Cyber Security Situational Awareness among Students: A Case Study in Malaysia

Yunos Zahri, Ab Hamid R. Susanty, Ahmad Mustaffa

***Abstract*—**This paper explores the need for a national baseline study on understanding the level of cyber security situational awareness among primary and secondary school students in Malaysia. The online survey method was deployed to administer the data collection exercise. The target groups were divided into three categories: Group 1 (primary school aged 7-9 years old), Group 2 (primary school aged 10-12 years old), and Group 3 (secondary school aged 13-17 years old). A different questionnaire set was designed for each group. The survey topics/areas included Internet and digital citizenship knowledge. Respondents were randomly selected from rural and urban areas throughout all 14 states in Malaysia. A total of 9,158 respondents participated in the survey, with most states meeting the minimum sample size requirement to represent the country's demographics. The findings and recommendations from this baseline study are fundamental to develop teaching modules required for children to understand the security risks and threats associated with the Internet throughout their years in school. Early exposure and education will help ensure healthy cyber habits among millennials in Malaysia.

***Keywords*—**Cyber security awareness, cyber security education, cyber security, students.

I. Introduction

CRIMINALS use cyber space to gain access to personal information, steal businesses' intellectual property and obtain knowledge of sensitive information for financial or political gains or other malicious purposes. In fact, the threat of cybercrime is increasing exponentially. According to statistics from the Royal Malaysian Police, cybercrime has surpassed drug trafficking as the most lucrative crime, with 70% of commercial crime cases now being categorised as cybercrime [1].

Dependency on 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. This is due to the government's initiatives to boost industry by means of expanding Internet penetration throughout the country. New technologies, such as cloud services, 3D printing, Big Data, Internet of Things (IoT) and mobile computing are also evolving and emerging every day. These either directly or indirectly contribute to the growing cyber threats in the country. As technology becomes increasingly sophisticated and advanced, cyber threats follow the trend of becoming more unique and complex.

II. Literature Review

At present, children are progressively more exposed to the harmful risks of the technological revolution in mobile phone and Internet technologies [2]. It has been reported that a rise in the number of children as Internet users has led to their vulnerability of becoming prey to Internet predators' criminal behaviours [3]. Several recent studies also report on matters regarding Malaysians' cyber security awareness, specifically the use of social networking sites [4], digital divide among different ethnic groups [5], digital resilience of staying safe online [6] and cyberbullying among young adults [7]. However, there has been a recent growth in the number of reports and studies concerning cyber security issues among the younger generations in Malaysia [6], [8], [9]. Cyber threats to children and youngsters are becoming more alarming. Among the most prevalent risks concerning children worldwide include easy access to illegal sites, sites with violence and sexual content, communication with unreliable people, child abuse and overdependence on games [10]. Therefore, in view of the escalating cyber-related threats concerning children in the ASEAN region [2] as well as the rise in Malaysian cyber citizens falling victim to various cybercrimes, CyberSecurity Malaysia, an agency under the Ministry of Science, Technology and Innovation has decided to develop awareness modules for school students at both the primary and secondary levels. The learning modules are aimed at exposing these target groups to the necessity for safe conduct while using the Internet. In other parts of the world, countries like Singapore, Australia and Oman have already initiated cyber security awareness modules within their school curriculums. As for Singapore, the country's Ministry of Education adopted the Cyber Wellness framework as part of the primary and secondary school curriculum [11]. In Australia, the National Safe Schools Framework provides Australian schools with a vision and a set of guiding principles to assist school communities with developing positive and practical student safety and wellbeing policies [12]. Oman, on the other hand, with the Oman Computer Emergency Readiness Team (OCERT) is working closely with the Ministry of Education to introduce an Information Security Curriculum in schools. In addition, OCERT is an advisory member of the Ministry of Manpower IT Committee, reviewing IT and Security curriculums for the higher technical colleges [13]. However, in the case of Malaysia, prior to developing a sound module for schools, it is necessary to identify the current level of cyber security situational awareness among school children. Therefore, it is imperative to conduct a study to provide

Y. Zahri, Ab Hamid R. Susanty, and A. Mustaffa are with the CyberSecurity Malaysia, Seri Kembangan, 43300 Malaysia (e-mail: zahri@ cybersecurity.my, ramona@ cybersecurity.my, mustaffa@ cybersecurity.my).

guidelines for developing comprehensive cyber security modules for school students.

