https://doi.org/10.31436/ijpcc.v9i2.406

SmartParents: Empowering Parents to Protect Children from Cyber Threats

Nurul Nuha Abdul Molok*, Nur Aiena Hajeerah Abdul Hakim, Nur Syazwani Jamaludin

Department of Information Systems, International Islamic University Malaysia, Malaysia.

*Corresponding author: nurulnuha@iium.edu.my

(Received: 23rd April 2023; Accepted: 20th May 2023; Published on-line: 28th July 2023)

Abstract— In today's interconnected world, parents and children face cyber safety and security issues and are exposed to cyber threats. During and after the COVID-19 pandemic, cyber safety and security cases are on the rise affecting people of all ages. During the movement control orders (MCO), children were given electronic gadgets to participate in online learning. Although there is no MCO and online learning anymore, children are still reliant on these gadgets, affecting their studies, health and safety. This study covers cyber threats that are happening to children and what can parents do about such threats to protect their children. It proposes educating parents about cyber safety and security through a web-based application prototype. Surveys were done to understand the actual cyber threats that were faced by both parents and children in order to collect user requirements for the development of the prototype. Findings suggest that such applications can help parents to recognise cyber threats that can happen to their children. The developed prototype may guide parents to implement cyber safety and security controls and protect their children from cyber threats such as cyberbullying, sexual grooming and gaming disorder.

Keywords— cyber safety, cybersecurity, cyber parenting, cyberbullying, gaming disorder, children.

I. Introduction

Cyber threats on children have been one of the significant concerns among parents especially after the COVID-19 pandemic. As children rely on electronic gadgets, such as smartphones, tablets and laptops, more than before, cyber safety and security cases of children becoming the victims of cyber threats continue to rise. To make this worse, many parents tend to share a lot of content online, including photographs and videos of their children, with and without clothes. These contents attract cyber paedophiles from all over the world, making Malaysia the top country in South East Asia for online child pornography [1]. According to United Nations Children's Fund (UNICEF) [2], 100,000 children in Malaysia are being sexually exploited by cyber predators. These cyber paedophiles are exploiting and manipulating young girls below 18 years old in social media by giving them gifts before exposing them to pornographic content and actions ([2],[3]). Other than that, Malaysia ranked second in Asia for cyberbullying among youth based on the UNICEF report and cyberbullies perform this behaviour in order to seek attention since they are lacking of affection from family members [4]. Victims of cyberbullying experience suicidal thoughts and behaviour, suffer from anxiety disorder and affect their academic performance [5]. Additionally, children have been spending too much time on gadgets playing online games. World Health Organization (WHO) has declared gaming disorder as an official medical condition, since "...gaming behavior shifts into a disorder when it takes precedence over other daily activities, and starts to impair a person's relationships, school or work responsibilities for at least a year." [6].

According to [7], other than sexual grooming, cyberbullying and gaming disorder, children are also susceptible to cyber stalking, identity theft, social issues such as isolation and loneliness, and also legal issues like being an accidental outlaw due to the disclosure of sensitive information on social media. Realizing that there are so many cyber threats that have huge impacts on children, authorities are urging parents to be more vigilant about monitoring their children while they are online ([3], [7]).

Thus, this study focuses on the role of parents and what they can do to combat cyber threats to their children. It starts with the introduction to the contemporary phenomenon, followed by review of literature on cyber parenting, different types of cyber threats that can happen to children, cyber threats that can happen to adults, and security controls that can be adopted to mitigate these threats. Then, it presents the research methodology and findings of a survey on parents and how our developed web-based application prototype can help parents to protect their children and also themselves from cyber threats. Finally, it concludes the article with recommendations to address cyber threats to both parents and children.

https://doi.org/10.31436/ijpcc.v9i2.406

II. Review of Literature

Reviews of literature were done to understand about cyber parenting, cyber threats that are faced by parents and children, and how parents can mitigate these threats.

