CYBER SECURITY AWARENESS AMONG SECONDARY SCHOOL STUDENTS IN MALAYSIA

ZAHIDAH ZULKIFLI [1]*, NURUL NUHA ABDUL MOLOK [1], NOOR HAYANI ABD RAHIM [1], SHUHAILI TALIB[1]

[1] Department of Information Systems, Kulliyyah of Information & Communication Technology, International Islamic University Malaysia, P.O. Box 10, 50450 Kuala Lumpur

[*]Corresponding author: zahidahz@iium.edu.my

(Received: 8th Sep 2020; Accepted: 26th Oct 2020; Published on-line: 30th Nov 2020)

ABSTRACT: It is people's choice to go online without worrying about their presence being at stake. However, there are too many unknown cyber risks and threats of attack in different forms lie ahead. These cause their presence along with personal data to be dangerously at risk. Moreover, the access to the cyber spaces is unlimited and unrestricted to all levels of ages. If this situation is ignored, it will create more unpredicted and new cyber-crimes as well as increase the existing ones. This paper explores the level of understanding of cyber security situational awareness among secondary school students, their teachers as well as their parents in Malaysia. Both physical and online survey methods were deployed to administer the data collection exercise. The target groups were divided into three categories: students (secondary students aged 13-16 years old), teachers and parents. A different questionnaire set was designed for each category. The survey topics/areas included Internet and digital citizenship knowledge. Respondents were selected from certain areas throughout the Klang Valley area in Malaysia. The results show most of the respondents are aware of the cyber threats and risks of being in cyber space, but very few of them take actions on security measures of being online. The findings and recommendations from this awareness study are fundamental to develop a model for secondary school students to understand the security risks and threats associated with the Internet throughout their years in school. Early exposure and awareness will help ensure healthy cyber habits among millennials and their environment in Malaysia.

KEY WORDS: *Cyber security, Cyber security awareness, Cyber security education*

1. INTRODUCTION

In Malaysia, it was reported that Malaysians are addicted to digital devices and the connected world due to time spent online. A survey by the Malaysian Communications and Multimedia Commission (MCMC) on Internet users in 2018 showed that Malaysians spent on average 6.6 hours online daily. Another study by MCMC in 2017 found that 89% of respondents were addicted to the Internet with 60% showing great levels of anxiety and a third suffering from major depression (Kamel, 2019). This is due to

dependency on information and communication technology (ICT) is increasing the number of Internet users from day to day, which also largely contributes to the changes in the cyber threat landscape in Malaysia (Zahri et al., 2017) including the teenagers.

Malaysian Education Blueprint Higher Education 2015-2025 (MEBHE) was proposed after being revised from the Malaysian Education Blueprint Higher Education 2013-2025 launched in 2013. One of the shifting pillars is leveraging ICT to scale up quality learning across Malaysia. Two of the proposed ways are by providing internet access and virtual learning environment for all 10,000 schools and maximizing the usage of ICT for distance and self-paced learning to expand access to high-quality teaching regardless of location or student skill level. It is important to have qualifications, and skills for Education 4.0 such as knowledge about ICT, technical know-how, ability to work with data, as well as social and personal skills (Muhamad Tahir, 2019). With these initiatives, evolution of new technologies in the cyber world begins. This contributes either directly or indirectly to the growing cyber threats in the country. As technology becomes up-to-date and advanced simultaneously, the trend of becoming more unique and complex is followed by cyber threats and cyber-crimes to the students.

Hosie (2017) reported the longer the time spent on social networks, the lonelier it is likely to be. People may think that social media allows people to be connected all the time, but it is making them feel lonelier (Hosie, 2017). This is because the longer someone spends on social media, the less time they have for real life social interactions. Also, this is a major reason for children becoming isolated from others when spending too much time online.

Other than that, spending too much time online can lead to children being bullied remotely or them bullying other children. The Star reported that three out of ten children in Malaysia are victims of online bullying or known as cyber bullying. Among the most common places for this kind of cyber-crime is social media, such as Facebook, Instagram and Twitter (Bernama, 2019). As this happened, the cyber bullying victims kept silent and did not report it to the authorized party. This is because they were not aware of the cyber bullying helpline services. Those who bullied other children enjoy their activities and are actively looking for other victims.

