INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 12, Issue 6, (2022) E-ISSN: 2222-6990

Secondary School Students' Online Activities and their Experience in Cyber Risks

Nurul Syaida Md Zuki, Fariza Khalid, Aidah Abdul Karim

Faculty of Education, Universiti Kebangsaan Malaysia, 43600 Bandar Baru Bangi, Selangor, Malaysia

Email: nurulsyaidazuki@gmail.com, fariza.khalid@ukm.edu.my, eda@ukm.edu.my

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v12-i6/13924 DOI:10.6007/IJARBSS/v12-i6/13924

Published Date: 02 June 2022

Abstract

Today's technology and communications (ICT) facility has seen the creation of various social media platforms, chat application and even online entertainment platforms. So, more and more generations are accessing these platforms in search of entertainment, information and even communicating with others. This situation actually opens the door to cyber risk when it is not used wisely and responsibly. As a result, in recent times, various incidents have been reported in adolescents that involve cyber risk, affecting psychological, mental and physical health. These include cyberbullying, digital games and social media addiction, pornography, grooming, cybersex and the misuse of personal information. The purpose of this research is to investigate the online activities among school students and to examine their online risks experienced by Malaysian secondary school students. A total of 1376 form four students (16 years old) were involved in this research. The research data was collected using a set of questionnaire. Descriptive data analysis was performed using SPSS version 20 software. The findings show a high trend of online student activities for communicating, socializing, watching videos and finding information. Although students' experiences of cyber risk are low, steps to control the situation need to be taken in order to prevent the any risks when they are online. Therefore, this research paper also discusses the role of all parties in ensuring that the cyber world is used wisely and responsibly.

Keywords: Cyber Risk, Online Activity, Secondary School, Cyberbullying, Cybersex, Pornography, Grooming, Addiction.

Introduction

Along with the change of time, now the use of Information Technology and Communication (ICT) has undergone changes in the Industrial Revolution 4.0 (IR4.0) where ICT is widely used in various fields (Osatuyi, 2013). The use of ICT has helped its users to communicate, obtain information, perform daily tasks, perform transactions and much more just at their fingertips (Balraj et al., 2013). Therefore, to further boost the use of ICT in IR4.0, the Malaysian government has drafted a Comprehensive Roadmap for the Industrial Revolution 4.0 (IR 4.0)

and National Digital to ensure that the implementation of digital infrastructure in Malaysia runs in line with current needs. It also aims to enable Malaysians to use broadband services to improve their quality of life which includes social and economic networks. Not only that, the authorities, state governments, communications companies and related agencies are also mobilized to achieve the Malaysian government's aspiration to make communication services a basic need in driving the country towards a digital economy.

The need for the use of ICT is seen to be a major need since the outbreak of covid-19 in Malaysia since 2020 until now. Based on the statistical report on the use of ICT in 2020 by the Malaysian Communications and Multimedia Commission (MCMC) found that the use of ICT among Malaysians showed a significant increase compared to the year before the outbreak of Covid -19. This is due to the implementation of the Movement Control Order (MCO) by the Malaysian government to control the spread of Covid-19 where Malaysians have used various applications available online to implement their purposes and needs. In fact, the demand for broadband services has also increased dramatically due to the need to conduct learning activities, business, conferences, and meetings conducted from home only. This has shown that with the use of ICT, many work and services can be done quickly and easily by various sections of society.

While ICT aids the community in carrying out its activities, digital citizens should be aware that they may be vulnerable to cyber hazards, which can result in property loss and psychological issues. This is due to the fact that a small number of digital citizens abuse the services supplied, causing harm to others and themselves (Pitchan & Omar, 2019). Digital citizens should use ICT in a responsible and ethical manner, which includes nine important elements: digital access, digital business, digital communication, digital literacy, digital law, digital assets, digital rights and duties, digital health, and digital security (Malaysian Digital Association, 2016). However, every year the mass media often reports an increase in cases related to terrorism, racist abuse, cyber fraud, gambling addiction, pornography, cyber bullying, and hacking of systems and impersonation around the world including Malaysia (Muniandy & Muniandy, 2012). The increase in cases is seen to have an impact on the level of cyber security not only to digital citizens but also to the country.

