ISSN 2319 - 5975

Volume 13, No.2, February 2024 – March 2024

International Journal of Networks and Systems

Available Online at http://www.warse.org/IJNS/static/pdf/file/ijns041322024.pdf

https://doi.org/10.30534/ijns/2024/041322024

Protecting our Youth Online: A Comprehensive Review on Strategies to Safeguard Children from Online Threats

Ankith D[1], Kartika M[2], Akash S T[3], Amith N H[4]

[1]Alvas Institute of Engineering and Technology, India, ankithankey123@gmail.com

[2]Alvas Institute of Engineering and Technology, India, karthikmanji4465@gmail.com

[3]Alvas Institute of Engineering and Technology, India, akashthamb@gmail.com

[4]Alvas Institute of Engineering and Technology, India, amithharikantra06@gmail.com

Received Date : January 13, 2024 Accepted Date : February 26, 2024 Published Date : March 07, 2024

ABSTRACT

The evidence about the potential benefits and hazards associated with children's internet usage is expanding along with the global interest in this topic. In order to facilitate comparative study of research findings from lower- and middle-income nations like South Africa, Serbia, the Philippines, Brazil, and Argentina, the Global Kids Online program provides tools and guidelines to national researchers. This study looks at how present child rights laws, particularly those pertaining to the internet, correspond with the expanding body of data. It also looks at ways to influence future policy orientations. It provides information and recommendations for protecting children online based on current research and policy studies [1].

Key words : Cyber safety, Online risks, Child protection, Digital literacy, Internet usage trends

1. INTRODUCTION

In a time when kids are spending more and more time online, it is critical to comprehend and reduce cybersecurity dangers. Although the terms cybersecurity, online security, online safety, and internet security are frequently used synonymously, their meanings differ. Researchers and practitioners have taken an interest in cybersecurity awareness education for kids, which has resulted in the creation of numerous platforms and initiatives. Nonetheless, to evaluate the current status of the discipline, pinpoint gaps, and investigate workable remedies, a thorough assessment of this topic is required. In the context of children's online safety, this study seeks to give such a review by discussing cybersecurity hazards, awareness-raising strategies, and evaluation techniques [2]. Children are increasingly present online, which presents serious issues for their rights, opportunities, and wellbeing as the Internet grows quickly. Although children have access to a multitude of services in the digital world, they also run the danger of experiencing online harassment and privacy violations. In addition, concerns over children's future job market skills are brought up by the changing digital landscape. Given that the Internet has the

ability to further sustainable development goals, regulations that protect children's rights while utilizing the advantages of the digital age are desperately needed. It is still difficult to incorporate evidence-based approaches into policymaking, despite efforts to overcome these problems. The possibilities for forming well-informed policy orientations involving children's Internet use are examined in this essay [1].

2. CONTENT RISKS

2.1 Bullying online

Cyberbullying poses a significant threat to children and young people in the UK, affecting between 8% to 34% of individuals in this demographic. Research indicates that 30% of secondary school students in England have encountered deliberate targeting, threats, or humiliation through online platforms. Alarmingly, girls are reported to be twice as likely as boys to experience persistent cyberbullying, highlighting a gender disparity in online victimization. Furthermore, vulnerable groups such as children with special educational needs, those receiving free school meals, and various ethnic minority groups are at heightened risk. The impact of cyberbullying is profound, often leading to significant distress, particularly among children aged 9-12, and is associated with adverse outcomes including school failure, depression, anxiety, and other psychological issues. Unlike offline bullying, cyberbullying's impersonal nature exacerbates negative feelings, instilling a sense of helplessness and fear among victims [3].

2.2 Porn and other inappropriate material

Startling data about the frequency and effects of children and young people being exposed to online pornography has been released in the US and the UK. According to a US survey, 42% of people between the ages of 10 and 17 had come across online pornography in the previous year, and an astounding 66% of that exposure was unintentional. Comparably, 11% of 9–16-year-olds in the UK reported seeing porn, and 24% said

the experience didn't worry them. Teenagers, those experiencing melancholy, and those facing online harassment or sexual solicitation had significantly greater rates of unwanted exposure. On the other hand, wanted exposure rates were associated with things like breaching rules and having sexual conversations online. There is still a lack of research on the effects of undesired pornography despite these alarming increases [3].