A. *Cyber Parenting, Cyber Safety and Cyber Security*

Cyber parenting is defined by [8] as "proficiency in digital literacy and digital citizenship while demonstrating the appropriate parenting style in digital culture" [8]. While the study agrees with this definition, it defines cyber parenting as the roles of parents in mitigating cyber threats to children through cyber safety and security controls. Following this definition, cyber safety and security consist of two terminologies which are cyber safety and cyber security. Although other studies may use the two terminologies interchangeably, this study begs to differ since they are actually quite distinct. Hence, it adopts the definition of cyber safety from [7] which means "the protection of people's privacy, physical, mental and emotional wellbeing, through safe and responsible use of Information and Communication Technology (ICT)". On the other hand, it refers to cyber security as "the protection of ICT infrastructure which includes data, hardware, software, and networks in order to preserve the confidentiality, integrity and availability of information and information processing facilities" [7].

In today's world that is becoming more interconnected especially after the pandemic, the number of internet users, especially children, are on the rise. With the surge of cyber threats to children, parents are urged to be vigilant about monitoring their children's use of Internet and electronic gadgets ([3],[7],[8]). This study posits that parents must update their knowledge about the current cyber threat landscape and understand how to address these threats through cyber safety and security controls.

B. *Cyber Threats*

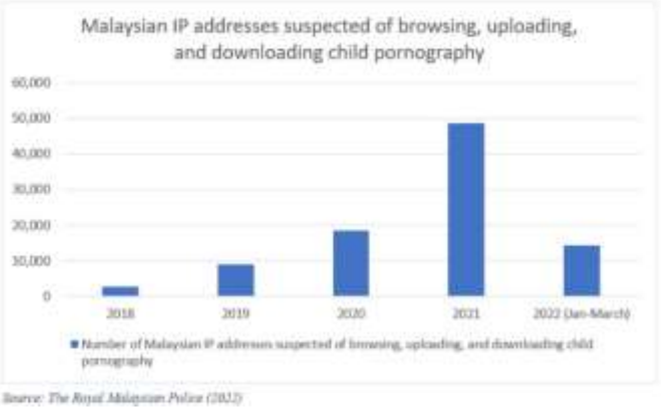
This study suggests that parents should understand not only the cyber threats that can happen to their children, but they themselves need to understand about cyber threats than can happen to them. They need to empower themselves with cyber safety and security, so that they can protect themselves in order to protect their children from cyber threats.

There are many types of cyber threats from the literature, however, this study lists them as "cyberbullying, sexual grooming, pornography, internet addiction, malware attacks, leakage of sensitive information, and physical and mental health due to computers and Internet use" [7] which is in line with findings from [8]. This study focuses on the top three cyber threats which are cyber paedophilia, cyberbullying and gaming disorder. The following subsections detail each of them:

1) *Cyber paedophilia*

Following [7]'s definition of paedophilia, this study defines cyber paedophilia as ongoing sexual interest in children and/or sexual exploitation of children through virtual contents. As many children engage on various online activities through social media and online games, paedophiles are using these virtual platforms to perform sexual grooming and accessing child pornography ([3],[7],[8]). While parents are exposing photographs and videos of their children on social media, they are actually putting their children at risk since this may attract paedophiles to collect information about children ([3],[8],[9]). During the first quarter of 2022, there were 93,368 IP addresses detected in Malaysia which are related to cyber paedophilia activities since 2017 until 2022 [9], making Malaysia number 1 in Southeast Asia for online child pornography [2], as highlighted earlier.

In line with [10]'s findings, it is alarming to discover that oversharing of children's contents by their own parents causes these children to be "blackmailed to engage in sexual activities, having their sexual images shared without permission, or being coerced to engage in sexual activities through promises of money or gifts" [2]. Do we want our children to become the victims of these cyber paedophiles? Of course not, therefore, this study suggests that parents must be aware of all these dangers that can happen to the children and stop sharing contents of their children online.



