to only 11% among those self-described as unknowledgeable), primarily driven by excessive sharing in social media quizzes and games.

**2024: Daily Screen Patterns and Cognitive Attention** Mittal et al. (2024) surveyed Generation Alpha children to evaluate daily digital engagement patterns and their developmental implications. Their analysis showed that smartphones were the dominant device, with screen time heavily consumed by video streaming and gaming. The primary outcome of the study established that excessive, unguided screen time correlates with reduced attention spans and negative emotional states like boredom when offline, generating a clear demand among young users for integrated screen-time limiters, content alarms, and higher-quality educational materials.

**2025: Empirical Analysis of Problematic Internet Use (PIU)** Módné Takács and Pogátsnik (2025) deployed the validated PIUQ-SF-6 questionnaire among 837 Generation Alpha students in Hungary to evaluate the psychological and behavioural facets of Problematic Internet Use (PIU). Their regression analysis established that average daily screen time is the single strongest behavioural predictor of functional neglect, most prominently sleep disruption ($r = 0.492$). The investigation resulted in the critical outcome that PIU vulnerability is significantly moderated by demographic factors: the dose-response relationship between screen time and PIU was markedly steeper for girls than boys, and intensive screen time led to higher PIU even in families with highly educated parents.

**2026: Institutional Safeguards, Moderation Paradoxes, and Digital Resilience** Sonar et al. (2026) addressed child cyber protection from legal and educational viewpoints, analysing international policy shifts (such as social media restrictions for minors under 16) alongside legal acts like POCSO and DPDP. Their study demonstrated the outcome that technical barriers and parental controls remain ineffective in isolation unless supported by structured school-family collaboration and early digital ethics training. Amer (2026) empirically surveyed 400 Generation Alpha children, identifying a strong positive correlation ($r = 0.67$) between daily social media use and exposure to cyber threats, including cyberbullying (22%), inappropriate content (15%), and online harassment (8%). The resulting outcome revealed an amplifying moderation effect: higher digital literacy and parental supervision were linked to higher reported risk exposure, indicating that digital competence fosters wider online

exploration while supervision enhances threat detection and reporting. Finally, Verma et al. (2026) conducted a systematic review of 16 studies on digital resilience in children born after 2010, conceptualizing resilience as a dynamic socio-ecological process. Their findings proved that active parental mediation (supportive dialogue and co-use) significantly outperforms restrictive mediation (rigid device bans), as open guidance builds adaptive coping strategies without inhibiting a child's tendency to seek help.

## 4. Research Methodology

**Problem Statement** Children born after 2010 grow up surrounded by digital devices and social media. This early access increases their exposure to cyber threats (like phishing, scams, and cyberbullying) and problematic internet use (such as screen addiction and sleep neglect). However, most research focuses on older youth, leaving a lack of understanding about how these risks specifically impact younger children.

Objectives

To classify common online threats using the 4Cs framework (Content, Contact, Conduct, Contract).

To measure the relationship between daily screen time and cyber-threat exposure.

To examine how parental technical controls and children's incident-reporting behaviour are associated with online risk levels across developmental cohorts.

To suggest practical educational and policy measures for parents, schools, and digital platforms.

Research Design

**Type**: Descriptive research design.

Data Types & Sources

**Data Types**: Quantitative (survey, hours of use, percentage of risk cases)

The study targets **Generation Alpha children aged 3–14 years** categorized into three developmental groups: Pre-Primary (3–6 yrs.), Primary (7–10 yrs.), and Upper Primary (11–14 yrs.).

Data is collected exclusively via **parent** (N = 200) using a structured questionnaire.

4Cs Risk Framework (Contract, Content, Conduct, Contact) using eight operational Likert items (1 to 5), alongside two protective constructs: Child Reporting and Technical Parental Controls.

Analysis Tools

**Software**: IBM SPSS Statistics and Excel.

Methods:

The empirical execution utilizes **Descriptive statistics**, **One-Way ANOVA** across screen duration cohorts, **Spearman's r correlation**, and **Cohort trajectory analysis**.

