The Importance of Cybersecurity Education in School

Rahman N. A. A, Sairi I. H., Zizi N. A. M., and Khalid F.

Abstract—**Despite the fact that the Internet has positively impacted people's lives, there are negative issues emerged related to the use of Internet. Cases like cyber-bully, online fraud, racial abuse, pornography and gambling had increased tremendously due to the lack of awareness and self-mechanism among Internet users to protect themselves from being victims to these acts. However, past research revealed that the level of awareness among Internet users is still low or moderate. One of the vital measures to be taken is to cultivate knowledge and awareness among Internet users from their early age, i.e., young children. Young children specifically, need to be educated to operate in a safe manner in cyberspace and to protect themselves in the process. The objective of this systematic review paper is to explore why it is so critical that modern learners are educated about the risks associated with being active in cyberspace and the strategies that stakeholders can use to promote cyber security education in schools. In this paper, few strategies are discussed as how cyber security education can be implemented in schools.**

Index Terms—**Cybersecurity, cyber safety, cyber education, cyber awareness.**

I. Introduction

Many of us use social media as a platform to express our feelings, to provoke discussions, or to become known. As many people want to be the first to share an issue, sometimes they ignore whether the information presented is authentic or otherwise [1]. Use of the internet is not limited to adults, but in this era of technology and multimedia, knowledge of cybersecurity is also important for children. Although Internet has vast potential and benefits for everybody, the exessive use of the Internet maybe harmful as it may lead to cyber risks for example cyber addiction [2], gaming and gambling addiction [3], cybersex [4], pornography [5], and personal information exposure [4], [6], [7].

Cybercrime against children and adolescents is certainly a concern for parents, as they sometimes do not realise their child is a victim of cybercrime. Many parents are unaware of the activities their children perform in cyberspace [8]. Some children are bullied through comments and insults; they may also be intimidated, harassed, abused or sexually exploited. According to statistics from the Royal Malaysian Police (PDRM), nearly 80% of rape cases reported in the country over the past two years involve friendships in the virtual world, and most of the victims are under the age of 18 [9]. Grooming children and adolescents to become victims of sexual abuse is worsening, as more and more of these sexual predators are using fake identities on the internet when seeking victims.

With regard to parents' efforts to protect their children from cyber threats, there is no doubt that children, despite their young age, are efficient and skilled in using their own or their parents' smartphones. Children are not only tech savvy, but proficient in using technology. In fact, there are also parents who give gadgets to their children as rewards for excellence in exams, birthday presents, and so on. This makes young children vulnerable to abuse through technology, while they are independently exploring the internet without boundaries or monitoring. When enjoying the benefits of the internet, it is important for everyone, whether parents or children, to be aware of potential risks such as cyberbullying, as well as to take safety precautions, as children now have internet access at an earlier age [10]. Educators need to disseminate cybersecurity messages in order to promote responsible online behaviour [11].

Children's use of the internet is changing fast, in response to considerable societal, market and technological innovation. As children's frequent engagement with online videos, music, gaming, messaging and searching implies, their internet use is broadly positive. Parents of three- to four-year-olds report that their child is likely to watch cartoons, mini-movies, animations or songs on YouTube. The content children watch as they grow older differs, as older children watch more music videos, vloggers, YouTube personalities, and funny videos [12]. The role of schools is important in teaching critical digital literacy to students, as well as in guiding and informing parents regarding children's internet use at home.

The objective of cybersecurity education is to educate the users of technology on the potential risks they face when using internet communication tools, such as social media, chat, online gaming, email and instant messaging. Although there are many past research has been conducted on cyber security, in different areas, for example [13]–[19], less articles focused on the steps that need to be done particularly by schools in order to help cultivate cyber security awareness in detail. The objective of this paper is to discuss why it is so critical that modern learners are educated about the risks associated with being active in cyberspace, what factors hamper this education, and the importance of a cybersecurity curriculum that can be used by teachers in junior or primary schools, in the specific context of the Malaysian education system.

