Cyber Security Experts Association of Nigeria (CSEAN)
Society for Multidisciplinary & Advanced Research Techniques (SMART)
West Midlands Open University
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Sekinah-Hope Foundation for Female STEM Education
ICT University Foundations USA
Academic Innovations City University Foundations

Proceedings of the Cyber Secure Nigeria Conference – 2024

Safeguarding Children in the Digital Age: Research Gaps and Future Directions

Oluwatoni Falade & Sadiq Nasir
Child Online Protection Network
School of Information Technology and Computing (SITC),
American University of Nigeria,
Yola, Adamawa State, Nigeria
E-mails: oluwatonifaladea@gmail.com; Sadiq.nasir@aun.edu.ng

ABSTRACT

Digital technology has had a significant impact on our lives. As a result, there is a growing concern about children's online safety. This research investigates children's cybersecurity risk in the digital era, focusing on Nigeria as a developing economy with objectives to understand the cybersecurity risk children face in the digital era, explore various ways to mitigate cybersecurity risk to enhance child online safety and present strategies that can be applied to build resilience in children to be better protected from various cybersecurity risks. This study has been able to identify and categorise various cybersecurity threats faced by children. This research has presented the role of risk assessment, data protection and real-time monitoring. This study offers strategies for making children more resilient and covers basic cybersecurity hygiene practices; open communication has been established as the key pillar in building resilience in children. The study concludes by opining that the use of digital technologies has made it essential to develop urgent strategies to mitigate cybersecurity risks. There is a need to develop age-appropriate digital literacy programs for children to educate them about various strategies, improve collaboration between parents, guidance and educators to aid with the development of a safe environment for children, advocate for stringent policies to help address the challenge of child online safety and promote continuous research to understand cybersecurity risk, which continues to evolve and can provide effective preventive measures and policies.

Keywords — Cyberbullying, Cyberstalking, Phishing, Stranger Danger, Privacy Concerns, Safety Concerns, Child Online Safety

Proceedings Citation Format
Oluwatoni Falade & Sadiq Nasir (2024): Safeguarding Children in the Digital Age: Research Gaps and Future Directions. Proceedings of the Cyber Secure Nigeria Conference held at The Ballroom Center, Central Business District, Federal Capital Territory, Abuja, Nigeria - 25th - 26th September, 2024. Pp 83-90. https://cybersecurenigeria.org/conference-proceedings/volume-1-2024/ dx.doi.org/10.22624/AIMS/CSEAN-SMART2024P8

1. INTRODUCTION

The increasing relevance of technologies, multimedia, and the internet in children's lives has encouraged a dynamic debate about their implications among parents, teachers, researchers, policymakers, and the general public, perhaps because of the frequent media coverage of disturbing stories about the activities of criminals in cyberspace [1]. Cybersecurity, internet security, internet safety, online security, and online safety are substituted for one another in various literature to express cybersecurity risk [2]. Children are regarded as human beings between the stages of birth and puberty. During this period, they require care and supervision to grow psychologically, logically, and socially. At an early age, parents often pacify and entertain their children with music and cartoons, which they become accustomed to as they grow older. As they mature, children gain greater access to devices and a more comprehensive range of applications, including social [3]. There are serious concerns about the conscience making digital devices available to children at an early age during their developmental stages; hence, the associated risks cannot be ignored [4].

Digital technologies offer numerous benefits, including quick access to information, chances for skill enhancement, social interaction, fostering creativity, and enhancing digital literacy [5]. However, they also present serious risks, such as cyberbullying, exploitation, exposure to inappropriate content, online predators, phishing, identity theft, and privacy concerns [2]. According to a 2018 report by the DQ Institute, approximately 54% of Nigerian children between the ages of 8 and 12 were exposed to at least one cyber risk. With the increasing digital literacy in the country, this percentage has probably risen [6]. There are various motivations for cybercriminals on the internet and social media.

One of the most common drives is accessing personal information and financial details. Some other reasons include sexual exploitation and the stealing of identities. Social media is used to build relationships with children and then gain their trust before exploiting them [7]; no wonder the American Academy of Paediatrics (AAP) suggests that parents restrict their children's social media usage and stay mindful of the possible cyber psychological hazards and cybersecurity threats that can result from using these platforms [8]. However, other studies have suggested implementing evidence-based policies that balance maximising opportunities and minimising risks [9].

