Students' Engagement in Cybersecurity Knowledgeability

Agung Prabowo*[1], Rommi Kaestria[1], Ika S. Windiarti[2]

[1] Department of Information Systems, STMIK Palangkaraya, Palangkaraya, 73112, Indonesia
[2] Department of Computer Science, Universitas Muhammadiyah Palangkaraya, Palangkaraya,73112, Indonesia
Emails: agungdosen@gmail.com rokafordev@gmail.com ikasafitri@gmail.com

Abstract

Teenagers nowadays are one of the largest groups of internet users. Teenagers internet users include Junior and Senior High School students. The students' activities on the Internet have become their daily life and necessities. Unfortunately, those students do not fully understand about personal security in internet related activities. The research purpose is to investigate students' engagement in terms of cybersecurity knowledgeability. This study will also explore how is their basic knowledge of digital society in terms of internet usage. The students' concern about the security of their personal information when using Internet still need to be investigate and resolved. The study also aims to reduce the risk of threats and cybercrime that possible to harm the students. The results from this study shows that most of the students have enough knowledge to do activities in the Internet safely. However, the students have less awareness about personal data protection to be used in the internet. Other result from this research revealed that most of the schools do not have education program about cyber security related material. The outcomes of this research are recommendation and education framework to teach cyber security for high school students.

Keywords: *cybersecurity; cyber-attack; digital society; personal information security; phishing*

1. Introduction

In the current situation most of the individuals, organizations, and countries very dependent on running their daily activities to the internet connection. Nowadays, the internet can connect the world immediately. People connected from different places in different time zone can work together, collaborating, and discussing by connected to the internet. Moreover, the government also running its activities through an internet connection. Also known as the e-government. However, even though cyberspace offers a variety of conveniences and so many opportunities, on the other hand, people do not realize that there are risks in using the internet [1].

Internet users who utilize Wi-Fi in public place for business or private purposes have to be careful about their personal information security. The users' personal information and data which will be process through the internet connection or internet network were not entirely secure [2]. There is opportunity because of their careless treatment in the internet usage their information or private data becomes unprotected and also becomes the target for cybercriminals to do things that endanger the organization or company [3]. Therefore various countries have developed and implemented cybersecurity awareness and also build programs to educate the internet users about the importance of security in internet connection activities [4].

ISSN: XXXX-XXXX IJXX

Supported by the increasingly broad range of Internet services, as well as the cheap price of supporting devices for the internet such as smartphones, personal computers, tablets, laptops, etc. make users of information technology devices grow rapidly in Indonesia [5]. As internet users are increasingly large, the number of cybercrimes in Indonesia is the second highest in the world after Japan. in total there were 90 million cyberattacks according to the Agency of the Assessment and Application of Technology (BPPT) [6].

This fact shows that Indonesian become a high-risk country in terms of cyber-attacks in cyberspace[7]. Also, Indonesia has low awareness of cybersecurity when the people connected to the virtual world. therefore oh, it is very important to increase awareness of the people about how to use the internet safely and securely especially for young people in Indonesia, such as high school students and the teenager [4].

As we know demographically, a citizen of Indonesia is dominant with people at a young age rather than older age. Therefore Indonesia referred to as having a demographic bonus in terms of economic growth factor [8]. So far, the introduction of the cybersecurity in using the internet is mostly only given to the older people. People in the younger age are rarely to get knowledge about cybersecurity. Therefore, the awareness among them is still very long low regarding the importance of this matter. This awareness can be included in the cross-cultural training as extracurricular lesson at school or college [9]. The purpose of this research in this paper is to investigate the level of their concern about the importance of implementing a security protocol in using the internet. In other words, this paper aims to investigate the cybersecurity awareness of the high school students and to find the best method to conduct awareness training [10].

2. Literature Review

In terms of literature, this research focused on three main literature topics. The first topic is about digital society specifically in teenagers' group of age. The second topic is personal information security, which discussed current and popular issues related to teenagers' behaviour towards information disclosure. The third topic is about teenagers' cybersecurity knowledgeability.

2.1 Digital society

Naturally, school students can be classified as a digital native of internet user groups. A digital native is a group that was born when internet technology was in the middle of their lives. so, when they use internet technology are browsing in cyberspace, they have high level of confidence. However, the fact is that they do not have enough knowledge or awareness about the importance of maintaining security in their activities in cyberspace [11, 12].