On the other side, it is very crucial to note that students reveal their own personal data when using the Internet without control or supervision. Therefore, children need to be taught how to be safe. They need to be taught on how to govern the Internet in a way that does not reveal too much personal information (Buttarelli, 2017). Thus, it is up to the adults around them, such as parents and teachers, either to give time limits or any other ways to control the Internet usage.

Hence, this paper aims to investigate the evidence related to the implementation of current cyber security knowledge in the context of secondary school students. The reason for targeting the secondary school population is due to the fact that this target group is growing and causing alarm to the society as a whole (Abdul Rahim et al., 2015). This study focuses on the importance of cybersecurity education as early as in secondary school and investigating the mobile application modules that will be implemented for future works.

This study employs the quantitative survey method. The survey contains close-end questions and thus this paper is using structured questionnaires. The advantages of this method are they are relatively quick and easy to administer.

In this paper, the results of this method are presented by indicating the behavior of respondents in line with the purposes of this paper. Next, this paper also reviews works done by other parties, such as individual researchers, research groups, agencies, organizations and so on. After that, this paper discusses key findings of the survey done based on the quantitative methods along with some suggestions or recommendations for future works. Finally, this paper concludes with some acknowledgement.

2. LITERATURE REVIEW

Children nowadays are more vulnerable to be exposed to harmful risks on revolution of technologies. As per mentioned above, due to the government's initiatives to scale up quality learning across Malaysia by utilizing ICT, the exposure to cyber risks become greater.

Zahri et al. (2017) found that secondary school students are the Internet's most frequent users at home. Their survey indicated that this group of students spend more than 10 hours per week on the Internet due to access to gadgets or specifically smartphones (Zahri et al., 2017). Therefore, there is a considerable need to educate them about programs on cyber security due to their existence in the cyber world.

VTT Technical Research Centre of Finland (2018) found that there is a lack of intangible resources in education including awareness programs on cyber security in schools (VTT Technical Research Centre of Finland, 2018). Therefore, it is suggested to create education to learn about privacy and security aspects at all levels.

Kats (2016) explained in her book that spending too much time online can lead to too little time developing real friendships. This may lead to a sense of isolation and loneliness for some students (Kats, 2016). Therefore, it is suggested to find a balance between spending some time socialising online and physically interacting with each other.

Mubarak (2015) mentioned in his paper that most of the contents found online are useful and beneficial to communities, but there are some which are not suitable for children and teenagers. To be specific, contents that are suitable only for adults can be easily accessed by children, aside from the misuse of cyber facilities such as social media, to harm the children (Mubarak, 2015). This causes a huge challenge to the normal development of children and teenagers.

DiGi CyberSAFE The National Survey Report (2015) reported that school children face multiple types of cyber risks when they are online. These include cyber bullying, inappropriate and harmful contents, chatting and sharing details with strangers and many more (DiGi CyberSAFE The National Survey Report, 2015). This indicates the need to keep themselves safe and responsible on the Internet.

Issa and Jali (2014) found in their research that secondary school students show a little bit of awareness in cyber security, but still lack accurate practicing information. The level of security awareness among Libyan secondary school students in Malaysia consists of social networks, passwords, and cyber bullying (Issa & Jali, 2014).

Therefore, it is recommended to conduct a full study on the level of awareness for secondary school students, as well as security training programs which are crucial to avoid security risks.

Yilmaz et al. (2017) studied internet security and computer usage awareness profiles of secondary school students in Bartin, Turkey. They found that many of the students have insufficient information security and computer usage awareness. They concluded that the students could be at risk of online threats. Their feedback was for the parents, schools and policy makers to increase awareness of information security and computer usage among the students (Yilmaz et al., 2017). Because the parents, schools and policy makers are too busy, children are left with their own activities. In this time where everything is digitized, the parents, schools and policy makers think that children can survive, so children spend plenty of time with the technologies and develop unwanted behaviours or habits.

Peker, Ray, and da Silva (2018) studied to understand the current level of security awareness among college and high school students. At the end of this study, Peker, Ray, and da Silva (2018) were expected to develop a module that would help raise awareness among college and high school students. Shockingly, the results of this study found careless cyber habits among common Internet or technology users (Peker et al., 2018). This shows that students lack awareness despite being a part of cyberspace.