It is crucial to comprehensively understand the challenges children may encounter in the digital world to ensure their safety and well-being. This can only be achieved by establishing healthy routines, supervising their online activity, and implementing parental controls. Parents must take steps to protect their children and safeguard their digital experiences [10]. Despite the importance of technology in safeguarding children online, studies to mitigate cyber risk using technologies are limited. This research reviews a significant number of studies on cybersecurity risks children face. It also explores building resilience in children and proposes a roadmap for addressing challenges. Additionally, the research identifies gaps in current knowledge and suggests future directions for further study. A limitation of this study is that it does not delve into the debate of whether children should have access to technology at a young age.

Hypothesis
The rising adoption and usage of digital technology among children in Nigeria have increased children's cybersecurity risk, affecting their safety and well-being. The implementation of good resilience and proactive measures ensures that children can be kept safe and helps in the migration of these risks.

Research question
1- What are the cybersecurity risks faced by children in Nigeria?
2- How does prolonged internet use affect children, mainly their well-being?
3- How can adopting resilience in children be better to ensure that children are safe from cybersecurity risk?

Research Methodology
In this work, literature from 2019 to 2023 was selected. The author used two databases for this research: Google Scholar and Proquest. The keywords used in this research are cyberbullying, cyberstalking, phishing, stranger danger, privacy concerns, safety concerns, and child online safety. The next stage was to group the researched papers into groups based on themes to allow proper evaluation and synthesis. During the search and selection of the research paper, about 100 documents were downloaded from the two databases, and then about 22 papers were selected based on relevance to the research work.

2. LITERATURE REVIEW

A. Cybersecurity Risks Faced by Children
There has been an increase in cybercriminal activities against children, thus increasing the risk of being online. Research has identified various cybersecurity risks which are associated with the usage of digital devices by children. These risks fall into four broad categories: content risks, sexually-oriented pictures and movies, materials considered violent, or even materials that can promote the utilisation of drugs.

Spending Too Much Time Online
Excessive internet use can have adverse effects [3]. This has been linked to various health problems [11] [12], accidents [13] [14] [14], and low school performance [14]. According to the 2020 Child Online Safety Index report, it was highlighted that children in Nigeria excessively use digital technology daily.

Cyberbullying
In this digital age, cyberbullying has emerged as a serious concern. It includes digital communication tools that can cause harm through threat, humiliation and more [8] (Hinduja & Patchin, 2020). This form of bullying can significantly impact young people's mental health challenges, resulting in anxiety and other side effects [8].

Privacy and Identity Theft
Children are highly susceptible to privacy issues as they may not fully grasp the implications of sharing their personal information online. Research has shown that children typically begin to get the concept of privacy management at around 8 to 11 years old [8] (Stoilova et al., 2019), meaning children below this age are unaware of the implications.

This can lead to severe consequences, including privacy breaches and identity theft, whereby their name, location, school, and contact information may be exposed [15]. Although Social media platforms like Snapchat and Instagram portray themselves as temporary content curators, allowing users to send text, images, and videos, this does not eliminate the potential risks users are exposed to [16]. Similarly, advancements in technology such as smart toys, online games, child trackers, and other innovations have raised significant concerns regarding privacy and safety [16] [17] [17].

Inappropriate Content

Children can inadvertently come across offensive, illegal, or inappropriate content while browsing the internet without even intending to. This content and contacts include stranger danger [8] (Muir & Joinson, 2020), pornography, sexting, texting, fraud, and harmful user-generated content [18]. These experiences have led to depression, anxiety, and suicide [8] (Sonthalia, 2021).

Online Predators

Although the internet can offer excellent prospects for communication and new relationships, it can also be a breeding ground for criminals who take advantage of its anonymity, bringing about severe risk to its users. The most typical contact risk situation is when a threat actor with a bias for sexual exploitation can take advantage of a child's vulnerability online. Unfortunately, there have been reports of predators using fake identities on social media to connect with children, gain their trust, and request in-person meetings. It is essential to be aware that online predators exist and may use deceitful tactics to form relationships with children for harmful reasons. These situations can put children at risk for abduction, exploitation, or grooming [7].

Social Engineering: Phishing and Malware

Cybercriminals may attempt to manipulate children into revealing sensitive information or performing harmful actions, such as sharing passwords or financial details. Phishing is a well-known form of social engineering in which threat actors attempt to deceive unsuspecting persons and steal their vital information [8] (Burrell & Nobles, 2023). Children may unknowingly download malicious software (malware) or fall victim to phishing scams that can compromise their devices or personal data [19].