III. Method

A. Overall Approach

The current study was executed in three main stages, as depicted in Fig. 1. Stage 1 regards project initialization, sessions with stakeholders, questionnaire development, sampling size and distribution, a pilot study and survey roll-out. Stage 2 involves data collection exercise and Stage 3 involves data analysis, results and findings, recommendations and a conclusion. The entire process took six months to complete.

B. Questionnaire Development

In the initialisation stage of the questionnaire design process, the survey objectives were clearly defined. This is crucial for identifying the data required from the target population. The question types and response options were then selected and individual questions were drafted for each target group.

In finalising the questionnaires, each question was evaluated for clarity, relevance and adequacy, and response options were provided. The overall process of questionnaire development is shown in Fig. 2.

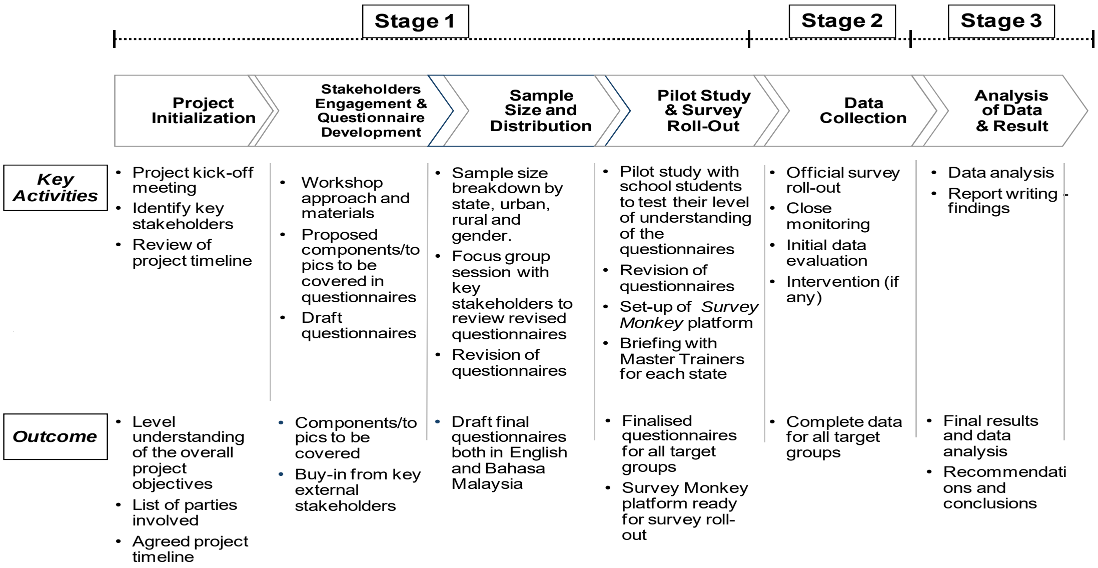

Stage 1
Stage 2
Stage 3
Project Initialization
Stakeholders Engagement & Questionnaire Development
Sample Size and Distribution
Pilot Study & Survey Roll-Out
Data Collection
Analysis of Data & Result
Key Activities
Project kick-off meeting
Identify key stakeholders
Review of project timeline
Workshop approach and materials
Proposed components/topics to be covered in questionnaires
Draft questionnaires
Sample size breakdown by state, urban, rural and gender.
Focus group session with key stakeholders to review revised questionnaires
Revision of questionnaires
Pilot study with school students to test their level of understanding of the questionnaires
Revision of questionnaires
Set-up of Survey Monkey platform
Briefing with Master Trainers for each state
Official survey roll-out
Close monitoring
Initial data evaluation
Intervention (if any)
Data analysis
Report writing - findings
Outcome
Level understanding of the overall project objectives
List of parties involved
Agreed project timeline
Components/topics to be covered
Buy-in from key external stakeholders
Draft final questionnaires both in English and Bahasa Malaysia
