Hyper-Connected: Information Security Education for Today's Children

Elekanyani Mukondeleli, Molebogeng Latakgomo, Oyena Mahlasela and Nokuthaba Siphambili
Council of Scientific and Industrial Research, Pretoria, South Africa

emukondeleli@csir.co.za
mlatakgomo@csir.co.za
omahlasela@csir.co.za
nsiphambili@csir.co.za

Abstract: The digital landscape has become an integral part of modern childhood. While technology offers a wealth of educational and social opportunities, it also presents a growing number of information security threats that children are often ill-prepared to handle. This research explores the critical need for information security education specifically tailored to the online habits and vulnerabilities of today's hyperconnected children. The literature review was conducted to assess the vulnerabilities faced by children. Therefore, this study proposed an information security framework to equip children with the knowledge and skills necessary to navigate the online world safely and responsibly. The framework comprises five components: education, awareness and training, technology and tools, community support network, policies and regulations, and behavioural strategy. The information security framework can be applied as a tool in protecting children from falling victim to online threats

Keywords: Information security education, Cybersecurity awareness, Cybersecurity training, Cyber threats for children, Cyber education

1. Introduction

The digital landscape has become an integral part of modern childhood, fundamentally altering how children interact, learn, and play. With the ever-growing presence of technology, children have unprecedented access to a wealth of educational resources and social opportunities (Kerridge, 2023). Educational platforms like online games and social media have become core elements of their daily lives, and ways of learning and communicating have evolved in ways one could have never imagined (Chaudron et al., 2018). This digital evolution also exposes children to many information security threats they are unprepared for (Livingstone et al., 2019). Digital tools have been embraced by children at such a rapid rate that their social and psychological functions can no longer be separated from their online activities (Granic et al., 2020).

Despite the potential benefits, the digital world is loaded with risks that can significantly impact children's safety and well-being. One of the primary concerns is the prevalence of online scams and phishing attempts (Laczi, and Póser, 2024). Cybercriminals exploit children's naivety and lack of awareness by making them prime targets for fraudulent schemes (Carpenter, 2019). Moreover, cyberbullying has emerged as a significant issue, worsening the effects on children's privacy (Wright, 2022). Privacy breaches are a critical threat as children often unknowingly share personal information that can be misused (Livingstone et al., 2019).

The General Data Protection Regulation (GDPR) is a European law that focuses on protecting European citizens' data when organisations handle data subjects' personal data (GDPR, 2016). The Protection of Personal Information Act (POPIA) is a South African act that aims to protect individual personal information when processed and ensures that personal information is protected against unlawful collection, use and disclosure (POPIA, 2020). These regulations also focus on protecting children's data and information online. In addition, the USA's Children Online Privacy Protection Rule (COPPA) restricts operators of websites or online services that target children under the age of thirteen and knowingly gather personal data from children under the age of thirteen (COPPA, 2013). The Cybercrimes Act focuses on the reduction of crimes committed online in South Africa (Cybercrimes Act, 2021).

Given these threats, there is an urgent need for comprehensive information security education tailored to the unique online behaviours and vulnerabilities of today's hyperconnected junior-school-aged children aged 5 to 13 years, as most children spend their time on mobile devices (Kopecký et al., 2021). Current educational approaches often fail to address these demographics' specific needs and challenges, leaving a significant gap in their preparedness to navigate the digital world safely (Stoilova et al., 2020). This research aims to explore the critical need for targeted information security education for children through a literature review. This study analyses current threats and proposes enhanced methods to equip children with the necessary knowledge and

skills by identifying and addressing the limitations of current approaches. This research seeks to develop robust information security education methods that can empower children to engage with the digital world safely and responsibly.

This paper is structured as follows. The methodology for the study is discussed in section 2, followed by a literature review in section 3. A discussion is provided in section 4, and section 5 concludes the paper with directions for future work.

2. Methodology

The main research question that guided the study was, "Is there a critical requirement for information security education for children? This qualitative research explored a literature review to examine the existing literature on the critical need for information security education for children. Examining different scholarly databases such as Web of Science, Scopus and Google Scholar search engine for comprehensive results. Thereafter, a thematic analysis was applied to formulate themes that were common in the literature. Therefore, the systematic review included publications from 2019 – 2024 which aimed to examine the critical need for information security education for children.

