Jurnal Komunikasi:
*Malaysian Journal of Communication*
Jilid 35(2) 2019: 485-498

# Parental Awareness on Cyber Threats Using Social Media

NAZILAH AHMAD@AHMAD ARIFIN
UMI ASMA' MOKHTAR
ZAIHOSNITA HOOD
SABRINA TIUN
DIAN INDRAYANI JAMBARI
*Universiti Kebangsaan Malaysia*

ABSTRACT

In recent years, the use of Internet has increased exponentially and most of the users are from adolescents. Internet technology has facilitated cyber threats activities and many of the cases are from adolescents. Users at this age need parental guidance and support because they are still naïve or immature to understand the risks of Internet. Hence, many developed countries have imposed on clear guidelines on the Internet to control and guide the users and understand the risks they will encounter when they are online. The guidance on how to use the Internet or social media begins at home and requires parental involvement to educate the children. Therefore, this study attempts to investigate on the parental knowledge and readiness whether they aware of the risks of Internet to their children. The level of parental awareness can be correlated with cyber safety at home. It is important to identify the awareness as one of the early cyber threat prevention. This study employed survey and questionnaire as the data collection techniques. The sample consisted of 872 parents with children aged 17 and below. A statistical analysis was performed using SPSS software. A mixture of descriptive and inferential statistics were used during the analysis method. The finding shows that parental awareness of the cyber threats is at the medium level and still need to be improved to promote cyber safety. Early exposure to parental awareness on cyber threats would aid in opening up knowledge about cyber security among parents.

**Keywords:** *Cyber safety, cyber threats, cyberparenting, parental awareness, social media.*

## INTRODUCTION

In Malaysia, national-level cyber safety awareness campaigns have been implemented through governmental agencies, corporate sectors and non-governmental organizations (NGOs) such as Ministry of Women, Family and Community Development (MWFCD) Malaysian Communications And Multimedia Commission (MCMC), Cyber Security Malaysia (CSM) and Digi Telecommunication Sdn. Bhd (Digi). The medium, as provided by the government, is important to raise awareness significantly among the target groups, especially students and parents.

MCMC has introduced a program known as Click Wisely in year 2016, organized more than 800 activities to an ever-widening audience of 1.7 million (SKMM, 2017). Parents who have little knowledge on their children's online activities indicate that their awareness about cyber threats is still low. This is rather seen as an apparent disadvantage through the unsympathetic eyes of children who realize that their parents may be technologically challenged (Byrne, Katz, Lee, Linz & McIlrath, 2014). Nadia (2017) and LPPKN (2013) report that only 4 out of 10 parents know what their children do online. In many cases, parents are unaware of their children's unwarranted access and exposure to inappropriate online sites (Wan Anita, 2016), subjecting the children to the threats lurking in the cyberspace.

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2019-3502-29

Despite its importance and wide educational influence among children, the Internet allows for the emergence of unhealthy elements marked with obscene content, cyberbullying, addiction, Internet scams, and personal information leakage. These cyber threats are said to be increasingly complex and drastically deteriorating from time to time (Wan Anita, 2016; O'Brien, 2014). Also, there is some evidence that social media addiction is more prevalent in certain groups specifically among younger people (Andreassen & Pallesen, 2014). Smith and Anderson (2018) in the US affirmed that younger people use a variety of social media platforms and using them frequently.

## LITERATURE REVIEW

According to (MCMC, 2017), the percentage of Internet use was 86.6% from which it was used mostly at home (85.6%), via the mobile devices at any location (84%) and at work (58.7%). The highest percentage of Internet use at home indicates the crucial place to control internet activities, especially among children. The role of a family institution to monitor and supervise Internet usage is critical to ensure that children are not exposed to cyber threats. Parental role to monitor the use of children's Internet is very important and pressing (Wan Anita, 2016; Livingstone, 2007; Muhammad Adnan, Siti Zobidah, Jusang & Akmar Hayati, 2017; Valcke, Bonte, de Wever & Rots, 2010). Children need support from parents as they are still immature to evaluate the information and threats in the cyberspace (Marshall & Jackman, 2015; Normah, Faridah, Wan Amizah, Fauziah, Chang & Maizatul Haizan, 2011).

Local Internet service providers such as Digi, Maxis and Celcom have taken initiative to provide parental control function but only 17.2% of parents used it because 59.1% of them claimed that they were not aware of the function. 69.2% of those who did not use the function imposed house rules on Internet use instead. However, if the parents have limited skills in technology, it might influence the monitoring and controlling process (Livingstone & Haddon, 2012; Wan Anita & Azizah, 2013).

