

# Intellectual Discourse

---

Volume 31

Number 1

2023



**International Islamic University Malaysia**  
<https://journals.iium.edu.my/intdiscourse/index.php/id>

# *Intellectual Discourse*

---

Volume 31

Number 1

2023

## **Editor-in-Chief**

Danial Mohd Yusof  
(Malaysia)

## **Editor**

Tunku Mohar Mokhtar  
(Malaysia)

## **Associate Editors**

Anke Iman Bouzenita (Oman)  
Khairil Izamin Ahmad (Malaysia)  
Saodah Wok (Malaysia)

## **Book Review Editor**

Mohd. Helmi Bin Mohd Sobri  
(Malaysia)

---

## **Editorial Board**

Abdul Kabir Hussain Solihu (Nigeria)  
Badri Najib Zubir (Malaysia)  
Daniel J. Christie (USA)  
Habibul H. Khondker (UAE)  
Hazizan Md. Noon (Malaysia)  
Hussain Mutalib (Singapore)  
Ibrahim M. Zein (Qatar)  
James D. Frankel (China)  
Kenneth Christie (Canada)  
Nor Faridah Abdul Manaf (Malaysia)  
Rahmah Bt Ahmad H. Osman  
(Malaysia)  
Serdar Demirel (Turkey)

Syed Farid Alatas (Singapore)  
Thameem Ushama (Malaysia)

## **International Advisory Board**

Anis Malik Thoha (Indonesia)  
Chandra Muzaffar (Malaysia)  
Fahimul Quadir (Canada)  
Habib Zafarullah (Australia)  
John O. Voll (USA)  
Muhammad al-Ghazali (Pakistan)  
Muhammad K. Khalifa (Qatar)  
Redzuan Othman (Malaysia)

## **Founding Editor**

Afar Afaq Ansari (USA)

---

*Intellectual Discourse* is a highly respected, academic refereed journal of the International Islamic University Malaysia (IIUM). It is published twice a year by the IIUM Press, IIUM, and contains reflections, articles, research notes and review articles representing the disciplines, methods and viewpoints of the Muslim world.

*Intellectual Discourse* is abstracted in *SCOPUS*, *ProQuest*, *International Political Science Abstracts*, *Peace Research Abstracts Journal*, *Muslim World Book Review*, *Bibliography of Asian Studies*, *Index Islamicus*, *Religious and Theological Abstracts*, *ATLA Religion Database*, *MyCite*, *ISC* and *EBSCO*.

ISSN 0128-4878 (Print); ISSN 2289-5639 (Online)

<https://journals.iium.edu.my/intdiscourse/index.php/id>

Email: [intdiscourse@iium.edu.my](mailto:intdiscourse@iium.edu.my); [intdiscourse@yahoo.com](mailto:intdiscourse@yahoo.com)

Published by:

IIUM Press, International Islamic University Malaysia  
P.O. Box 10, 50728 Kuala Lumpur, Malaysia  
Phone (+603) 6196-5014, Fax: (+603) 6196-6298  
Website: <http://iiumpress.iium.edu.my/bookshop>

**Intellectual Discourse**  
**Vol. 31, No. 1, 2023**

**Contents**

<i>Note from the Editor</i>	1
 <b>Research Articles</b>	
Validation of a <i>Sejahtera</i> Living Index Using the Rasch Model <i>Muhammad Faris Abdullah</i> <i>Mohamad Sahari bin Nordin</i> <i>Suhailah binti Hussien</i> <i>Norhayati Mohd. Alwi</i> <i>Noor Suzilawati binti Rabe</i>	7
Investigating Ismā‘īl Rājī al-Fārūqī’s Methodology in the Study of Christianity through Selected Textual Analysis from His <i>Christian Ethics</i> <i>Fatmir Shehu</i>	31
Paradoxical and Insufficient? Gender Quotas and Placement Mandates in Bosnia and Herzegovina’s 2020 Local Elections <i>Mirsad Karić</i> <i>Šejma Aydin</i> <i>Huseyin Korkut</i> <i>Muhidin Mulalić</i>	57
Gestalt and Semiotic Analyses of Brand Communication on Disability Inclusion: The Case of Malaysia and the US <i>Aida Mokhtar</i> <i>Faiswal Kasirye</i>	83
Understanding the Decline of Pakistan-US Alliance and the Growing Influence of China in Pakistan <i>Roy Anthony Rogers</i> <i>Noraiz Arshad</i> <i>Iftikhar Ali</i>	113

