Volume 4 Issue 1, January-June 2022: pp. 39-46.
Department of International Law, Faculty of Law, Universitas Lampung, Bandar Lampung, Indonesia.
p-ISSN: 1978-5186 E-ISSN: 2723-2603
http://jurnal.fh.unila.ac.id/index.php/lajil

THE IMPORTANCE OF CYBERSECURITY AWARENESS FOR CHILDREN

Yuliana
Universitas Udayana, Indonesia, E-mail: yuliana@unud.ac.id

Submitted: Feb 10, 2022; Reviewed: Jun 29, 2022; Accepted: Jun 30, 2022

Article Info

Keywords:
Awareness, Children, Cybersecurity.

DOI:
10.25041/lajil.v4i1.2526

Abstract

During the COVID-19 pandemic, the shift to online schooling increased children's vulnerability to cyberattacks and malware. Consequently, cultivating cybersecurity awareness among children is essential. Moreover, engaging with online games and stories can lead children to neglect their studies, underscoring the need for balanced internet usage. This paper highlights the importance of cybersecurity awareness among children, employing a literature review methodology. The results indicate that cybersecurity awareness among children can be effectively enhanced through digital literacy training. Programs should educate children on how to avoid risky behaviors online, including interactions susceptible to phishing, exposure to inappropriate content such as pornography, cyberbullying, identity theft, and privacy breaches. Additionally, children must learn the importance of keeping their passwords secure and private and adopting a cautious approach while playing online games. In conclusion, digital literacy and cybersecurity programs are not only teachable to children but are also crucial for boosting their cybersecurity awareness.

A. Introduction

Internet users all vulnerable to various security risks. Several terms are used interchangeably to describe the risks, including cybersecurity, online safety, and internet security. Cybersecurity is a term that is widely used as it covers wider perspectives. The term cybersecurity is defined the collection of policies and concepts about guidelines, risk management, and technologies to protect the cyber environment and users' assets.[1] Cybersecurity ensures the security of organizations and users, including underage users. The distant learning or online learning that was applied during the COVID-19 pandemic posed children to cyberattacks and malwares. It

[1] Farzana Quayyum, Daniela S Cruzes, and Letizia Jaccheri, "Cybersecurity Awareness for Children: A Systematic Literature Review," *International Journal of Child-Computer Interaction* 30, no. 1 (2021): 1–25, https://doi.org/10.1016/j.ijcci.2021.100343.

is necessary to raise children's awareness of cybersecurity as they often neglect their online learning sessions due to online game distractions.[2]

Students' logic that is still developing makes them prone to online risks. Therefore, developing a cybersecurity program awareness is essential to increase students' awareness. Consideration should be given to cybersecurity risks facing children, as well as various approaches, theories, and solutions for enhancing their cybersecurity awareness.[3] A substantial amount of time is spent online for educational and entertainment purposes as the internet offer wide range of opportunities. However, children still find it difficult to discern between the opportunities and risks of digital systems. However, these online activities pose threats to children's privacy and safety, with the severity of the risks often unrecognized until it is late, potentially leading to online abuses.[4]

Some critical aspects need to be evaluated and concerned to design solutions, recommendations, and approaches to raising cybersecurity awareness among children. This paper describes the importance and strategies to raise cybersecurity awareness for children. In this narrative literature research, relevant articles were collected from Science Direct and Google Scholar databases based on several inclusion and exclusion criteria. The inclusion criteria were review articles and research articles. Meanwhile, papers that are not peer-reviewed articles and unavailable full-text were excluded. Articles were read twice to reduce the bias. The selected articles were summarized and narrated descriptively.

B. Discussion

1. The Threats of Internet Use among Children

The advancement of internet services provides comfort for the users as it allows online working, studying and easier access to entertainment. Internet can both increase the social well-being of children and pose them to some threats such as cyberbullying, identity theft, pornography, etc. Children should be taught how to identify and avoid risky behavior online. Cybersecurity awareness can be increased through digital literacy training to save children from phishing, pornography, cyberbullying, identity theft, and breaking of privacy. Children need to learn how to keep their passwords safe and private and they have to stay aware and cautious when playing online games.[5]

2. The importance of cybersecurity awareness

In regards to the importance of raising the awareness of children on cybersecurity, several programs have been implemented by some countries. In African countries, a specific program was developed to raise awareness of a cyber-safety culture for the children. [6]

A research on internet users aged 12 to 19 in Malaysia revealed that children this age dominated the number of internet users. Unfortunately, they often overshare information and perceived every content shared on the internet truthful. They have not yet developed the competence to protect sensitive information such as personal data. Challenges in boosting security awareness include both understanding and awareness. Messages that are clearly understood are more likely to be accepted and acted upon. [7]

---

[2] Quayyum, Cruzes, and Jaccheri.