3. Literature Review

It is important for parents to identify Artificial intelligence (AI) related cyber threats to protect children from online dangers. Therefore, parents need to take proactive measures to protect children's digital footprint. This paper discusses the impending threats trending threats that children may face online. AI has changed the digital landscape, making it easy for anyone to use AI to create realistic videos, images and audio (Center for Countering Digital Hate, 2023). AI-generated content can be used to create false or distorted images of children and friends to attack or shame them. For example, deepfakes can be used to force children to take action that they would not normally do, like giving out personal information to predators unknowingly.

The introduction of generative AI can also pose a danger to children as it can easily spread stereotypes, biases and even hate, as deepfakes can be created without having the computational skill or knowledge (Mahlasela et al., 2024). Studies show that the increase of generative AI content advances stereotypes, biases, and hate, to which children may fall victim. Thus, parents or guardians must take a proactive role in educating children on the negative outcomes that may be caused by deepfakes. Even though there are no universal AI policies in place to safeguard children, there are Acts that protect children online such as the USA's Kids Online Safety Act adopted in 2021 which addresses the protection of minors in social media platforms (Center for Countering Digital Hate, 2023). However, this legislation only addresses social media platforms and not how data is collected about minors through educational institutions' platforms, email services, and web service providers.

The other impending threat associated with generative AI that is observed in literature is how generative tools are used to encourage eating disorders among young users (CCDH). The study done by Ahmed (2023) examined 6 popular platforms: ChatGPT, Gemini, MyAI, Dall-E, MidJourney, and DreamStudio on how they can generate images that promote eating disorders. The results show that minors can easily create harmful content, for example, chewing and spitting food for weight loss.

3.1 Social Media Dominance

Social media use has become a crucial part of children's lives (Hadjipanayis et al., 2019). Applications such as TikTok, Facebook, and Twitter have radically altered how children engage with their peers and parents, obtain information, and share their interests (Rao and Kalyani, 2022). These platforms encourage creative and social interaction, but they also bring up issues with excessive screen time, mental health effects, and privacy. Social networking offers kids and teenagers many advantages and opportunities, but it also has a lot of concerns. Benefits include better communication and sociability, enhanced learning, favourable effects on schooling, and access to health information. Falsifying one's age and identity, cyberbullying, Facebook depression, games and sleep difficulties are some of the potential risks associated with social media use (Hadjipanayis et al., 2019). The constant pressure to create interesting content, together with the risk of cyberbullying and exploitation, can be harmful to kids' mental health and well-being. Excessive use of social media and the desire to become an online celebrity have been related in research to higher rates of anxiety, sadness, and concerns about body image in young people (Abi-Jaoude et al., 2020).

3.2 Increased Screen Time

Excessive screen time in child and adolescent populations is associated with short sleep duration (Chaudron et al., 2018). This is because spending too much time on electronic devices can have adverse consequences for important developmental processes, such as short sleep duration. Additionally, screen time has been linked to obesity, sleep problems, depression, and anxiety (Oswald et al., 2020). The use of screens by children has increased due to technological advancements in recent years, which has decreased their interaction with nature and negatively impacted their mental and general well-being (Domingues-Montanari, 2017). It can hinder the growth of focus, attention, and social skills. Children who spend a lot of time on social media may have trouble with empathy and face-to-face communication. Increasing the amount of screen time at an early age has negative effects on language development (Karani et al., 2022). However, beginning screen time at a later age has some potential benefits (Karani et al., 2022). The characteristics of videos, their content, and co-viewing also play a role in influencing language development (Karani et al., 2022). However, other studies have reported negative effects on speech, language, motor skills, cognitive development, and social development (Karani et al., 2022).

3.3 Increased Targeting on Popular Platforms

The other cyber threat that children can face is the increasing target on popular platforms. Online criminals are becoming intelligent about where to find children. These cyber criminals are using popular online games, virtual reality (VR) products and even educational apps to target their victims. The popularity of virtual reality products has created a new market for social media platforms to sell new social experiences to children (CCDH). However, the use of VR imposes threats to minors, as some VR chats enable minors to interact with others using avatars in a virtual world, exposing them to inappropriate content such as racial slurs and threats of violence (CCDH). Thus, VR platforms can be a breeding ground for inappropriate content and exposure to cybercriminals.