The increase in cybercrime cases in Malaysia is seen to be more significant in 2020 following the implementation of the MCO. Based on the statistical report released by the Malaysian Communications and Multimedia Commission (MCMC) in 2020 found that a total of 20 805 complaints were received compared to 10 426 complaints received in 2019 (MyCERT, 2021). This shows an increase in cybercrime cases of 99.5% in 2020. Among the complaints received by SKMM are related to cyber bullying, fraud, information theft, system hacking, and pornography. Therefore, to prevent these cybercrime activities, appropriate action has been taken by the authorities, PDRM, MCMC, and Cybersecurity Malaysia in order to protect digital citizens from becoming victims of cybercrime. In fact, the Malaysian government remains committed to building a peaceful, reliable and resilient cyberspace by creating an action plan under the Malaysian Cyber Security Strategy 2020-2024 (MCSS 2020-2024) which will be coordinated with the MyDigital initiative.

Cyber Risk

There are various risks in the cyber world that have been identified to have threatened the well -being of universal humanity. Among them are cyber bullying which includes threats, insults, swearing or swearing, incitement, dissemination of false information and fights (Dilmac, 2017; Bada & Sasse, 2014; Donegan, 2012; Erdur-Baker & Tanrikulu, 2010). Even the messages, videos and pictures sent by the perpetrators of cyber bullying are also intended to hurt or hurt the victim, insult, as well as degrade the victim of cyber bullying (Ali et al., 2018; Brady, 2010) directly or indirectly (Kowalski et al., 2012). Apart from that, the perpetrators of cyber bullying also incite others by creating provocations, spreading false information about the victim with the aim of triggering fights as well as discomfort of the victim on social networks or in cyberspace (Vlachos et al., 2011).

Meanwhile, information theft is among the cyber risks that often occur to users of online platforms, especially users of social media and chat applications. This information theft can occur when users are not careful in displaying personal information or sharing their personal information (Ratten, 2015; Tamrin et al., 2015). Information and data shared on social media or chat applications in an uncontrolled manner may be used by third parties for certain purposes (CyberSecurity Malaysia, 2015) so as to result in loss (Andrews, 2011). The next cyber risk is grooming in which a criminal will approach the victim and gain the victim's trust until the victim is made a sex slave or other criminal activity (Tamrin et al., 2015; Krotidou et al., 2012). This grooming activity is very popular nowadays because in this way, criminals are able to manipulate victims for their sexual activities as well as their crimes (Krotidou et al., 2012). In fact there are a handful of teenagers today who fall victim to grooming as a result of their social activities on social media. The risk for a cyber citizen to become a victim of social media addiction is also high where they spend a lot of time browsing social media without doing other activities (Annasingh & Veli, 2016). Individuals who experience this social media addiction are individuals who use social media indefinitely over a period of time to seek information, relax, and be friends on social media thus affecting themselves and the organization (Hawi & Samaha, 2016; Erickson, 2011).

Furthermore, the risk for a person to be exposed to pornographic materials consisting of pictures, videos and animations is also high if online access is not restricted (Griffiths & Kuss, 2015; Krotidou et al., 2012). These pornographic materials can lead to cyber sexual activity if a person is unable to control themselves as a result of watching and reading pornographic materials (Tiara & Rulita, 2013). This occurs due to the emergence of sexual feelings in the self that affect a person's sexual behavior (Tiara & Rulita, 2013). Cybersex is a virtual sex activity that includes voice, video and text conversations mixed with sex which is one of the cyber risks that may occur to a person when having a close relationship with someone in the virtual world (Krotidou et al., 2012). This cyber sexual activity if not controlled can cause harm to the perpetrator and may lead to more serious social symptoms (Ningsih, 2016).

Given the cyber risks found in the cyber security environment it is not surprising that today's digital citizens may be victims of such cyber risks. This is evidenced by the increase in cybercrime cases reported to the Malaysian Communications and Multimedia Commission (MCMC) every year. The problem in this issue is, this cybercrime case does not only focus on adults but it also involves adolescents in Malaysia where every year various reports are

received related to the involvement of adolescents with cyber risk leading to cybercrime among adolescents (Alaui, 2018). In 2018, a total of 395 complaints were received by the Malaysian Communications and Multimedia Content Forum (CMCF) from users related to pornographic content and cyberbullying involving adolescents (Alaui, 2018). Not only that, the Malaysian Mental Health Association (MMHA) also reports receiving 500 calls per month related to complaints and interventions related to cyber bullying among adolescents (Harian, 2022). This figure is likely to continue to rise if it is not taken seriously by all parties.