Finalised questionnaires for all target groups
Survey Monkey platform ready for survey roll-out
Complete data for all target groups
Final results and data analysis
Recommendations and conclusions

Fig. 1 Overall Study Approach

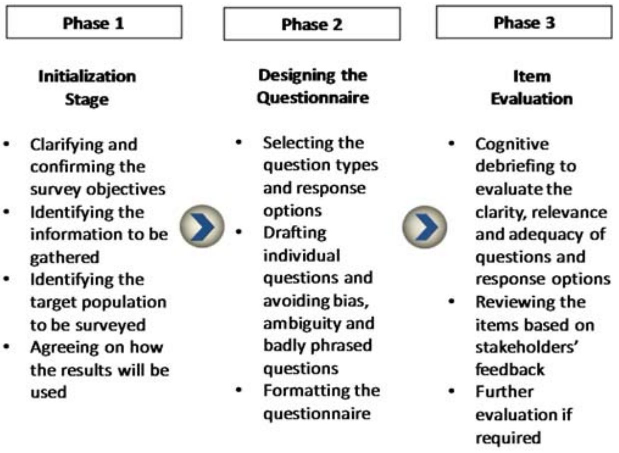

Phase 1
Phase 2
Phase 3
Initialization Stage
Clarifying and confirming the survey objectives
Identifying the information to be gathered
Identifying the target population to be surveyed
Agreeing on how the results will be used
Designing the Questionnaire
Selecting the question types and response options
Drafting individual questions and avoiding bias, ambiguity and badly phrased questions
Formatting the questionnaire
Item Evaluation
Cognitive debriefing to evaluate the clarity, relevance and adequacy of questions and response options
Reviewing the items based on stakeholders' feedback
Further evaluation if required

Fig. 2 Questionnaire Design Process

The questionnaire component mapping for this study is given in Table I. It is based on the constructs that were shortlisted during focus group discussions with the identified stakeholders as well as previous literature on cyber security.

TABLE I
Questionnaire Component Mapping

No	Component	Area of Inquiry
1	Demographics	Gender, Age
2	Internet Usage	Usage time, Ways of access, Activities online
3	Social Media Usage	Social media accounts, Activities on social media, Social media safety
4	Parental Control	Password sharing, Parental supervision
5	General Internet Safety	Usage of passwords, Browsing safety, Dealing with cyber threats
6	Digital Citizenship (Perception)	Cyber bullying, Online gaming, Posting content, Interaction with others (Covers: Digital Communication, Digital Etiquette, Digital Law, Digital Security)

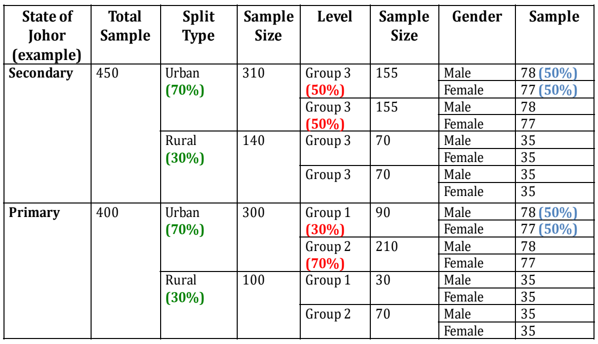
C. Target Respondents, Sampling and Distribution

The target respondents identified for this study were school students. The groups were divided into three categories: Group 1 (primary school aged 7-9 years old), Group 2 (primary school aged10-12 years old), and Group 3 (secondary school aged 13-17 years old).