In New Zealand, Tirumala, Sarrafzadeh and Pang (2016) conducted a survey on internet usage and cybersecurity awareness among students aged between 8 - 21 years old. The results showed that most of the secondary school students are using the Internet for entertainment purposes. In terms of access, this group of students are relatively high in providing access rights to various applications including details on contacts and privacy information (Tirumala et al., 2016). This study showed the importance of security awareness not only to secondary school students but also to primary school students and adults as well.

Tosun et al. (2020) had organized a workshop in Istanbul to discuss cyber security and proper use of social media. The workshop discussed current problems of cyber security and proper use of social media in Istanbul, SWOT analysis to solve these problems and suggested some solutions. SWOT analysis is a management method used commonly to determine and analyse resources of an organization and surrounding elements in four dimensions such as Strengths, Weaknesses, Opportunities and Threats (Tosun et al., 2020). However, the paper of the workshop indicated the lack of students' perceptions on cyber security and highlighted how to raise awareness in cyber security using social media. Therefore, it is essential to point out these matters.

From parental perspectives, Ahmad@Ahmad Arifin et al. (2019) conducted a survey on parental knowledge and readiness as to whether they are aware of the risks of the Internet to their children. The level of parental awareness can be correlated with cyber safety at home. It is important to identify awareness as one of the early cyber threat preventions (Ahmad@Ahmad Arifin et al., 2019). Lower cyber security parental awareness level can lead to lower cyber security children awareness level. This directly relates to lower cyber security awareness level among school students, which are coming from home. However, Ahmad@Ahmad Arifin et al. (2019) found that cyber

security awareness among parents are at medium level. This has impact on their children which are also school students. Therefore, it is important to increase parental awareness which hugely influences the children.

In South Africa, even at university level, a study found that there is a lack of cyber security awareness among students. It was suggested that academic institutions can contribute to the awareness of students by providing information through social media platforms and online communication mediums on a regular basis (Potgieter, 2019). However, these initiatives could be a distraction to students as the access to the Internet is unlimited and unrestricted. The students may be surfing other things while using the Internet. Therefore, the objective of sending and receiving cyber security awareness through social media platforms and online communication mediums are not suitable. It suggested traditional ways of communication mediums and platforms to spread cyber security awareness effectively.

Practically in South Africa, Bhatnagar and Pry (2020) developed cyber security social media, risk awareness and countermeasure maturity model (SMRA-CMM) to understand students' perceptions of personal social media risks and their knowledge of the use of privacy and security settings in social media applications. From the survey, it was indicated that students are aware of the risk of using social media and do value the need for training on cyber security and privacy in the use of social media. Therefore, Bhatnagar and Pry (2020) formulated a model based on the survey. However, the model did not include the importance of reading and understanding the privacy policies of students' perceptions on cyber security.

Zakaria et al. (2019) had developed an Online Project-based module (m-PAT) to cultivate positive values among students. The data were collected through questionnaire, students' reflection, students' online learning activity and discussion, interviews with the students, as well as teacher's checklist after each participant generated a physic-learning blog by using the m-PAT as a platform. The results showed that m-PAT has important implications for contributing to a new approach in learning which integrates the use of information technology and communication via project-based online learning as well as making it possible for the cultivation of students' positive values especially in relation to the use of the Internet (Zakaria et al., 2019). However, Zakaria et al. (2019) did not mention what area to focus on in developing interactive learning modules to achieve more accurate results.

In the United States of America, Smith and Ali (2019) presented a technique that they developed for raising cyber security awareness in school students, college students and others. The technique is a one-hour lecture with a hands-on activity to engage the participants. It was promoted as a session in game programming. The real intent of cyber security awareness was kept hidden and was not exposed until near the end of the lecture. By doing so, attendees would directly feel the impact of cyber security threats (Smith & Ali, 2019). Smith and Ali (2019) used indirect approach in promoting and instilling the awareness of cyber security as well as guiding the students in practice. This method may be effective but still need a huge amount of effort and consistency to implement it.

However, in the case of Malaysia, prior to developing a mobile application module for secondary schools, it is necessary to identify the current level of cyber security

awareness among school children. Therefore, it is important to conduct a study to provide guidelines for developing a comprehensive cyber security mobile application module for secondary school students.