In digital native group of age, the level of needs to be connected to the internet is very high. for them being connected to Internet to the internet is such a primary necessity on top of other needs. they also frequently using public Wi-Fi connection. the main reason of using a public Wi-Fi connection is because public Wi-Fi offers a variety of conveniences and it cost very low. even in some public space, the Wi-Fi connection is free for any internet users. this fact causes a risk that the user does not really aware of the importance of their own personal information security. Moreover the risk it's become higher when is that users doing activities such as Internet banking or private or confidential information related activities [13, 14].

One other important thing that happens in the Indonesian Society is the effects of living in the Digital Society causing serious social aspects in people's life. People at a younger age becoming more like to make friends in the digital world. This has become Unstoppable things in these students Society especially among internet users. there is a need to educate the young people that friendship in cyberspace was very different from friendship in the real world. Knowing someone online, we cannot give me something you know about the kindness and authenticity of our friends online. Gayatri et al. explained that they can be the object of cyberbullying, pornography, or another kind of crime [15].

At this time the use of internet technology or commonly referred to as cyberspace has been used in various fields of human daily activities. the user of internet technology is at different levels of age, education, and occupation. Younger people especially teenagers we're using internet more frequently than other groups of age. On the other hand, the teenagers are being the target of the cybercrime criminals in cyberspace. This is caused by the lack of awareness of the teenagers are students in terms of maintaining security and personal information that will be used during their activities in cyberspace [16].

2.2 Personal information security

In cyberspace space activities the cybercrime criminals of the weaknesses of the internet users who are teenagers especially students at a younger age. These criminals use the data or personal information of students who are unaware about the danger that can affect the user of the student itself, as well as affect the organization or institution of the users.

Modern smartphone platforms have various applications. meaning of them asking permission to access the data and personal resources, such as email account, camera, contacts, or user's current location. the smartphone users are the control holder of this permission. They have to be realized that's does permission to access the private information is not always should be approved.

The users need an application as the requirement to do activities in cyberspace. this application is installed in the PC or mobile phone. As we know if we conduct the application installation there will be user agreement regarding the application. There are still many users of these applications that ignore or do not read the user agreement when installing the application. One of the reasons for all of this fact is because in the user agreement sometimes contain difficult words are sentences to understand. Users tend to "click I accept/agree" without concern of knowing the detailed purposed and objectives of these applications, even the risk on the application installation that is officially installed with the users' consent [17].

About the concept of video surveillance for younger users of the Internet such as in the examination situation, it has become popular and usual in some education institutions. the positive impact of video surveillance in the examination. Such as the convenience of the exam committee to ensure that the examination is running well without any fraud in the exam. on the other hand, there is a negative impact on using surveillance cameras in the exam situation. For example, the students in the exam become not confident, low self-esteem, feeling of suspicion among them [18].

Research about the response of people in using camera surveillance resulting in camera or online surveillance causing a higher sense of privacy violation and situational pressure. With awareness of surveillance, the respondents in the research realize that the information they shared online will be possible to be exposed to other unknown Observers. moreover, this case can be the victim of saving and sharing which resulted in an invasion of privacy [19].

The use of internet technology among teenagers especially school students in carrying out learning activities is inseparable. however, there are threats of cybercrimes and also personal information security use [20]. This threat increases significantly along with the increasing number of internet users. Therefore, cybersecurity or security protocol in carrying out connectivity to cyberspace is a very important thing to understand. this is because actually cybersecurity is away or effort to protect Hardware, software, data, or systems from the criminals in cyberspace [21].

2.3 Cybersecurity knowledgeability

This fact leads to the need for socialization the understanding of cybersecurity among internet users especially young people such as students at school. It is very important to know their level of understanding and also their level of concern in maintaining security especially in sharing information particularly private and personal matters in cyberspace [22].

Teaching cybersecurity in school has become a very important part of information technology that has been widely used by the school. The use of Information Technology in schools including carrying out learning and teaching, Financial Administration, and general administration in the school wide. The importance of awareness or knowledge about cybersecurity is not only the responsibility of the IT staff or only a few people in the school but all individuals involved. Persons involved in cybersecurity awareness including teachers, students, and all employees. that has two half sufficient knowledge about cybersecurity because this knowledge is a very useful skill in daily life. this is because their life now is part of the life of the Digital Society [23].