II. Cybersecurity

The emergence of the internet allows humans to enjoy two realms: their real life, and the virtual world [20]. With search engines such as Google and Yahoo, and video sharing sites such as YouTube, all information is now available at people's

Manuscript received December 30, 2019; revised March 23, 2020. This work was conducted under FRGS/1/2017/SSI09/UKM/02/3 grant.

The authors are with the Universiti Kebangsaan Malaysia, Malaysia (e-mail: nurulamirah.abdrahman@gmail.com, ihanis25@gmail.com, nurulakma.mzizi@gmail.com, fariza.khalid@ukm.edu.my).

doi: 10.18178/ijiet.2020.10.5.1393

fingertips. However, the growing world of cyberspace may also have negative effects on internet users, such as through cybercrime. Such issues should therefore be contained early so they do not have a major impact. In this context, cybersecurity implementation among internet users is very important. Cybersecurity education is necessary because cybercrime cases can occur anywhere regardless of individuals, organisations and places.

The definition of cybersecurity is the state of being protected against the criminal or unauthorised use of electronic data, or the measures taken to achieve this [21]. The explosion of Information Communication Technology (ICT) has brought great changes to our lives. With the existence of the World Wide Web, individuals and organisations can easily display any information, but if this is used for damaging purposes it will have a negative effect on people's lives [11]. In addition, the internet makes pornography accessible, which can generate social problems, including crime. The internet can also be an unhealthy channel for crimes and misbehaviour, being the main cause of Malay teenagers truanting from school.

Cybersecurity can also be defined as the activity, process, ability or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorised use or modification, or exploitation [22]. The internet undoubtedly increases one's knowledge. For example, online computer games require users who are highly skilled in English, in order to understand game settings and procedures. This will indirectly encourage the development of reading, writing and speaking skills in English. However, a computer game will usually be fun, and take the user a long time to complete. This can cause teens to become lazy, or to concentrate on gameplay and gadgets. Adolescents can also become addicted, and productive activities, such as reviewing their lessons, are ignored.

III. The Need for Cybersecurity Education

Statistical reports released by the Cyber Crime and Multimedia PDRM Investigation Division, cases of cyber-love scams or better known as the African Scam are in a state of concern [23]. The number of internet fraud cases in Malaysia increased in 2013, when 1095 cases were reported, compared to only 814 cases in 2012. Additionally, [24] notes an incident of an 18-year-old Malaysian boy who was arrested for committing an offense under the 1987 Copyright Act for uploading and downloading local music and international films without the owner's consent. The uploaded films included *Gravity*, *Pacific Rim*, *47 Ronin*, *The Hangover 3*, *We Are the Millers*, *The Hobbit: The Desolation of Smaug*, *Ride Along* and *The Wolverine*. Furthermore, according to [25], fraudulent purchase of goods online increased in Malaysia in 2015, with a loss of more than RM4.9 million involving the automobile, housing and tourism sectors.

Cybersecurity education is also needed to control addiction to computer games. This addiction certainly has a negative impact. Teenagers spend a lot of time on computers and socialise through their gadgets. Over time, an addiction to online games cannot be avoided, and teenagers' precious time is taken up by addiction to their gadgets. This has a very bad impact on teenagers. Nighttime is spent browsing the internet, which will exacerbate the situation and may even cause teenagers to have health problems. These threats and attacks can come in many forms, and users are not always aware that they are being attacked. It is therefore essential to educate and empower users, especially children, on the safe and responsible use of online resources and platforms, to establish a culture of cybersafety [10].

IV. Challenges of Cyber security Education

Social media platforms such as Facebook, Instagram, LinkedIn, YouTube and Twitter are the most popular internet applications for Malaysians [26]. This explosion of available information contributes to various risks involving privacy and security. The authenticity and accuracy of information in this virtual space can also be disputed. Children need to be equipped to defend themselves and take responsibility when faced with possible cyber threats. There are challenges, however, in ensuring teachers are sufficiently trained and up-to-date in their ability to promote critical understanding rather than restrictive approaches to cybersafety, as well as guiding students and parents in their use of the internet at home.

