ACADEMICIA

ISSN: 2249-7137 Vol. 11, Issue 5, May 2021 Impact Factor: SJIF 2021 = 7.492

ACADEMICIA
An International Multidisciplinary Research Journal
(Double Blind Refereed & Peer Reviewed Journal)

DOI: 10.5958/2249-7137.2021.01450.6

THE RELEVANCE OF CYBER SECURITY EDUCATION IN THE CLASSROOM

Zebo Bekmurodovna Sharipova*; Farrukh Yuldashev Khudayarovich**

*Senior Lecturer,
Department of Economics,
Yeoju Technical Institute in Tashkent,
UZBEKISTAN

**Student,
Business Management Administration,
Yeoju Technical Institute in Tashkent, UZBEKISTAN

ABSTRACT

Despite the fact that the Internet has had a positive effect on people's lives, there have been some negative problems associated with its use. Owing to a lack of knowledge and self-mechanism among Internet users to protect themselves from being victims of cyber-bullying, online fraud, racial abuse, pornography, and gambling, cases of cyber-bully, online fraud, racial abuse, pornography, and gambling have risen dramatically. However, previous research has shown that Internet users' awareness is still poor or moderate. One of the most important steps to take is to instill information and understanding in Internet users as early as possible, i.e., young children. Young children, in particular, must be taught how to act safely in cyberspace and how to defend themselves in the process. The aim of this systematic review paper is to investigate why it is so important for modern learners to be informed about the dangers of being involved in cyberspace, as well as the methods that stakeholders may use to encourage cyber security education in schools. A few methods for implementing cyber security education in schools are addressed in this article.

KEYWORDS: *Cyber Security, Cyber Safety, Cyber Education, Cyber Awareness.*

1. INTRODUCTION

Many of us use social media to share our emotions, start conversations, or make ourselves known. Since many people want to be the first to bring attention to a problem, they can overlook whether the information provided is accurate or not (Khalid, August 2017). The internet is not only for adults; in this age of technology and multimedia, children need to know about cyber security as well. While the Internet has a lot of potential and advantages for everyone, it can also be dangerous because it can lead to cyber risks like cyber addiction (Muniandy, 2013), gaming and gambling addiction (Ratten, 2015), cybersex (Kuss, 2015), pornography (L. Mosalanejas, 2014), and personal information disclosure (Kuss, 2015), (D. Krotidou, 2012), (N. Ahmad, November 13-15, 2019).

Parents should be concerned about cybercrime against children and teenagers because they do not realize their child is a target. Many parents are completely unaware of their children's online behaviors (Talib, 2017). Bullying can take many forms, including remarks and threats, as well as intimidation, harassment, bullying, and sexual exploitation. According to the Royal Malaysian Police (PDRM), nearly 80% of rape cases registered in the country in the last two years include virtual friendships, and the majority of the victims are under the age of 18 (R. S. Hamid, 2018). As more and more sexual predators use false identities on the internet to find victims, the grooming of children and teenagers to become victims of sexual assault is becoming more common.

There is no question that teenagers, considering their young age, are effective and competent at using their own or their parents' smart phones when it comes to protecting their children from cyber threats. Children are not only tech-savvy, but also adept at using it. In reality, some parents reward their children with gadgets as prizes for good grades, birthday gifts, and so on. As a result, while they are independently discovering the internet without limits or supervision, young children are exposed to technology-based violence. Since children now have internet access at an earlier age (al., 2018), it is vital for everyone, whether parents or children, to be aware of possible risks such as cyber bullying and to take safety precautions while using the internet. To foster responsible online conduct, educators must disseminate cyber security messages (Anon., 2016).

Children's internet use is rapidly evolving in response to significant social, industry, and technical advancement. Children's internet use is generally positive, as shown by their regular interaction with online videos, music, gaming, texting, and searching. Parents of three- to four-year-old's say their children are likely to watch YouTube cartoons, mini-movies, animations, or songs. Children's viewing habits change when they get older, with older kids watching more music videos, vloggers, YouTube celebrities, and funny videos (al., 2017). Schools play an important role in teaching students' critical digital literacy as well as guiding and informing parents about their children's internet use at home.