To learn cyber-security is not only conducting a curriculum or a special subject at school. Moreover, the most important thing is to raise their awareness that living in digital society needs a level of understanding of cybersecurity. living in Digital Society, they are almost every day connected to the world of the internet and share various kinds of information on it. So we need to know the level of Desire of students whether the teachers need to the socialization of the knowledge of cybersecurity [24].

In some school, cybersecurity education becomes compulsory and also become elective for the student to learn about it. Become included in the curriculum, cybersecurity not only in these classes about cyber-security itself but also about cyber ethics and cyber safety. Therefore, teachers need to conduct socialization with the students, so they have a willingness or readiness to learn it. To ensure that the student has willingness and Readiness to learn about cybersecurity, the study program should be an interactive and interesting learning program. Some of standard knowledge that need to be taught to school students are about internet cookies, web phishing, and the use of e-commerce websites.

Internet cookies are one of the novel new technology on website matters. Cookies is a notification that always showed in the form of notification on the computer screen or mobile phone screen when did user access the website. Most users do not understand the meaning and purpose of cookies. They will ignore the notification or directly give permission or rejection without knowing the meaning and the proposed. The internet cookies are a feature that automatically records or restore data in a website. So the users' data such as name email address can be stored well in the website [25].

The internet cookies that can be seen in the browser is named as a simple cookie, Internet cookie, web cookie, or HTTP cookie. An Internet cookie is a tiny data fragment that stores in the computer as a result of a user's previous activities on certain websites [26]. The purpose of this digital data is meant to give convenience and ease in accessing a website, such as e-commerce. Some of the advantages of using cookie are Username and passwords have been stored automatically by cookie technology. Moreover, name, address, and credit card number that previously entered in the websites are stored and accessible.

On the other hand, there are also disadvantages of using cookie. Some of the disadvantages such as the risk of malware or virus infection of the computer because of the cookie content. This caused a computer or smartphone operating system to break down. Other disadvantage is the risk of a hacker to hack user's account and privacy abuse [27].

Web phishing is a method of committing fraud by tricking the target to steal the target account. Web phishing can be referred to a website that designed to do crime acts such as steal important information by taking over the victim's account for a specific purpose [28, 29]. This could be to look for opportunities for multiple accounts it's all connected to the account that has been obtained. Web phishing is provided with information that leads to fake website pages to trap victims. To avoid web phishing users should be more careful by paying attention to some security matters. For instance, if you access a website page make sure you are on the correct domain URL page. This is also a very important thing as a basic knowledge of cyber-security that should be on by students, teachers, or other people to prevent the occurrence of acts of cybercrime [30].

Another possibility of Internet fraud is the use of e-commerce sites. Shopping sites, marketplace, or e-commerce become an inseparable part of the digital society. The users of this site are not only among adults but also among internet users as long as they have money. These sites conduct a financial transaction or buying and selling online. Therefore, it is very important for teenagers to always get guidance from their parents especially in online shopping. this is because internet users at a young age or among teenagers need to pay attention to Security in online transactions [31]. The parent or adult should make sure whether the teenagers have supervision or permission especially when they buy items that are not normally used by teenagers. parents are adult guidance also needed to supervise whether they wisely use their money in a bank account to pay in online shopping [32].

3. Research Method

This research conducted using mixed methods design that is The Explanatory Design. In Figure 1, The Explanatory Research Design consists of two phase that starts with quantitative data phase [33]. This quantitative data is being collected and analysed. The data then used to build up the qualitative analysis on the research.

Quantitative data were collected from survey questionnaire to male and female students in 7 (seven) Junior and Senior High Schools in Palangkaraya city. This phase was conducted in August to October 2019. The survey conducted in manual form to have optimal results as targeted.

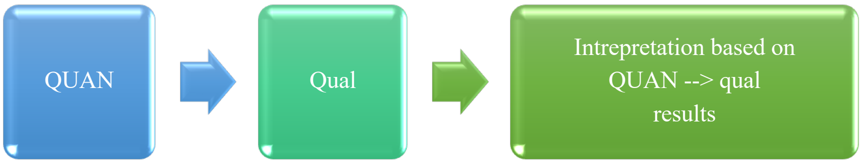

Fig.1. The Explanatory Research Design

The collected quantitative data then being analysed using frequency counting on each of the questions. The results of quantitative data analysis built up quantitative analysis using literature explanatory method.