The carious challenges schools face in implementing cybersecurity education include lack of expertise, funding and resources [27]. Teachers lack knowledge and expertise regarding cyberspace. Schools and government ministries may lack resources and facilities to implement cybersecurity education. The speed of technological change results in new risks, requiring new solutions. Teachers may face problems in developing their knowledge of the latest technology and thus ensuring students are safe [28]. This is a major obstacle for teachers, as they lack access to learning materials and need to be sensitive to technological change. Early exposure and training for students at schools should be promoted through cybersecurity symposiums. The people who are exposed to and trained on cybersecurity are expected to be the country's future source of cyber defense.

V. Methodology

The research highlights research studies conducted in the field of cybersecurity in education. Multiple databases (Emerald, Google Scholar, Sci, Scopus and EBSCOhost) were explored, using keywords such as: Cybersecurity, cyber awareness, cyber education. The literature chosen was in the two languages that can be understood by the researcher, which are Malay and English. In addition, the search was limited to studies published between 2011 until 2019. More than 240 studies were found, but only 25 studies were selected. The selected studies were chosen based on their context, scope and respondents. Table I summarises of the selected studies in terms of the methodology, location, research focus, area and application of the research. Fig. 1 summarises the selection process.

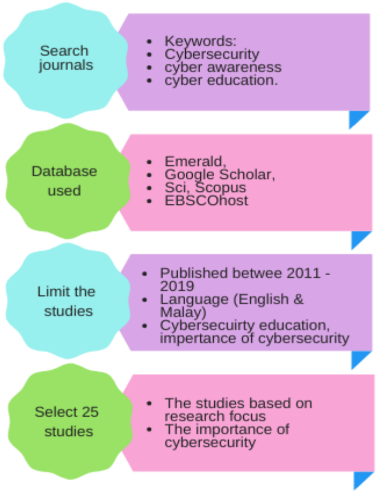
Search journals
Keywords:
Cybersecurity
cyber awareness
cyber education.
Database used
Emerald,
Google Scholar,
Sci, Scopus
EBSCOhost
Limit the studies
Published betwee 2011 - 2019
Language (English & Malay)
Cybersecuirty education, impertance of cybersecurity
Select 25 studies
The studies based on research focus
The importance of cybersecurity

Fig. 1. The selection process of past studies.

TABLE I: SUMMARY OF STUDIES REVIEWED

Methodology	**Location**	**Research focus**	**Area**	**Application of cybersecurity education**
Qualitative (5) Quantitative (9) Quasi-experimental (4) Concept paper (5) Action research (1) Case study (1)	USA (8) UK (2) Malaysia (6) South Africa (2) Afghanistan (1) Middle East (2)	Students (16) Educators (3) Parents (3) Employees (3)	Cybersecurity (12) Conception/ perception (2) Behaviour (1) Cybercrime (2) Cyberethics (2) Awareness (4) Reasoning (1)	Mobile apps (1) Safety (1) Curriculum (1) Legislation (2) Infrastructure (2) Security training, programme, seminar, workshop (4)

This paper has two research questions:

1) What is the importance of cybersecurity education in schools?
2) What are the strategies that stakeholders can use to promote cybersecurity education in schools?

VI. Results and Discussions

The research findings, below, are structured according to the research questions.

A. *The Importance of Cybersecurity Education in Schools*

According to the literature review, there are many benefits if a school is able to fully apply cybersecurity education. A survey on adults and cybersecurity states that participants are less willing to spend money or time on seminars or programmes about cybersecurity. It is therefore crucial for schools to become knowledge centres to expose issues around cybersecurity to the community. School administrators and teachers can discuss together and organise school programmes or activities about cybersecurity. In addition, schools in Malaysia are provided with financial allocations from the government, meaning that they will be able to cover the expenses of organising such events for the community. Moreover, cybersecurity education is beneficial for changing the mindset of individuals. Every person who lacks cybersecurity awareness is a result of not being informed of the importance and effects of cybersecurity itself.