A minimum of 5,000 student respondents were required for this exercise to be statistically representative of the country's population. However, in previously conducted DiGi-

CyberSAFE [6] national surveys among schools, the data rejection rate was as high as 30%. Taking this into account, the school student sample size required for this study was set to a minimum of 6,500 respondents.

As for sampling distribution, the number of samples in each target group must be representative of the total population of primary and secondary school students in Malaysia. The sampling distribution is presented in Fig. 3. The sampling distribution shows a 70:30 split between urban and rural schools; an equal split (50:50) between male and female students; a 30:70 split between the lower and upper primary levels; and a 50:50 split between lower and upper secondary levels.



State of Johor (example)	Total Sample	Split Type	Sample Size	Level	Sample Size	Gender	Sample
Secondary	450	Urban (70%)	310	Group 3 (50%)	155	Male	78 (50%)
						Female	77 (50%)
				Group 3 (50%)	155	Male	78
						Female	77
		Rural (30%)	140	Group 3	70	Male	35
						Female	35
				Group 3	70	Male	35
						Female	35
Primary	400	Urban (70%)	300	Group 1 (30%)	90	Male	78 (50%)
						Female	77 (50%)
				Group 2 (70%)	210	Male	78
						Female	77
		Rural (30%)	100	Group 1	30	Male	35
						Female	35
				Group 2	70	Male	35
						Female	35

Fig. 3 Sampling distribution for primary and secondary schools

D.Fieldwork

Prior to the fieldwork, a pilot study was conducted to assess the level of respondents' understanding of the questions, to validate the overall questionnaire flow and to identify any potential technical issues pertaining to the Survey Monkey platform. Participants were from the three target groups of school students mentioned. A total of 30 students participated in the pilot study, of which 10 answered each respective set of questions representing each target group.

Following the pilot study, a workshop was held with a team of Master Trainers from the Educational Technology Division, Ministry of Education. This group served as liaison officers between CyberSecurity Malaysia and the selected schools. During the workshop, each questionnaire set was presented to all Master Trainers in order to gather feedback on the ease of answering the survey questions. All feedback was taken into account for the final modifications of every questionnaire set.

Once all questionnaires were ready, each set was uploaded to the Survey Monkey platform under a different URL address. In order to assist the Master Trainers and school teachers with guiding the students to participate in the survey, a glossary and guide sheets were prepared for the students. These were intended to help provide guidelines and clarifications on the questionnaires as well as to address possible technical issues encountered by the respondents. The survey was officially initiated on 27 June 2016 and lasted for one month.

IV. Key Findings

A. Internet Usage

Group 1 - Primary School Level 1

This group of students tend to use the Internet most frequently at home and at school. About 60% stated that they use the Internet at least 2-3 days per week. These students tend to use a desktop the most to use the Internet, followed by a laptop and smartphone. They generally use the Internet to watch online videos, play online games and do schoolwork. Parents and teachers seem to be the two main persons responsible for teaching these students to use the Internet.

Group 2 - Primary School Level 2

Students in this group tend to use the Internet most frequently at home and at school. This is in line with the fact that almost 75% of the students surveyed stated that they have an Internet connection at home. About 70% stated that they use the Internet at least 2-3 days per week. It is good that students do not tend to spend so much time online, with only about 15% spending more than 10 hours on the Internet per week. More than half the students stated that they use smartphones to access the Internet, and this is not surprising as 60% said they own a smartphone. This high device ownership percentage means that students at this age are very much exposed to the Internet, which goes to show there is a serious need to educate them on using the Internet for their benefit as well as their safety. It is also quite surprising that about 70% have an e-mail account. The website with the largest number of student visits from this age group is YouTube, and it is thus essential to include safety education in the school curriculum.