3. METHODOLOGY

3.1 Research Objectives

The objective of this study is to answer the following scope:

1. Cyber security awareness among secondary school students, their career plan, current career planning modules and their expectations to achieve their career journey.
2. Cyber security awareness among teachers, their student's career plan, current career planning modules for the student and their expectations to achieve the student's career journey.
3. Cyber security awareness among parents, their children's career plan, current career planning modules for the children and their expectations to achieve the children's career journey.

3.2 Research Questions

The study questions are divided into three different parts for each category of respondents. The first part is demographic questions for classification purposes and two questions on general cyber security awareness. All categories have almost the same set of questions. The second part is in-depth questions on cyber security awareness for each category. All categories have different sets of questions. For the student category, the questions are to learn about students' preferences on receiving cyber security awareness education. In this section, students were asked about any experiences, if any, of doing wrong things online. This is to identify the cyber-crimes experienced by the students. For the teacher category, the questions are to learn about teachers' preferences on receiving cyber security awareness education. In this section, teachers were asked about any experiences, if any, of doing wrong things online. This is to identify the cyber-crimes experienced by the teachers in relation to performing their tasks. For the parent category, the questions are to learn about the parents' concerns on cyber-crimes. In this section, parents were asked about any concerns or experiences, if any, in relation to their children being online without being monitored. This is to identify the most worrying things that concern the parents.

3.4 Research Method

This study was carried out in three main phases. Phase 1 assessed the preliminary investigation. This is to study the current level of awareness on cyber security among secondary school students, teachers, and parents. This phase identified categories of respondents and developed a set of questionnaires for each category. The questionnaires were structured for each category of respondents. The design of the survey was based on the need to identify cyber security awareness levels among secondary school students, teachers and parents. Motivating this study was to use the

outcomes as input to the development of cyber security mobile application education modules that would be carried out at the next few phases of this research.

Phase 2 distributed and spread the questionnaires for data collection of the study. As for the data collection, this study exercised a quantitative approach by methods of paper-based survey and online questionnaire. All questionnaires were structured based on the category of respondents. There were three categories of respondents involved in this study: students (secondary students aged 13-16 years old), teachers and parents. Upon receiving the research approval, the authors obtained a list of secondary schools as target respondents. The schools' administration was contacted and asked for permission to come to their schools to administer the paper-based survey. The survey was administered during the school time. The paper-based survey and online survey methods were employed since they would provide greater access to students and a larger sample size. The authors visited selected classes and provided each student with a copy of the survey paper script. Students completed the survey in-class or self-reported the survey. A total of 98 secondary school students completed the survey. After that, the authors approached the teachers to do the survey. Teachers completed the survey outside the class or self-reported the survey or used the online questionnaire method. A total of 10 teachers completed the survey. Parents completed the survey fully using the online questionnaire method. A total of 4 parents completed the survey.

Next, Phase 3 involved data analysis, key findings and discussion, recommendations, and a conclusion. Data collected from surveys conducted was analysed to produce the results and findings. All responses were entered into an Excel spreadsheet for analysis. Surveys were numbered and closed-ended questions were coded. For the open-ended questions, that required a text response, a consolidation process was used to synthesize the many responses into similar categories. The process began with the authors reviewing all of the responses provided within a specific question. From the responses, common themes emerged, and these became the designated "categories" for classification purposes. Each response was re-read, and a decision was made as to which category the response belonged to. This allowed for the consolidation of the responses into categories for analysis purposes. From there, recommendations would be suggested to the modules for mobile application. Therefore, the contents of mobile application modules for future works could be concluded.

4. KEY FINDINGS AND DISCUSSION

4.1 Internet Usage

Category 1 – Secondary School Students

This target group of students (aged 13-16 years old) are secondary school students. More than half of this group of respondents are 16 years old. Around half of them had been using the Internet for 5-10 years, while nearly one-quarter of the students had been using the Internet for more than 10 years with another more than one-quarter had been using the Internet less than 5 years. Almost all students agreed that identity card (IC) number is personal data, but only 35% agreed that birthday, which is a very important component to generate the IC number, is personal data, name aside, only 36% agreed as personal data. On the other hand, although about one-third of the students confidently aware that somebody is watching their online activity with around

half of the students not very sure of it, about three-quarter of the respondents of this category are aware that somebody can steal their data. From this finding, it is proven that students may be aware of personal data but less exposure to the impact of online activities.