3.INTERNET AND GADGET USAGE TRENDS

One of the notable contemporary trends involves the widespread utilization of diverse applications catering to various activities such as gaming, video creation, photo editing, music, anonymous chatting, ride-hailing, sports, fitness, banking, payment wallets, online shopping, educational resources, and more. Another significant cyber trend revolves around the growing prominence of cloud computing. According to the Australian Bureau of Statistics (ABS), the adoption of paid cloud computing services by businesses exhibited continuous growth, with 42% of businesses utilizing cloud computing in 2018 compared to 31% in 2015-16. Additional trends encompass the widespread embrace of location-based services facilitated by GPS-enabled mobile devices and the increased reliance on web-based platforms. These advanced location and positioning services amalgamate real-world data with virtual information. Navigation services. enable individuals to track each other's locations, locate amenities and transportation options, and even recover lost devices. The heightened usage of web- based platforms and emerging technologies is particularly evident in sectors such as education, healthcare, and government services. This shift reduces the reliance on in-person services like Centrelink and enables the development of large-scale digital solutions.

The digital realm has facilitated enhanced connectivity and accelerated long-distance communication. The widespread availability of high-speed internet has simplified virtual networking, distance learning, and recreational pursuits. Moreover, the advent of cloud computing and data sharing has fostered online collaborations among various entities striving towards shared objectives, such as combating crime or implementing health initiatives. Increasingly, mobile phones and the internet are recognized as valuable tools for augmenting personal safety and well- being.

4. OBSTACLES BROUGHT ABOUT BY CURRENT LAWS AND REGULATIONS

The multiplicity of settings and the complexity of children's online experiences may appear to be rather complicated, making it difficult to implement straightforward policies that support digital inclusion and better realize children's rights.15 It should come as no surprise that there are many problems with the laws and regulations in place, not the least of which is the inconsistent use of evidence in the policy-making process. Our quick scan of the policies turned up a few. The conceptualization of legislative frameworks is overly limited. Certain legal systems may be too limited in scope to adequately reflect all the nuances of the experiences that children have. According to UNICEF (2012), "sexting," or the exchange of sexualized or naked photographs among teens, is prohibited in several nations and can lead to youth prosecution and punishment under national pornography laws [1].

5 . THE ECOSYSTEM OF HAZARDS AND PROTECTIVE FACTORS IN THE CYBER WORLD

Researchers argue that adopting an ecological framework is crucial for understanding contextual risks, vulnerabilities, and protective factors related to online behavior. The larger social context, which include elements like race, ethnicity, gender, class, and religion, influences both offline and online behaviors. Thus, children and young people encounter risks and protective factors at multiple levels, influenced by complex interactions within individual, family, peer, and community spheres. Offenders and bullies operate within a societal framework where gender stereotypes, inequalities, coercion, victim- blaming, blurred boundaries between sexting and harassment, and a lack of compression of consent are normalized. Some studies suggest that technology-facilitated abuse is a form of gender-based violence, with data indicating that girls are at higher risk.

These research findings are supported by a 2017 survey conducted in Australia on experiences of image-based abuse, which reveals that young people, women, individuals with disabilities, and those from LGBTIQ, culturally and linguistically diverse (CALD), and Aboriginal and Torres Strait Islander communities face a higher proportion of risks. There is evidence that kids and young people who have witnessed family violence or experienced child maltreatment, and suffer from emotional dysregulation, internalize a belief system that normalizes violence. Consequently, some individuals are more likely to engage in victimizing behaviors towards their peers, while others become victims themselves, regardless of whether the abuse occurs online or offline.

Insufficient technical skills, such as a lack of knowledge about privacy settings, filtering mechanisms, security monitoring, or the ability to recognize fake news, among children, young people, parents, and educators, can increase threat to various risks.

6 PROTECTIVEELEMENTS FOR CHILDREN AND ADOLESCENTS

Enhancing individual capabilities: Empowering children to recognize their agency and fostering their social and emotional competencies contribute to critical thinking, self-esteem, and empathy.

Enhancing technical capabilities: Equipping children, parents, caregivers, and educators with the necessary technical knowledge to understand online risks and establish informed filters and security measures.

Implementing age-appropriate mediation strategies: Employing appropriate strategies for actively monitoring and supervising technology use, tailored to the age and developmental stage of children, can act as additional protective measures.