Group 3 - Secondary School

This target group of students (aged 13-17 years) use the Internet most frequently at home. This is because about 75% of the students surveyed said they have an Internet connection at home. Around 80% of students stated that they use the Internet at least 2-3 days per week. Compared to the Primary School Level 2 target group, about 35% of secondary school students spend more than 10 hours on the Internet per week. Over 75% indicated that they use smartphones to access the Internet, and this is not surprising as 85% said they own a smartphone. This high device ownership rate means that these students are highly exposed to the Internet. Consequently, there is a considerable need to educate them about using the Internet to their benefit and safety. About 88% claimed to have an e-mail account. Rather than YouTube, most secondary school students visit Facebook more instead.

B. Social Media Usage

Group 1 - Primary School Level 1

Close to 50% of 7 to 9-year-old students surveyed have social media accounts. The types of social media accounts they mostly have are social networking and video accounts. Accordingly, it is clear on which types of accounts the module should focus in terms of teaching students to use them safely. Parents were most frequently stated as the people helping these students to create social media accounts. About 60% use a real photo of themselves on their social media accounts. Not surprisingly, 85% of the students surveyed said they watch videos on YouTube and about 43% play games online. The students also seem to be relatively aware of the danger of talking to strangers, as only 19% have chatted with someone they have just met online.

Group 2 - Primary School Level 2

More than 50% of Primary School Level 2 students surveyed have social media accounts. The types of social media accounts they have include social networking, video, and picture accounts. In terms of social media usage, these students do not tend to post very much, with only 30% posting at least once a day. This is also reflected by the time spent on social media daily, with 66% of respondents only using it for 1-2 hours a day. About 60% use their real name as well as a real photo on their social media accounts. In terms of safety issues with social media usage, students tend not to share their location, talk to people they do not know or accept friend requests from strangers.

Group 3 - Secondary School

Almost all Secondary School students surveyed have social media accounts (92.47%). The types of social media accounts they have include social networking, picture and video accounts. Students who have social media accounts mostly said they have these for interaction purposes. In terms of social media usage, the students do not tend to post frequently, with only about 25% posting at least once a day. However, about 32% spend at least 5-6 hours on social media daily. About 63% use their real name and 72% use their real photo on social media accounts. Around 65-70% of students share pictures and information they see online on their social media accounts. Regarding safety issues with social media usage, results signify that secondary school students also tend not to share their location, talk to people they do not know or accept friend requests from strangers.

C. Parental Control

Group 1 - Primary School Level 1

A large percentage of students (about 75%) said they know what a password is. More than half of these students share their social media account passwords with their parents. Parents seem to monitor what their children are doing on the Internet, but about 25% of students said that their parents never sit with them when they are using the Internet.

Group 2 - Primary School Level 2

More than half the students in this group share their e-mail and social media account passwords with their parents. Their parents seem to monitor what their children are doing on the Internet, but only 22% of parents have installed some sort of parental control apps to filter unsuitable content.

Group 3 - Secondary School

Only about 25% of secondary school students share their e-mail and social media account passwords with their parents, indicating a decreasing trend with age. About half of these students stated that their parents seem to monitor what they are doing on the Internet, but only 20% of parents have installed some sort of parental control apps to filter unsuitable content. 73% of students also claimed they are ‘connected’ to their parents on their social media

D. General Internet Safety

Group 1 - Primary School Level 1

About 65% of the students in this group said they generally feel safe when browsing the Internet. If they feel unsafe, parents are the first point of contact to whom they would reach out.

Group 2 - Primary School Level 2

Only a small percentage of students from this group (9.34%) share their password with other people. At the same time, only about half use different passwords for different Internet accounts and 84% do not change their passwords often. Students generally feel safe when using the Internet and parents are still the first contact should they feel unsafe while on the Internet, followed by friends and siblings. These students do not seem to be fully aware of the available relevant bodies and authorities they can reach out to, should they ever face any form of threat when using the Internet (only 5% are aware).