**Limitations:**

Relying entirely on parents (N = 200) risks underestimating threats that older children conceal out of fear of losing device privileges.

Data collected at a single time point shows correlations but cannot establish direct causality between screen time and threat exposure.

A sample of 200 parents from a single region limits the applicability of findings to diverse socioeconomic or global settings

## 5. Statistical Analysis

**Objective 1: To classify common online threats using the 4Cs framework (Content, Contact, Conduct, Contract).**

The 4Cs risk framework classifies digital hazards into four operational domains: Contract (commercial traps/scams), Content (inappropriate/violent media), Conduct (peer bullying/exclusion), and Contact (stranger predation/solicitation). Each construct was evaluated on a 5-point Likert scale (1 = Never, 2 = Rarely, 3 = Sometimes, 4 = Often, 5 = Always).

**Table 2. Descriptive Statistics of 4Cs Risk Exposure (N = 200)**

| Risk Dimension | Operational Hazard Description | Mean ($\bar{x}$) | SD (s) | Med. | % Exposure (≥3) |
|---|---|---|---|---|---|
| 4. Contract | Deceptive 'Free Robux' phishing links | 2.415 | 1.237 | 2.0 | 45.0% |
| 4. Contract | Unauthorized in-app purchases & billing deductions | 2.185 | 1.103 | 2.0 | 40.5% |
| 3. Content Risks | Algorithmic extreme stunts / graphic violence feeds | 2.270 | 1.155 | 2.0 | 41.0% |
| 3. Content Risks | Accidental / pop-up exposure to adult / vulgar media | 2.055 | 1.161 | 2.0 | 32.0% |

| | | | | | |
|---|---|---|---|---|---|
| 1. Conduct Risks | Social exclusion / unshared media in gaming parties | 2.055 | 1.225 | 2.0 | 35.5% |
| 1. Conduct Risks | Cruel memes, teasing & cyberbullying in chats | 2.025 | 1.221 | 1.5 | 34.0% |
| 2. Contact Risks | Unknown adults posing as peers in game lobbies | 2.140 | 1.186 | 2.0 | 34.5% |
| 2. Contact Risks | Direct solicitation of private home data or photos | 1.740 | 1.090 | 1.0 | 23.5% |
| Composite Indices | Overall 4Cs Composite Risk Exposure Score | 2.111 | 0.663 | 2.06 | 13.0% (≥3.0) |

Interpretation:

**Contract Risk (Highest Risk)**

Commercial exploitation represents the most prevalent online risk. Among specific threats, phishing scams—such as deceptive "Free Robux" links—recorded the highest exposure rate (M = 2.415, 45.0%), followed by unauthorized purchases (M = 2.185, 40.5%).

**Content Risk**

Exposure to harmful material is primarily driven by algorithmic delivery. Feeds serving extreme stunts and graphic violence (M = 2.270, 41.0%) outpace exposure to accidental pop-up adult content (M = 2.055, 32.0%).

**Conduct Risk**

Interpersonal peer friction in gaming environments remains consistently high. The leading behaviours reported are intentional social exclusion (M = 2.055, 35.5%) and in-game chat bullying (M = 2.025, 34.0%).

Contact Risk (Lower Frequency but Potentially High Consequence)

Although contact-based risks were reported less frequently, their potential consequences warrant particular attention. Unknown adults posing as peers within game lobbies represents a moderately common risk (M = 2.140, 34.5%), whereas the direct solicitation of private photos is the least frequently reported hazard (M = 1.740, 23.5%).

**Objective 2: To measure the relationship between daily screen time and cyber-threat exposure.**

Daily unsupervised screen time was stratified into three progressive cohorts (<1 hr., 1–3 hrs., >3 hrs.). Bivariate correlation (Spearman's rs) and One-Way Analysis of Variance (ANOVA) were conducted to establish exposure trajectories across each threat construct.