B. *Strategies That Stakeholders Can Use to Promote Cybersecurity Education in Schools*

Video cartoons were identified as resources for teachers to use when discussing cybersecurity principles with primary school learners, for example, using the Upin and Ipin stories to raise awareness of cybersecurity [29]. The primary school subjects of Information and Communication Technology need to be improved to include cybersecurity topics. In addition, the safety aspects of cybersecurity can be taught through other subjects. For example, under the subject of Bahasa Melayu, students can be given essays on the subject of cybersecurity. In addition, cybersecurity can be a topic of discussion in the classroom or for speech competitions, and cybersecurity awareness weeks can be held.

Teacher education programmes must also prepare their pre-service teachers to model and teach cybersecurity topics and safe computing practices so that future generations will know how to behave ethically, as well as to keep themselves safe and secure online [30]. Despite their young demographic and access to technology, the pre-service teachers surveyed do not possess adequate cybersecurity knowledge, or the ability to teach their future students to keep themselves and their data safe from harm. This is in conflict with the concept of digital natives, as natives would know what clues in the environment indicate that they are safe and protected.

Providing knowledge to upgrade teachers' and students' understanding of cyber issues is one step that could be taken by relevant parties to protect such groups from evolving cybersecurity threats [31]. Cybersecurity awareness education is important to protect internet users from potential cybercrimes as well as evolving cyber threats. Although some security experts doubt the importance of cybersecurity education or training [32], many researchers believe that education or training is essential in protecting cyber users from cybersecurity threats [33], [34]. Education is important in addressing evolving cybersecurity threats, as all protection factors play an essential role in curbing them.

Moreover, security awareness programmes are one of the strategies that can promote cybersecurity education in school. The principles of cybersecurity awareness have been refined over many years of research in the social psychology arena, but have been largely ignored by IT professionals when developing information security awareness programmes [35]. For example, a cybersecurity education programme called GenCyber is a summer camp for American grade school students and teachers that is supported NSA/NSF. This kind of awareness programme should be implemented in every school, as this initiative is able to promote cybersecurity awareness and preparedness among the school community.

School administrations can also establish cybersecurity organisation like student clubs or councils in school. This offers good exposure not only to students but to the whole school community. The students can get guidance from their teachers to learn more about cybersecurity. According to [36], students will learn how to navigate the learning management system. In addition, students need to understand about cybersecurity for themselves, and the most effective way of promoting understanding is through active learning. In this type of 21st century learning, students follow a learner-centred approach whereby they find the information about cybersecurity from the internet, and the teacher only monitors their actions from time to time. ctive learning encourages better understanding, especially for the students themselves. Even though students develop a high level of awareness on some cybersecurity issues such as cyberbullying, sharing personal information and internet banking, little information is given to them regarding cyber-sex and self-protection. It is very important for teachers, parents and the government to be more proactive in educating students about these areas, and to overcome the taboo on sex education [11].

VII. Conclusions

Based on a synthesis of the literature selected, it was found that it is very important to protect children through cybersecurity education so that they can become aware of the potential risks they face when using internet communication tools, such as the social media, chatting and online gaming. However, there are several challenges to cybersecurity education. These include the level of teachers' knowledge, and the lack of expertise, funding and resources. It is very important for all relevant parties, including teachers, parents, peers and the government, to work together to find the best solution to protecting children from cybercrime and cyberbullying through school-based cybersecurity education. The media, such as television and radio, must also play an important role in educating children through cybersecurity campaigns because such campaigns are more interactive and interesting for children to understand.

Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Author Contributions

Amirah, Izzah and Akma analyzed the papers and wrote the draft of the article and Fariza supervised the research, review and improved the article; all authors had approved the final version.

Acknowledgment

This study is conducted under FRGS/1/2017/SSI09/UKM/02/3 grant.

References

[1] F. Khalid, "Understanding university students' use of facebook for collaborative learning," *International Journal of Information and Education Technology*, vol. 7, no. 8, pp. 595-600, August 2017.

[2] F. Annasingh and T. Veli, "An investigation into risks awareness and e-safety needs of children on the internet," *Interactive Technology and Smart Education*, vol. 13, no. 2, pp. 147-165, 2016.