The method of sampling in this research using the homogeneous type purposive sampling technique for qualitative research. Homogeneous type purposive sampling is a sampling technique that employ research participants with a set of characteristics.

4. Results and Discussion

The survey sheets were conveyed and takes two months to gather the appropriate responses from the respondents. An absolute number of 612 participants have filled the inquiries as shown in Figure 2.

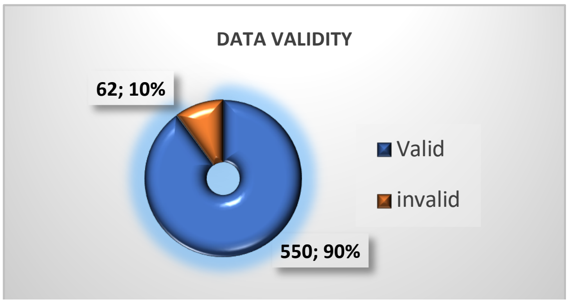

Fig. 2. Data validation results

After validation of the outcomes, we found that 62 polls were not filled appropriately. A portion of the slip-ups brought about by pick more than one alternative and left the inquiry with no answer. The data validation results 550 surveys.

4.1 Participants' profile

The survey was conducted in 7 Junior and Senior High Schools in Central Kalimantan, Indonesia with age range 15-20 years old. We grouped the respondents into three groups which are 13-14, 15-16, 17-18 years old. Table 2 shows number of participants based on age and gender. A total number of 332 respondents are male, while 218 ones are female.

Table 1. Age Groups of the participants

Ages	Male	Female
13-14	97	93
15-16	121	56
17-18	114	69
TOTAL	332	218

4.2 Basic idea of digital society

The participants were asked about their knowledge on basic questions about digital society. These questions were made to give a picture on how the students realized their other side of life about being online in their digital society. Teenagers are one of the biggest age groups as internet users. Many portions of the teenagers in the world were not cognizant that security issues in internet usage is very important. We ask 5 questions, as shown in Table 2, related to the students' basic knowledge about digital society.

Table 2. Questions about Basic idea of Digital Society

Questions	
Q1.	Do you feel secure when using internet connected PC or mobile phone?

Q2.	Do you have a sense of safety when you utilize Wi-Fi in public place?
Q3.	Do you make friends more in the internet instead of in reality?
Q4.	When you get an email from a new sender, do you open it?
Q5.	Will you meet in person a new friend that you have just met on the web?

Based on the survey, as shown in Figure 2, Q1 ask the participants about their sense of safety in using the PC or mobile phone which connected to internet [34]. A number of 378 participants out of 550 people said that they feel secure. Based on research by Livingstone et al. and Tomczyk et al., In Europe, most children feel secure to be connected in the internet [35, 36].

Moreover, for Q2, 356 participants also feel secure when utilize Wi-Fi in public place. This is emerged consideration that the high school students have less protective behaviour in public Wi-Fi networks. This shows that students are feel very comfortable when using the internet, therefore there is a need to educate them on how to use the internet securely.

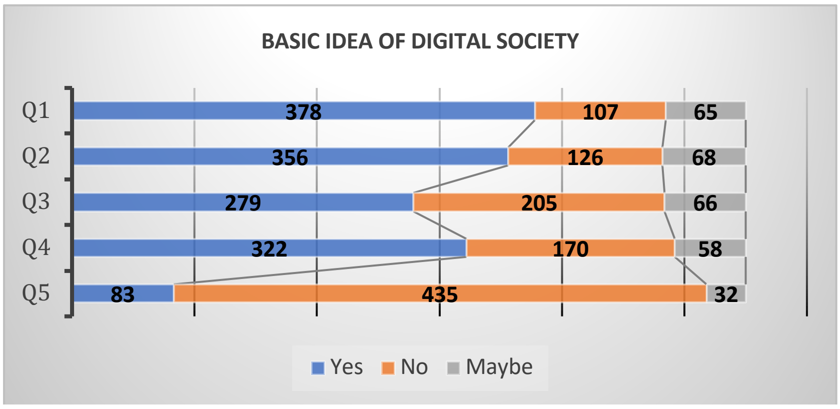

Fig.3. Basic Idea of Digital Society

Students seem do not have reluctance to make friends through the internet rather than real life, as shown in Figure 3 for Q3, a number of 279 students say Yes. In the same figure we also ask their responses when receiving email from someone not in their contacts. The results of Q4 is 322 students will open the email. They do not concern that their action may harm their identity and personal information safety. Surprisingly, when they asked whether they will meet somebody that they recently know in the internet, the answer is that they will not meet him/her in person. A number of 324 students, calculated 58,90% refuse to do this. This data means that students have apprehension that someone they newly known on the web is not trusted.