Let's Think They are Safe Online! A Malaysian Perspective on The Classification of Children's Cyber Risks <i>Sarina Yusuf</i> <i>Misha Teimouri</i> <i>Muhamad Shamsul Ibrahim</i> <i>Nan Zakiah Megat Ibrahim</i> <i>Syahida Mohd Nazri</i> <i>Stephanie Ann Victor</i>	139
Social Media Use for English Learning in Southeast Asia: A Systematic Review <i>Farah Fazlinda Mohamad</i> <i>Khazaila bt Zaini</i> <i>Nur Syahidatul Idany</i>	161
<i>Maqāṣid al-Sharī'ah</i> as Goal Framing for Sustainable Behaviours: A Conceptual Framework <i>Ali Mehellou</i> <i>Mohamad Saifudin Mohamad Saleh</i> <i>Bahiyah Omar</i>	183
Faith in The Time of Coronavirus: A Corpus-assisted Discourse Analysis <i>Siti Aeisha Joharry</i>	211
COVID-19: Analysing the Principle and Application of <i>I'tibār Ma'ālāt</i> in the Selected <i>Fatwas</i> Issued by the Malaysian National Council for Islamic Religious Affairs (MKI) <i>Abdul Manan Ismail</i> <i>Ahmad Syukran Baharuddin</i> <i>Muhammad Hazim Ahmad</i>	233
The Challenges of Civil Society Organisations: NGO-isation of Resistance in Malaysia? <i>Sharifah Nursyahidah Syed Annuar</i> <i>Muhamad Takiyudin Ismail</i>	257

The Authenticity of Theology in Scientific and  
Technological Thinking

*Anhar Anshory*

*Ahmad Faizuddin Ramli*

*Ramli Awang*

283

**Research Notes**

The Seminar on *Da'wah* in Kuala Lumpur in 1977 and  
the Emergence of *Hijab* Awareness in Indonesia

*Alwi Alatas*

*Agus Setiawan*

*Achmad Sunjayadi*

*Yunadi Ramlan*

303

**Book Review**

Osman Bakar, *Environmental Wisdom for Planet Earth:  
The Islamic Heritage* [Revised New Edition] (Kuala Lumpur:  
Islamic Book Trust, 2022). 114 pp. ISBN 978-967-2795-00-1.

Reviewer: *Senad Mrahorović*

315



## Transliteration Table: Consonants

Arabic	Roman		Arabic	Roman
ب	b		ط	ṭ
ت	t		ظ	ẓ
ث	th		ع	‘
ج	j		غ	gh
ح	ḥ		ف	f
خ	kh		ق	q
د	d		ك	k
ذ	dh		ل	l
ر	r		م	m
ز	z		ن	n
س	s		ه	h
ش	sh		و	w
ص	ṣ		ء	’
ض	ḍ		ي	y

## Transliteration Table: Vowels and Diphthongs

Arabic	Roman		Arabic	Roman
اَ، اِ، اُ	a		آ، عَ، يَ	an
وُ	u		وُ	un
يَ	i		يَ	in
آ، اَ، اِ، عَ، يَ	ā		وُ	aw
وُ	ū		يَ	ay
يَ	ī		وُ	uww, ū (in final position)
			يَ	iyy, ī (in final position)

Source: ROTAS Transliteration Kit: <http://rotas.iium.edu.my>





# **Let's Think They are Safe Online! A Malaysian Perspective on The Classification of Children's Cyber Risks**

**Sarina Yusuf** \*

**Misha Teimouri** \*\*

**Muhamad Shamsul Ibrahim** \*\*\*

**Nan Zakiah Megat Ibrahim** \*\*\*\*

**Syahida Mohd Nazri** \*\*\*\*\*

**Stephanie Ann Victor** \*\*\*\*\*

**Abstract:** Children currently spend more time on the Internet and corresponding technologies to socialise virtually and play video games. Scholars have not reached a consensus on whether children's participation in such recreational activities is beneficial or detrimental. Although Malaysian parents are concerned about the digital threats that may be encountered by their children, most of the detriments remain unknown. Children still hesitate to inform their

---

\* Senior Lecturer, Department of Communication and Media, Faculty of Languages and Communication, Universiti Pendidikan Sultan Idris. Email: [sarinayusuf@fbk.upsi.edu.my](mailto:sarinayusuf@fbk.upsi.edu.my). Corresponding author.