[3] L. Muniandy and B. Muniandy, "The impact of social media in social and political aspects in Malaysia: An overview," *International Journal of Humanities and Social Science*, vol. 3, no. 11, pp. 71-76, 2013.

[4] V. Ratten, "A cross-cultural comparison of online behavioral advertising knowledge, online privacy concerns and social networking using the technology acceptance model and social cognitive theory," *Journal of Science & Technology Policy Management*, vol. 6, no. 1, pp. 25-36, 2015.

[5] M. D. Griffiths and D. Kuss, "Online addictions, gambling, video gaming and social networking," *The Handbook of the Psychology of Communication Technology*, Chichester: John Wiley, pp. 384-406, 2015.

[6] L. Mosalanejas, A. Dehghani, and K. Abdolahofard, "The students' experiences of ethics in online systems: A phenomenological study," *Turkish Online Journal of Distance Education*, vol. 15, no. 4, pp. 205-216, 2014.

[7] D. Krotidou, N. Teokleous, and A. Zahariadou, "Exploring parents' and children's awareness on internet threats in relation to internet safety," *Campus-Wide Information Systems*, vol. 29, no. 3, pp. 133-143, 2012.

[8] N. Ahmad, U. A. Mokhtar, Z. Hood *et al*., "Cyber security situational awareness among parents," presented at the Cyber Resilience Conference, Putrajaya Malaysia, pp. 7-8, November 13-15, 2019.

[9] Y. Y. A. Talib. (2017). Keselamatan di alam siber. *MyMetro*. [Online]. Available: https://www.hmetro.com.my/hati/2017/12/295907/keselamatan-di-alam-maya

[10] R. S. Hamid, Z. Yunos, and M. Ahmad, "Cyber parenting module development for parents," in *Proc. INTED2018 Conference*, 5th-7th March 2018, Valencia, Spain, 2018.

[11] F. Khalid *et al*., "An investigation of university students' awareness on cyber security," *International Journal of Engineering & Technology*, vol. 7, pp. 11-14, 2018.

[12] Children and parents: Media use and attitudes report. *Ofcom*. [Online]. Available: http://www.ofcom.org.uk/__data/assets/pdf_file/0034/93976/Children-Parents-Media-UseAttitudes-Reports-2016.pdf

[13] C. S. Kruse *et al*., "Cybersecurity in healthcare: A systematic review of modern threats and trends," *Technology and Health Care*, vol. 25, no. 1, pp.1-10, 2017.

[14] P. Dong *et al*., "A systematic review of studies on cyber physical system security," *International Journal of Security and Its Applications*, vol. 9, no. 1, pp. 155-164, 2015.

[15] U. Franke and J. Brynielsson, "Cyber situational awareness — A systematic review of the literature," *Computers & Security*, vol. 46, pp. 18-31, 2014.

[16] N. H. A. Rahim *et al*., "A systematic review of approaches to assessing cybersecurity awareness," *Kybernetes*, 2015.

[17] D. Mellado *et al*., "A systematic review of security requirements engineering," *Computer Standards & Interfaces*, vol. 32, no. 4, pp. 153-165, 2010.

[18] A. V. Herrera, M. Ron, and C. Rabadão, "National cyber-security policies oriented to BYOD (bring your own device): Systematic review," in *Proc. 2017 12th Iberian Conference on Information Systems and Technologies (CISTI)*, pp. 1-4, 2017.

[19] F. Mishna *et al*., "Interventions to prevent and reduce cyber abuse of youth: A systematic review," *Research on Social Work Practice*, vol. 21, no. 1, pp. 5-14, 2011.

[20] H. F. Lokman, N. Nasri, and F. Khalid, "The effectiveness of using twitter application in teaching pedagogy: A meta- synthesis study," *International Journal of Academic Research in Progressive Education and Development*, vol. 8, no. 2, pp. 205-212, 2019.