4.3 Personal information security

This research also investigates about students' knowledge and experiences on their personal information security. The questions are shown in Table 3.

The second groups of questions are about students' knowledge on personal information security as shown in Figure 4. In Q6, they intuitively post their own or family picture on the social media or various other website, without permission from their parents. A number of 465 students or 84,54% of the total respondents do not realize that this action may harm their family in the future. This also shows that there is a lack of basic knowledge of privacy.

Table 3. Questions about Personal Information Security

Questions	
Q6.	Have you ever posted your image or family picture online without permission from your parents?
Q7.	Have you ever rejected a mobile application that need access to your contacts, camera, or area?
Q8.	Do you believe that it is essential to read the user agreement in program installation before clicking, “I accept"?
Q9.	Have you ever known are being observed online without your assent, for instance in CCTV, or in test circumstance?
Q10.	Do you believe that your information on the educational system is secure?
Q11.	Do you utilize similar passwords for email accounts and online communities, for example, Facebook, Instagram and Twitter?
Q12.	Do you realized that whatever you post online will affect you in the future?

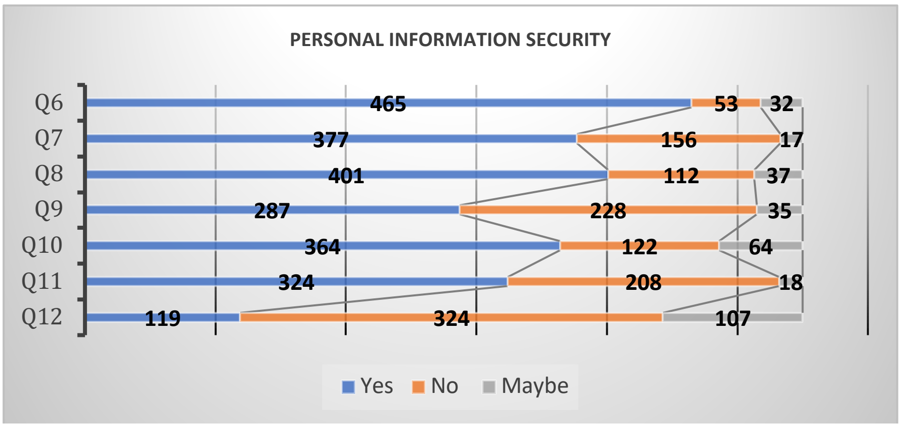

Fig. 4 Personal Information Security

Contrary, in the next 3 questions Q7, Q8, and Q9, they are concern about their security in the internet. 377 students ever rejected access request to their contacts, camera or else when installing certain mobile application. This is a good sign that they are aware of the risky action. Most of them also said it is essential to read user agreement before the click “I Accept” button in the middle of program installation. This shows students aware of the need to agree to a term and condition. Lavesson et.al and Putnam in their research explained that students are group of people that need to learn how to avoid personal information intervention by using spyware detection [37, 38].

In Q9, students realized that in certain circumstances they were being watched and monitored on the internet. There are more than half of them (52,18%) recognize it. Every student’s data and information recorded in school and education department system. This matter raised concern of the society whether the data safe and free of security abuse. According to data in Figure 4, Q10 answer that 364 students feel their data and personal information safely and securely stored in the system.

In terms of password management, 324 participants use similar passwords for email accounts and online communities such as Facebook, Instagram and Twitter. On the other hand, 208 students said that the used different password for such account. Therefore, there is a need to give education to the students about password management for security awareness.

Murillo et al. conducted a research on student awareness of their privacy implication on their future [39]. Most of the participants in this research do not realize that any picture, video, or written post in the internet will remain stay in the internet, there is 324 participants or about 58,90% answer.