Monitoring the children's use of social media such as short message service (SMS), social messaging or messaging apps such as WhatsApp, WeChat and Telegram by their parents need to be improved. The parents must be vigilant and proactive as the monitoring process should start at home. If parents fail to monitor children's online activities at home, it will expose the children to cyber threats such as addiction, pornography, paedophiles, internet fraud, personal data leakage and social problems such as cyberbully (Utusan Malaysia, 2017). For example, internet addiction has become a big issue because it affects the development of a person's self-identity. World Internet Statistics Review reveals nearly 78.8 percent of internet users in the country, especially children have serious internet addiction (Nadia, 2017). Andreassen and Pallesen (2014) defined internet addiction as "being overly concerned about social media and be driven by a strong motivation to log on or use the application, and to devote so much time and effort that impairs other social activities, studies/job, interpersonal relationships, and/or psychological health and well-being". Social media addiction cannot only be measured through time spent on the application rather it relates with other consequences including relational conflicts or behaviour that is compulsive and uncontrolled. The addiction among children is prevailing due to the nature that requires the users to be active and engage to the Internet (Normah, Wan Amizah, Fauziah, Maizatul Haizan & Mohd Helmi, 2013).

Since cyber safety has become prevalent, many countries have initiated programs in related to safety and wellness. In Singapore, the effort has started in schools, by introducing the Cyber Wellness Education. It is guided by a holistic framework which is known as the Cyber

Wellness Framework (Looi, Park, Goh & Wu, 2016). Cyber Wellness Education is planned, implemented according to the suitability of student profiles and school environments. The ultimate goal of Cyber Wellness Education is to equip students with lifelong social-emotional competencies and sound values so that they can become safe, respectful and responsible users of information, communication and technology. The implementation is continued at home by making parents as a partner of the program. The Cyberparenting Guide was developed to support the implementation of the program (Ministry of Education Singapore, 2018). Following the neighbour country, Malaysia has also taken an initiative to promote cyber safety by implementing the cyber education program. However, the program is still new and has yet to be implemented as a major syllabus.

*1. Definition of Concepts*

This paper has briefly defined the concepts in order to have better understanding of the terms used. The definition of concepts are as follows:

*(i) Children*

According to the Convention on the Rights of the Child and the Child Act 2001, children are those who are under the age of 18 (KPWKM, 2015). For the context of this study, children are further categorized into three age groups: children six years and below are pre-school children, seven to 12 years old children are primary school children and children aged 13 to 17 are teenagers.

*(ii) Cyberparenting*

The cyberparenting is referred to "proficiency in digital literacy and digital citizenship while demonstrating the appropriate parenting styles in digital culture" (Mohammad Nizam, 2015)

*(iii) Cyber Safety*

Cyber Safety is a field within the broader context of computer security. It is a branch of computer technology that is applied to networks and corresponding computers. The intention is to limit computer crimes, especially those associated with hacking and identity theft. For example, the cyber safety course taught children to be wary of strangers online.

*2. Cyber Threats*

Cyber threats are a malignant and destructive act that tries to access a computer network through a data communications pathway, without gaining the right authorization or consent from the owners.

*a) Types of Cyber Threats*

There are five types of cyber threats discussed in this paper which are cyberbullying, cyberstalking, cybergrooming, paedophilia, and identity theft. The threats commonly occur in Malaysia.

- Cyberbullying

Cyberbullying is one of the biggest threats facing by teenagers in the world (Hackectt, 2017) that children are threatened, harassed, humiliated, or targeted by other children.

- Cyberstalking

Cyberstalking is a criminal offense for victims using electronic communications such as email or instant messaging (IM) or messages sent to a website or forum. A cyber stalker disguises as an anonymous person to enable him/her to spy on victims [24]. Cyberstalking is performed to scare or harm the victims physically or emotionally (Asiah, Shariffah Nuridah Aishah & Akmal, 1994).

- Cybergrooming

Cybergrooming is defined as the process used by cyber-offenders to make use of their targets by pretending to be friends with children in cyberspace to gain trust until they are unaware they have been used (KPWKM, 2015). de Vaus. (2001) revealed that one out of ten children had been asked to upload their own private photos or videos on the Internet; an increase of 300% of rape cases started with Internet relationships between 2010 to 2015; and 80% of rape cases reported by the victims over the last two years involved Internet acquaintances, and majority of the victims are under the age of 18. The threat of child pornography starts with the threat of cybergrooming.