[21] Oxford University Press. (2014). *Oxford Online Dictionary*. Oxford: Oxford University Press. [Online]. Available: http://www.oxforddictionaries.com/definition/english/Cybersecurity

[22] DHS. (2014). A glossary of common cybersecurity terminology. *National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security.* [Online]. Available: http://niccs.uscert.gov/glossary

[23] S. S. Anuar. (2018). 8313 Kes Penipuan Siber Direkodkan. [Online]. Available: https://www.bharian.com.my

[24] M. Rosman. (2014). KPDNKK Tahan Remaja 18 tahun muat turun muzik tanpa kebenaran. [Online]. Available: http://www.utusan.com.my

[25] M. Marimuthu. (2016). Pembelian secara online catat kes penipuan paling tinggipada 2015. [Online]. Available: http://www.nccc.org.my

[26] F. Khalid, M. Y. Daud, and A. A. Karim, "Pemilihan Aplikasi Teknologi sebagai Medium Perkongsian Maklumat oleh Pelajar Siswazah Universiti," presented at the ASEAN Comparative Education Research Network Conference, 2015.

[27] K. Salamzada, Z. Zarina, and M. A. Bakar, A framework for cybersecurity strategy for developing countries: Case study of Afghanistan," *Asia-Pacific Journal of Information Technology and Multimedia*, vol. 4, no. 1, pp. 1-10, 2015.

[28] D. Miles, *Second Worldwide Cybersecurity Summit (WCS)*, Youth Protection: Digital Citizenship- Principles and New Recourses, 2011.

[29] M. A. Pitchan, S. Z. Omar, J. Bolong, and A. H. Ghazali, "Analisis keselamatan siber dari perspektif persekitaran social: Kajian terhadap pengguna internet di Lembah Klang," *Journal of Social Science and Humanities*, vol. 12, pp. 16-29, 2017.

[30] P. Pusey and A. S. William, "Cyberethics, cybersefety, and cybersecurity: Perservice teacher knowledge, preparedness, and the need for teacher education to make a difference," *Journal of Digital Learning in Teacher Education*, pp. 82-88, 2012.

[31] L. Muniandy, B. Muniandy, and Z. Samsudin, "Cyber security behavior among higher education students in Malaysia," *Journal of Information Assurance & Cybersecurity*, pp. 1-13, 2017.

[32] B. Schneier, *Security Awareness Training*, 2013.

[33] R. Moore, *Cybercrime: Investigating High-Technology Computer Crime*, MA: Andarson Publishing, Burlington, 2011.

[34] L. Muniandy and B. Muniandy, "The impact of social media in social and political aspects in Malaysia: An overview," *International Journal of Humanities and Social Science*, vol. 3, no. 11, pp. 71-76, 2013.

[35] M. Kabay, "Psychological factors in the implementation of information security policy," *EDPACS, The EDPAudit, Control and Security Newsletter*, vol. XXI, no. 10, pp.1-10, 1994.

[36] D. Nakama and K. Paullet, "The urgency for cybersecurity education: The impact of early college innovation in hawaii rural communities," *Information System Education Journal*, vol. 16, no. 4, pp. 41-52, 2019.

Nurul Amirah Abdul Rahman is currently doing her masters in resource and educational technology at the Faculty of Education, Universiti Kebangsaan Malaysia. Her research interests are teaching and learning English via technology, online communities of practice, sustainable development goal (SDG), and also equality and equity of exposing English language and technology in rural area.

Nurul Akma M. Zizi is currently doing her masters in resource and educational technology at the Faculty of Education, Universiti Kebangsaan Malaysia. Her research interest are pre-schoolers behaviour, technology in education and the use of augmented reality among preschool students.

Izzah Hanis Sairi is currently doing her masters in resource and educational technology at the Faculty of Education, Universiti Kebangsaan Malaysia. She is passionate about early childhood education, adore working with preschoolers and deeply committed to providing quality and learner-centered instruction optimizing preschoolers success.

Fariza Khalid is a senior lecturer at the Faculty of Education, Universiti Kebangsaan Malaysia. Her research interests include e-learning, online communities of practice and emerging technologies for educational purposes.