[3] Quayyum, Cruzes, and Jaccheri.

[4] Quayyum, Cruzes, and Jaccheri.

[5] Martina J Zucule De Barros and Horst Lazarek, "A Cyber Safety Model for Schools in Mozambique," in *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018)*, 2018, 251–58, https://doi.org/10.5220/0006573802510258.

[6] Barros and Lazarek.

[7] Noor Hayani Abd Rahim, "Assessment of Cybersecurity Awareness Program on Personal Data Protection among Youngster in Malaysia" (2017).

Cybersecurity awareness can be enhanced by using proper strategies to educate users about cyber threats and data stealing. The level of users' understanding is directly linked to the importance of information security. The two primary objectives of cybersecurity awareness are to alert users and help them understand the risks involved. Vulnerabilities related to human factors can occur at both personal and organizational levels.[8]

3. Solution for increasing awareness of security program in education program

The widespread use of tablets and smartphones has led to a rapid shift among children towards Game-Based Learning (GBL), driven by the convenience of mobility and built-in sensors. As a result, blended and mobile learning have become ubiquitous. The critical dimensional framework of this learning includes six key aspects as follows. [9]

a. Spatio-temporal
b. Collaboration/Social
c. Pedagogy
d. Personalization
e. Data security & privacy
f. Session

The educational program is developed based on these solutions, ensuring that both technological aspects and pedagogical qualities are maintained during online learning.[10]

In recent years, cybersecurity awareness has become a significant area of study, including children as subjects. According to the World Health Organization, children are defined as anyone under 18 years old. One particular concern in children's cybersecurity is password practices; a simple password can easily be hacked. [11]

Children are essential to the community since they are the future generation whose safety should be prioritized. The extensive use of smartphones and computers bring several risks for children. However, limiting their access to online resources is not a solution. Therefore, children need to be supervised when accessing online resources. The Ministry of Education of the Union of Arab Emirates has implemented a cybersecurity awareness program for students aged 8 to 10 years old. The program has been proven effective in reducing the online risks for children as students learned how to behave online safely.[12]

The Ministry of Education in the Union of Arab Emirates focused on training and education programs for students in internet best practices. The goal is to increase cybersecurity and cyber awareness. Grade 4 students (8-10 years old) were given the internet safety topic as the primary subject of the Design and Technology program as a compulsory module for three months. The materials covers topics about internet usage, online dangers, the strategies to protect themselves online, as well solutions to respond to online risks appropriately. At the end of the program, children are able to answer the questions mentioned in Figure 1. This is a unique program that

[8] Filippos Giannakas et al., "Security Education and Awareness for K-6 Going Mobile," *International Journal of Interactive Mobile Technology* 10, no. 2 (2016): 41–48.
[9] Filippos Giannakas, Georgios Kambourakis, and Andreas Papasalouros, "A Critical Review of 13 Years of Mobile Game-Based Learning," *Educational Technology Research and Development* 2, no. 1 (2017): 1–20, https://doi.org/10.1007/s11423-017-9552-z.
[10] Giannakas et al., "Security Education and Awareness for K-6 Going Mobile."
[11] Suzanne Prior and Karen Renaud, "Age-Appropriate Password 'Best Practice' Ontologies for Early Educators and Parents," *International Journal of Child-Computer Interaction*, 2020, 100169, https://doi.org/10.1016/j.ijcci.2020.100169.
[12] Arwa A Al Shamsi, "Effectiveness of Cyber Security Awareness Program for Young Children : A Case Research in UAE," *International Journal of Information Technology and Language Studies (IJITLS)* 3, no. 2 (2019): 8–29, https://doi.org/10.13140/RG.2.2.28488.14083.

should be developed for more comprehensive theme and constricts as shown in Figures 2 and 3.[13]

Research main question	Interview sub-question	Purpose of interview question
1. What online risks children may expose to?	1.1 What online risks you learn about?	To discover the ability of the child to identify different online risks.
	1.2 What online risks you may expose to?	To investigate the ability of children to identify online risks they may expose to.
2. How cyber security awareness training influences student's online behavior?	2.1 Can you give an example to show how the awareness program influenced your online behavior?	To investigate how the cyber security awareness program influenced children's behavior online.
3. How effective is the Cyber Security Awareness program adopted by the Ministry of Education in UAE in educating students aged 8 to 10 about the safe use of the internet?	3.1 Do you think that this awareness program is effective? To what extent?	To find out the children opinion about the benefits of the cyber security awareness program.