The goal of cyber security education is to inform technology users about the threats they may encounter when using internet communication tools like social media, chat, online gaming, email, and instant messaging. While there has been a lot of previous research on cyber security in various fields, such as (al., 2015) – (F. Lokman, n.d.), fewer studies have centered on the measures that need to be taken specifically by schools to help cultivate cyber security knowledge in depth. In the context of the Malaysian education system, the aim of this paper is to address

why it is so important that modern learners are informed about the risks associated with being involved in cyberspace, what factors impede this education, and the value of a cyber security curriculum that can be used by teachers in junior or primary schools.

2. Problem Statement

Humans can now enjoy two worlds: their real life and the virtual one, thanks to the internet (Press, 2014). All knowledge is now at people's fingertips thanks to search engines like Google and Yahoo, as well as video sharing sites like YouTube. However, the expanding cyberspace environment can have negative consequences for internet users, such as cybercrime. As a result, such problems should be addressed as soon as possible so that they do not have a significant effect. In this context, internet users' adoption of cyber security measures is critical. Since cybercrime may occur anywhere, regardless of individuals, organizations, or locations, cyber security education is needed.

The state of being protected against the criminal or unauthorized use of electronic data, or the steps taken to achieve this, is described as cyber security (Homeland, 2014). Our lives have changed dramatically as a result of the explosion of information and communication technology (ICT). Individuals and organizations can easily view any information thanks to the World Wide Web, but if it is used for harmful reasons, it can have a negative impact on people's lives (Anon., 2016). Furthermore, pornography is easily available on the internet, which can lead to social issues such as violence. The internet can also be a dangerous conduit for criminal activity and misbehavior, and it is the leading cause of Malay teenagers skipping school. Cyber security is also described as the operation, process, capacity, or state of protecting and/or defending information and communications systems and the information they contain from harm, unauthorized use or alteration, or exploitation (Anuar., n.d.). The internet unquestionably expands one's awareness. Online video games, for example, necessitate users who are fluent in English in order to comprehend game settings and procedures. Indirectly, this would promote the improvement of English reading, writing, and speaking skills. A computer game, on the other hand, is normally entertaining and takes a long time to complete. Teens may become sedentary as a result of this, or they may become fixated on video games and electronic devices. Adolescents may often become addicted, and constructive tasks like reviewing lessons are often neglected.

3. Research Questions

According to the Cyber Crime and Multimedia PDRM Investigation Division's statistics, cases of cyber-love scams, also known as the African Scam, are on the rise (Rosman, 2014). In 2013, 1095 cases of internet fraud were registered in Malaysia, compared to just 814 cases in 2012. (Marimuthu, 2016) also mentions an 18-year-old Malaysian boy who was arrested for violating the 1987 Copyright Act by uploading and downloading local music and foreign films without the permission of the owners. Gravity, Pacific Rim, 47 Ronin, The Hangover 3, We Are the Millers, The Hobbit: The Desolation of Smaug, and Ride Along were among the films uploaded. According to (F. Khalid, 2015), fraudulent online purchases increased in Malaysia in 2015, resulting in a loss of over RM4.9 million in the automotive, housing, and tourism sectors.

To control video game addiction, cyber security education is also needed. This addiction has unquestionably detrimental consequences. Teenagers spend a lot of time on computers and use

their devices to socialize. Addiction to video games becomes unavoidable over time, and adolescents' valuable time is consumed by their devices. This has a devastating effect on adolescents. Teenagers spend their nights surfing the internet, exacerbating the epidemic and potentially causing health issues. These threats and attacks can take several different forms, and users are often unaware that they are being targeted. To create a culture of cybersafety, it is critical to educate and empower users, especially children, on the safe and responsible use of online tools and platforms (Khalid, August 2017).

4. Purpose of the Study

The most common internet applications for Malaysians are social media sites such as Facebook, Instagram, LinkedIn, YouTube, and Twitter (K. Salamzada, 2015). This avalanche of information leads to a number of privacy and security concerns. Knowledge in this virtual space may also be questioned for its authenticity and accuracy. When confronted with potential cyber threats, children must be prepared to protect themselves and take responsibility. However, ensuring that teachers are adequately educated and up-to-date in their ability to encourage critical awareness rather than restrictive approaches to cyber safety, as well as directing students and parents in their use of the internet at home, presents challenges. Lack of skills, funding, and support are among the many obstacles that schools face in integrating cyber security education (D. Miles, 2011). Teachers are lacking in cyberspace skills and experience. Cyber security education can be difficult to introduce in schools and government ministries due to a lack of resources and facilities. The rapid pace of technological change creates new risks that necessitate new solutions. Teachers can have difficulty keeping up with the new technologies and therefore ensuring the safety of their students (M. A. Pitchan, 2017). Teachers face a significant challenge in this area because they lack access to learning materials and must be aware of technical advancements. Cyber security symposiums can be used to encourage early exposure and preparation for students in schools. People who have been exposed to and educated in cyber security are expected to be the country's potential cyber protection resource.