\*\* Senior Lecturer, Department of Public Relation, University of Applied Science and Technology, Tehran, Iran. Email: [misha.teimoury@gmail.com](mailto:misha.teimoury@gmail.com)

\*\*\* Senior Lecturer, Department of Media and Communication Studies, Faculty of Arts and Social Sciences, University Malaya. Email: [mshamsul@um.edu.my](mailto:mshamsul@um.edu.my)

\*\*\*\* Senior Lecturer, Universiti Poly-Tech Malaysia. Email: [zakiah@uptm.edu.my](mailto:zakiah@uptm.edu.my)

\*\*\*\*\* Senior Lecturer, Faculty of Sports Science and Recreation, UiTM. Email: [syahidanazri@uitm.edu.my](mailto:syahidanazri@uitm.edu.my)

\*\*\*\*\* Graduate Research assistant, Department of Communication and Media, Faculty of Languages and Communication, Universiti Pendidikan Sultan Idris. Email: [stephylaura13@gmail.com](mailto:stephylaura13@gmail.com)

families about their online exposure to inappropriate content, such as cybersex and pornography, which remain taboo subjects in Malaysian households. This study performed a descriptive analysis to determine the risk factors associated with children's internet use with 420 school-going children aged from 9 to 16 years around Selangor. Resultantly, children were highly exposed to unwanted exposure to pornography (17.4 %), potentially dangerous user-generated content (9 %), sexting (8.8 %), personal data misuse (6.4 %), cyber grooming (3.3 %), and cyberbullying (1.7 %) in the past 12 months of using the Internet.

**Keywords:** cyberbullying, digital generation, personal data misuse, sexting, unwanted exposure to pornography

**Abstrak:** Kanak-kanak pada masa ini menghabiskan lebih banyak masa di Internet dan menggunakan teknologi untuk bersosial secara maya dan bermain permainan video. Para penyelidik belum mencapai kata sepakat sama ada penyertaan kanak-kanak dalam aktiviti rekreasi tersebut bermanfaat atau memudaratkan. Walaupun ibu bapa Malaysia bimbang tentang ancaman digital yang mungkin dihadapi oleh anak-anak mereka, kebanyakan kemudaratannya masih tidak diketahui. Kanak-kanak masih teragak-agak untuk memaklumkan keluarga mereka tentang pendedahan dalam talian mereka kepada kandungan yang tidak sesuai, seperti seks siber dan pornografi, yang masih menjadi subjek tabu dalam isi rumah Malaysia. Kajian ini melakukan analisis deskriptif untuk menentukan faktor risiko yang berkaitan dengan penggunaan Internet kanak-kanak dengan 420 kanak-kanak bersekolah berumur dari 9 hingga 16 tahun di sekitar Selangor. Penemuan penyelidikan mendapati kanak-kanak sangat terdedah kepada pendedahan yang tidak diingini iaitu pornografi (17.4%), kandungan yang dijana pengguna yang berpotensi berbahaya (9%), sexting (8.8%), penyalahgunaan data peribadi (6.4%), dandanan siber (3.3%) dan buli siber (1.7 %) dalam tempoh 12 bulan yang lalu.