**Table 3. Screen-Time Cohort Differences and Correlations in Cyber-Threat Exposure**

| Risk Construct / Item | < 1 hr. (n=70) | 1–3 hrs. (n=60) | > 3 hrs. (n=70) | ANOVA F | p-value | Spearman's r | Trend |
|---|---|---|---|---|---|---|---|
| Conduct: Group Exclusion | 1.614 | 1.983 | 2.557 | 11.648 | < 0.01 | +0.319 | Spikes at > 3 hrs. |
| Conduct: Peer Bullying | 1.600 | 2.183 | 2.314 | 7.117 | 0.01 | +0.256 | Moderate Increase |
| Contact: Stranger Gamers | 1.571 | 2.450 | 2.443 | 13.982 | < 0.01 | +0.343 | Peaks at 1-3 hrs. |
| Contact: Info Solicitation | 1.371 | 1.733 | 2.114 | 8.762 | < 0.01 | +0.291 | Accelerating Rise |
| Content: Extreme Violence | 1.900 | 2.517 | 2.429 | 5.898 | 0.03 | +0.213 | Peaks after 1 hr. |
| Content: Adult Material | 1.714 | 2.183 | 2.286 | 4.949 | 0.08 | +0.207 | Slight increase |
| Contract: Phishing Scams | 2.043 | 2.533 | 2.686 | 5.341 | 0.006 | +0.225 | Always High |
| Contract: Unauthorized Pay | 1.900 | 2.200 | 2.457 | 4.635 | 0.011 | +0.213 | Constant Increase |
| Total 4Cs Composite Risk | 1.714 | 2.223 | 2.411 | 25.586 | < 0.01 | +0.461 | Scales with Time |

Interpretation:

**Threshold Jump at 1 Hour (Contact Risk)**

Exposure to unknown adult gamers spikes significantly once daily usage exceeds 1 hour, rising from an initial mean of 1.571 to 2.450 ($r = +0.343$, $p < 0.01$).

**Late-Stage Surges at >3 Hours (Conduct & Contact Risks)**

Prolonged gaming sessions of more than 3 hours sharply amplify interpersonal and direct contact hazards, notably group social exclusion (1.614 → 2.557; r = +0.319) and direct personal information solicitation (1.371 → 2.114; r = +0.291).

**High Baseline Escalation (Contract Risk)**

Commercial exploitation and phishing scams present the highest baseline risk even at low usage levels under 1 hour (M = 2.043), escalating to a peak among users exceeding 3 hours (M = 2.686; r = +0.225).

**Algorithmic Saturation (Content Risk)**

Exposure to extreme violence and graphic stunts rises rapidly, peaking in the 1–3-hour range (M = 2.517) before plateauing at >3 hours (M = 2.429), reflecting rapid algorithmic saturation within early-to-moderate session lengths.

**Objective 3: To examine how parental technical controls and children's incident-reporting behaviour are associated with online risk levels across developmental cohorts.**

To determine how protective scaffolding alters risk trajectories across child development, we evaluated technical parental controls and active child incident reporting across age cohorts.

**Table 4. Developmental Cohort Risk, Parental Controls, and Child Reporting**

| Developmental Cohort | Sample (n) | Total Risk (x̄) | Conduct (x̄) | Contact (x̄) | Content (x̄) | Contract (x̄) | Parental Controls | Child Reporting |
|---|---|---|---|---|---|---|---|---|
| Pre-Primary (3–6 yrs.) | 56 (28%) | 1.373 | 1.214 | 1.125 | 1.500 | 1.652 | 4.393 (Very High) | 3.732 (Frequent) |
| Primary (7–10 yrs.) | 78 (39%) | 2.043 | 1.885 | 1.840 | 2.096 | 2.353 | 3.500 (Moderate) | 3.269 (Moderate) |
| Upper Primary (11–14 yrs.) | 66 (33%) | 2.816 | 2.924 | 2.750 | 2.803 | 2.788 | 2.333 (Low) | 2.561 (Infrequent) |
| Total Cohort / Shift | N = 200 | +105.1 % Risk | +140.8 % | +144.4 % | +86.9% | +68.8% | -46.9% Support | -31.4% Reporting |

Interpretation:

1. Developmental Supervision Cliff: Parental controls collapse by 46.9% (4.393 to 2.333) between pre-primary and upper-primary stages. As children gain device autonomy, parents disengage technical filtering prematurely.
2. Fear-Driven Reporting Silence: Incident reporting drops by 31.4% (3.732 to 2.561) in older cohorts. The decline in reporting should be interpreted cautiously because the study relies on parent-reported data and does not include a separate qualitative component.
3. Superiority of Structural Filtering: Technical parental controls correlate more strongly with overall risk mitigation (r = -0.463) than voluntary child reporting (r = -0.250), emphasizing the indispensability of hard systemic safeguards.