5. Research Methods

The study focuses on research findings in the area of educational cybersecurity. Using keywords like "cybersecurity," "cyber awareness," and "cyber education," several databases (Emerald, Google Scholar, Sci, Scopus, and EBSCOhost) were searched. The literature chosen was in Malay and English, the two languages in which the researcher is fluent. Furthermore, the quest was restricted to studies conducted from 2011 to 2019. There were over 240 studies found, but only 25 were chosen. The studies that were chosen were chosen based on their background, scope, and participants. Table I summarizes the chosen studies in terms of methodology, venue, research emphasis, field, and research implementation. The selection process is summarized in Figure 1.

SEARCH JOURNALS	KEYWORDS
	CYBERSECURITY
	CYBER AWARENESS
	CYBER EDUCATION
	EMERALD

USED DATABASE	GOOGLE SCHOLAR
	SCI, SCOPUS
	EBSCOhost
LIMITS THE STUDIES	PUBLISHED BETWEEN 2011-2019
	LANGUAGE ENGLISH & MALAY
	CYBERSECURITY EDUCATION
	IMPORTANCE OF CYBERSECURITY
SELECT 25 STUDENTS	THE STUDIES BASED ON RESEARCH FOCUS
	THE IMPORTANCE OF CYBERSECURITY

Methodology	**Location**	**Research focus**	**Area**	**Application of cyber security 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)	Cyber security (12) Conception/ perception (2) Behavior(1) Cybercrime(2) Cyberethics (2) Awareness (4) Reasoning (1)	Mobileapps (1) Safety(1) Curriculum(1) Legislation (2) Infrastructure (2) Security training, programme, seminar, workshop (4)

There are two research questions in this paper:

1) What role does cyber security education play in schools?

2) What are some methods that stakeholders should use to encourage students to learn about cyber security in schools?

6. RESULTSANDDISCUSSIONS

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

The Importance of Cyber security Education in Schools

According to the literature review, if a school is able to completely implement cyber security education, there are several benefits. According to a study on adults and cyber security,

participants are less likely to spend money or time on cyber security workshops or programs. As a result, it is critical for schools to transform into information centers in order to raise awareness of cyber security problems in the community. School administrators and teachers may collaborate to plan cyber security-related school programs or events. Furthermore, the Malaysian government provides financial support to schools, allowing them to cover the costs of organizing community activities. Furthermore, cyber security education is useful in improving people's mindsets. Any person who is unaware of cyber security is a product of not being told about the value and consequences of cyber security.

Strategies That Stakeholders Can Use to Promote Cyber security Education in Schools

Teachers have described video cartoons as tools to use when addressing cyber security concepts with primary school students, such as using the Upin and Ipin stories to increase cyber security knowledge (William, 2012). Information and communication technology (ICT) subjects in primary schools should be expanded to include cyber security topics. Furthermore, other topics may be used to teach the security aspects of cyber security. Students can be assigned essays on cyber security under the subject of Bahasa Melayu, for example. Furthermore, cyber security can be discussed in the classroom or used as a subject for speech competitions, and cyber security awareness weeks can be conducted.

Teacher education programs must also train pre-service teachers to model and teach cyber security topics and safe computing practices so that future generations can know how to act ethically when online (L. Muniandy, 2017). Despite their young age and easy access to technology, the pre-service teachers polled lack sufficient cyber security expertise and the ability to teach their potential students how to protect themselves and their data. This contradicts the idea of digital natives, as natives will recognize which environmental cues mean that they are safe and secure.

One action relevant party might take to protect such groups from emerging cyber security threats is to provide information to upgrade teachers' and students' awareness of cyber issues (Schneier, n.d.). To protect internet users from possible cybercrime and emerging cyber threats, cyber security awareness education is critical. While some security experts question the value of cyber security education or training (Moore, 2011), several researchers agree that it is critical in protecting cyber users from cyber threats (Muniandy, 2013), (Kabay, 1994). Education is critical in dealing with emerging cyber security threats, as all defense factors play a role in thwarting them.