This situation occurs because, adolescents are a group that is easily influenced by a certain culture and environment (Shanti & Kia, 2013). Negative displays can cause their behavior to worsen and lead to negative effects because they easily emulate something through sight, hearing and speech without a parent or guardian (Balraj et al., 2013). For example, the Malaysian Child Welfare Council (MKMM) has reported suicides and cases of personal injury among adolescents due to cyber bullying and addiction to cyber games. A survey study conducted by the Malaysian Communications and Multimedia Commission (MCMC) in 2020 also found that internet use by children and adolescents aged five to 17 in Malaysia increased by 155% in 2020 compared to 2016. So it is not surprising if adolescents in Malaysia are vulnerable to cyber risks leading to cybercrime or other crimes.

Therefore, the aims of this study are to investigate the online activities among school students and to examine their online risks experiences. This study is necessary to learn about the activities that students engage in while online so that stakeholders could implement suitable cyber risk prevention measures for adolescents and parents in particular to be aware of and pay attention to their children's online activities.

Research Methodology

This study uses a survey research design to collect data from the population to understand an identified situation (Noraini, 2016). Therefore, the random sampling method is easy to use to obtain the sample of this study which consists of form four students of national secondary schools in Malaysia. Research participants were 1376 from four students from seven states i.e., Sarawak, Kedah, Selangor, Kuala Lumpur, Putrajaya, Malacca and Terengganu (See Table 1). The selection of the participants who are 17 years old was done based on the characteristics proposed by Jose (2010); Tiara et al (2013) who asserted that those who age between 15 to 17 years are in a phase of self-identity building that involves the development of their identity via social relationships with other online or face to face.

Table 1
Distribution of respondents by state and Gender

Variable	Number Of Respondents (n)	Percentage(%)
State		
Kedah	236	17.2
Selangor	202	14.7
Kuala Lumpur	243	17.7
Putrajaya	126	9.2
Melaka	177	12.9
Sarawak	216	15.7
Terengganu	175	12.7
Total	**1376**	**100.0**
Gender		
Male	593	43.1
Female	783	56.9
Total	**1376**	**100.0**

To obtain data from the sample, a set of questionnaire forms were used. This questionnaire form has been adapted and modified from previous studies (Balraj et al., 2013; UNICEF Malaysia, 2014). There are 19 items in this questionnaire of which 13 items are related to online activities performed by students while 6 items are related to students' experience of cyber risk. For 13 items related to online activities, the items were measured using nominal data that students were asked to choose either 'Yes' or 'No'. While for 6 items related to students 'experience of cyber risk, the items were measured using ordinal data on a 7 -point Likert scale, namely' Never ',' 1 time ',' 2 times ',' 3 times ',' 4 times ',' 5 times' and 'Many times' to indicate the frequency of risks that students have encountered while online.

The questionnaire was first tested by 93 students from states who were not involved in the actual research. The reliability of items using Cronbach's coefficient alpha for the pilot test ranged from 0.79 to 0.91. Values have exceeded minimum consistent guidelines for acceptable instrumentation (Cohen, 1988). Statistical Software Package for the Social Science (SPSS) version 20 was used to analyze the data obtained. Descriptive analysis with frequency and percentage interpretation was conducted to report the findings of this study.

Findings and Discussion

A brief profile of the respondents related to the technological devices owned by the students, where to access the internet and the period of use were displayed as in Table 2. Findings were reported using frequency and percentage interpretation. (See Table 2).

Table 2
Demography of Respondents

Type	Frequency (n)	Percentage (%)
Owned Technology Devices		
Smart phone	1294	94.0
Laptop	614	44.6
Tablet/ipad	257	18.7
Internet Access Point		
Own house	1272	92.4
Friend's house	288	20.9
School	221	16.1
Cyber Cafe	259	18.8
others	411	29.9
Internet Surfing Period		
0 to 4 hours	398	28.9
5 to 8 hours	532	39.7
9 to 12 hours	296	21.5
13 to 16 hours	56	4.2
17 to 20 hours	22	1.5
21 to 24 hours	72	5.2