- Paedophilia

Paedophilia is defined by the American Psychiatric Association as an ongoing sexual interest in children (Seto, Cantor & Blanchard, 2006). According to the Royal Malaysia Police (RMP), 12,987 cases of child sexual abuse cases were reported to RMP between January 2012 and July 2016 and 2,189 cases were successfully filed. However, only 140 were convicted.

- Identity Theft

Identity theft occurs when a person uses personal information of others that is accidentally exposed or stolen. Examples of the information are: name, date of birth, phone number, home address or anything related to personal data. This information is retrieved (without consent) by the cyber-thief for committing fraud or other crimes (KPWKM, 2015). The improvement of the Internet's accessibility has helped the cyber-thief to easily steal information. In Malaysia, there is an increasing trend of identity theft cases: 220, 255 and 262 cases in 2015. 2016, and 2017 respectively.

*b) Cyber Threats Using Social Media*

Statistics of cyber threats have shown an increase from 2012 to 2017, as shown in Table I.

Table I: Cyber threats cases from 2012 to 2017

| **Threat** | **Year** | | | | | |
|---|---|---|---|---|---|---|
| | **2012** | **2013** | **2014** | **2015** | **2016** | **2017** |
| Cyberbullying | 260 | 389 | 291 | 256 | 338 | - |
| Cyberstalking | 300 | 512 | 550 | 442 | 529 | 560 |
| Cybergrooming | 54 | 44 | 60 | 184 | - | - |
| Child pornography | - | - | 60 | 184 | 183 | 117 |
| Identity theft | - | - | 223 | 220 | 255 | 262 |
| Paedophilia | - | - | - | 184 | - | - |

Study from (MCMC, 2017) revealed that 83% of users aged between five and 17 years old are the users of Internet and 93% of them used it through their personal devices. The ownership of personal devices amongst children are common as 85% of the children


E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2019-3502-29

confessed that they own smart phones (Yunos, Ab Hamid & Ahmad Mustaffa, 2017). Most of the users especially children use the Internet to communicate via social media apps, share pictures and videos, watch videos and retrieve information. The findings from the survey, Yunos et al. (2017) found more than 50% of primary school children (6 to 12 years old) have social media accounts. The types of social media accounts they have are social networks, videos, and picture accounts. Almost all secondary school students (13 to 18 years old) have social media accounts (92.47%). The types of social media accounts registered include social networks, picture and video accounts. Students with social media accounts mostly say they registered for interaction purposes (Yunos et al., 2017).

Excessive use of the Internet has a negative impact on children. Previous studies reveal some of the effects are on health, addiction and emotional disturbances (Yunos et al., 2017). Exposure to risky content among children in Malaysia also threatens good values and self-identity (Zakaria, Ahmad Munawar & Noranizah, 2012). According to Nadia (2017), World Internet Statistic revealed the addiction to internet in Malaysia is almost 78% and most of the internet addicts are children and youth.

The wide use of internet has exposed the children the risk of these threats. Parents play an important role in monitoring their children's behaviour in cyberspace and ensuring the safety of children from any cyber threats.

It can be observed in Table 1 that most of the cyber threats cases have increased. The increased use of social media has contributed to the rise of cyberstalking cases. Asiah et al. (1994) asserted that the social media has given opportunity to cyber stalkers as people especially children freely share their information and nobody can forbid from sharing sensitive information with strangers. Moreover, children like to use social media because it is more interactive compared to other applications. Past researches affirmed that the use of social media among children is uncontrollable due to the fast-changing technology, interactive use, and the increase of smart phone or personal devices ownership.

The users of social media have reached 25.08 million in Malaysia and ranked number 9th in the world as active users. The active users refer to users who frequently update their status on social media sites (Ili, 2018). Mahyuddin and Juriah (2017) agreed that personal information can be easily obtained through Instant Messaging (IM) because there is no boundary and control on what to share with the other party. If the user is ignorant or innocent (easily trust people) on how to use the IM safely, then the possibility to share personal information is high.

Table I also shows a sharp increment in child pornography cases: 60 cases in 2014 and the number of reported cases tripled in the following year. Similarly, cybergrooming cases saw an increase of 124 cases in 2015 from 60 cases in the previous year. A similar number of cases in child pornography and paedophilia was reported in 2015. Nadia (2017) affirmed that there is a relation between child pornography and paedophilia cases. Three threats were intertwined: cybergrooming, child pornography and paedophilia. It begins with cybergrooming, to groom the children before they become the victims of paedophilia. The paedophile likes to watch child pornography which is one of the paedophile traits.