Group 3 - Secondary School

Only 10% of secondary school students share their password with other people. About 65% have different passwords for different Internet accounts, but 77% do not change their passwords often. Students generally feel safe when using the Internet (about 59%) and they would reach out mainly to friends (59%) followed by parents (51%) and siblings (40.62%) in the event they would encounter any threats while using the Internet. Awareness of the availability of relevant bodies and authorities for reaching out is still low, at 7.83%.

E. Digital Citizenship Knowledge

Group 1 - Primary School Level 1

No component of digital citizenship knowledge was included in the survey questionnaire for primary school Level 1 students. The target group is between 7 years and 9 years of age and they are deemed still too young to understand the context of digital citizenship.

Group 2 - Primary School Level 2

Table II presents the proportion of students and what they are comfortable doing on the Internet in order from the highest to lowest percentage.

Group 3 - Secondary School

Table III represents the proportion of secondary school students and what they are comfortable doing on the Internet in order from the highest to lowest percentage.

TABLE II
PRIMARY SCHOOL LEVEL 2 – ACTIVITIES STUDENTS ARE COMFORTABLE DOING ON THE INTERNET

	Items	Percentage
1	Downloading movies/songs from websites	39.38
2	Uploading movies/songs from websites	32.01
3	Talking or chatting with people in online gaming portals	20.35
4	Posting daily activities and whereabouts	12.19
5	Using file-sharing sites	12.08
6	Playing games that are violent	11.79
7	Posting information about where you live and to which school you go	11.59
8	Deliberately excluding someone from an online group	7.77
9	Giving out personal details online	6.80
10	Name-calling	6.73
11	Sending photos of yourself to someone you have just known on the Internet	6.56
12	Imitating someone online	5.67
13	Sharing information without first checking its truth	5.48
14	Sending rude messages to others	4.70
15	Texting or emailing intimidating, rude or cruel messages to people	3.71
16	Posting, forwarding or obtaining someone’s personal or private information without their permission	3.62
17	Sending nasty messages to others	3.05
18	Spreading nasty rumours about others	2.96
19	Playing gambling games	2.93
20	Playing games that portray sexual nature	2.88
21	Teasing in a hurtful manner	2.81
22	Posting indecent photos online	2.64
23	Posting embarrassing videos	2.59
24	Posting embarrassing photos	2.17

TABLE III
SECONDARY SCHOOL – ACTIVITIES STUDENTS ARE COMFORTABLE DOING ON THE INTERNET

	Items	Percentage
1	Downloading movies/songs from websites	71.03
2	Uploading movies/songs from websites	41.64
3	Stating/quoting the original source of information	33.29
4	Talking or chatting with people in online gaming portals	30.29
5	Using file-sharing sites	25.11
6	Playing games that are violent	23.02
7	Posting information about where you live and to which school you go	19.62
8	Deliberately excluding someone from an online group	12.70
9	Posting daily activities and whereabouts	11.92
10	Name-calling	10.63
11	Imitating someone online	10.08
12	Sending rude messages to others	7.95
13	Sharing information without first checking its truth	6.54
14	Giving out personal details online	6.29
15	Sending photos of yourself to someone you have just known on the Internet	5.34
16	Playing gambling games	4.38
17	Teasing in a hurtful manner	4.25
18	Posting, forwarding or obtaining someone’s personal or private information without their permission	4.01
19	Sending nasty messages to others	3.83
20	Playing games that portray sexual nature	3.21
21	Texting or emailing intimidating, rude or cruel messages to people	3.06
22	Posting embarrassing photos	2.35
23	Spreading nasty rumours about others	1.93
24	Posting embarrassing videos	1.75
25	Posting indecent photos online	1.43

V. DISCUSSION

Based on the study, there is generally a sense of cyber security awareness among primary and secondary school students in Malaysia. However, a number of issues need to be addressed in order to ensure a safer environment for future younger generations. The discussion focuses on findings that indicate a common trend and which cut across all three groups of students.