Moreover, in gaming, cyber criminals are using online games to target children. They may befriend and create fake profiles to appear younger to build trust. These predators target children through fake websites and even emails disguised as legitimate game stores to steal children's credentials (Bennani, 2022). Sometimes, they may sell fake items in games with fake currency to defraud children. For example, they can ask a child to claim free rewards to buy a new outfit by clicking /logging on a website to claim the rewards.

3.4 Complexity of Cyber Threats

There is also a growing complexity of cyber threats. Children are increasingly facing more cyber threats due to their exposure to digital environments. Cases of cyberbullying have grown as perpetrators are now targeting their victims anonymously across different social media platforms so they can connect with children online (Bennani, 2022; van Tiel, 2020). Children normally download and play games on mobile phones and cybercriminals sneak malware into the apps (Abi-Jaoude et al.,2020). Malware can display inappropriate content to children and steal data. Kaspersky Baciu-Ureche et al., (2019) claims that online criminals increasingly use clone apps with the help of AI. There is an increase in unwanted ads or pop-ups that show inappropriate content and images. Criminals are continuously using social engineering tactics to impersonate children's friends and family so that children share their personal information (Center for Countering Digital Hate, 2023). Mahlasela et al., (2024) states that deepfakes are now used to create fake content to manipulate victims into giving out their personal information and to commit fraud. Cybercriminals are using emerging technology to get personal information on children by targeting them.

3.5 Impersonation

Children's trust and persuasion by peers and authority figures make them vulnerable to impersonation attempts, classified as social engineering in which the perpetrator poses as someone they are not, frequently with malicious intent. Impersonation can be done with a variety of techniques and resources. These attacks can be conducted in person or through technological methods like smishing, spear-phishing, phishing, and vishing. Children may suffer psychological distress due to betrayal and fear of being ruled out (Guo and Zhang, 2020).

3.6 Botnet Attack

A Botnet attack involves automated social media accounts that can create posts, follow new accounts, and perform various malicious activities. This can expose children to inappropriate substances, violate their privacy by stealing their data, and manipulate them by spreading false information. Additionally, botnets can send phishing messages, automate cyberbullying, and use Distributed Denial of Service (DDoS) attacks to interfere with online activities (Orabi et al., 2020).

3.7 Malware Attack

Malware attack are the most common type of attack on social media platforms. It begins with the hacker injecting malware scripts into the actual user's account (Stankov & Tsochev, 2020). When children click on malicious URLs, which can cause system disruption and data theft. Unauthorised device access, exposure to improper content, and theft of personal information are possible outcomes of this. By affecting files and slowing down devices, malware can also interfere with their education and cause serious emotional distress.

4. Discussion

It is evident that there is a need for information security education for children. As discussed in the literature, in this digital age, children are more connected than ever, and this presents unique challenges for information security education. Therefore, a comprehensive approach is required to effectively address these challenges. As children are exposed to the digital world at an early age, it is important to teach and raise awareness about safe online behaviour and cyber threat prevention. Children need to be taught about their digital footprints and the repercussions of their online behaviour by their parents, guardians, and teachers (Karabatak & Karabatak, 2020). Children must learn that anything posted online stays online and should be cautious about what they share since online criminals are constantly looking for vulnerabilities. It is also imperative that children acquire knowledge about phishing attempts and the significance of creating robust, unidentifiable passwords to ward off cybercriminals (Sprung et al., 2020). Children can be shielded from online predators by taking these precautions.

On the other hand, parents and guardians must use privacy settings and restrictions to restrict children's usage of social media and what they access online (van Tiel, 2020). By doing this, instances of children being exposed to inappropriate content will be prevented. Therefore, to build a safe online environment for everyone, regardless of age, it is crucial to teach children how to respond to cyber threats and how to interact with others (Karabatak & Karabatak, 2020; Sprung et al., 2020; van Tiel, 2020). Awareness of cyber threats is critical to combating cyberbullying and the spread of inappropriate content. When children understand appropriate internet behaviour, it can help reduce mental health issues and depression instances of depression.