7. THE ECOSYSTEM OF DANGERS AND SAFEGUARDS IN THE CYBER WORLD

As scholars arguing for an ecological paradigm have pointed out, a sophisticated knowledge of hazards and protective variables is critical in the cyber world. This approach acknowledges the complex interplay between individual, familial, peer, and community factors and online behaviour, including cultural standards pertaining to race, ethnicity, gender, and class. Offenders can operate freely in an atmosphere where gender stereotypes, inequality, and the boundaries between online interactions are blurred. Research indicates that abuse enabled by technology frequently mirrors gender-based violence, with a disproportionate impact on females. Furthermore, those who belong to marginalized groups—like the disabled or people from different cultural backgrounds—face increased dangers. Children's, parents', and educators' low technological literacy increases their susceptibility to internet threats. Nonetheless, protective variables, which include personal aptitude, technical expertise, supportive peer [4].

8.THE LITERATURE HIGHLIGHTS TYPES OF MEDIATION STRATEGIES:

Facilitating/active social mediation: Engaging in direct and indirect conversations with children to openly discuss and evaluate the risks and benefits associated with their online activities.

Facilitating technical mediation: Monitoring children's digital media usage and physical movements through surveillance and checking their online activities.

Restrictive social mediation: Implementing conditional, time-based, or activity-based restrictions on children's online behaviors.

Restrictive technical mediation: Utilizing filtering software and restricting access to certain types of online content.

9. STRATERGY USED TO PROTECT CHILD

Child rights perspective: Emphasizing equitable and age-appropriate access, meaningful participation, and involving children and young people in decision- making processes related to school and legal policy development.

Digital resilience: Enhancing the technical skills and critical thinking abilities of all stakeholders to empower them in navigating the online environment safely.

Evidence-informed and context-specific approach: Designing cyber-safety programs based on research evidence, with clear outcomes in mind, while tailoring them to the specific context in which they will be implemented.

Training and education: Providing adequate training to teachers, parents, caregivers, program delivery consultants, and community members about safe internet practices and understanding kids and young people's perspectives of the internet.

Systemic collaboration: Encouraging collaborations between families, schools, and communities to collectively address cyber-safety issues.

Reporting mechanisms: Establishing clear, safe, and effective pathways for reporting incidents of abuse or concerning online behavior.

Consistent support: Providing ongoing support and guidance to all stakeholders involved in implementing the cyber-safety program.

10. CONCLUSION

This review emphasizes that the rapid advancements in technology have brought both unprecedented risks and opportunities for children and young people. With the right utilization of technical tools, age- appropriate filters, and access to accurate information, the cyber world can become a space where young minds can flourish. Research indicates the emergence of a multidimensional approach to cyber-safety that recognizes the power and potential of the internet, emphasizing harm minimization rather than strict protection. The recent COVID-19 pandemic has further underscored the importance of building digital literacy and resilience. There is a growing interest in understanding children's and young people's perspectives of the digital environment, including their motivations for engaging with the online world. Studies like the Global Kids Online contribute to the expanding body

of knowledge on these perspectives on a global scale. This new approach aligns with the child rights perspective, valuing and respecting children's skills, capabilities, and meaningful participation in decision- making processes. The literature highlights the significance of enhancing digital literacy and technical skills among parents, caregivers, educators, and community members. It also stresses the need for a systems approach involving policymakers, commercial stakeholders, and law enforcement bodies. Regular data collection, monitoring, research, and the continued development of an evidence base are crucial for understanding and implementing effective cyber-safety approaches.

REFERENCES

1. Jasmina Byrne & Patrick Burton. Children as Internet users: how can evidence better inform policy debate? Published by Informa UK Limited, trading as Taylor & Francis Group, Journal of Cyber Policy, Vol. 2, No. 1, pp. 39-55, 22 Feb 2017
2. Farzana Quayyum, Daniela S. Cruzes, and Letizia Jaccheri. Cybersecurity awareness for children: A systematic literature review. Norwegian University of Science and Technology (NTNU), Trondheim, Norway. International Journal of Child-Computer Interaction, 16 June 2021.
3. Emily R. Munro. The protection of children online: A brief scoping review to identify vulnerable groups, University College London, June 2011.
4. Dakhina Mitra. Keeping children safe online: A literature review. cfecfw.asn.au, July 2020.