Furthermore, one of the methods for promoting cyber security education in schools is through security awareness programs. The concepts of cyber security awareness have been perfected through several years of social psychology study, but IT practitioners have largely overlooked them while designing information security awareness programs (Paullet, 2019). For example, the National Security Agency and the National Science Foundation (NSA/NSF) fund a cyber security education initiative called GenCyber, which is a summer camp for American grade school students and teachers. This type of awareness programme should be introduced in every school because it can raise cyber security awareness and preparedness among the student body.

Cyber security organizations, such as student clubs or councils, may be formed by school administrations. This gives students, as well as the rest of the school community, valuable

attention. Students can learn more about cyber security with the help of their teachers. Students will learn how to use the learning management system, according to. Furthermore, students must gain a personal understanding of cyber security, and the most successful way to do so is through active learning. Students use a learner-centered approach in this style of 21st-century learning, in which they gather knowledge about cyber security from the internet and the instructor only tracks their activities from time to time. active learning promotes better understanding, especially among students. Despite the fact that students gain a high degree of knowledge about cyber security concerns such as cyber bullying, exchanging personal details, and internet banking, they receive little information about cyber-sex and self-protection. Teachers, parents, and the government must be more involved in educating students about these issues, and the stigma on sex education must be broken (Anon., 2016).

7. CONCLUSIONS

Based on a review of the literature, it was determined that protecting children through cyber security education is critical so that they are aware of the possible risks they pose while using internet networking resources like social media, texting, and online gaming. However, there are a number of obstacles to overcome when it comes to cyber security education. All stakeholders, including teachers, parents, peers, and the government, must collaborate to find the best approach for protecting children from cybercrime and cyberbullying through school-based cyber security education. Since such campaigns are more engaging and exciting for children to understand, the media, such as television and radio, must also play an important role in educating children through cyber security campaigns.

REFERENCES

1. (Khalid, August 2017)F.AnnasinghandT.Veli,―Aninvestigationintorisksawarenessand e-safety needs of children on the internet, ‖ Interactive Technology andSmartEducation,vol.13,no.2,pp.147-165,2016.
2. L.MuniandyandB.Muniandy,―Theimpactofsocialmediainsocial and political aspects in Malaysia: An overview, ‖ International JournalofHumanitiesandSocialScience,vol.3,no.11,pp.71-76,2013.
3. V.Ratten,―Across-culturalcomparisonofonlinebehavioral advertising knowledge, online privacy concerns and social networkingusing the technology acceptance model and social cognitive theory, ‖Journal of Science & Technology Policy Management, vol. 6, no. 1, pp.25-36,2015.
4. M.D.GriffithsandD.Kuss,―Onlineaddictions,gambling,video gaming and social networking, ‖ The Handbook of the Psychology ofCommunication Technology, Chichester: John Wiley, pp. 384-406,2015.
5. L.Mosalanejas,A.Dehghani,andK.Abdolahofard,―Thestudents' experiences of ethics in online systems: A phenomenological study, ‖Turkish Online Journal of Distance Education, vol. 15, no. 4, pp.205-216,2014.
6. D.Krotidou,N.Teokleous,andA.Zahariadou,―Exploringparents' and children's awareness on internet threats in relation to internetsafety, ‖Campus-WideInformationSystems,vol.29,no.3,pp.133-143,2012.

7. N.Ahmad,U.A.Mokhtar,Z.Hoodetal.,—Cybersecuritysituational awarenessamongparents, ‖presentedattheCyberResilienceConference,PutrajayaMalaysia,pp.7-8,November13-15,2019.

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

9. R.S.Hamid,Z.Yunos,andM.Ahmad,—Cyberparentingmodule development for parents, ‖ in Proc. INTED2018 Conference, 5th-7thMarch2018,Valencia,Spain, 2018.

10. F.Khalidetal.,—Aninvestigationofuniversitystudents'awarenesson cyber security, ‖ International Journal of Engineering & Technology,vol.7,pp.11-14,2018.