Hence, children are at the risk of being exposed to such threats due to the lack of understanding and parental knowledge of these threats. There is an interest in raising parents' awareness and knowledge on cyberspace skills to address the increase of cyber threat cases. Awareness and understanding of cyber threats against children among parents can help to save children from becoming victims.

*3. Bring Your Own Device*

According to Malaysian Ministry of Education, Bring Your Own Device (BYOD) to school program will be proposed and implemented to increase the quality of teaching and learning. The initiative is carried out in conjunction with the growth of technology to assist teaching and learning in schools. Many of the developed countries such as the United States of America, United Kingdom and Australia have implemented BYOD. Recently, Singapore has jumped on the same bandwagon to allow students bring their own devices i.e. the laptop or tablets excluding handphones to schools. These devices must have internet connection and register to the school as personal belonging.

In support of the proposed policy implementation, the role of parents should be strengthened to enable the continuation of mobile devices for formal learning of children to be continued at home. Education is the foundation of the every generation. Parents need to play a more serious role in educating children to prepare them to be knowledgeable, ethical and responsible digital citizens while at the same time keeping them safe from cyber threats that can jeopardize them.

The use of internet or cyber-use is aggressive among Malaysian children. This group has been exposed to the cyber-use from a very young age, with device ownership from as early as seven (7) years old. Parental role is crucial in monitoring online activity and establishing child's self-identity in the cyber-use due to the presence of cyber threats and risks (Wan Anita, 2016). This rapid and dynamic technology development requires a specialized education regarding cyber-use. In addition, parents need to be aware of the various cyber threats and increase the knowledge in technology utilization so that the threats can be addressed more effectively.

## METHODOLOGY

This study employed a quantitative approach by means of survey and online questionnaire for data collection. The respondents involved were 872 parents of children below 17 years old. This study aims to answer the following questions:

- What is the level of parental awareness of cyber threats at home?
- What is the level of parental readiness for the use of personal devices for formal learning of children? This question is to identify parents' readiness for the initiative of the Bring Your Own Device to school program.

*a. Research Hypothesis*

There are two hypotheses that were formulated to investigate two scenarios which are:
First hypothesis, there is no significant relationship between parents' awareness of cyber threats with cyber safety at home.
Second hypothesis, there is no significant relationship between the role of the school in educating parents with parental readiness to the use of personal devices for formal learning of children.

*b. Research Design*

This descriptive study uses quantitative approaches adapted from Creswell's design framework. A survey was used to collect data from respondents consisting of parents throughout Putrajaya. The study has three phases/levels: the preliminary study, the pilot research for validity and reliability and the actual study/discovery. Table II depicts the research design for this study.


E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2019-3502-29

Table II: Research design

| No | Phase | Objective/Activities | Output |
|---|---|---|---|
| 1 | Preliminary study | To identify issues and problems | Problem statement |
| | | Determine the purpose of the study | Research objective |
| | | Determine the scope of the study | Scope of the research |
| | | Review the results of relevant research from previous researchers, involving model theory, factors influencing cyber safety | A comprehensive literary study on children's Internet use at home |
| | | Design research instruments | Study instrument is developed |
| 2 | Pilot research | Verify and finalize the research instrument | Reliable research instrument |
| 3 | Actual study / discovery | Implement an online survey | Data collection from survey |
| | | Analyze collected data using SPSS | Respondent profiling and descriptive statistics results |

Phase one is a preliminary study focusing on the issues, research objectives and scope of research involving activities to identify issues, objectives, scope and purpose to study the findings of relevant research studies through literature studies that are in line with the research questions and the development of research instruments. Information related to the theory, model and implementation framework are sought in indexed journals through the UKM Digital Library, UKM Journal System, IEEExplore, Google Scholar Database and other related articles. Expert groups from various ministries and departments were also called upon to highlight the status of implementation of department initiatives and implementation issues to give a clear picture of what has been studied.

The second phase of the pilot study (validity and reliability) involved the evaluation of the instrument implemented before being distributed to the actual respondents by executing reliability testing and getting recommendations from experts. Through the pilot study, legitimate and reliable research instruments were produced. This approach was taken to improve the accuracy of the research findings.

The third phase is a real study or findings involving the implementation of a survey on parents' respondents. Data collected from surveys conducted was analyzed using SPSS, Survey Monkey, Microsoft excel and other software related to home-level cyber-use and important factors affecting safe cyber-use among children in the home.