Source: The Royal Malaysian Police (2022)

Fig. 1 Malaysian IP Addresses suspected of browsing, uploading, and downloading child pornography [9]

2) Cyberbullying

Once again, Malaysia is in the limelight for the wrong reason as it is ranked second in Asia for youth cyberbullying. ([4],[11]). [11] states while there are no standard definition for cyberbullying, UNICEF defines cyberbullying as "bullying with the usage of digital technologies that can take place on social media, gaming platforms, messaging platforms, and mobile phones". [4] reports that cyberbullies who perform this behaviour often lack of love and affection by their family and they bully to seek attention from their family and the society. Cyberbullying is more dangerous than physical bullying since the latter causes visible bruises that can be noticed by parents while the former does not. It causes victims to be in constant fear of being vulnerable, harassed, shamed and targeted by the bully [8]. Two notable cyberbullying cases in Malaysia are the 20-year-old who hanged herself after her TikTok video went viral and the 16-year-old who jumped from a roof of a building after online friends voted for death in her Instagram poll [11]. Parents are urged to be aware of such cases, monitor their children's online and offline behaviours, advise their children not to respond to cyberbullies' messages and remind children to report to parents or teachers if they received those messages.

3) Gaming Disorder

According to the Ministry of Health Malaysia, Internet Gaming Disorder has become a serious problem that can be considered as a psychiatric disorder under Section III in the Diagnostic and Statistical Manual of Mental Disorder (DSM-5). Similarly, [7] reports that the World Health Organization (WHO) has declared gaming disorder as an official medical condition. Its addiction level is similar to alcohol and drugs, it can increase aggression and dopamine effects (which influence gaming desire), and reduce prosocial behaviour (empathy and good behaviour) among children [7]. However, this study does not posit that online games should be stopped because there are advantages of playing online games since it improves children's reading, mathematics and analytical skills [7].

This study proposes parents to monitor children's use of electronic gadgets and mobile devices and advise their children to play online games according to the games rating that is right for their children and make informed choices as recommended by the Entertainment Software Ratings Board (ESRB - a self-regulatory organization that assigns age and content ratings to consumer video games in the United States and Canada).

III. Review of Existing systems

This study highlights the role of parents in combatting cyber threats to their children. Parents must be empowered with the knowledge in contemporary cyber threats that can happen to their children and mitigating actions that they can perform to address these threats. While awareness programs through talks, news articles, reminders through digital media may influence parents to be more alert about such threats, their coverage and exposure are limited. Hence, this study proposes a web-based application system called SmartParents that is available online to educate parents about cyber safety and security.

In order to develop this application, reviews on the similar existing application were done to understand and compare their functionalities. The best five applications that were reviewed are Internet Safety 101, CyberWise, CyberParent, Idaho Cybersecurity and ThinkUKnow. The summary of each application is provided below:

A. *Internet Safety 101*

It provides a compact interface on each topic. It has comprehensive contents and it shows each threat along with the statistics of cases and how to control them. Under the 'Social Media' topic, there is a list of social media and it provide guidance on how each platform works.

B. *Cyberwise*

CyberWise website has a great interface that makes it easy for users to use it. However, some of the contents are limited for children.

C. *CyberParent*

CyberParent website offers learning materials, practicing and a help tab that provide related articles about cybersecurity. It is also equipped with voiceover on each functionality.

D. *Idaho Cybersecurity*

The fourth existing system is the Idaho Cybersecurity that offers content to multiple groups of users including children, parents, senior citizens and employees. They provide short quizzes for senior citizens and children. There are also videos and games to get the children to interact. They provide online courses for employees to attend cybersecurity classes.

E. *ThinkUKnow*

ThinkUKnow web application provide contents according to age range. There are sections on videos, games and questions for people in different ages to interact and ask questions.

Table 1 sums up the features of the five web applications versus the features that are included in SmartParents, our proposed web application.

TABLE I
SUMMARY OF SYSTEM REVIEW

Web App	Features			
	Log In	*Quiz / Assessment*	*Content for Different Age Range*	*Cyber Threats & Controls*
Internetsafety 101	Yes	No	No	Yes
Cyberwise	Yes	No	No	Yes
Cyberparent	No	Yes	No	Yes
Idaho Cybersecurity	Yes	Yes	No	Yes
ThinkUKnow	No	Yes	Yes	Yes
SmartParents	Yes	Yes	Yes	Yes

IV. METHODOLOGY

A. *User Requirements*

This study employed the snowballing technique which is a sampling method where existing subjects provide referrals to recruit new samples that are required for a study. In this study, an online survey was conducted on parents as the targeted users of the proposed web application. The online survey was done using Google Form and distributed among parents during the the project planning phase. The aim of the survey was to find out about examples of cyber threats that parents had experienced and their feedback on having a website application to educate parents about cyber safety and security among children.