4.4. Cybersecurity knowledgeability

There are 7 questions to be asked to the students about their cybersecurity knowledgeability. The question can be seen in Table 4.

Table 4. Questions about Cybersecurity Knowledgeability

Questions	
Q13.	Do you understand about the idea of cybersecurity?
Q14.	Does your school have a cybersecurity course?
Q15.	Do you need to learn more about cybersecurity?
Q16.	Will you take a cybersecurity course when made as an educational program?
Q17.	Do you know about Internet cookies?
Q18.	Do you know about web phishing concept?
Q19.	Have you ever bought online without permission from your parents?

The third group of questions is discussing about students' cybersecurity knowledgeability. In Q13, most of the students do not understand about the idea of cybersecurity. About 52,54% of the students said no in this question. This result seriously indicates that the students need an education program containing basic knowledge about cybersecurity.

When Q14 being asked, 432 students said that in their school do not have a cybersecurity course. This results strongly support the objective of this research to provide cybersecurity education program for high school students to enrich their knowledge when accessing the internet in order to minimizing the risk behind it.

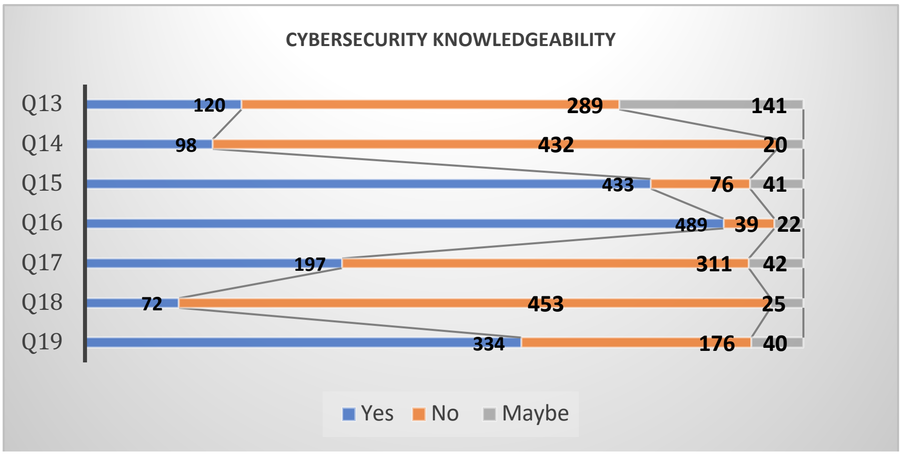

Figure 5. Cybersecurity Knowledgeability

Also, in Q14 and Q15 results, the students have eagerness to learn more about the cybersecurity knowledge, proven by 433 of the say yes to learn more about cybersecurity. In both questions, a substantial number of people, more than 78% of them say Yes to discover security in internet usage. Tirumala et.al. and Pusey et.al researched the importance of giving such education for school students. This result indicates the longing and needs of the students to become familiar with cybersecurity. This shows mindfulness is exceptionally required.

There is a surprising outcome with respect to whether the students are eager to accept cybersecurity as a course in their educational program and the outcome shows a passionate willingness. More than 80% of the participants in Q16 answer that the want to take cybersecurity.

Apparently, they also do not understand about the Internet cookies, shown from 311 students say No in Q17. Students have to cognize that the Internet cookies can be harmful for their personal data when they browse in the internet. They have to realize that the Internet cookies, stored their data when accessing websites such as e-commerce.

Moreover, they also do not understand about the concept of web phishing. More than 75% of the students stated that they do not know that web phishing is an attempt to redirect to fake webpage in order fraud someone identity including bank account private information. This outcome demonstrates most of students lack the information on web phishing assaults. This represents a danger to students' data and the school as well. A critical mindfulness is expected to clear this uncertainty before happening from any occurrence.

From the last question result, the participants not asking their parents' permission in buying something online. A number of 334 participants said that they ever buy online without permission from their parents. The students need to be protected from such potential internet security threats.

5. Conclusions

From the finding, data analysis and discussion, we can conclude the following points:

1. The students have a good basic idea of digital society. They know the benefit and harmful sides of internet usage in their daily activities.
2. The students have less awareness about personal information security. It reflected from the ignorance of personal data protection when they surf and make contact in the internet.
3. There is a need for conducting cybersecurity training and curriculum development at school, particularly in junior and senior high schools.