Category 2 – Teachers

This target group of teachers (aged 25-44 years old) are university graduates. 80% of them had been using the Internet for more than 10 years. All teachers agreed that that IC number is personal data, but only 60% of them said name and address, which are a part of the IC, are both personal data. Worse, only 40% of the teachers agreed that birthdays are personal data. On the other hand, although all teachers agreed that they are aware that somebody can steal their data, only 70% confidently aware that somebody is watching their online activity, while 20% are still in doubt. From this part only, there is cyber security awareness among the teachers, but lack of practice. Therefore, it is recommended for the teachers to practice a more secured way of cyber-lifestyle as a role model for students at the school.

Category 3 – Parents

This target group of parents (aged 35-44 years old) are employed for wages. All of them had been using the Internet for more than 10 years. All parents agreed that IC number and address are personal data, but 75% of them said name and birthday, which are a part of the IC, are both personal data. On the other hand, although all teachers agreed that they are aware that somebody can steal their data, only 75% confidently aware that somebody is watching their online activity, while 25% still in doubt. From this part only, there is cyber security awareness among the parents, but lack of practice. Therefore, it is recommended for the parents to practice a more secured way of cyber-lifestyle as a role model for students at home.

According to the questions from this part, the results show most of the respondents are aware of what can be classified as personal data or information. Although most of the respondents are aware that other people can access their data or watch them online, the respondents are still taking it easy on these matters. From these questions alone, it is shown that secondary school students are impacted by their environment, such as parents and teachers. Therefore, it is recommended that future works include finding out how the respondents keep their online activities in control without being affected by cyber-crimes. Last not least, the answers to the questionnaires in future works should be fundamental to develop cyber security awareness among secondary school students to reduce risks and threats when they are doing online activities.

4.2 Cyber Security Awareness

Category 1 – Secondary School Students

Most of the students prefer working in groups and doing practical activities as the teaching method in cyber security awareness. This is because two-third of the students had received cyber security education, and they may have something to share to others or practice through these teaching methods. Majority of the students are interested to learn about cyber security awareness at school with 86% agreeing. This is followed by

their opinion that online safety should be formalized within the education system with 85% agreeing. However, when it comes to responsibilities, 55% of the students felt that there should be a clear regulation endorsed by the government, while the other 33% felt that it is the parents' responsibilities for cyber safety. The top four experiences by this group of respondents are becoming a victim of online grooming, getting bullied online by other children, seeing sexually/violently explicit images on the internet and revealing personal or private information when using the internet. Therefore, the education that should be given to school children are initiatives aimed at preventing exposure to pornography, gaming and other addictive behaviours, initiatives promoting awareness through guidance on healthy limits of screen time excessive internet use, campaigns promoting cyber safety explaining the use of filters and parental controls and any other education suitable solutions. This group of respondents also feel that education would be the best option to promote their safety online, with a little bit of regulation. There are many suggestions on protecting themselves online. Among the suggestions are do not disclose personal information, do not be fooled by online scams, ending the call if they feel suspicious and privatised social media. Some suggest ensuring that the people we communicate online are not hackers or scammers and to be careful. Some even suggest not having any social media account and not making online transactions, such as purchases.

Category 2 – Teachers

All teachers agreed that online safety should be formalized within the education system. When it comes to responsibilities, 50% felt that there should be a clear regulation endorsed by the government, only 20% thought that it should be a mutual responsibility between all parties. However, none of the teachers thought that schools should be responsible for cyber safety. The top three that most concerns teachers when students go online are students are spending too much time online, students could be bullied online by other children and students are seeing sexually/violently explicit images on the internet. Therefore, the teachers felt that campaigns promoting cyber safety explaining the use of filters and parental controls is the best solution with 90% votes. However, there are challenges that cyber-bullying represents for teachers as opposed to traditional bullying, such as types of aggression that are not carried out face-to-face and the harm a single incident can cause to the victim even without repetition over time. Based on the survey, the best option to promote student's safety online is through education. Therefore, it is encouraged that teachers monitor their student's online activity in the way of religious teaching by explaining the danger of surfing the Internet to do bad things. Another way of monitoring can be the use of screen mirroring as per parental control. By using this method, the teachers know the log activities of devices used at school. From Islamic perspective, we must advise and remind each other to do good things. Quran and Hadith used the term evil to refer to wrong belief or practice. Quran (31:17) asks us to join people all that is good and forbid them from all that is evil (The Quran, 31:17).