As for the data collection instrument, a total of 20 questions were included in the Google Form as questionnaires. A total of 35 respondents' feedbacks were successfully recorded.

B. *System Development*

For the purpose of developing the application, the agile software development lifecycle approach was used. The development process started with an initial planning and ended with the deployment and maintenance of the application. The agile software development method consists of planning, designing, developing, testing, release and maintenance. It is an iterative approach to software development and project management that offers value to the users more quickly and with fewer difficulties. Additionally, this approach is equipped with feedback and continuous improvement.

V. FINDINGS AND DISCUSSION

Among the 35 respondents, 71.4% were females and 28.6% were males. Majority of the respondents (88.6%) had their tertiary education as their level of education. The respondents were asked what they use the Internet for and the result showed that 94.3% of them used the Internet to get information and news, 88.6% for social media and 85.7% for communicating with friends and family.

It is interesting to note that, the respondents had experienced a variety of cyber threats. As shown in Fig.2, most respondents (77.1%) had experienced online scams via messaging applications particularly through WhatsApp and Telegram. 74.3% of them had received fake news, 54.3% experienced malicious software (malware) attacks, 8.6% which is 3 respondents had their computers being hacked, only 1 respondent (2.9%) experienced love scam.

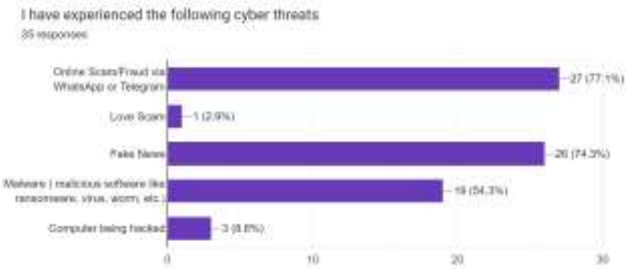


Fig. 2 Examples of cyber threats experienced by the respondents

It was good to know that most respondents (91.4%) understood about cyber safety and security and 94.3% of the total respondents stated that they would use a web-based application to enhance their understanding. When asked about what did they expect to learn from the application, 80% stated that they wanted to know about how to implement security controls and 71.4% wanted to know about cyber threats. These findings validate the need of having a web-based application that can educate parents about cyber safety and security. These results are in line with the study by [8] which highlights the significant relationship between the level of cyber safety awareness among parents and controlling their children's use of the Internet. The more they are aware of cyber threats, the risks to their children can be minimized.

They were also asked about their children's use of the Internet particularly, the devices that their children use and how long their children spent their time using social media and playing games. Most children used smartphones (74.3%), followed by tablets (54.3%), 28.6% used laptops and only 1 parent (2.9%) did not allow his/her children using the Internet. These results are very common among today's children and in line with [7] and [8] in which most children prefer the use of smartphones while accessing the Internet.

Fig.3 and Fig.4 below show the number of hours their children spent on social media and playing games consecutively. In terms of using social media (Fig.3), 40% of the respondents informed that their children spent 1-2 hours, 37.1% said 3-5 hours, 14.3% less than 1 hour, and 8.6% more than 5 hours. For playing online games, Fig.4 depicts that 37.1% of the respondents stated that their children spent less than 1 hour for playing online games, 31.4% between 3-5 hours, 20% 1-2 hours and 11.4% more than 5 hours. The only concern that the researchers had about this is, how much did these parents really know about how many hours their children were using the social media and playing online games? This is because, studies done by [7] and [8] proved that children are move tech-savvy than their parents and therefore their children's use of the Internet may be overlooked. Hence, parents must be prepared to educate themselves so that they are able to protect their children in this challenging cyber world.