Based on the frequency for each technology device owned by the respondents, it was found that 1294 respondents (94%) had a smartphone, 614 respondents (44.6%) had a laptop, and 257 respondents (18.7) had a tablet or Ipad. The findings show that the majority of respondents use smartphones to surf the internet followed by the use of laptops and tablets or Ipads. Meanwhile, for the place where the respondents accessed the internet, it was found that a total of 1272 respondents (92.4%) accessed the internet at home, 288 respondents (20.9%) accessed the internet at a friend's house, 221 respondents (16.1%) accessed the internet at school, 259 respondents (18.8%) access the internet in cyber cafes and 411 respondents (29.9%) access the internet elsewhere. This indicates that the majority of respondents access the internet in their own homes. This is because home may be a more comfortable place for them to access the internet than accessing the internet elsewhere. In addition, the duration of internet usage per day by respondents is also seen to be more than 5 hours per day where the number of respondents who use the internet more than 5 hours per day is higher than the number of respondents who use the internet in the estimated around 0 to 4 hours per day.

Online Activities For High School Students

Among the aims of this study is to investigate the activities respondents often engage in online. Table 3 shows a summary of the number of students and the percentages for each activity that the student frequently engaged in.

Table 3
Online Activities For High School Students

Bil	Item	Frequency (n)	Percentage (%)
1.	Chatting with friends in the chat app (Whatsapp, Wechat, FB Messenger)	1240	90.1
2.	Watching Videos on Youtube	1140	82.8
3.	Searching Specific Information on Google	1128	82.0
4.	Using Social Network (Facebook, Twitter, Instagram, Wechat, Tumblr)	1087	79.0
5.	Getting the Latest News (Related to Artist, Country, Current Issue)	797	57.9
6.	Playing Online Games	785	57.0
7.	Finding New Friends on Social Networks (Facebook, Instagram, Tumblr, Wechat)	624	45.3
8.	Shopping Online	620	45.1
9.	Uploading / Downloading Video on Youtube	393	28.6
10.	Other Activities	233	16.9
11.	Using Frog VLE	212	15.4
12.	Sending email	186	13.5
13.	Writing a Blog	38	2.8

The analysis showed that the highest number of students and the percentage was for “Chat with Friends in The Chat Application” activity (n= 1240, percentage= 90.1%), followed by the second highest activity was “Watch Videos on Youtube” (n = 1140 , percentage= 82.8%), “Search Specific Information on Google” (n= 1128, percentage= 82.0%) and finally “Using Social Network” activity (n= 1087, percentage= 79.0%). Further, the analysis also found that there were four activities at the moderate level where only half of the respondents did. These include “Get the Latest News” (n= 797, percentage= 57.9%), “Play Online Game” (n= 785, percentage= 57%), “Finding New Friends on Social Networks” (n= 624, percentage= 45.3%) and “Online Shopping” activity (n= 620, percentage= 45.1%). In addition, the lowest online activity was “Upload / Download Video on Youtube” (n= 393, percentage= 28.6%), “Another Thing” (n= 233, percentage= 16.9%), “ Uses Frog VLE ”(n= 212, percentage= 15.4%),“ Sending Email ”(n= 186, percentage= 13.5%) and “ Writing a Blog” (n= 38, percentage = 2.8%). Based on the findings, it can be concluded that the main activity performed among the respondents is to chat with friends, watch videos and search for information on Google.

Student Experience in Cyber Risks

Next, this research is also to investigate respondents experiences in cyber risks that include cyberbullying, pornography, cybersex, information theft, social media addiction and grooming activities. The analysis is based on the percentage of cyber risk experience faced by respondents each time they are online according to a frequency scale that has been set from "Never" to "Many Times". While the analysis data is displayed in percentage. (See Table 4)

Table 4
Respondents experiences in cyber risks

Category Cyber Risk	Item	Never	One Time	Twice	Three Times	Four Times	Five Times	Many Times
Cyberbully	I was bullied by my friends on social media.	74.5 %	13.8 %	5.5 %	3.2 %	0.8 %	0.2 %	2.0 %
Information Theft	My information such as pictures is often used by others.	75.2 %	12.9 %	6.0 %	1.8 %	1.2 %	0.5 %	2.3 %
Pornography	I'm automatically shown immoral things while using the internet.	58.9 %	10.3 %	8.4 %	5.6 %	2.4 %	1.9 %	12.4 %
Cybersex	I do immoral activities with my online contacts. (Eg: conversation porn)	81.7 %	7.1 %	4.2 %	2.0 %	1.1 %	0.9 %	3.0 %
Social Media Addiction	I get really bored when I can't use social media.	10.0 %	11.7 %	10.5 %	11.5 %	4.7 %	3.1 %	48.5 %
Groomimg	I was instructed to engage in immoral activity by my contacts online.	90.0 %	6.3 %	1.4 %	0.9 %	0.6 %	0.3 %	0.5 %