Figure 1. The questions for children's assessment after finishing the cybersecurity awareness program[14]

Main constructs	Main Dimensions
Online risks	O1: Cyber Bullying O2: Pornography O3: Identity theft O4: Online Phishing O5: Break to privacy
Content of awareness program	C1: Internet Safety C2: Cyber Bullying C3: Identity theft C4: Online Phishing C5: Privacy C6: Password C7: securing private information C8: Internet Strangers
Effectiveness of cyber security awareness program	E1: Positively affects children's behavior online E2: effective in raising cyber security awareness level among students E3: efficient in helping students to protect themselves online
Effects on students	EF1: protect their personal information EF2: use strong passwords EF3: respond properly to different incidents online EF4: more cautious while playing online games EF5: keep their parents aware if they feel uncomfortable online EF6: aware of phishing emails and messages. EF7: Transfer the knowledge their family members
Limitations	L1: narrative L2: little awareness videos, more should be included L3: little hands-on activities, more should be included
Suggestions	S1: society engagement S2: cyber security training for parents

Figure 2. The primary construct and theme of the cybersecurity awareness program[15]

[13] Shamsi.
[14] Shamsi.
[15] Shamsi.

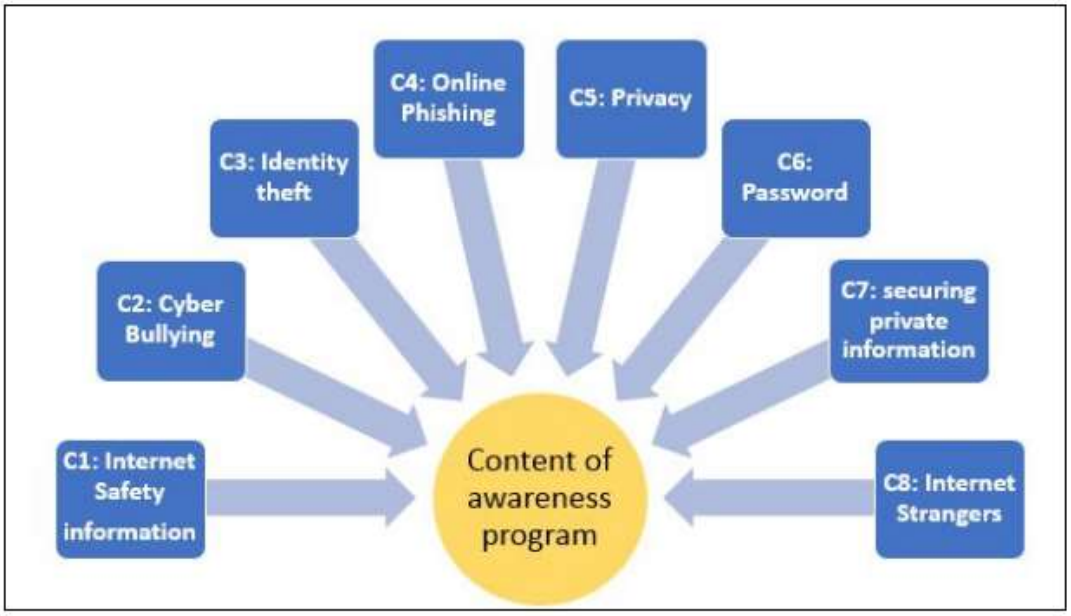

Figure 3. The content of the cybersecurity awareness program[16]

Smartphone usage is prevalent across many countries, including South African society. Despite this, there is currently no specific curriculum on cybersecurity in schools. Universities do offer some principles of cybersecurity, but these are generally limited to students enrolled in computing-related courses, who represent only a small portion of the community. Therefore, there is a strong case for teaching cybersecurity to children, starting as early as primary school. It is crucial to embed these skills into the national curriculum to equip children early with the necessary skills for cyber safety.