4.1 Lack of Awareness and Education

The lack of awareness and education among children regarding cybersecurity is one of the main challenges. Even though children are growing up in the digital age, many of them do not possess a fundamental understanding of online risks and safe practices. This lack of knowledge can lead to increased vulnerability to cyber threats. While it can be assumed that children are native to the digital world and believe that they should naturally be equipped to navigate the online world safely, research shows that this is not necessarily the case (Drevin et al., 2022). Children can be proficient in using the technology but often lack the critical awareness needed to identify and avoid online risks (Drevin et al., 2022). A study by Drevin et al., (2022) found that children do not understand the implementation of sharing personal information online and the risks associated with interacting with strangers on social media.

There is also a knowledge gap in the absence of structured information security education within the school curriculum (Rahman et al., 2020). Many education systems do not prioritise cybersecurity education, which leaves children without the necessary skills to protect themselves online (Ayyash et al., 2024; Iradat, 2024; Ondrušková & Pospíšil, 2023; Hart et al., 2020). The integration of cybersecurity awareness into the school curriculum is important as it will address this issue (Quayyum et al., 2021). Regions like sub-Saharan Africa have particularly low levels of information security awareness among students, highlighting the need for comprehensive educational programs in these areas (Granic et al., 2020). To solve this problem, it is essential to develop, implement and maintain comprehensive security education, training and awareness programs. These programs should aim to educate about the basics of cybersecurity, including phishing attempts, understanding the importance of strong passwords, and understanding the importance of not sharing personal information. These educational initiatives should be incorporated into the school curriculum from an early age to build a strong foundation of cyber hygiene.

Other studies present various cybersecurity risks and awareness approaches, one approach was training, where different techniques were found to train children about cybersecurity risks and concepts: Desimpelaere et al. (2020) informative video, an interactive presentation with storytelling and digital comics, Abi-Jaoude et al., (2020), making a school curriculum, developing and using tools and proposing a best-practice ontology for passwords (Alemany et al., 2019). All the techniques showed positive outcomes and provided effectiveness at raising awareness of various cybersecurity risks. However, one study reported the ineffectiveness in cybersecurity awareness due to the simple user interface provided by these tools (Prior and Renaud, 2020). The

other issue was the privacy management tool, as some believed that their privacy on social networks was already protected by those networks' privacy rules and regulations (Alemany et al., 2019).

Therefore, to alert children to cybersecurity concerns, it is important to implement the warning strategy (Alemany et al., 2019; Jeong & Chiasson, 2020). The study by Jeong and Chiasson (2020) investigated how children interpreted warning signals. It has been discovered that the principles influencing how adults and children perceived risk were similar when it comes to which signal components denoted the most dangerous and safest circumstances. Additionally, it was found that various cybersecurity warning symbols, such as the "open lock" and "police officer" emblems, were ambiguous and subject to different interpretations (Jeong & Chiasson, 2020). Alemany et al. (2019) also discovered the technique of employing warnings to caution users about potential phishing dangers. Furthermore, Alemany *et al.* (2019) encourage users to think twice before disclosing personal information on social media. The literature further emphasizes that demonstrating the success of warning mechanisms in alerting users of possible risks generates positive results. Therefore, this study proposed an information security education framework for children to assist in combating the threats they may encounter online.

5. Information Security Framework

The importance of protecting children online is crucial, especially as AI technologies have also come into play. Exposing children to even more complex cyber threats that are difficult to detect. Therefore, this study proposed an information security education framework for children, as illustrated in Figure 1. The framework consists of five components that can assist parents and educators in educating and raising awareness for a cyber-safe online environment.