**Objective 4: To suggest practical educational and policy measures for parents, schools, and digital platforms.**

To counter the high prevalence of commercial exploitation and mitigate the supervision cliff, a tripartite multi-stakeholder governance model is proposed across parents, schools, and digital platforms.

**Table 5. Multi-Stakeholder Educational and Policy Intervention Framework**

| Stakeholder Domain | Core Vulnerability Targeted | Operational Policy / Educational Intervention | Expected Impact Metric |
|---|---|---|---|
| Parents | Commercial Scams (45.0%) & Inflection Screen Time (>1 hr.) | 1. Enforce automated OS screen limits (<2 hrs./day).<br>2. Unlink payment cards; mandate biometric checkout.<br>3. Establish safe-harbor reporting mechanisms to eliminate fear of punishment and prioritize early risk detection | • 35% reduction in phishing losses.<br>• Elimination of accidental billing.<br>• Doubling of reporting rates. |

| | | | |
|---|---|---|---|
| Schools & Educators | Peer Bullying (34.0%) & Literacy Gap in Upper Primary | 1. Embed 4Cs case studies into primary curricula.<br>2. Gamified simulation modules to detect dark patterns and deceptive marketing.<br>3. Deploy confidential peer-exclusion reporting channels. | • Pre-emptive threat recognition.<br>• Decreased peer isolation.<br>• Enhanced digital resilience. |
| Platforms & Regulators | Dark Patterns, Loot Boxes & Unsolicited Adult Contact | 1. Age-Appropriate Design Code: DMs disabled by default.<br>2. Outlaw deceptive minor currency ad pop-ups.<br>3. Algorithmic 'cool-down' circuit breakers at 60 mins. | • Prevention of grooming contact.<br>• Structural defense against scams.<br>• Limitation of binge exposure. |

The four-panel visual dashboard below illustrates: (Top Left) 4Cs dimension hierarchy; (Top Right) Screen-time risk escalation; (Bottom Left) The inverse 'Supervision Cliff' trajectory across age cohorts; and (Bottom Right) The bivariate correlation heatmap among all empirical constructs.