Category 3 – Parents

All parents agreed online safety should be formalized within the education system. When it comes to responsibilities, 50% felt that it is parents' responsibility for cyber safety. The top two that most concerns parents when their children go online are that

their children might become isolated from others when spending too much time online and seeing sexually/violently explicit images on the internet. Therefore, the parents felt that keeping up with evolving technologies and talking to their teen children about what they do online are the current challenges parents faced today with regards to protecting their children. Therefore, the most preferred education that should be given to parents is campaigns promoting cyber safety explaining the use of filters and parental controls. Based on the survey, the most unique challenges that cyber-bullying represents to parents as opposed to traditional bullying are vast numbers of bystanders, which very often do not even know the victim and victims feel imprisoned in their own homes and more secretive and unseen – anonymous. Parents felt that the best option to promote their child's safety online is through education. Therefore, it is encouraged that parents monitor their children's online activity by regularly checking their phones, scheduling their children's online activities, and proactively participating in and monitoring their activities.

Generally, the survey shows that it is the government's responsibility to ensure safety in the cyber world. The government should provide clear rules and regulations as well as guidelines and procedures. Aside from that, the implementation and enforcement are essential to safeguard people from doing illegal things. Parents also play important roles in the students' lives. They are responsible for educating their children at early ages. Matondang and Siddik (2017) explained a verse from Quran (66:6) that parents are obliged to teach the children to do good and keep away the bad by getting them in the truth or kindness and setting an example (Matondang & Sidik, 2017). Insignificantly, a few respondents felt that it is the students themselves who need to be responsible for cyber safety. This is because anything can happen if the students explore the Internet unethically. Therefore, this indicates that the influences surrounding the students are important. Essentially, education should be a top priority for future work while enforcing laws and regulations as well as teachers and parents become good role models.

4.3 Cyber Security as A Career

Category 1 – Secondary School Students

Most of the students viewed that they may have an interest in cyber security as a career. This is because 64% of the students have taken courses related to computers and technology although they do not have any friends or family members or relatives who work in the cyber security field. Among career exploration activities they have participated in are hearing guest speakers about careers at school, looking at websites, videos or books about careers, clubs or activities related to career interests, and doing classroom project(s) related to career interests. According to the students, among the most helpful things that school or program does to help them learn about careers are the school should establish a career club, have a career campaign, appoint a peer mentoring, promote work to get others' opinions, create a lesson program that has games so students would enjoy and indirectly developing interests in the cyber security field, organise activities related to careers, organise security awareness programs, organise career day, invite experts to give talks to motivate the students, and give exposure on career availability by showing the benefits or advantages of a career. In

fact, the students think the school or program should do more to help them learn about careers. They should do job matching, personality tests, help to know more about a career that interests the students, get a good speaker or public figure on social media and introduce applications or online websites, so the students can familiarize with the environment and information. As far as the students' knowledge, cyber security career options are only limited to IT-based opportunities, like website creator, security system creator, application creator, internet security, programmer, cyber security expert, computer science background, system analyst, Google security and ethical hacker. If non-IT sector, the options are to go into banking sector, consultant, editor, police, psychologist and accountant. Therefore, it is essential to have early exposure to the students on career options available that are suitable according to the background of the students as well as their preferences.

Category 2 – Teachers

Most of the teachers viewed that students have an interest in cyber security as a career. This is because 60% of teachers do not have experience teaching courses related to computers and technology but have friends or family members or relatives who work in the cyber security field. The most popular career exploration activities their school has done so far are school-break program(s) related to career interests, clubs or activities related to career interests, career days or career fairs and having guest speakers about careers at school. Based on the teachers' opinions, there are many ways the school can help students to learn about careers. These include having a close collaboration with a university that has a cyber-security field, YouTuber education, visiting colleges and universities to create interest in study fields, school can share information about the career, invite speakers to give talk about careers, career courses, expose early education on career and the school can organise career-related programs. All these can give impact to the school for being active in engaging with universities as well as the teachers and students can broaden their knowledge on career options. According to the survey, there are many methods the school should use to help teachers assist their student's college and career planning. After-school programs, career week or career day, courses or training for the teachers on career and motivation talk from the teachers on careers can be organised by the school. There are many career options in the cyber security field, such as forensic cyber, IT security analyst and ethical hacker. In fact, there are various options available for students. Therefore, exposure on cyber security careers are not in technology but from education as well.