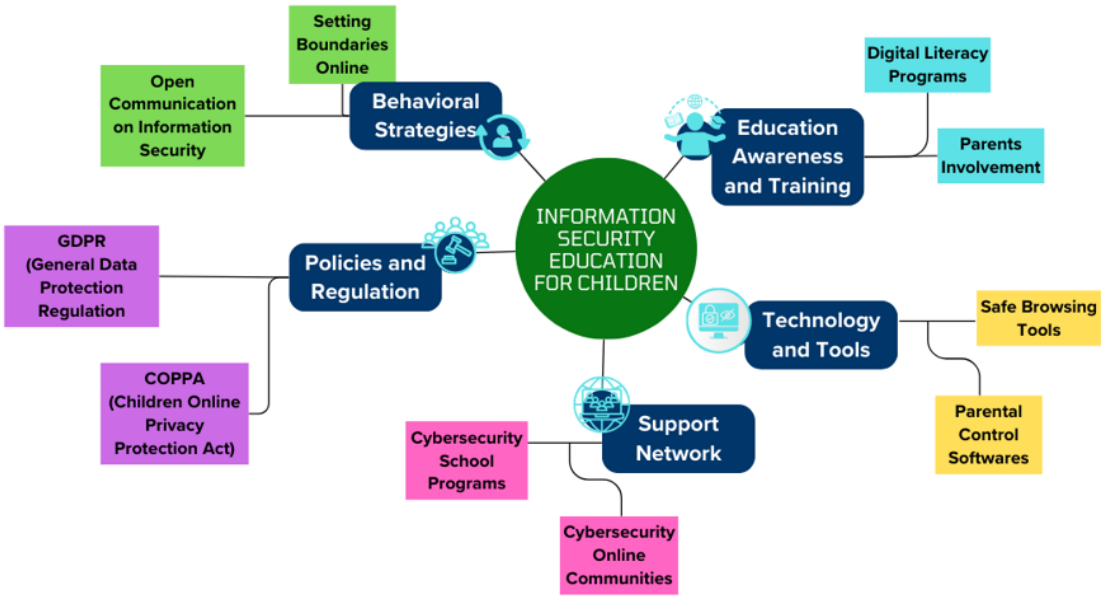

Figure 1: Information Security Education Framework

5.1 Education: Awareness and Training

The importance of cybersecurity training and awareness cannot be stressed enough to combat children in addressing cyber threats. Therefore, digital literacy programs need to be incorporated into the school curriculum at both primary and secondary levels. This will assist in creating a cybersecurity culture. Furthermore, parents' involvement is needed to ensure that even at home, children are not exposed to threats such as inappropriate content.

5.2 Technology and Tools

There are various tools that are available online to safeguard children from being exposed to content that is meant for adults. Parents can use parental control settings to limit screen time to avoid online addiction. Safe browsing tools can also be enabled to control the type of content children can access online. For example, children (0-5 years) can only access YouTube Kids.

5.3 Support Network

The other important component of the framework is the community support network. Communities can have online cybersecurity networks that will alert children about cyber threats and update them on which websites to avoid prevailing scams. Schools can also introduce information security awareness programs to create a cyber resilience environment.

5.4 Policies and Regulations

There was limited information on policies and regulations to safeguard children's online literature. Therefore, policymakers should consider incorporating regulations such as the USA's Children Online Privacy Protection Act (COPPA) and the General Data Protection Regulation (GDPR) to be applied in schools when children are accessing digital applications, even educational Apps.

5.5 Behavioural Strategies

Behavioural strategies should also be considered to promote online safety. This can include setting boundaries on activities children browse online. For instance, adopting cyber hygiene and the intolerance of cyberbullying should be the norm. Furthermore, another behavioural strategy that can be used is open communication on information security to promote transparency in online activities, such as education about digital footprints.

6. In Conclusion

From this review, it was clear that there is a need for information security education for children to create a safe online environment. This study explored the impending threats children face online, such as deepfakes and AI-generated content, social media dominance, increased screen time, increased targeting on popular platforms and the complexity of cyber threats. Thus, this study proposed an information security framework to prevent children from being exposed to cyber threats. The framework comprises five components: education, awareness and training, technology and tools, community support network, policies and regulations, and behavioural strategy. This framework will assist both schools and parents in protecting children from falling victim to cyber threats.

7. Future Work

When it comes to future research, even though policies and regulations such as the COPPA address the children's online privacy and protection, there is, however, further research that is needed to provide guidance to educators and parents on how they can protect children from online abuse. Future research could also explore the behavioural strategies that can be used to safeguard children from online overstimulation. More awareness strategies are also needed to keep up with the evolving use of new emerging technologies such as Artificial Intelligence, as children can be overdependent on them, which can have an impact on their critical thinking development. Thus, both technical and psychological use and impact should be studied to assist in coming up with solutions for safeguarding children from the inappropriate use of the internet.