Further development of this research will be building a framework for cybersecurity curriculum for high school students. The objective is to provide them enough knowledge and awareness for the to be ready in using internet technology.

References

[1] M. C. B. Umanailo *et al.*, "Cybercrime Case as Impact Development of Communication Technology That Troubling Society," *Int. J. Sci. Technol. Res,* vol. 8, no. 9, pp. 1224-1228, 2019.

[2] E. Shahin, "Is WiFi Worth It: The Hidden Dangers of Public WiFi," *Catholic University Journal of Law and Technology,* vol. 25, no. 1, p. 7, 2017.

[3] M. Btoush, A. Alarabeyat, M. ZBOON, O. RYATI, M. HASSAN, and S. AHMAD, "INCREASING INFORMATION SECURITY INSIDE ORGANIZATIONS THROUGH AWARENESS LEARNING FOR EMPLOYEES," *Journal of Theoretical & Applied Information Technology,* vol. 24, no. 2, 2011.

[4] P. D. Persadha, A. Waskita, M. Fadhila, A. Kamal, and S. Yazid, "How inter-organizational knowledge sharing drives national cyber security awareness?: A case study in Indonesia," in *2016 18th International Conference on Advanced Communication Technology (ICACT)*, 2016: IEEE, pp. 550-555.

[5] A. Z. Tayibnapis, L. E. Wuryaningsih, and R. Gora, "The Development of Digital Economy in Indonesia," *IJMBS International Journal of Management and Business Studies,* vol. 8, no. 3, pp. 14-18, 2018.

[6] R. Broadhurst and L. Y. Chang, "Cybercrime in Asia: Trends and challenges," in *Handbook of Asian criminology*: Springer, 2013, pp. 49-63.

[7] R. W. Saputra, "A survey of cyber crime in Indonesia," in *2016 International Conference on ICT For Smart Society (ICISS)*, 2016: IEEE, pp. 1-5.

[8] A. A. G. O. Wisnumurti, I. K. Darma, and N. N. R. Suasih, "Government policy of Indonesia to managing demographic bonus and creating Indonesia gold in 2045," *Journal Of Humanities And Social Science (IOSR-JHSS),* vol. 23, no. 1, pp. 23-34, 2018.

[9] A. Prabowo, I. S. Windiarti, and Rosmiati, "Cross-cultural training as part of policy and business strategies to prepare Indonesian IT engineers in global job market competition," in *2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT)*, 2017: IEEE, pp. 1-5.

[10] A. Prabowo, I. Windiarti, and Sulistyowati, "Towards the best method of cross cultural training for IT engineering graduates from eastern Indonesia region: Ready to be global engineers," in *2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, 2017: IEEE, pp. 115-119.

[11] D. Pencheva, J. Hallett, and A. Rashid, "Bringing cyber to school: Integrating cybersecurity into secondary school education," *IEEE Security & Privacy,* vol. 18, no. 2, pp. 68-74, 2020.

[12] H. Hardika, E. N. Aisyah, K. M. Raharjo, and D. U. Soraya, "Transformation the Meaning of Learning for Millennial Generation on Digital Era," *2020,* Transformation; The Meaning of Learning; Millennial Generation vol. 14, no. 12, p. 13, 2020-07-31 2020, doi: 10.3991/ijim.v14i12.15579.

[13] D. Maimon, M. Becker, S. Patil, and J. Katz, "Self-protective behaviors over public WiFi networks," in *The {LASER} workshop: Learning from authoritative security experiment results ({LASER} 2017)*, 2017, pp. 69-76.

[14] Alshira, #039, and M. H. H, "The Effects of Usability and Accessibility for E-Government Services on the End-user Satisfaction," *2020,* Website Usability, Website Accessibility, Human Computer Interaction, End-User Satisfaction. vol. 14, no. 13, p. 13, 2020-08-14 2020, doi: 10.3991/ijim.v14i13.14659.

[15] G. Gayatri, U. Rusadi, S. Meiningsih, D. Mahmudah, and D. Sari, "Digital citizenship safety among children and adolescents in Indonesia," *Jurnal Penelitian dan Pengembangan Komunikasi dan Informatika,* vol. 6, no. 1, p. 122672, 2015.