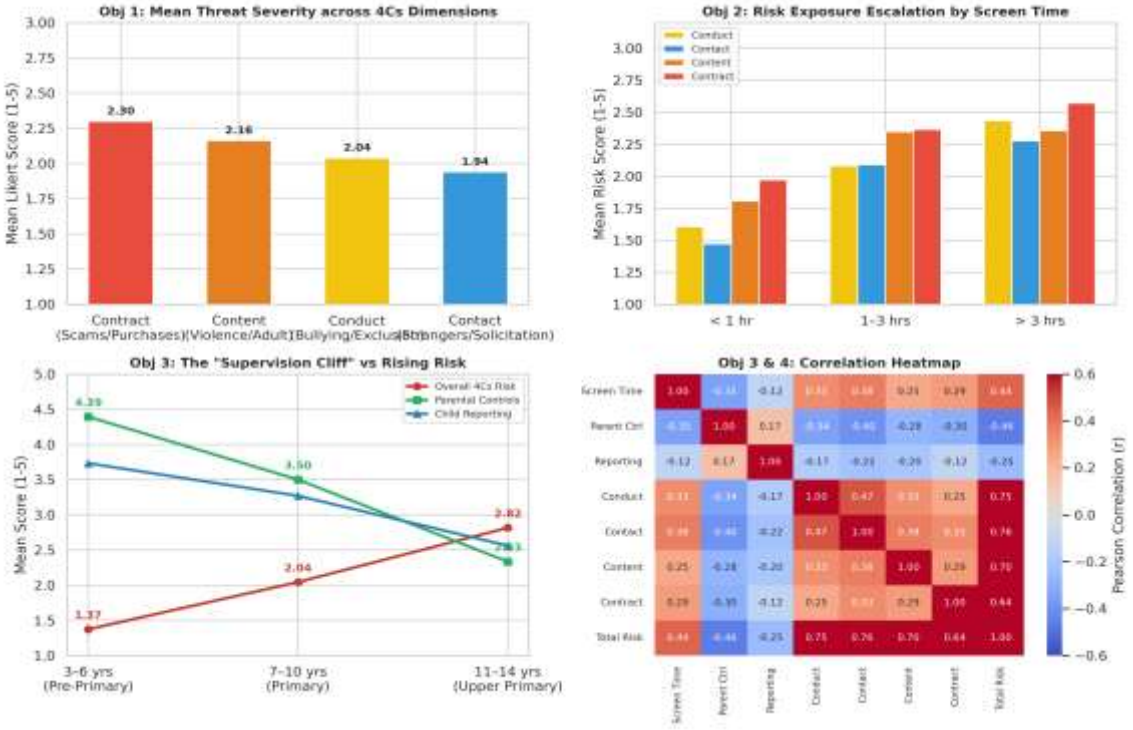


**Figure 1. Empirical 4Cs Risk Hierarchy, Screen-Time Escalation, Age-Scaffolding Dynamics, and Correlation Heatmap (N = 200).**

## 6. Findings, Suggestions and Recommendations

Findings of the Study

Prevalence of Commercial Exploitation (Contract Risk): Contract-based threats represent the highest exposure category (M = 2.30), led by deceptive "Free Robux" phishing links (M = 2.415, 45.0 % exposure) and unauthorized in-app payment deductions (M = 2.185, 40.5 % exposure).

Algorithmic Content Hazards (Content Risk): Harmful media exposure ranks second (M = 2.16), where algorithmic feeds pushing extreme stunts and graphic violence (M = 2.270, 41.0 %) exceed accidental adult pop-up media (M = 2.055, 32.0 %).

Peer Conflict and Bullying (Conduct Risk): Peer hostility in gaming spaces affects over one-third of children, predominantly through intentional group exclusion (M = 2.055, 35.5 %) and in-game chat harassment (M = 2.025, 34.0 %).

High-Severity Stranger Contact (Contact Risk): While registering the lowest overall frequency (M = 1.94), unknown adults posing as peers in game lobbies impact 34.5 % of children (M = 2.140), and direct solicitation of private photos or home data impacts 23.5 % (M = 1.740).

The 1-Hour and 3-Hour Screen Time Thresholds: Unsupervised screen time strongly correlates with total composite risk ($r = +0.461$, $p < 0.01$). Stranger gamer contact experiences a sharp step-jump at the 1-hour mark (M = 1.571 right arrow 2.450), while prolonged usage beyond 3 hours produces peak surges in group exclusion (M = 2.557) and private data solicitation (M = 2.114).
The Developmental "Supervision Cliff": Technical parental controls collapse by 46.9 % (4.393 down to 2.333) from pre-primary (3–6 years) to upper-primary (11–14 years), during which total cyber risk surges by +105.1 % (1.373 to 2.816).
Fear-Driven Reporting Silence: Voluntary incident reporting drops by 31.4 % in older age groups (3.732 down to 2.561) due to children's fear of device confiscation.
Superiority of Technical Controls: Technical filtering correlates more strongly with overall risk reduction ($r = -0.463$) than voluntary incident reporting by the child ($r = -0.250$).
Suggestions
Implement Graduated Technical Filtering: Transition parental controls into age-adapted monitoring as children mature rather than abruptly removing protections during upper-primary years.
Establish Household "Amnesty" Protocols: Create non-punitive disclosure agreements ensuring children are not punished with device confiscation when reporting cyber threats, scams, or accidental purchases.
Integrate Early Digital Scam Literacy: Provide foundational classroom training on identifying deceptive links, fraudulent currency generators, and dark marketing patterns before children engage in unsupervised gaming.
Recommendations
**For Parents:**
Enforce automated operating-system screen limits to keep daily unsupervised use below 2 hours.
Unlink payment cards from minor-accessible devices and require biometric authentication or master passwords for all in-app transactions.
Establish a blame-free reporting culture at home to encourage immediate disclosure of suspected phishing attempts.
**For Schools and Educators:**
Embed the 4Cs threat framework into primary school curricula using practical case studies.
Deploy gamified learning modules focused on identifying phishing traps and predatory dark patterns.
Establish confidential reporting channels for students experiencing peer exclusion and in-game cyberbullying to build digital resilience.
**For Platforms and Regulators:**
Adopt Age-Appropriate Design Codes that disable direct messaging from non-friends and strangers by default for minor accounts.
Legally ban deceptive pop-up advertisements offering free minor-targeted virtual currencies.
Mandate algorithmic "cool-down" circuit breakers that interrupt gameplay or continuous feeds after 60 minutes of uninterrupted screen time...