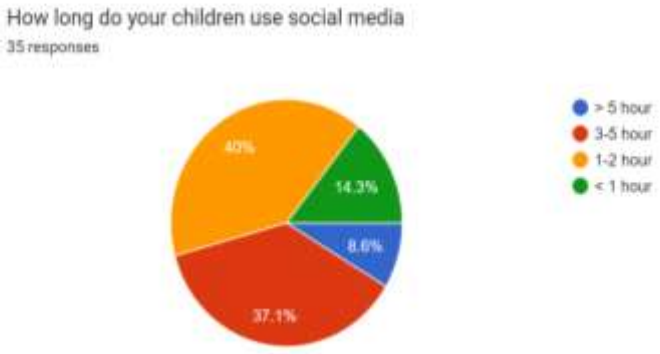


Fig. 3 The number of hours children used of social media

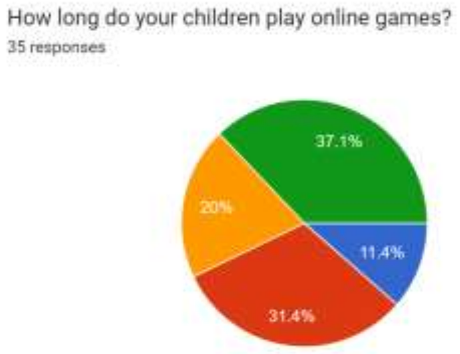


Fig. 4 The number of hours children played online games

Additionally, the parents were asked about what kinds of cyber threats that their children had experienced. Fig.5 illustrates that, most parents which is 51.4% of the respondents admitted that their children were addicted to online games, 40% said that their children were exposed to violent content, 34.3% addicted to social media, 31.4% exposed to sexual content and 11.4% or 4 respondents specified that their children were cyberbullied. It is surprising to note that 3 out of 35 respondents (8.6%) admitted that their children had met online strangers in person. The results portrayed that most parents were aware of the problems that were faced by their children due to the use of social media and playing online games. The thought that majority of them were ready to learn more about cyber safety and security was a relief and a way forward to combat cyber threats to children.

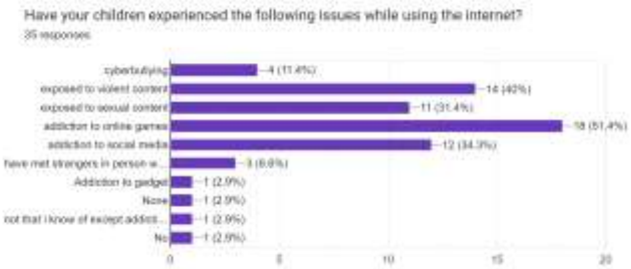


Fig. 5 Cyber threats that were experienced by their children

Finally, the respondents were asked about the features that they wanted to include in the web-based application. Majority of respondents wanted the application to teach the parents and children about cyber threats (94.3%), 80% stated they wanted the app to teach them about overcoming those threats, 65.7% wanted to include online forum for parents to discuss about cyber safety and security among children and 37.1% wanted the app to include online assessments like quizzes. These feedbacks from parents were appreciated and were incorporated in the development of the web-based application prototype.

VI. SmartParents Web Application Prototype

Based on the above findings, this project developed a web-based application prototype called SmartParents. This prototype was developed to educate parents about cyber threats that can happen to them and to their children, so that parents are able to protect their children from cyber threats. The figures below show SmartParents navigation flow (Fig.6), the screenshots of the home page (Fig.7), cyber threats to parents (Fig.8), parental controls (Fig.9), cyber threats to children (Fig.10). and controls for children (Fig.11).