[16] M. Näsi, A. Oksanen, T. Keipi, and P. Räsänen, "Cybercrime victimization among young people: a multi-nation study," *Journal of Scandinavian Studies in Criminology and Crime Prevention,* vol. 16, no. 2, pp. 203-210, 2015.

[17] D. Susser, "Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't," *Journal of Information Policy,* vol. 9, pp. 148-173, 2019.

[18] N. Desai, K. Pathari, J. Raut, and V. Solavande, "ONLINE SURVEILLANCE FOR EXAM," *Jung,* vol. 4, no. 03, 2018.

[19] W. H. Ip, "Am I being watched on the internet?: examining user perceptions of privacy, stress and self-monitoring under online surveillance," 2013.

[20] B. O. Sekyere, "Studying Information Security Behaviour among Students in Tertiary Institutions," ed, 2015.

[21] A. McIntyre, "Developing a Cybersecurity Protocol for Your Operational Environment," *Natural gas & electricity,* vol. 34, no. 9, pp. 23-27, 2018.

[22] K. S. Jones, A. S. Namin, and M. E. Armstrong, "The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals," *ACM Transactions on Computing Education (TOCE),* vol. 18, no. 3, pp. 1-12, 2018.

[23] P. Pusey and W. A. Sadera, "Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference," *Journal of Digital Learning in Teacher Education,* vol. 28, no. 2, pp. 82-85, 2011.

[24] E. Kritzinger, M. Bada, and J. R. Nurse, "A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK," in *IFIP World Conference on Information Security Education*, 2017: Springer, pp. 110-120.

[25] M. L. Jones, "Cookies: a legacy of controversy," *Internet Histories,* vol. 4, no. 1, pp. 87-104, 2020.

[26] P. Paul *et al.*, "Using Browser Cookies for Event Monitoring and User Verification of an Account," in *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 2018: IEEE, pp. 455-460.

[27] A. Dabrowski, G. Merzdovnik, J. Ullrich, G. Sendera, and E. Weippl, "Measuring cookies and web privacy in a post-gdpr world," in *International Conference on Passive and Active Network Measurement*, 2019: Springer, pp. 258-270.

[28] B. M. Cerda and S. Yuan, "A Study of Anti-Phising Methodologies and Phishing Detection Algorithms," in *Proceedings of the International Conference on Security and Management (SAM)*, 2019: The Steering Committee of The World Congress in Computer Science, Computer …, pp. 79-83.

[29] G. Aaron, "The state of phishing," *Computer Fraud & Security,* vol. 2010, no. 6, pp. 5-8, 2010.

[30] D.-w. Park, "Analysis of Phising, Pharming and Smishing Spam Mail Trend and Techniques from Other Countries," *International Information Institute (Tokyo). Information,* vol. 19, no. 3, p. 895, 2016.

[31] P. Thaichon, "Consumer socialization process: The role of age in children's online shopping behavior," *Journal of Retailing and Consumer Services,* vol. 34, pp. 38-47, 2017.

[32] W. Shin and H. Kang, "Adolescents' privacy concerns and information disclosure online: The role of parents and the Internet," *Computers in Human Behavior,* vol. 54, pp. 114-123, 2016.

[33] J. W. Creswell and V. L. P. Clark, *Designing and conducting mixed methods research*. Sage publications, 2017.

[34] L. De Kimpe, M. Walrave, K. Ponnet, and J. van Ouytsel, "Internet safety," *The International Encyclopedia of Media Literacy,* pp. 1-11, 2019.

[35] Ł. Tomczyk and K. Kopecký, "Children and youth safety on the Internet: Experiences from Czech Republic and Poland," *Telematics and Informatics,* vol. 33, no. 3, pp. 822-833, 2016.

[36] S. Livingstone, L. Haddon, A. Görzig, and K. Ólafsson, "Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries," 2011.

[37] N. Lavesson, M. Boldt, P. Davidsson, and A. Jacobsson, "Learning to detect spyware using end user license agreements," *Knowledge and Information Systems,* vol. 26, no. 2, pp. 285-307, 2011.

[38] C. Putnam, "Teaching in a Digital Age: Internet Safety Education," 2019.

[39] A. Murillo, A. Kramm, S. Schnorf, and A. De Luca, "" If I press delete, it's gone"-User Understanding of Online Data Deletion and Expiration," in *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*, 2018, pp. 329-339.

ISSN: XXXX-XXXX IJXX