11. Childrenandparents:Mediauseandattitudesreport. Ofcom.[Online].Available:

12. http://www.ofcom.org.uk/data/assets/pdf_file/0034/93976/Children-Parents-Media-UseAttitudes-Reports-2016.pdf

13. C.S.Kruseetal.,—Cybersecurityinhealthcare:Asystematicreviewof modernthreatsandtrends, ‖TechnologyandHealthCare,vol.25,no.1,pp.1-10,2017.

14. P.Dongetal.,—Asystematicreviewofstudiesoncyberphysical systemsecurity, ‖InternationalJournalofSecurityandItsApplications,vol.9,no.1,pp.155-164,2015.

15. U.Franke and J.Brynielsson,—Cybersituationalawareness—A systematicreviewoftheliterature, ‖Computers&Security,vol.46,pp.18-31,2014.

16. N.H.A.Rahimetal.,—Asystematicreviewofapproachestoassessing cybersecurityawareness, ‖Kybernetes, 2015.

17. D.Melladoetal.,—Asystematicreviewofsecurityrequirements engineering, ‖ Computer Standards & Interfaces, vol. 32, no. 4, pp.153-165,2010.

18. A.V.Herrera,M.Ron,andC.Rabadão,—Nationalcyber-security policiesorientedtoBYOD(bringyourowndevice):Systematicreview, ‖inProc.201712thIberianConferenceonInformationSystemsand Technologies(CISTI),pp.1-4,2017.

19. F.Mishnaetal.,—Interventionstopreventandreducecyberabuseof youth: A systematic review, ‖ Research on Social Work Practice, vol.21,no.1,pp.5-14,2011.

20. H.F.Lokman,N.Nasri,andF.Khalid,—Theeffectivenessofusing twitter application in teaching pedagogy: A meta- synthesis study, ‖InternationalJournalofAcademicResearchinProgressiveEducationandDevelopment,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).Aglossaryofcommoncybersecurityterminology.NationalInitiativeforCybersecurityCareersandStudies:Departmentof Homeland Security. [Online]. Available:http://niccs.uscert.gov/glossary

23. S.S.Anuar.(2018).8313KesPenipuanSiberDirekodkan.[Online].

24. Available:https://www.bharian.com.my

25. M. Rosman. (2014). KPDNKK TahanRemaja 18 tahunmuatturunmuziktanpa kebenaran. [Online]. Available:http://www.utusan.com.my

26. M. Marimuthu. (2016). Pembeliansecara online catatkespenipuanpalingtinggipada 2015.[Online].Available:http://www.nccc.org.my

27. F.Khalid,M.Y.Daud,andA.A.Karim,―Pemilihan Aplikasi Teknologisebagai Medium Perkongsian Maklumatoleh Pelajar Siswazah University, ‖ presented at the ASEAN Comparative Education Research Network Conference,2015.

28. K.Salamzada,Z.Zarina,and M.A.Bakar,Aframe work for cyber security strategy for developing countries: Case study of Afghanistan, ‖ Asia-Pacific Journal of Information Technology and Multimedia, vol. 4,no.1,pp.1-10,2015.

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

30. M.A.Pitchan,S.Z.Omar,J.Bolong,andA.H.Ghazali,―Analisiskeselamatansiberdariperspektifp ersekitaran social: Kajianterhadappengguna internet di LembahKlang, ‖ Journal of Social Science andHumanities,vol.12,pp.16-29,2017.

31. P.PuseyandA.S.William,―Cyberethics, cyber sefety, and cyber security: Per service teacher knowledge, preparedness, and the need for teacher education to make a difference, ‖ Journal of Digital Learning in Teacher Education,pp.82-88,2012.

32. L.Muniandy,B.Muniandy, and Z.Samsudin,―Cybersecurity behavior among higher education students in Malaysia, ‖ Journal of Information Assurance & Cyber security, pp.1-13,2017.

33. B.Schneier, Security Awareness Training,2013.

34. R.Moore, Cybercrime: Investigating High-Technology Computer Crime, MA: Anders on Publishing, Burlington,2011.

35. 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.

36. M.Kabay,―Psychological factors in the implementation of information security policy, ‖EDPACS, The EDPAudit,ControlandSecurityNewsletter,vol.XXI,no.10,pp.1-10,1994.

37. D.NakamaandK.Paullet,―The urgency for cyber security education: The impact of early college innovation in hawaii rural communities, ‖Information System Education Journal,vol.16,no.4,pp.41-52,2019.