Category 3 – Parents

Most of the parents viewed that their children may have an interest in cyber security as a career. This is because 50% of children never take any courses related to computers and technology. This may be impacted by friends or family members or relatives who work in the cyber security field. The most popular career exploration activities their children have done so far is career interest checklists/assessments. Based on the parents' opinion, there are many ways the school can help students to learn about careers. Courses, career day and career talks by people whom children looked up to are the most helpful things that the school or program does to help children learn about careers. Courses including cyber security in school counselling programs are among the ways, schools could do to help children learn about careers. Courses,

and collaboration and active involvement in PIBG are among the school programs to help parents assist their children's college and career planning. There are many career options in the cyber security field, such as cyber security specialist. In fact, there are various options available for children but less exposure to them.

Overall, there are future careers in the cyber security field. All categories of the respondents seem interested in careers towards cyber security. However, the knowledge on options in the professions itself is very limited. From the findings above, it can be seen that the students have interests in cyber security with support from teachers and parents. However, because the students are not being exposed to that direction, they are not aware of the occupations available in the cyber security field.

5. RESEARCH LIMITATION

The data, as collected by the survey, are considered limited as they only apply to respondents in the Klang Valley area only. This study provided information about some secondary school students, teachers and parents, and not all of them. Such respondents should be included in future studies to create a more comprehensive scope towards developing a module for mobile application on cyber security awareness and education in Malaysia. Other than that, a part of this survey was conducted through paper-based method. Most of the paper-based questionnaires are incomplete. There are many unanswered questions. Such a method should be the most effective method because the data are collected directly from respondents. Therefore, for future work, we need to ensure that the data collected are as complete as possible with a minimum level of unanswered questions.

6. CONCLUSION

Based on the findings, there is clear evidence that Malaysians are well-exposed to Internet use from a very young age as a teenager. However, online activities need to be monitored more frequently and closely, and the existence of cyber threats were also reported in the data gathered. Children are also expected to be well-informed of current cyber world issues and must learn to develop an instinct to stay safe online. The data gathered in this study will be useful for developing mobile application modules for secondary school students in Malaysia. The data can also serve as a useful guideline for parents and teachers. The findings of this study offered some valuable understanding and provided more data to the existing level of knowledge on cyber security among teenagers in Malaysia. It is hoped this study will create public interest to initiate new research on cyber security as well as develop other relevant programmes to enhance the security of future generations.

ACKNOWLEDGEMENT

This research was funded by IIUM Flagship Research Initiative Grant Scheme (IRF). Code Grant: IRF19-033-0033 entitled “The Development of Cyber Security Awareness Model Using CTC – Chaos Theory of Careers for Secondary Schools.”, International Islamic University Malaysia.

REFERENCES

KAMEL, H. (2019). Malaysians are addicted to the Internet. The Malaysian Reserve. Retrieved from https://themalaysianreserve.com/2019/09/26/malaysians-are-addicted-to-internet/

ZAHRI, Y., R. SUSANTY, A., & MUSTAFFA, A. (2017). Cyber Security Situational Awareness among Students: A Case Study in Malaysia. World Academy of Science, Engineering and Technology International Journal of Educational and Pedagogical Sciences, 11(7): 1654-1660. doi: 10.5281/zenodo.1131053

MUHAMAD TAHIR, R. (2019). Industrial Revolution 4.0: Implication of Future Works and TVET & Education. Presentation, Malaysia

HOSIE, R. (2017). People Who Use Social Media a Lot Are Isolated, Study Says. Independent. Retrieved from https://www.independent.co.uk/life-style/social-media-high-usage-more-isolated-lonely-people-study-university-pittsburgh-a7614226.html

BERNAMA. (2019). Three in 10 are bullied online. The Star. Retrieved from https://www.thestar.com.my/news/nation/2019/09/06/three-in-10-bullied-online

BUTTARELLI, G. (2017). Teenagers on Privacy. [Blog] European Data Protection Supervisor. Available at: https://edps.europa.eu/press-publications/press-news/blog/teenagers-privacy_en [Accessed 20 Feb. 2020].

ABDUL RAHIM, A., TENGKU ZAINUDIN, T. & RAJAMANICKAM, R. (2015). The Involvement of School Students in Criminal Activities and Its Position in the Malaysian Law. Mediterranean Journal of Social Sciences.