Referring to the question: "On what devices do you use the Internet?" Primary School Level 1 students tend to use desktops the most for accessing the Internet as compared to Primary School Level 2 and Secondary School students who opt to use smartphones most of all among other devices. Desktop use falls considerably from Primary School Level 1 to Secondary School students. This could very well be due to older students having more access to smartphones than younger students. Moreover, at an older age, children tend to value their privacy more and the desktop might be in a common area in the house, and hence privacy becomes limited. On the other hand, smartphone usage increases considerably from Primary School Level 1 to Secondary School students. With the rapid shift in technology and more affordable prices, more children have access to smartphones, making this their device of choice as it ensures privacy. Mobile phone, tablet/iPad and laptop usage does not show a significant difference among the three groups.

When asking Primary School Level 2 and Secondary School students about "device ownership", there is a 15% greater smartphone ownership for Secondary School students. A similar trend can be seen for laptop ownership, with an increase of almost 20%. There seems to be only a decrease in tablet/iPad ownership among Secondary School students. Since smartphones and laptops are very mobile, it is not a surprise that older respondents own such devices. There are many smartphone brands on the market and so the prices are more varied, which increases the affordability of owning one. However, it is surprising that 60% of 10-12 year olds surveyed own a smartphone. With this trend, there is a pressing need to educate children on safe Internet use.

As for the question: "Who taught you to use the Internet?" Primary School Level 1 students stated that it was mainly their parents and teachers who taught them to use the Internet. But for secondary school students, the highest percentage said they were self-taught, followed by being taught by their friends. Hence, there is a clear increasing trend (from Primary Level School 1 to Secondary School) for the self-taught and friends categories, in contrast to a clear decreasing trend of parents and teachers as the responsible persons who teach school children to use the Internet. Based on this, parents and teachers (as the first persons who teach children how to use the Internet) should also be educated on the necessity to teach their children how to use the Internet in a safe way.

When asked whether school students "own a social media account", a steady increase is evident in students having social media accounts from Primary School Level 1 to Secondary School students. This increase is about 20% from Primary School Level 1 to Primary School Level 2, and a 25% increase from Primary School Level 2 to Secondary School. A total of 92.47% of Secondary School students surveyed stated that they have social media accounts. Even at the young age of 7-9 years old, almost 50% of the students surveyed said they have social media accounts. This goes to show the crucial need to teach children of this age how to use social media responsibly. Parents also need to be educated and made aware that children at this age should not have social media accounts, as they have not even reached the permissible age to have social media accounts.

In terms of "types of social media accounts that students have", there is a general increasing trend for almost all types of social media accounts except for document-type accounts. The largest percentage increase is for social network accounts as well as picture accounts. For video and blog accounts, the percentage increase is not as large as for social network and picture accounts. The three types of social media accounts on which awareness education should focus are social network, picture and video accounts. Since all three types facilitate posting pictures and videos, children should be educated on what is appropriate to post and otherwise.

On the question of whether students "share their social media account passwords with parents", there is a decreasing number of students who do so from Primary School Level 1 to Secondary School students. This clearly indicates that as children get older, they value their privacy more and are less willing to share their passwords with their parents. This also indicates that it is harder for parents to check on their children's activities online.

Based on the discussion above, it is clear that as students grow older, they are more inclined to utilize the Internet. There is a trend of how things change in terms of the way students use the Internet and for what; hence, it is necessary to educate them on different issues and various usage stages. Although it is important to educate children, it is equally important to educate parents as well, since they are regarded as their children's first 'teachers' of safe Internet use.