**Kata Kunci:** buli siber; generasi digital; penyalahgunaan data peribadi; sexting; pendedahan yang tidak diingini kepada pornografi

## Introduction

The Internet has transformed adolescents from a physical world to a virtual reality. Youths are more attracted to the leisure activities derived from the Internet, such as socialising, playing games, and watching television. In this vein, children denote the highest number of internet users. A survey revealed that 75% of internet users worldwide were under 24 years old (Statista, 2023). Similarly, 73% of internet users in

Asia-Pacific were under 24 years of age (Statista, 2023). Over 90% of the people in Malaysia use the Internet daily, not unlike other countries (UNICEF, 2020). Specifically, more than 80% of these users are children under 15 years old (UNICEF, 2020). Children in Malaysia could easily access the Internet through personal computers, laptops, tablets, and smartphones, specifically following the emergence of COVID-19, which has characterised the Internet as a new norm in the education system. Students must connect to the Internet for educational activities. Despite the advantages of using the Internet (seamless information and knowledge attainment), children are susceptible to multiple internet-associated risks, such as cybercrime and cyberbullying.

Online risks generally denote a set of “intended or unintended” and “wanted or unwanted” experiences that adversely impact Internet users (Zlamal et al., 2020). Children who receive inappropriate content, participate in risky behaviour with communication, or contribute to harmful content or communication are vulnerable to online pornography or sexual solicitations (Keen et al., 2020; Kwan et al., 2020), online harassment and cyberbullying (Bakar et al., 2018; Blaya et al., 2020; Costello et al., 2020), exposure to hateful content (Costello et al., 2020), X-rated contents, such as “rough sex” on the Internet (Vogels & O’Sullivan, 2019), violent or coercive pornography (Landripet et al., 2019), and other desired or undesired and inappropriate behaviour arising from internet use.

Malaysian families are relatively aware of cyber dangers (Ahmad et al., 2019). As 80% of Malaysian children from 10 to 17 years old have access to inappropriate content, including pornography (Ahmad et al., 2019), Malaysian parents believe that their children may encounter such content. Nevertheless, most children are susceptible to online risks following their parents’ lack of supervision. Almost 89 % of adolescents between 13 and 17 years old, who were victims of internet grooming, fell prey to inappropriate acts (New Strait Times, 2019). Based on a national survey, 83% of students in Malaysia were exposed to various types of online risks. Specifically, 70% of them were victims of online harassment, while 64% received or sent improper messages or images online (DiGi Cyber Safe report, 2014). It is deemed challenging for parents to keep constant surveillance of their children, who are required to use portable devices (smartphones) to perform educational activities.

The Malaysian government has taken initiatives to decrease cyber risks by drafting laws on cyberbullying, such as cybersecurity outreach (Digital, 2020). Much research on cyber risk and cyberbullying has also been conducted. For example, Kee et al. (2022) investigated cyberbullying predictors through social media, while Ooi et al. (2022) examined the factors associated with adolescent cyberbullying. Notwithstanding, cyberbullying, and cyber risk in Malaysia are steadily increasing despite extensive research in this area and governmental initiatives. A recent survey revealed that “Malaysia is 2nd in Asia for youth cyberbullying” (Star, 2022). Overall, the question of how to decrease cyberbullying and cyber risk in Malaysia remains unaddressed.

The significant rise in internet-using children has garnered much attention from scholars and regulatory bodies. As such, this study aims to investigate the classification of cyber risk and its subsequent effect on children’s life. The empirical outcomes would facilitate regulatory authorities to establish and implement relevant rules and regulations.

## **Literature Review**

The increasing use of digital technologies has highlighted cyber risk as a growing concern for children (Bevan Jones, 2020). Children are vulnerable to cyberbullying following the anonymity and accessibility of digital technologies, which serve as a platform for harassment and abuse (Mkhize, 2021). Children who are victims of cyberbullying may experience depressive symptoms, anxiety, and low self-esteem (Zhong, 2021). Online predators, such as perpetrators who utilise social media and other digital platforms to groom and exploit children, are a significant cyber threat (Karadimce, 2023). Such manipulations could negatively affect the victim’s physical and mental health and future prospects.

A multidimensional approach involving parents, educators, and law enforcement proves necessary to safeguard children from cyber risk (Abd Rahman et al., 2022). Parents can play a pivotal role in supervising their children’s online activities and establishing guidelines for the safe and responsible use of digital technologies (Lamsal, 2022). Meanwhile, educators could equip students with digital literacy and cyber safety knowledge and skills to remain safe online (Nascimbeni & Vosloo, 2019). Law enforcement agencies that effectively identify and prosecute cybercriminals indicate that such conduct would not

be tolerated (Graham, 2023). Community members must collectively address cyber risk challenges and protect children from digital hazards (Jain et al., 2021). Overall, relevant statistics reveal a steady rise in cyber risks despite the efforts of academicians, law enforcement institutions, parents, and teachers to decrease such risks.