VTT TECHNICAL RESEARCH CENTRE OF FINLAND. (2018). ASEAN Cybersecurity Innovation Ecosystem: A Co-creation approach (pp. 32-42). Retrieved from https://project-yaksha.eu/wp-content/uploads/2019/05/D1.2_ASEAN-Cybersecurity-Ecosystem-a-co-creation-approach_vf.pdf

KATS, Y. (2016). Supporting the Education of Children with Autism Spectrum Disorders (pp. 37-40). USA.

MUBARAK, A. R., (2015). Child Safety Issues in Cyberspace: A Critical Theory of Trends and Challenges in the ASEAN Region, International Journal of Computer Applications 129(1): 48-55

DiGi CyberSAFE The National Survey Report 2015. (2015). Growing Digital Resilience among Malaysian Schoolchildren on Staying Safe Online. Digi Telecommunications. Retrieved from https://digi.cybersafe.my/files/article/CyberSAFE_Survey_Report_2015_en.pdf

ISSA, S., & JALI, Z. (2014). A Second Look at the Information Security Awareness among Secondary School Students. In The International Conference on Information Security and Cyber Forensics 2014. Kuala Terengganu.

YILMAZ, R., KARAOĞLAN YILMAZ, F., ÖZTÜRK, H., & KARADEMIR, T. (2017). Examining Secondary School Students' Safe Computer and Internet Usage Awareness: An Example from Bartın Province. Pegem Eğitim Ve Öğretim Dergisi, 7(1): 83-114. doi: 10.14527/pegegog.2017.004

PEKER, Y., RAY, L., & DA SILVA, S. (2018). Online Cybersecurity Awareness Modules for College and High School Students. 2018 National Cyber Summit (NCS). doi: 10.1109/ncs.2018.00009.

TIRUMALA, S., SARRAFZADEH, A. & PANG, P. (2016). A Survey on Internet Usage and Cybersecurity Awareness in Students. 2016 14th Annual Conference on Privacy, Security and Trust (PST).

TOSUN, N., ALTINÖZ, M., ÇAY, E., ÇINKILIÇ, T., GÜLSEÇEN, S., & YILDIRIM, T. (2020). A SWOT Analysis to Raise Awareness About Cyber Security and Proper Use of Social Media: Istanbul Sample. International Journal of Curriculum and Instruction, 12(Special Issue), 271-294.

AHMAD@AHMAD ARIFIN, N., MOKHTAR, U., HOOD, Z., TIUN, S., & JAMBARI, D. (2019). Parental Awareness on Cyber Threats Using Social Media. Jurnal Komunikasi: Malaysian Journal of Communication, 35(2), 485-498. doi: 10.17576/jkmjc-2019-3502-29

POTGIETER, P. (2019). The Awareness Behaviour of Students on Cyber Security Awareness by Using Social Media Platforms: A Case Study at Central University of Technology. In 4th International Conference on the Internet, Cyber Security and Information Systems 2019 (pp. 272–280). Johannesburg, South Africa: Kalpa Publications in Computing

BHATNAGAR, N., & PRY, M. (2020). Student Attitudes, Awareness, And Perceptions of Personal Privacy and Cybersecurity in The Use of Social Media: An Initial Study. Information Systems Education Journal (ISEDJ), 18(1), 48-58

ZAKARIA, A., MOHD. SALLEH, A., ISMAIL, M., & GHAVIFEKR, S. (2019). Cultivating Positive Values via Online Project-Based Module (m-PAT). Social And Management Research Journal, 16(1), 1. doi: 10.24191/smrj.v16i1.6077

SMITH, D. & ALI, A. (2019). You've Been Hacked: A Technique for Raising Cyber Security Awareness. Issues in Information Systems, [online] 20(1), pp.186-194. Available at: https://iacis.org/iis/2019/1_iis_2019_186-194.pdf [Accessed 21 Feb. 2020].

THE QUR'AN 31:17 (Translated by Shaykh Muhammad Ibn Ibraaheem Al-Tuwayjri)

MATONDANG, A., & SIDDIK, D. (2017). Family Education in The Quran. IOSR Journal of Humanities and Social Science, 22(06): 07-16. doi: 10.9790/0837-2206010716