The results show that the percentage of respondents who have never been involved with the risk of cyber bullying for the item "I was bullied by my friends on social media" is 74.5%. However, the percentage of respondents who have experience of cyberbullying from the frequency of "1 time" to "Many Times" is as much as 25.5%. Furthermore, the results also found that the percentage of respondents who have never been involved with the risk of information theft for the item "My information such as pictures is often used by others" is also 75.2%. While the percentage of respondents who have experience in the risk of information being stolen from the frequency of "1 time" to "Many Times" is 24.5%. The findings also found that the percentage of respondents who have never been involved with the risk of cybersex and grooming also respectively for the item "I do immoral activities with my online contacts" is 81.7% and the item "I was instructed to engage in immoral activity by my online contacts" is 90%. For the percentage of respondents who have experience with the risk of cybersex and grooming from the frequency of "1 time" to "Many times" is 18.3% respectively for cybersex and 10% for grooming.

Apart from that, the results also show that the percentage of respondents who have never been involved with the risk of pornography and also social media addiction are respectively with the item "I'm automatically shown immoral things while using the internet" is 58.9% and the item "I get really bored when I can't use social media " is 10%. However, the percentage of respondents who have experience in the risk of pornographic material from the frequency of "1 time" to "Many times" is 41.1%. While the percentage of respondents

who have experienced social media addiction from the frequency of "1 time" to "Many times" is the highest at 90%.

Discussion

After looking at the results of this study, the percentage of respondents who are not involved in cyber bullying, information theft, cybersex, and grooming is low, however, the percentage of respondents who have experienced the risk is more than 10% of the total respondents of this research which is 1376. While the percentage of respondents involved with the risk of pornography and social media addiction is seen as high. This shows that, various parties need to be concerned about cyber risks. This is because, based on the average duration of internet use by respondents is more than 5 hours a day, and activities that respondents often do while online that is chatting with friends, watching videos and searching for information on Google, it is not impossible for respondents to engage with any cyber risks in the future. This is also stated by Khalid et al (2018), for which there is still a lack of appropriate knowledge on aspects of self-protection against cyber risks involving children and adolescents. Even the awareness of parents as well as the role of parents on cyber security is also seen as low (Ahmad et al, 2019). This indirectly affects children and adolescents in relation to cybersecurity as the family institution plays a key role in shaping a society that is efficient using technology in line with human values (Haslina et al., 2021).

Thus, various initiatives have been implemented in spreading awareness related to cyber risks which the Malaysian Communications and Multimedia Commission (MCMC) has introduced the "Klik Bijak" program to cultivate positive internet use among the community since 2014. In addition, CyberSecurity Malaysia in collaboration with Syarikat Telekomunikasi DIGI has also implemented the CyberSAFE program with the aim of raising awareness on the risks of internet use for school children with the involvement of parents to create a safe environment for children. Both of these programs are implemented using websites as a platform to disseminate information related to cyber risks. However, the implementation of this program is still insufficient to spread awareness related to cyber risks that all parties need to be involved in educating children and adolescents in this regard (Khalid et al., 2018; Nazilah, 2018). Even the effectiveness of the programs implemented by MCMC and CyberSecurity is still in question (Nazilah, 2018). While Rahman et al (2020) stated that it is very important to protect children and adolescents through cyber security education so that they can know the risks they will face when using communication technology.

Therefore, in order to redouble efforts in spreading cyber risk awareness, the third party, namely schools, teachers and parents need to have the initiative to provide cyber risk awareness to students by increasing the number of modules related to cyber risk (Rahman et al., 2020; Rafik & Fariza, 2020). In addition, for future studies it is proposed to conduct case study research by deepening the cases of adolescents who have been victims of cyber risk to understand in more depth related to the effects they face in terms of moral, behavioral, and psychological after becoming a victim to cyber risk.