Location Tracking

Location tracking services and other phone-tracking features also put users at risk, especially children [8] (Özkul, 2022; Mantelero, 2016). It can expose their whereabouts to people with bad intentions. Furthermore, when specific tracking tools are installed on a child's mobile device, their location and activities can be monitored, which is a severe risk. Many parents and guardians depend on the smartphone feature to enable them to track and protect their children (Sukk & Siibak, 2021).

B. Role of Technology in Cyber Risk Mitigation

Technology has become critical in managing cyber risks in today's fast-paced world. With the constantly emerging technologies, one of the essential roles of technology is data-driven risk assessment. This can be achieved through machine learning, artificial intelligence, and advanced analytics.

This approach allows for identifying, analysing, and evaluating risks, leading to improved risk insights, informed decision-making, and timely responses. Another role of technology is cybersecurity and data protection. This framework involves the implementation of various cyber risk security solutions and tools, for example, Firewalls, Intrusion Detection/ Prevention Systems (IDS/IPS), Antivirus and Anti-malware Software, and Multi-Factor Authentication [20].

Furthermore, technology enhances real-time risk monitoring. With real-time data collection, potential risks or threats can be immediately identified, analysed, and treated. Advanced monitoring tools and automated alerts enable prompt risk identification and response, minimising potential damage. Also, technology enhances communications, information sharing, and collaboration amongst risk management teams. In addition, it provides timely risk insight. Finally, technology improves training and awareness. It enhances training and awareness programs' planning, design, and implementation.
Building Resilience in Children

There is rapid development in the ICT field [21]; the constant evolution of software and hardware is the reason here. This and other changes also affect children's cybersecurity threats; the threats are continuously evolving and becoming more complex. Some of the side effects of these threats are children's emotional, psychological, and physical well-being. Resiliency in children has a lot of interest from researchers as a means by which these risks can be mitigated. This proactive method is applied to children to gain an aggressive advantage over cyber risk. Resilience in children refers to recognising threats and for the child to be able to mitigate these threats.

3. BENEFITS OF MITIGATING CYBER RISKS

Cyber resilience refers to the capacity to adapt when confronted with cybersecurity risk; this has witnessed an evolution in the cybersecurity posture of establishments. This skill is required for children to have; this is important because it allows individuals to adapt to the challenges by reducing the possible outcomes of the effects of cybersecurity risk. In cybersecurity, resilience gives these individuals a defence mechanism towards potential harm.

How to develop resilience in children

The process of developing resilience in children requires multiple approaches; this is because there is no silver bullet as to which method will work best. This process involves a lot of education, awareness and the correct skill set. Various researchers have proposed multiple strategies in this domain.

Digital Literacy Education

Children must have completed an excellent digital literacy education course. Keep children informed [22] [23]. An excellent, structured curriculum should enable the children to understand the risks that are available online and the possible mitigation strategies.

Cybersecurity hygiene practice

Cyber hygiene refers to the set of safe and responsible practices that individuals must follow to ensure that their devices and online presence remain secure from various cybersecurity attacks, such as hacking, phishing, malware, and other forms of cybercrime. There is a need for children to be aware of the essential cybersecurity hygiene practices [23]; some of the basic cybersecurity hygiene practices are the use of strong passwords, how the privacy setting works and how to manage it on various platforms, not clicking on every link, making decisions on what to post online and what not to post.

Open Communications

[23] suggest the need for parent-child collaboration. This collaboration needs to help children become cyber-reliant. Open communication between the parents and children can help reduce children's bullying behaviour. [23] was able to suggest that children start their learning process at home. This makes it very important for the child to learn more about cybersecurity as they use mobile devices. This means the children need good and sound cybersecurity education and digital skills development. [23] suggests that collaboration can lead to faster learning from children, centred around reading books and using computers. This means that cooperation between the child and parents is essential.

4. RESULTS AND DISCUSSION

From the synthesis of the literature, this research work has highlighted the critical cybersecurity risks children face in the digital era. Technology has been established as necessary in the role and management of cybersecurity risk; this has been presented as a risk. Assessment, cyber security measures, real-time monitoring and enhanced communication. Also, this literature's findings have been able to establish that building resilience in children is very important, placing importance on literacy education, cybersecurity hygiene practices and the continuous open communication between parents/ guardians and the children,

4.1 Limitation of Research

Timeframe limitation: This research focuses on publications from 2019 to 2023. Geographical focus: The research is limited to publications relevant to developing countries, and Nigeria is a developing economy. Data source: This research relied on Google Scholar and Proquest data.