The questionnaire was a standard form that provided 71 questions to the respondents. It was organized by specific sections and spaces and it was also logical, scientific and specialized. The form of questions asked to respondents was structured (closed) and guided where the answers were accurate or closest to the questions or questions asked by the respondent. This method is easier to code and analyze directly based on the questionnaire.

The level of parental awareness and parental readiness can be measured and determined based on the indicators as shown in Table III.

Table III: Indicator Level Based On Mean Score

| No | Mean Score | Level |
|---|---|---|
| 1 | 4.00 – 5.00 | High |
| 2 | 3.00 – 3.99 | Medium/Average |
| 3 | 2.00 – 2.99 | Low |
| 4 | 1.00 – 1.99 | Very Low |
| 5 | 0.00 – 0.90 | Not Available |

## RESULTS AND DISCUSSION

This paper discusses the findings in three parts. The first part is the level of parental awareness and its correlation with cyber safety at home. The second part is dedicated to the parental readiness towards personal device for formal learning in schools. The third part discusses on the conclusion to correlate between cyber parenting and cybersafe at home.

### *i. First Part: The Level of Parental Awareness and Its Correlation with Cybersafe at Home*

The Table IV shows that 80.9% of the parents were aware on the cyber threats towards their children. According to the respondents, there are many mechanisms to control and monitor their children's online activities, including software parental control; discussions among parents; or attend to talks provided by CyberSecurity Malaysia. Ghazvini and Shukur (2016) also affirmed that the threats can be minimized via awareness training program. On the contrary, 68.6% respondents admitted most of them have yet to attend any talks regarding cyber awareness, and 31.4% of them have attended the talk. About 68.6% of the respondents who went to the talk felt satisfied with the program, while 31.38% respondents were not satisfied and felt the contents were not sufficient.

The respondents were also asked whether they were aware on the existing Acts that are related to cyber laws such as Computer Criminal Act 1997, Digital Signature Act 1997, Multimedia and Communication Act 1998, and Copyright Act 1997. Most of them knew the existence of Multimedia and Communication Act (52.06%); Digital Signature Act (13.3%); and Copyright Act (23.50%). Surprisingly, 39.10% of the respondents did not know any of the Acts, which is worrying due to the advancements of technology. If the parents do not realize the laws to curb, control and convict the illegal activities, the tendency to get fair treatment is significantly low. This finding is in parallel with report from the Royal Malaysia Police on paedophilia activity, which out of 12,987 cases were reported, only 140 were successfully convicted.

Table IV: Parental awareness on cyber safety

| Item | Level of Agreement (Percentage) | | | | |
|---|---|---|---|---|---|
| | SDA | DA | MA | A | SA |
| I'm aware of cyber threats towards my children | 2.2 | 2.6 | 14.7 | 61.6 | 18.9 |
| I'm aware of my children's online activities | 1.8 | 4.8 | 27.8 | 50.3 | 15.3 |
| I'm aware that my children use the Internet the right way | 1.5 | 9.5 | 34.7 | 45.2 | 9.1 |
| I'm aware of difficulty to control my children's Internet consumption | 1.9 | 6.9 | 24.8 | 45.1 | 21.3 |

Legend: SDA – Strongly Disagree; DA – Disagree; MA – Moderately Agree; A – Agree; SA – Strongly Agree.


E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2019-3502-29

Table V depicts the level of parental awareness. The respondents were at a medium level of awareness on their children's online activities and cyber threats towards their children. They also claimed that their children used the Internet in the right way although they felt it was difficult to control the children's Internet consumptions. Since the parents admitted they could not control their children Internet consumptions, this can lead to Internet addiction, which needs to be addressed at an early stage before exposing the children to other cyber threats. Addiction to Internet is harmful, and the extreme case was reported that addiction could lead to depression and suicide

Table V: Level of parental awareness based on mean score

| Item | Mean Score | Std Deviation | Level of Awareness |
|---|---|---|---|
| I'm aware of cyber threats towards my children | 3.92 | 0.80 | Medium |
| I'm aware of my children's online activities | 3.71 | 0.84 | Medium |
| I'm aware of difficulty to control my children's Internet consumption | 3.77 | 0.93 | Medium |
| I'm aware that my children use the Internet the right way | 3.51 | 0.84 | Medium |

The Table VI discusses on the relationship between parental awareness and cyber safety at home (refer to the First Hypothesis).

The result shows that there is a significant relationship between the level of parental awareness of cyberspace with cyber safety at home. If the parents were aware of the cyber threats, then they can control their children at home and the risks of exposing to the threats can be minimized.

Therefore, the parental awareness of cyber threats is important and should begin at home.