Conclusion

In conclusion it can be seen that, although the results of this research found that the percentage of respondents exposed to the risk of cyber bullying, information theft, cybersex and grooming is at a low level but so when looking at the trend of online activities often done

by respondents, the possibility to respondents are at high cyber risk. This is because, when respondents prefer to communicate or socialize on social media and also chat applications over a long period of time, it is likely for respondents to be exposed to cyber risks for which they may not be aware that they may be victims of such cyber threats.

Even activities like watching videos on youtube can also expose respondents to the threat of pornographic materials unintentionally or intentionally by respondents. This can certainly result in an increase in social symptoms among adolescents if this is not controlled or curbed. Therefore, in order to curb the involvement of students in cyber risks, all parties need to redouble their efforts by providing various initiatives which start from students, parents, teachers, schools and authorities in spreading awareness related to cyber risks to children and adolescence. This is so that, we can create a digital society that is prudent, responsible and respectful of each other and ultimately create a safe cyber environment.

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

References

Ahmad, N., Mokhtar, U. A., Hood, Z., Tiun, S., & Jambari, D. I. (2019). Parental Awareness on Cyber Threats Using Social Media. *Jurnal Komunikasi: Malaysian Journal of Communication*, 35(2), 485-498.

Andrews, L. (2011). I Know Who You Are And I Saw What You Did: Social Networks And The Death Of Privacy. New York: Free Press.

Annasingh, F., & Veli, T. (2016). An Investigation Into Risks Awareness And E-Safety Needs Of Children On The Internet. *Interactive Technology And Smart Education*, 13(2), 147-165.

Bada, M., and Sasse, A. (2014). Cyber Security Awareness Campaigns: Why Do They Fail To Change Behaviour?

Balraj, S., Pandian, A., Nordin, M. Z., Nagalinganm, S., Ismail, J., & Jing Yi, L. (2013). Young People And New Media: Social Uses, Social Shaping And Social Consequences. Media Matters: Network Media Content Research Summary 1, 7-11.

Brady, K. P. (2010). Cyberbullying. Encyclopedia of Law and Higher Education. Sage Publications, Inc.

Cohen, J. (1988). Statistical Power Analysis For The Behavioral Sciences (2nd Ed.). Hillsdale, NJ: Lawrence Earlbaum Associates.

CyberSecurity Malaysia. (2015). Kisah Benar Cyber 999. Shah Alam: Karangkraf Sdn Bhd.

Dilmac, B. (2017). The Relationship between Adolescents' Levels of Hopelessness and Cyberbullying: The Role of Values. *Educational Sciences: Theory &* Practice, 17: 1119-1133.

Donegan, R. (2012). Bullying and Cyberbullying: History, Statistics, Law, Prevention and Analysis. *Journal of Undergraduate Research in Communications*, 3(1), 33–42.

Erdur-Baker, O., & Tanrikulu, I. (2010). Psychological Consequences of Cyber Bullying Experiences among Turkish Secondary School Children. *Procedia Social and Behavioral Sciences*, 2, 2771-2776.

Erickson, L. B. (2011). Social Media, Social Capital, And Seniors: The Impact Of Facebook On Bonding And Bridging Social Capital Of Individuals Over 65. Paper presented at the AMCIS 2011, Detroit, Michigan.

Griffiths, M. D., & Kuss, D. (2015). Online Addictions, Gambling. Video Gaming And Social Networking. In Sundar, S. (Ed.), The Handbook Of The Psychology Of Communication Technology. John Wiley, Chichester, Pp. 384-406.

Hassan, H. M., Salleh, M. A. M., & Ahmad, A. K. (2021). Keibubapaan Digital dan Mediasi Ibu Bapa Terhadap Penggunaan Internet Remaja di Malaysia. *Malaysian Journal of Social Sciences and Humanities*, 6(8), 121-132.

Hawi, N. S., & Samaha, M. (2016). The Relations Among Social Media Addiction, Self-Esteem, and Life Satisfaction in University Students. *Social Science Computer Review*, 35(5), 576–586.

Jose RL Batubara. 2010. Adolescent Development (Perkembangan Remaja). *Sari Pediatri*, 12(1): 21-29.

Khalid, F., Daud, Y. M., Rahman, M. J. A., & Nasir, M. K. M. (2018). An Investigation of University Students' Awareness on Cyber Security. *International Journal of Engineering & Technology*, 7 (4.21), 11-14.

Kowalski, R. M., Limber, S. P., & Agatston, P. W. (2012). Cyberbullying: Bullying in the Digital Age. Second Edition. John Wiley & Sons Ltd Publication, UK.