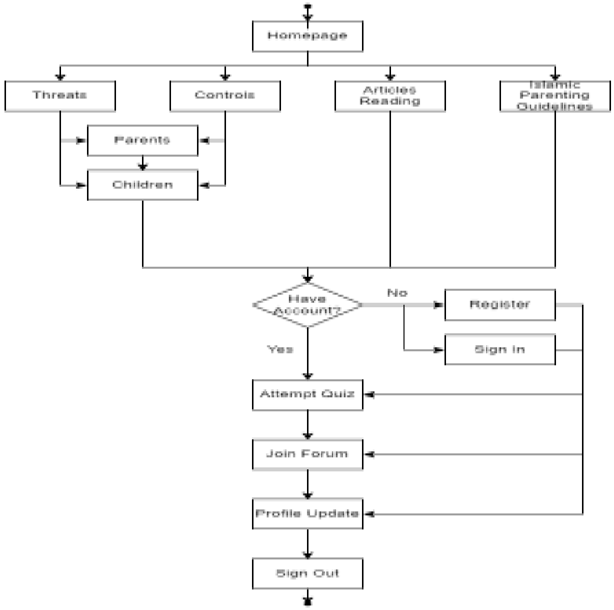


Fig. 6 Navigational flow of SmartParents web app

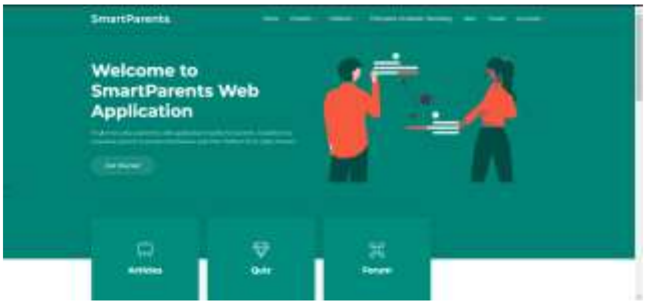


Fig. 7 Screenshot of the home page of SmartParents web app

Based on Fig.6, the home page of the SmartParents web prototype provides the description of the application, users can access articles that are related to cyber parenting, quiz and online forum.

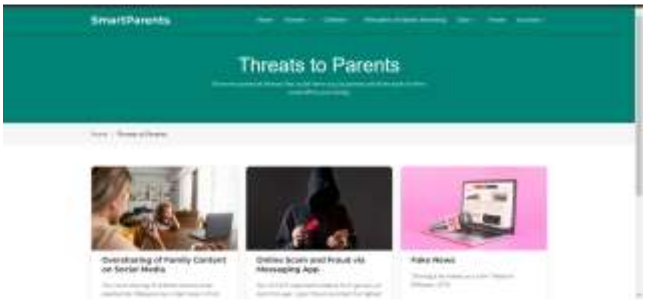

SmartParents
Threats to Parents
Oversharing of Family Content on Social Media
Online Scam and Fraud via Messaging App
Fake News

Fig. 8 Screenshot of the cyber threats to parents

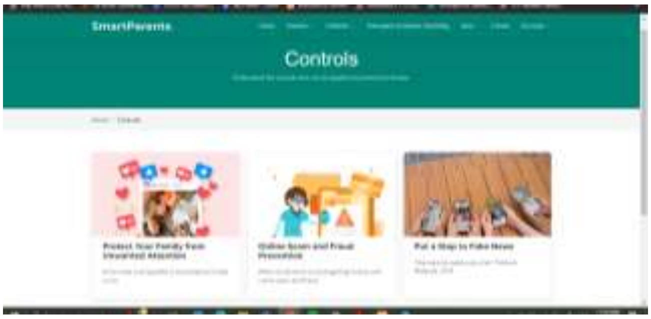

SmartParents
Controls
Protect Your Family from Unwanted Attention
Online Scam and Fraud Prevention
Put a Stop to Fake News

Fig. 9 Screenshot of the security controls for parents

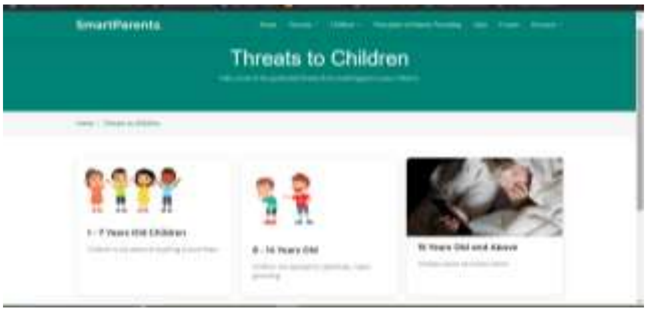


Fig. 10 Screenshot of the cyber threats to children of different age groups

Fig. 11 Screenshot of the security controls for children

Due to the limitation of the article, not all features of the prototype can be included in this article. It is important to note that, the prototype provides different types of cyber threats to both parents and children. The security controls that are recommended covers the categories of people, process and technology. In line with recommendations from [7], one of the researchers' earlier studies in cyber parenting. For example, the security controls should be implemented based on different age groups. The use of Internet among children aged 0-2 must be supervised by parents at all times and only 30 minutes screen time should be allowed.