4.2 Research Gaps

The following are some of the identified research gaps in the domain;

a) There is not much extensive research on the long-term work longitudinal effects of exposing children to digital devices for extended periods.
b) There are research gaps around developing more effective digital resilience strategies for children.
c) There are gaps in research on the effects of policy and regulation in addressing online child protection challenges.

5. CONCLUSION

Children in modern times have their lives so much connected to digital technologies. Keeping the children safe online has become a matter of concern. Children are vulnerable to online fraud and exposure to risky content. The rise of cyber risk that children are exposed to is mainly due to social media and other technological innovations. This research has highlighted the research gap in this domain and presented models and a roadmap to mitigate these growing concerns. This research was able to synthesise 100 relevant research papers and categorise them into various themes. As a result, the study has presented the best way to build resilience in children and suggests keeping children safe online.

5.1 Future Directions

Researchers and stakeholders can consider the following directions for future studies and actions:

a) Future research in this domain can consider the effects of long-term exposure of children to digital devices.
b) There is a need to research the positive effects of digital devices on children.

BIBLIOGRAPHY

[1] J. Guan and J. Huck, “Children in the digital age: exploring issues of cybersecurity,” in Proceedings of the 2012 iConference, 2012, pp. 506–507.
[2] F. Quayyum, D. S. Cruzes, and L. Jaccheri, “Cybersecurity awareness for children: A systematic literature review,” Int. J. Child-Comput. Interact., vol. 30, p. 100343, 2021.
[3] S. Yadav and P. Chakraborty, “Psychological Impact of Using Smartphone on Four-to Ten-Year-Old Children,” in International Conference on Innovative Computing and Communications: Proceedings of ICICC 2022, Volume 2, Springer, 2022, pp. 569–576.
[4] S. Madigan, B. A. McArthur, C. Anhorn, R. Eirich, and D. A. Christakis, “Associations between screen use and child language skills: a systematic review and meta-analysis,” JAMA Pediatr., vol. 174, no. 7, pp. 665–675, 2020.
[5] V. Rideout and M. B. Robb, “The Common Sense census: Media use by kids age zero to eight,” San Franc. CA Common Sense Media, vol. 263, p. 283, 2017.
[6] S. Liverpool et al., “Engaging children and young people in digital mental health interventions: a systematic review of modes of delivery, facilitators, and barriers,” J. Med. Internet Res., vol. 22, no. 6, p. e16317, 2020.
[7] D. N. Burrell and C. Nobles, “A Practical and Real-world Discussion of Safety Risks to Children in Cyberspace,” 2023.
[8] E. Bozzola et al., “The use of social media in children and adolescents: Scoping review on the potential risks,” Int. J. Environ. Res. Public. Health, vol. 19, no. 16, p. 9960, 2022.
[9] A. O. Opesade Dr, “An Assessment of Global Research Activities on Children and Adolescent Online Security,” J. Cybersecurity Educ. Res. Pract., vol. 2020, no. 1, p. 4, 2020.
[10]P. Limone and G. A. Toto, “Psychological and emotional effects of Digital Technology on Children in Covid-19 Pandemic,” Brain Sci., vol. 11, no. 9, p. 1126, 2021.
[11] T. N. Robinson et al., “Screen media exposure and obesity in children and adolescents,” Pediatrics, vol. 140, no. Supplement_2, pp. S97–S101, 2017.

[12] Y. Zou, N. Xia, Y. Zou, Z. Chen, and Y. Wen, "Smartphone addiction may be associated with adolescent hypertension: a cross-sectional study among junior school students in China," BMC Pediatr., vol. 19, pp. 1–8, 2019.
[13] A. A. Elsheikh, S. A. Elsharkawy, and D. S. Ahmed, "Impact of smartphone use at bedtime on sleep quality and academic activities among medical students at Al-Azhar University at Cairo," J. Public Health, pp. 1–10, 2023.
[14] T. Kliesener, C. Meigen, W. Kiess, and T. Poulain, "Associations between problematic smartphone use and behavioural difficulties, quality of life, and school performance among children and adolescents," BMC Psychiatry