Krotidou, D., Eteokleous, N., & Zahariadou, A. (2012). Exploring Parents' And Children's Awareness On Internet Threats In Relation To Internet Safety. *Campus-Wide Information Systems*, 29(3), 133-143.

Malaysian Digital Association. (2016). Malaysia Digital Landscape Exploring The Digital Landscape In Malaysiaboosting Growth For A Digital Economy. Presented at The Digital Integration & Business Transformation Asia Conference 3 - 4 August 2016, |JW Marriott Kuala Lumpur, Malaysia.

Muniandy, L., & Muniandy, B. (2012). State Of Cyber Security And The Factors Governing Its Protection In Malaysia. *International Journal of Applied Science and Technology*, 2(4), 106-112.

MyCERT. (2021). Incident Statistics. Reported Incidents Based on General Incident Classification Statistics.https://www.mycert.org.my/portal/statistics-content?menu=b75e037d6ee3-4d118169-66677d694932&id=2650ed29-88be-4cec-86cc13f8e07ae228.

Ahmad, N. (2018). Model Keibubapaan Siber Untuk Kanak Kanak. Laporan Akhir Universiti Kebangsaan Malaysia.

Ningsih, W. (2016). Knowledge and Attitudes toward Internet Porn Videos Within Teenagers. Degree in Education Degree (Educational Psychology) dissertation. Sultan Idris Education University. Perak. Malaysia.

Idris, N. (2016). Penyelidikan Dalam Pendidikan. Edisi Kedua. Mc. Graw Hill Education (Malaysia) Sdn Bhd.

Osatuyi, B. (2013). Information Sharing On Social Media Sites. *Computers in Human Behavior*, 29(6), 2622–2631.

Pitchan, M. A., & Omar, S. Z. (2019). Malaysia's Cyber Security Policy: A Review Of Netizens Awareness And The Law. *Journal of Communication: Malaysian Journal of Communication*, 35 (1).

Rahman, N. A. A, Sairi, I. H., Zizi, N. A. M., and Khalid, F. (2020). The Importance of Cybersecurity Education in School. *International Journal of Information and Education Technology*, 10(5).

Ratten, V. (2015). A Cross-Cultural Comparison Of Online Behavioral Advertising Knowledge, Online Privacy Concerns And Social Networking Using The Technology Acceptance

Model And Social Cognitive Theory. *Journal Of Science & Technology Policy Management*, 6(1), 25-36: Https://Doi.Org/10.1108/JSTPM-06-2014-0029.

Shanti, C. S., & Kia, L. C. (2013). The Use of Digital Stories for Listening Comprehension among Primary Chinese Medium School Pupils: Some Preliminary Findings. *Jurnal Teknologi (Social Sciences)*, 65(2), 125–131.

Harian, S. (2022). 500 panggilan kes buli siber diterima setiap bulan: MMHA. Full Article : https://www.sinarharian.com.my/article/181984/BERITA/Nasional/500-panggilan-kes-buli-siber-diterima-setiap-bulan-MMHA.

Alaui, S. A. (2018). Child Cyber Crime Complaints Complaint Oline messenger. Accessed January 4, 2019 at http://www. Result.com.my/mega/rona/crime-criminal-crime-date-1.779317.

Tiara, D. F., Sri, M. D., & Rulita, H. (2013). Factors Causing Sexual Behavior Disorders in SLB N Semarang Teenagers. *Development and Clinical Psychology*, 2(1), 26-32.

United Nations Children's Fund (UNICEF) Malaysia. (2014).

Vlachos, V., Minou, M., Assimakopouos, V., & Toska, A. (2011). The Landscape Of Cybercrime In Greece. *Information Management & Computer Security.*

Ismail, W. R. W., & Khalid, F. (2020). Pembangunan Modul (Kusedar) Untuk Meningkatkan Kesedaran Keselamatan Siber Dalam Kalangan Pelajar Sekolah. Proceeding-Malaysia International Convention on Education Research & Management (MICER) 14-16 March, 2020. Bangi Resort Hotel, Bandar Baru Bangi, Malaysia.

Ali, W. N. H. W., Mohd, M., and Fauzi, F. (2018). Cyberbullying Detection: An Overview. Cyber Resilience Conference (CRC), pp. 1-3, doi: 10.1109/CR.2018.8626869.