Cyber risk is generally considered an online security issue (HWEE, 2009). Nevertheless, several studies have classified this risk in terms of cyberbullying and cyber harassment (Quayyum et al., 2021). Despite much research on the cross-cultural variation in cyberbullying in different countries (Smith et al., 2018), most of the empirical works were performed in North America, Europe, and Australia (Hinduja & Patchin, 2013; Kowalski et al., 2014; Smith & Berkun, 2017). These scholars conceded that the meaning and classification of cyber risk differed across nations, cultures, and norms. Existing cyber risk and cyber bullying studies in the Asian Pacific region also highlighted certain classification-related drawbacks. As numerous studies categorised cyber risk differently following their local culture, scope, and context (Kamaruddin et al., 2023; Smith et al., 2019), this study posited that cyber risk is different in Malaysia compared to other countries. Hua et al. (2019), who explored the linguistic features of cyberbullying in Malaysia, analysed the language used in cyberbullying incidents on social media platforms to identify patterns and characteristics that could distinguish cyberbullying from other online communication types. The authors evaluated a sample of cyberbullying messages gathered from social media platforms, with emphasis on linguistic features: syntax, lexical choices, and use of emoticons. Resultantly, cyberbullying messages frequently employed negative language and derogatory terms and emoticons to convey negative emotions. The authors suggested using these linguistic features to develop algorithms that could automatically identify and classify cyberbullying messages. Internalising the linguistic features of cyberbullying could develop effective strategies to prevent and address this issue locally and globally. Based on the study, most of the abusive remarks began with the word “Kepala”, which means head in Malay. Other local studies on cyberbullying (Adebayo et al., 2020; Sivabalan et al., 2020) were also conducted in Malaysia.

The definition of cyberbullying varies following the research context and purpose. In Malaysia, de-hijabbing (a voluntary act of removing the hijab) (Noor & HAMID, 2021) and its promotion is considered

cyberbullying (Noor & HAMID, 2021). Thus, cyberbullying could be characterised in terms of harassment, flaming, denigration, impression, exclusion, cyberstalking, and impersonation (Willard, 2007). Relevant scholars have investigated cyberbullying with different linguistic methods. For example, several researchers used natural language processing (NLP) and machine learning programme to detect the matching text. The bag-of-words approach, part-of-speech tagging, and grammar features were initially applied for detection purposes (Dinakar et al., 2011), followed by content-based features: lexical, syntactic, and sentiment information (Ptaszynski et al., 2016; Zhao et al., 2016).

Contrarily, some studies contended with the insufficiency of these methods and tools to detect cyberbullying given the pliability of the term, which changes based on the context (Zhong et al., 2022). Despite inconsistent statements about cyberbullying, the existing literature gap may be bridged by categorising cyberbullying based on profession, age, religion, and other demographic attributes. This research only included cybercrime categories and considered cyberbullying as inappropriate messages, receiving, or sending nasty messages, or being left out. Additionally, the study proposed cyberbullying as a personal insult and sexual harassment, albeit with insufficient literature to identify the cyber risk classification.

### *Classification of Cyber Risk*

In line with the knowledge gaps, this study categorised the cyber risk type based on relevant literature and surveys:

- (1) Cyberbullying includes inappropriate messages, receiving nasty messages, and being left out. The Child Online Safety Index (COSI) is a global think-tank institute that collected data from 145,426 children and adolescents in 30 countries between 2017 and 2019 as part of the DG Every Child project. Reportedly, 60% of children from 8 to 12 years old were generally exposed to cyber risks, with 45% of them experiencing cyber-bullying, 39% experiencing reputational risks, 29% exposed to risky (violent or sexual) content, 28% exposed to cyber threats, 17% experiencing risky contact (offline with strangers or sexual contact), 13% at risk for a gaming disorder, and 7% at risk for social media disorder (DGInstitute, 2020). The DG Lab Report (2020) disclosed Spain and Australia to have the highest rate

of Child Internet Safety Act, followed by Malaysia ranking second, Singapore ranking third, and Singapore ranking fourth.