Ethics declaration: This study employed previously published peer-reviewed journal articles, and since no human subjects were engaged, ethical approval was not necessary.

References

Abi-Jaoude, E., Naylor, K.T. and Pignatiello, A. (2020) 'Smartphones, social media use and youth mental health', *CMAJ : Canadian Medical Association Journal,* 192(6), pp. E136–E141 Available at: https://doi.org/10.1503/cmaj.190434.

Ahmed, I. (2023) *AI and Eating Disorders.* Available at: https://counterhate.com/research/ai-tools-and-eating-disorders/ [Accessed: 11 November, 2024].

Alemany, J., Del Val, E., Alberola, J. and García-Fornes, A. (2019) 'Enhancing the privacy risk awareness of teenagers in online social networks through soft-paternalism mechanisms', *International Journal of Human-Computer Studies,* 129, pp. 27–40.

Ayyash, M., Alsboui, T., Alshaikh, O., Inuwa-Dute, I., Khan, S. and Parkinson, S. (2024) 'Cybersecurity Education and Awareness among Parents and Teachers: A Survey of Bahrain', *IEEE Access.*

Baciu-Ureche, O., Sleeman, C., Moody, W.C. and Matthews, S.J. (2019) *The adventures of scriptkitty: Using the raspberry pi to teach adolescents about internet safety.* pp. 118.

Bennani, H. (2022) 'Cybersecurity, Cybercrime and the Video Gaming Industry'.

Carpenter, S. (2019) 'Children are becoming more vulnerable to cybercriminals as IoT device use explodes', *Open Access Government,* -09-04. Available at: https://www.openaccessgovernment.org/children-vulnerable-to-cybercriminals/72665/ [Accessed: 11 November, 2024].

CCDH *CCDH'S NTIA PUBLIC COMMENT SUBMISSION.* Available at: https://counterhate.com/research/ccdhs-ntia-public-comment-submission/ [Accessed: 10November, 2024].

Center for Countering Digital Hate (2023) *New Report: Horizon Worlds Exposed.* Available at: https://counterhate.com/research/horizon-worlds-exposed/ [Accessed: 15 November, 2024].

Chaudron, S., Di Gioia, R. and Gemo, M. (2018) 'Young children (0-8) and digital technology, a qualitative study across Europe. Publications Office of the European Union'.

Desimpelaere, L., Hudders, L. and Van de Sompel, D. (2020) 'Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior', *Computers in Human Behavior,* 110, pp. 106382.

Domingues-Montanari, S. (2017) 'Clinical and psychological effects of excessive screen time on children', *Journal of paediatrics and child health,* Vol 53, No.4, pp. 333–338.

Drevin, L., Miloslavskaya, N., Leung, W.S. and von Solms, S. (2022) 'Information Security Education-Adapting to the Fourth Industrial Revolution'.

Granic, I., Morita, H. and Scholten, H. (2020) 'Beyond screen time: Identity development in the digital age', *Psychological Inquiry,* Vol 31, No. 3, pp. 195–223.

Guo, L. and Zhang, H. (2020) *A white-box impersonation attack on the FaceID system in the real world.* IOP Publishing, pp. 012037.

Hadjipanayis, A., Efstathiou, E., Altorjai, P., Stiris, T., Valiulis, A., Koletzko, B. and Fonseca, H. (2019) 'Social media and children: what is the paediatrician's role?', *European journal of pediatrics,* Vol 178, No 10, pp. 1605–1612.

Hart, S., Margheri, A., Paci, F. and Sassone, V. (2020) 'Riskio: A serious game for cyber security awareness and education', *Computers & Security,* Vol 95, pp. 101827.

Iradat, S. (2024) 'Securing futures by bridging the gap in online safety education for youth'.

Jeong, R. and Chiasson, S. (2020) *'Lime','Open Lock', and'Blocked' Children's Perception of Colors, Symbols, and Words in Cybersecurity Warnings.* pp. 1.

Karabatak, S. and Karabatak, M. (2020) *Z generation students and their digital footprints.* IEEE, pp. 1.

Karani, N.F., Sher, J. and Mophosho, M. (2022) 'The influence of screen time on children's language development: A scoping review', *South African Journal of Communication Disorders,* Vol 9, No 1, pp. 825.