Table VI: Correlation between parental awareness and cyber safety at home

| Item | Cyber Safety at Home | |
|---|---|---|
| | Correlation (R) | *P Value |
| Parental awareness of the cyber threats | 0.559 | 0.000 |

*ii. Second Part: The Level of Parental Readiness and Its Correlation with Bringing the Personal Device for Formal Learning at School*

Malaysia has acknowledged that technology can optimize the student's learning at school and has proposed an initiative of Bring Your Own Device to school. Findings tabulated in Table VII show that the level of parent's readiness on the proposition is still low and they feel burdened if the plan is carried out. However, the respondents also believed if the government wants to proceed with the plan, they are more comfortable if the network is provided by the school due to safety reasons and the ease of control. The security control to monitor a student's online activities must be enforced to gain parents' confidence and readiness.

Table VII: A proposition of bring your own device to school based on mean score

| Item | Mean Score | Std Deviation | Level of Readiness |
|---|---|---|---|
| I prefer to use the network services provided by schools | 3.97 | 0.97 | Medium |
| School needs to a provide better relation with the parents to increase cyber security awareness | 3.82 | 0.86 | Medium |
| I agree to subscribe to parental control function | 3.63 | 1.04 | Medium |
| I agree to buy the device for children's learning activities | 3.28 | 1.09 | Medium |
| I'm satisfied with school's information on cyber security | 3.27 | 0.92 | Medium |
| I feel burdened with the proposition | 2.85 | 1.20 | Low |
| I agree with government proposition to bring your own device at school | 2.82 | 1.29 | Low |

The Table VIII discusses on the relationship between parental readiness and its correlation to bring the personal device at school for the purpose of formal learning (refer to the Second Hypothesis).

Result shows that there is a significant relationship between the role of the school in educating parents with the level of parental readiness to the use of personal devices for formal learning of children. Hence, if the schools insist on implementing Bring Your Own Device at school, then they must provide a conducive network, mechanism to control and monitor students' online activities and proper security measures to protect the children.

Table VIII: Correlation between school roles to improve parental awareness on bring your own device for formal education

| Item | Parental Awareness on BYOD for Formal Education | |
|---|---|---|
| | Correlation (R) | *P Value |
| School roles to improve the parental awareness | 0.508 | 0.000 |

*iii. Third Part: The Cyberparenting and Cybersafe are Interrelated*

The third part of this discussion is dedicated to reveal the connection between cyberparenting and cybersafe at home.

Table IX is tabulated to identify whether the parents have set rules for their children's use of internet and personal device. The findings show that, majority of the parents (85.4%) have agreements with their children when they give the personal device, and 88.6% of them have set rules for internet use. A juxtaposition of results shows that only some of them (56.3%) realized of the importance to keep the children's password. If the parents do not know the password, they cannot access the children's device, consequently they cannot monitor and control their children's online activities. The children can manipulate the trust given if they know their parents cannot access the devices. Thus, it is crucial for the parents to keep all the passwords, and monitor their children's online activities frequently.


E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2019-3502-29

Table IX: Cyber-use Basic Rules at Home

| Item | Yes % | No % |
|---|---|---|
| I set rules for Internet use at home | 88.6 | 11.4 |
| I have agreement with my children when I give the personal device | 85.4 | 14.6 |
| I keep all the passwords from my children's devices | 56.3 | 43.7 |

It is also a proven that cyberparenting and cybersafe are interconnected as shown in the Table X where the correlation exists and is significant. Moreover, Looi, Park, Goh & Wu (2016) also affirmed that the lack of knowledge and skills in technology and Internet services are often the main reason why concerned parent remain helpless in raising digital era children. The generational divide between the parents and children has caused the parents to not fully understand the associated cyber threats. The concerned parents are not fully aware of the needs for digital literacy and the importance of cyberparenting although cyberparenting can influence the cyber safety at home. Efforts from the parents are more demanding to ensure their children are safe especially from cyber threats.

Table X: Correlation between cyberparenting and cyber safety at home

| Item | Cyber safety at Home | |
|---|---|---|
| | Correlation (R) | *P Value |
| Cyberparenting | 0.170 | 0.000 |

* Significance Value P<0.05

## LIMITATION AND SUGGESTION

The data, as collected by the survey, are considered limited as they only apply to parents in mainstream schools. This study provided information about some parents and not all of them; parents in private, international, homeschool or special education schools are not included. Such schools should be included in future studies in order to create a more comprehensive scope towards developing a national module for cyber parenting in Malaysia.