VII. Conclusion

This article presents the introduction to cyber safety and security that must be understood by parents, review of literature in this area, review of existing application systems that are similar to the proposed web-application system SmartParents, methodology for both data collection and system development, findings from the survey on parents and the discussion of the findings, the overview of the development of the prototype including the screenshots of important pages and finally the conclusion. It is suggested the proposed web application system is able to educate parents about cyber safety and security. Through the application that details the cyber threats to both parents and to their children, it is recommended that parents must be well-versed about the cyber threats that can happen to them and be able to counter those threats. Once they know how to protect themselves, they can protect their children from cyber threats.

Acknowledgment

This study is based on a Final Year Project under the system development category for Bachelor of Information Technology program, Kulliyyah (Faculty) of Information and Communication Technology (ICT), International Islamic University Malaysia.

CONFLICT OF INTEREST

The authors declare that there is no conflict of Interest

References

[1] The Straits Times, Asia (2018), Malaysia tops in South-east Asia for online child pornography. [Online]. Available: https://www.straitstimes.com/asia/se-asia/malaysia-tops-in-south-east-asia-for-online-child-pornography

[2] The Star (2022), Unicef: 100,000 children in Malaysia face online sexual exploitation. [Online]. Available: https://www.thestar.com.my/news/nation/2022/09/29/100000-children-in-msia-face-online-sexual-exploitation-and-abuse-says-unicef-report

[3] New Straits Times (2023), Parents play big role against cyber-paedophilia threat. [Online]. Available: https://www.nst.com.my/news/nation/2023/06/922049/parents-play-big-role-against-cyber-paedophilia-threat

[4] The Star (2022), Malaysia is 2nd in Asia for youth cyberbullying. [Online]. Available: https://www.thestar.com.my/news/nation/2022/01/14/malaysia-is-2nd-in-asia-for-youth-cyberbullying

[5] W.H. Woo, H.N. Chua, and M.F. Gan, “Cyberbullying Conceptualization, Characterization and Detection in Social Media – A Systematic Literature Review”, *International Journal on Perceptive and Cognitive Computing*, vol. 9, no. 1, pp. 101-120, 2023.

[6] Time (2019), 'Gaming Disorder' Is Now an Official Medical Condition, According to the WHO. [Online]. Available: https://time.com/5597258/gaming-disorder-icd-11-who/

[7] N.N. Abdul Molok, and Z. Zulkifli, “Parents’ Roles in Mitigating Cyber Threats to Children in the New Norm”, Persidangan Kependudukan Kebangsaan, Nov. 2021.

[8] N. Ahmad@Ahmad Arifin, U.A. Mokhtar, Z. Hood, S. Tiun, & D.I. Jambari , “Parental awareness on cyber threats using social media”, *Jurnal Komunikasi: Malaysian Journal of Communication*, vol. 35, no. 2, pp. 485–498, 2019. https://doi.org/10.17576/jkmjc-2019-3502-29

[9] J. Loh, and N.N. Zulkifli, “The rising danger of cyber-paedophilia in Malaysia (Part 1)”, *Focus Malaysia*, Aug 2021. https://focusmalaysia.my/the-rising-danger-of-cyber-paedophilia-in-malaysia-part-1/

[10] A.M. Iskül, and K. Joamets, “Child right to privacy and social media – personal information oversharing parents”, *Baltic Journal of Law & Politics*, vol.14, no. 2, pp. 101–122, 2021. https://doi.org/10.2478/bjlp-2021-0012

[11] N. Ahmad Razali, N.I. Nawang, and S.N.A. Syed Nong Mohamad; “Cyberbullying in Malaysia: An Analysis of Existing Laws”, *International Journal of Law, Government and Communication*, vol. 7, no. 30, p.p. 124-135, Dec 2022.