Kerridge, S. (2023). Fostering a love for reading in the digital age. Metaphor, (4), pp.15-20.

Laczi, S.A. and Póser, V. (2024, May). Navigating Children's Cybersecurity Landscape: Understanding the impact of cyberbullying, online harassment and identity theft on children. In 2024 IEEE 18th International Symposium on Applied Computational Intelligence and Informatics (SACI) (pp. 1-6). IEEE.

Livingstone, S., Stoilova, M. and Nandagiri, R. (2019) 'Children's data and privacy online: growing up in a digital age: an evidence review'.

Mahlasela, O., Baloyi, E., Siphambili, N. and Khan, Z.C. (2024) 'Artificial Intelligence Impact on the realism and prevalence of deepfakes' South African Institute of Computer Scientists and Information Technologists (SAICSIT). Gqeberha, South Africa, pp. 224–239.

Ondrušková, D. and Pospíšil, R. (2023) 'The good practices for implementation of cyber security education for school children', *Contemporary Educational Technology,* Vol 15, No 3, pp. ep435.

Orabi, M., Mouheb, D., Al Aghbari, Z. and Kamel, I. (2020) 'Detection of bots in social media: a systematic review', *Information Processing & Management,* Vol 57, No 4, pp. 102250.

Oswald, T.K., Rumbold, A.R., Kedzior, S.G. and Moore, V.M. (2020) 'Psychological impacts of "screen time" and "green time" for children and adolescents: A systematic scoping review', *PloS one,* Vol 15, No 9, pp. e0237725.

Prior, S. and Renaud, K. (2020) 'Age-appropriate password "best practice" ontologies for early educators and parents', *International Journal of Child-Computer Interaction,* Vol 23, pp. 100169.

Quayyum, F., Cruzes, D.S. and Jaccheri, L. (2021) 'Cybersecurity awareness for children: A systematic literature review', *International Journal of Child-Computer Interaction,* Vol 30, pp. 100343.

Rahman, N.A.A., Sairi, I.H., Zizi, N.A.M. and Khalid, F. (2020) 'The importance of cybersecurity education in school', *International Journal of Information and Education Technology,* Vol 10, No 5, pp. 378–382.

Rao, B.N. and Kalyani, V. (2022) 'A study on positive and negative effects of social media on society', *Journal of Science & Technology (JST),* Vol 7, No 10, pp. 46–54.

Sprung, B., Froschl, M. and Gropper, N. (2020) *Cybersafe young children: Teaching internet safety and responsibility, K–3* Teachers College Press.

Stankov, I. and Tsochev, G. (2020) 'Vulnerability and protection of business management systems: threats and challenges', *Problems of Engineering Cybernetics and Robotics,* Vol 72, pp. 29–40.

Stoilova, M., Livingstone, S. and Nandagiri, R. (2020) 'Digital by default: Children's capacity to understand and manage online data and privacy', *Media and Communication,* Vol 8, No 4, pp. 197–207.

van Tiel, J. (2020) 'Cyberbullying, an overlooked and ever growing danger to the development of children', .

Wright, M.F. (2022) 'The Nature of Cyberbullying Among Youths', *Research Anthology on Combating Cyber-Aggression and Online Negativity*, pp. 35–55.

Kopecký, K., Fernández-Martín, F. D., Szotkowski, R., Gómez-García, G., & Mikulcová, K. (2021). Behaviour of children and adolescents and the use of mobile phones in primary schools in the Czech Republic. *International Journal of Environmental Research and Public Health*, *18*(16), 8352.

COPPA, 2013. Children's Online Privacy Protection Rule ("COPPA"). [on-line] Available at: <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa> [Accessed: Apr 10, 2025].

Cybercrimes Act, 2021. Cybercrimes Act. [on-line] Available at: <https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf> [Accessed: Apr 11, 2025].

GDPR, 2016. General Data Protection Regulation (GDPR) – Legal Text. [online] Available at: <https://gdpr-info.eu/> [Accessed: Apr 10, 2025].

POPIA, 2020. Protection of Personal Information Act (POPI Act). [online] Available at: <https://popia.co.za/> [Accessed: Apr 10, 2025].