## CONCLUSION

This paper is a crucial study to seek the level of parental awareness towards cyber threats which consequently can determine the correlation between the awareness and cybersafe at home. The context of this study is focused to the Malaysian environment where the country is still in developing mode and eager to embrace technologies to become a developed nation.

Nonetheless, the parental awareness is still at the medium level, which is not sufficient to protect the children from cyber threats. The efforts to raise awareness and parental knowledge for parents in the field of cyber security are deemed necessary. This is because, without awareness and knowledge, parents cannot apply skills to protect their children efficiently and effectively. Programs to increase the parental awareness should be implemented widely and openly to promote for cyber safety. The parental readiness to use the Bring Your Own Device/personal device for the formal learning should also be improved by promoting technology as one of the effective learning methods. This effort must be in parallel with the cyber safety promotion to ensure the children safety is not compromised particularly when using the Internet.

ACKNOWLEDGEMENT

We would like to thank Universiti Kebangsaan Malaysia for financial support through grant DCP-2017-013/6.

BIODATA

*Nazilah Ahmad@Ahmad Arifin* was a Master's student at the Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia. She currently works at the Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU). Email: Gp04717@siswa.ukm.edu.my

*Umi Asma' Mokhtar* is a senior lecturer of information science at the Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia. Her research interests are Electronic Records Management, Function-based Classification, and Information Policy. Currently, she is the co-researcher of InterPARES Trust project for Malaysian Team and a member of the Information Governance Lab, FTSM, UKM. Email: umimokhtar@ukm.edu.my

*Zaihosnita Hood* is a lecturer at the Faculty of Information Science and Technology in Universiti Kebangsaan Malaysia. Her research interest is Human Computer Interaction. She is one of the principal researchers in the Information Systems Lab, under the Center for Software Technology and Management, FTSM, UKM. Email: zaihosnita@ukm.edu.my

*Dr. Sabrina Tiun* is a senior lecturer at the Faculty of Information Science and Technology in Universiti Kebangsaan Malaysia. Her range of research interests are from Natural Language Processing to Speech Processing and Information Retrieval. She is a member of the Knowledge Computing research group, under the Center for Artificial Intelligence Technology, FTSM, UKM. Email: sabrinatiunh@ukm.edu.my

*Dr. Dian Indrayani Jambari* is a Senior lecturer at the Faculty of Information Science and Technology (FTSM) in Universiti Kebangsaan Malaysia (UKM). Her range of research interests are from Information Systems Management to Business IT Strategic Alignment. She is one of the principal researchers in the Information Systems Lab, under the Center for Software Technology and Management, FTSM, UKM. Email: dian@ukm.edu.my


E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2019-3502-29

REFERENCES

Andreassen, C. S., & Pallesen, S. (2014). Social network site addiction – An overview. *Current Pharmaceutical Design*, 20(25), 4053-4061.

Asiah Bidin, Shariffah Nuridah Aishah Syed Nong Mohamad, Akmal Mohamad. (1994). *Intipan siber: Jenayah baru dalam masyarakat kontemporari.* Retrieved from https://journal.unisza.edu.my/jimk/index.php/jimk/article/view/134

Byrne, S., Katz, S. J., Lee, T., Linz, D., & McIlrath, M. (2014). Peers, predators, and porn: Predicting parental underestimation of children's risky online. *Journal of Computer-Mediated Communication*, 19(2), 215-231.

de Vaus., D. A. (2001). *Research design in social research.* Thousand Oaks: SAGE.

*DIGI*. (2018). Retrieved from GuidetoFamilyFriendlyInternet_BM.pdf

Ghazvini, A., & Shukur, Z. (2016). Awareness training transfer and information security content development for healthcare industry. *International Journal of Advanced Computer Science and Applications*, 7(5), 361-370.

Hackectt, L. (2017). *The annual bulllying survey 2016.* Retrieved from https://www.ditchthelabel.org/research-papers/the-annual-bullying-survey-2016/

Ili Hadri Khalil (2018, Januari 30). *Malaysia negara ke-9 paling aktif media sosial, ke-5 paling ramai guna e-dagang - Laporan. Astro Awani Online*.

KPWKM. (2015). *Pelan tindakan perlindungan kanak-kanak dalam dunia siber*. Putrajaya: Kementerian Pembangunan Wanita, Keluarga dan Masyarakat.

Livingstone, S. & Haddon, L. (2012). *EU Kids Online: Final Report*. LSE, London: EU Kids Online.

Livingstone, S. (2007). Strategies of parental regulation in the media-rich home*. Computers in Human Behavior*, 23.