Moreover, addressing gender imbalance in cybersecurity awareness programs is essential to ensure equal participation and representation. Cybersecurity awareness should be considered as fundamental as reading, writing, and arithmetic in our technology-driven era. This approach will prepare all children to navigate and protect themselves in an increasingly digital world. [17]

In the United Kingdom, unique curricula targeting early-age learners have been implemented, which incorporate Information and Communications Technology (ICT) as a foundational skill. This initiative is crucial to ensure that children understand and adopt safe online behaviors, including the ability to evaluate fake news and hoaxes. Cybersecurity education in these programs is built on two fundamental elements: awareness and the specific precautions necessary to ensure safety.

These essential steps for maintaining cybersecurity are detailed in Figure 4. Additionally, exceptional measures for infrastructure security and data protection are imperative to provide a safe and secure learning environment for these young digital citizens.[18]

[16] Shamsi.

[17] Isabella M Venter et al., "Cyber Security Education Is as Essential as 'the Three R's,'" *Heliyon* 5, no. August (2019): 1–7, https://doi.org/10.1016/j.heliyon.2019.e02855.

[18] Yuchong Li and Qinghui Liu, "A Comprehensive Review Research of Cyber-Attacks and Cyber Security ; Emerging Trends and Recent Developments," *Energy Reports*, no. Article in Press (2021), https://doi.org/10.1016/j.egyr.2021.08.126.

Figure 4. Security triangle of cybersecurity[19]

C. Conclusion

In conclusion, digital literacy and cybersecurity programs are not only feasible for children but also crucial for enhancing their cybersecurity awareness. These programs are designed to educate young users about cyber threats and the risks of data theft, emphasizing the methodology of raising awareness. The effectiveness of these programs hinges on the degree of the users' understanding, which underscores the importance of information security. The primary purposes of cybersecurity awareness—alerting users to potential threats and deepening their understanding of these risks—highlight the necessity of these educational efforts. Given that vulnerabilities can occur at both personal and organizational levels, it is vital to tailor cybersecurity education to various age groups. Future research should focus on developing age-appropriate online behavior training that accounts for the specific needs and cognitive abilities of different stages in children's development.

REFERENCES

Barros, Martina J Zucule De, and Horst Lazarek. "A Cyber Safety Model for Schools in Mozambique." In *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018)*, 251–58, 2018. https://doi.org/10.5220/0006573802510258.

Giannakas, Filippos, Georgios Kambourakis, and Andreas Papasalouros. "A Critical Review of 13 Years of Mobile Game-Based Learning." *Educational Technology Research and Developmentt* 2, no. 1 (2017): 1–20. https://doi.org/10.1007/s11423-017-9552-z.

Giannakas, Filippos, Georgios Kambourakis, Andreas Papasalouros, and Stefanos Gritzalis. "Security Education and Awareness for K-6 Going Mobile." *International Journal of Interactive Mobile Technology* 10, no. 2 (2016): 41–48.

[19] Li and Liu.

Li, Yuchong, and Qinghui Liu. "A Comprehensive Review Research of Cyber-Attacks and Cyber Security ; Emerging Trends and Recent Developments." *Energy Reports*, no. Article in Press (2021). https://doi.org/10.1016/j.egyr.2021.08.126.

Prior, Suzanne and Karen Renaud. "Age-Appropriate Password 'Best Practice' Ontologies for Early Educators and Parents." *International Journal of Child-Computer Interaction*, 2020, 100169. https://doi.org/10.1016/j.ijcci.2020.100169.

Quayyum, Farzana, Daniela S Cruzes, and Letizia Jaccheri. "Cybersecurity Awareness for Children: A Systematic Literature Review." *International Journal of Child-Computer Interaction* 30, no. 1 (2021): 1–25. https://doi.org/10.1016/j.ijcci.2021.100343.

Rahim, Noor Hayani Abd. "Assessment of Cybersecurity Awareness Program on Personal Data Protection among Youngster in Malaysia," 2017.

Shamsi, Arwa A Al. "Effectiveness of Cyber Security Awareness Program for Young Children : A Case Research in UAE." *International Journal of Information Technology and Language Studies (IJITLS)* 3, no. 2 (2019): 8–29. https://doi.org/10.13140/RG.2.2.28488.14083.

Venter, Isabella M, J Blignaut, Karen Renaud, and M Anja Venter. "Cyber Security Education Is as Essential as 'the Three R's.'" *Heliyon* 5, no. August (2019): 1–7. https://doi.org/10.1016/j.heliyon.2019.e02855.