**References**

1. Amer, G. H. G. (2026). The effect of social media on the rise of cybersecurity crimes among Generation Alpha. Journal of Intelligent Decision Making and Information Science, 3(7s), 333–358.
2. Sonar, P., Pardeshi, S., & Shellar, D. (2026). Raising cyber-smart children in the digital age. International Journal of Science and Research, 15(3), 296–298.
3. Verma, S., Bajpai, R., & Singh, I. (2026). Digital resilience among children born after 2010: A systematic review of Generation Alpha research [Unpublished manuscript / Preprint].
4. Módné Takács, J., & Pogátsnik, M. (2025). Screen natives becoming digital orphans: The online challenges of Generation Alpha. In AIS 2025: Proceedings of the 20th International Symposium on Applied Informatics and Related Areas (pp. 197–202). IEEE.
5. Lahti, H., Kokkonen, M., & Hietajärvi, L. (2024). Social media threats and health among adolescents. Child and Adolescent Psychiatry and Mental Health, 18, Article 62.
6. Ma, J., Su, L., Li, M., Shi, M., & Sun, Y. (2024). Analysis of prevalence and related factors of cyberbullying–victimization among adolescents. Children, 11(10), Article 1193.
7. Mittal, V., Chakrabarti, N., & Mehta, H. (2024). Generation Alpha's engagement with digital media and technology. International Journal of Creative Research Thoughts, 12(6), d620–d630.
8. Sánchez, R., González, A., & Ortiz, D. (2024). Fake profiles and time spent online: Risks for cyberbullying among youth. Current Psychology, 43(30), 26639–26647.

9. Chang, V., Golightly, L., Xu, Q. A., Boonmee, T., & Liu, B. S. (2023). Cybersecurity for children: An investigation into the application of social media. Enterprise Information Systems, 17(11), Article 2188122.
10. Jang, Y., & Ko, B. (2023). Online safety for children and youth under the 4Cs framework: A focus on digital policies in Australia, Canada, and the UK. Children, 10(8), Article 1415.
11. Kaspersky. (2023). Overconfident and over exposed: Are children safe online? (A Kaspersky Report). Kaspersky Lab.
12. Tintori, A., Ciancimino, G., Bombelli, I., Cerbara, L., & Palomba, R. (2023). Children's online safety: Predictive factors of cyberbullying and online grooming involvement. Societies, 13(2), Article 47.
13. Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. International Journal of Child-Computer Interaction, 30, Article 100343.
14. UNICEF. (2021). The state of the world's children 2021: On my mind – Promoting, protecting and caring for children's mental health. United Nations Children's Fund.
15. Ziatdinov, R., & Cilliers, J. (2021). Generation Alpha: Understanding the next cohort of university students. European Journal of Contemporary Education, 10(3), 783–789.
16. Kircaburun, K., & Griffiths, M. D. (2020). The dark side of social media: Understanding cyberbullying and online victimization among adolescents. International Journal of Mental Health and Addiction, 18(4), 1032–1048.
17. Livingstone, S., Mascheroni, G., & Staksrud, E. (2020). European research on children's online risks: Assessing the past and anticipating the future. New Media & Society, 22(3), 517–535...