Looi, C.-K., Park, Y., Goh, J., & Wu, L. (2016). Affecting children's ability to understand other's feelings through an online cyber-wellness programme. *ICCE 2016 - 24th International Conference on Computers in Education: Think Global Act Local - Main Conference Proceedings.*

LPPKN. (2013). *How Internet and communication technologies affect both family and society*.

Mahyuddin Daud, & Juriah Abd Jalil. (2017). Protecting children against exposure to content risks online in Malaysia: Lessons from Australia*. Jurnal Komunikasi: Malaysian Journal of Communication*, 33(1).

Marshall, I. A., & Jackman, G. A. (2015). Parental involvement, student active engagement and the 'secondary slump' phenomenon — Evidence from a three-year study in a Barbadian Secondary School. *International Education Studies*, 8(7), 84-96.

MCMC. (2017). Kawalan Teknologi ke atas Capaian Internet dan Pelaksanaan Program Klik dengan Bijak.

Ministry of Education, Singapore. (2018). *Cyber wellness: What is cyber wellness?*. Retrieved from https://www.moe.gov.sg/education/programmes/social

Mohammad Nizam Kassim. (2015). *The 5 strategies to effective cyberparenting.* Malaysia: Senior Analyst Cyber Safety, Outreach Division, CyberSecurity Malaysia.

Muhammad Adnan Pitchan, Siti Zobidah Omar, Jusang Bolong, & Akmar Hayati Ahmad Ghazali. (2017). Analysis of cyber security from the perspective of social environment: A study of Internet users in Klang Valley. *Journal of Social Sciences and Humanities,* 12(2), 16-29.

Nadia Hamid. (2017, Oktober 22). Remaja, kanak-kanak ketagihan Internet serius. *BH Online*.

Normah Mustaffa, Faridah Ibrahim, Wan Amizah Wan Mahmud, Fauziah Ahmad, Chang Peng Kee, & Maizatul Haizan Mahbob. (2011). Diffusion of innovations: The adoption of Facebook among youth in Malaysia. *The Innovation Journal: The Pulic Sector Innovation Journal,* 16(3), 1-15.

Normah Mustaffa, Wan Amizah Wan Mahmud, Fauziah Ahmad, Maizatul Haizan Mahbob & Mohd Helmi Abd Rahim. (2013). Kebergantungan Internet dan aktiviti online remaja di Lembah Kelang*. Jurnal Komunikasi: Malaysian Journal of Communication,* 29(1).

O'Brien, W.. (2014). Australia's digital policy agenda: Adopting a children's rights approach. *Int. J. Child. Rights*, 22, 748-775.

Seto, M. C., Cantor, J. M., & Blanchard, R. (2006). Child pornography offenses are a valid diagnostic indicator of pedophilia*. J. Abnorm. Psychol.,* 115(3), 610-615.

SKMM. (2017). Inisiatif - Inisiatif advokasi Suruhanjaya Komunikasi dan Multimedia Malaysia. Retrieved from http://www.klikdenganbijak.my/Landing-Page.aspx

Smith, A., & Anderson M. (2018). Social media use in 2018. Pew Research Center: Internet and technology. Retrieved from https://www.pewinternet.org/2018/03/01/social-media-use-in-2018/

*Utusan Online* (Rencana). (2017). Melindungi anak daripada ancaman siber. Malaysia: MCMC. Retrieved from http://www.utusan.com.my/rencana/melindungi-anak-daripada-ancaman-siber-1.489136

Valcke, M., Bonte, S., de Wever, B., & Rots, I. (2010). Internet parenting styles and the impact on Internet use of primary school children. *Computers & Education*, 55(2), 454-464.

Wan Anita Wan Abas, & Azizah Hamzah. (2013). Media dalam kehidupan dan perkembangan kanak- kanak. *Malaysian Journal of Media Studies,* 15(2), 27-39.

Wan Anita Wan Abas. (2016). Hubungan antara gaya keibubapaan dengan penggunaan Internet kanak-kanak. *Global Media Journal – Malaysian Edition*, 6(1), 15-30.

Yunos Zahri, Ab Hamid R. Susanty, & Ahmad Mustaffa. (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).

Zakaria Stapa, Ahmad Munawar Ismail, & Noranizah Yusuf. (2012). Faktor persekitaran sosial dan hubungannya dengan pembentukan jati diri (Social environmental factors and their relation to identity formation). *Jurnal Hadhari: An International Journal,* Special Edition 2012*.*


E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2019-3502-29