VI. Research Limitation

The only research limitation of this study is that the sample was only from national primary and secondary schools in the country. The study did not include any private, international or special education schools. Such schools should be included in future studies in order to gain a more comprehensive scope toward developing a national module for cyber security awareness in Malaysia.

VII. Conclusion

Based on the findings, it is obvious that young Malaysians are well-exposed to Internet use since a very young age, with device ownership starting as early as seven years of age. However, activities online need to be monitored more frequently and closely, and the existence of cyber threats was also reported in the data gathered. Children ought to be well-informed of current cyberspace issues and must learn to nurture an instinct to stay safe online.

The data gathered in this study will be useful for developing teaching and learning modules for primary and 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 insight and provided more data to the existing level of knowledge on cyber security among the younger generation 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 our future generations.

References

[1] M. Majid, “Royal Malaysian Police Statistics,” 2013. (Online). Available: http://www.skmm.gov.my/skmmgovmy/media/General/pdf/DSP-Mahfuz-Majid-Cybercrime-Malaysia.pdf (Accessed: 24-Apr-2016).

[2] A. Mubarak, “Child Safety Issues in Cyberspace: A Critical Theory on Trends and Challenges in the ASEAN Region,” Int. J. Comput. Appl., pp. 48–55, 2015.

[3] “New avenues for cooperation: Tackling human trafficking in Asia,” International Labour Organization (ILO), 2014. (Online). Available: http://www.eurasiareview.com/05042014-new-avenuesfor-regional-cooperation-tackling-human-trafficking-inasia-analysis. (Accessed: 26-Aug-2016).

[4] I. Ishak, A. Sidi, F., M. Jabar, N. Mohd Sani, A. Mustapha, and S. Supian, “A Survey on Security Awareness among Social Networking Users in Malaysiatle,” Aust. J. Basic Appl. Sci., vol. 6, no. 12, pp. 23–29, 2012.

[5] P. Soh, Y. Yan, T. S. Ong, and B. Teh, “Digital Divide amongst Urban Youths in Malaysia – Myth or Reality?,” Asian Soc. Sci., vol. 8, no. 15, pp. 75–85, 2012.

[6] “DiGi CyberSAFE The National Survey Report 2015: Growing Digital Resilience among Malaysian Schoolchildren on Staying Safe Online,” DiGI, CyberSecurity Malaysia, Kementeri. Pendidik. Malaysia, 2015.

[7] V. Balakrishnan, “Cyberbullying among Young Adults in Malaysia: The Roles of Gender, Age and Internet Frequency,” Comput. Human Behav., vol. 46, pp. 149–157, 2015.

[8] K. Pawelczyk, P. Kaur Karam Singh, and I. Nadchatram, “Exploring the Digital Landscape in Malaysia: Access and Use of Digital Technologies by Children and Adolescents,” UNISEF Malaysia, 2014.

[9] S. Al-Jerbie and M. Jali, “A Second Look at the Information Security Awareness among Secondary School,” Proc. Int. Conf. Inf. Secur. Cyber Forensics, pp. 88–97, 2014.

[10] M. Tekerek and A. Tekerek, “A Research on Students’ Information Security Awareness,” Turkish J. Educ., vol. 2, no. 3, 2013.

[11] “School Programmes - Social and Emotional Learning - Cyber Wellness,” Ministry of Education, Singapore. (Online). Available: https://www.moe.gov.sg/education/programmes/social-and-emotional-learning/cyber-wellness (Accessed: 26-Apr-2016).

[12] “Education Resources – School Policies – Implementing Policies,” Office of the Children’s eSafety Commissioner, Australian Government. (Online). Available: https://www.esafety.gov.au/education-resources/school-policies/implementing-policies. (Accessed: 26-Apr-2016).

[13] “International Telecommunication Union (ITU) Global Cybersecurity Index & Cyberwellness Profiles,” ABI Research & International Telecommunication Union (ITU), 2015. (Online). Available: http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf. (Accessed: 26-Apr-2016).