- (2) Sexting includes all received or sent inappropriate material, including images videos and text. Youth and Media (YaM) covers research and development initiatives among youths from 12 to 18 years old and digital technology whilst closely interacting with other teams at the Berkman Klein Cent. The dynamic global, social, and cultural environments impact the current discourse with input on new youth and digital media topics, whereby methodologies were introduced that could capture young adults' experiences to contribute to the economic and social effects of novel technologies (YaM, 2020). The Berkman Center has initiated the Internet Safety Technical Task Force (ISTTF) project to identify sexual solicitation, online harassment, and problematic content as a subgroup of online risks and digital technology (Berkman Center for Internet & Society, 2008).
- (3) Risky online conversation includes sending phone numbers and addresses or seeking someone for an intimate relationship. The Family Online Safety Institute (FOSI) surveyed adolescents from ages 13 to 17 and introduced classifications of teen identity theft, fraud, being tracked for marketing, being bullied, ugly or unflattering pictures posted, and security issues on the Internet (Family Online Safety Institute, 2013). The FOSI aims to promote a culture of responsibility online and encourages a sense of digital citizenship through research, resources, events, and special projects.
- (4) Unwanted exposure to pornography includes all the unwanted materials in pornography, such as unwanted e-mails, unwanted obscene materials on messages or links, and similar encounters. The Youth Internet Safety Survey (YISS) group conducts another systematic study, which is repeated every five years in the United States. The YISS-1, YISS-2, and YISS-3 and the Fourth National Survey of Internet & Technology Facilitated Child Exploitation (Mitchell, 2020) were conducted in 2000, 2005, and 2010 to quantify younger Internet users' unwanted

or problematic experiences, including unwanted exposure to pornography and sexual solicitation or harassment.

- (5) Potentially harmful user-generated content includes all the content on danger or threat, such as bloody photos, videos related to being beaten up, and other related material, including images and texts. The Online Safety and Technology Working Group (OSTWG, 2010) defined the online risk categories as predator danger, cyberbullying, sexting, and inappropriate content.
- (6) Personal data misuse includes data misuse activities, such as password misuse and being hacked. The European Kids Online survey, known as “EU Kids Online”, is a research network that interviewed European children and their parents from 25 European countries from 2006 to 2009. The EU kids online has since conducted periodic research among European children. The latest project reports were published (Smahel et al., 2020; Zlamal et al., 2020) to evaluate online opportunities and risks for children. Another study entitled ‘Be safe, Go online’ was conducted in a Malaysian university-grant project (2012-2015) to study Internet usage and online risks among 1800 respondents, including 800 Malaysian adolescents from 8 to 16 years and their parents (Daud et al., 2014; Teimouri et al., 2014; Yusuf et al., 2014). The study included the risk of hacking activities and data misuse.

Multiple studies have been conducted on cyber risk. To date, cyber risks imply security risks, such as information misuse or hacking. Regardless, other empirically-excluded categories indicate a knowledge gap in cyber risk categories. The current study proposed some additional categories to fill the literature gap. As this research was conducted in Malaysia, multiple factors (parenting style in Malaysia, educational situations, norms, culture and language) were regarded while proposing new cyber risk categories.

### **Research Methodology**

This study adapted global classifications of online risks and measurements, a modified national-classification version of online risks to children in the Malaysian index, based on the ‘Be Safe, Go Online’



project following Teimouri et al. (2016). The risks were classified into (1) unwanted exposure to pornography (adapted from Wolak et al., 2007), (2) potentially harmful user-generated content, (3) sexting, (4) personal data misuse ( adapted from Livingstone et al., 2012), (5) risky online conversation that asked children whether they had sought someone online to talk about sex, have sex, or sent a sexual photo or video (adapted from Baumgartner et al., 2010; Finkelhor et al., 2011), and (6) cyberbullying. This study provided a descriptive outcome of the risks (adapted from Livingstone et al., 2012).

The current work included 420 children from primary and secondary schools, with an average age of 12, in two districts of Selangor (Gombak and Sepang), Malaysia. Purposive sampling was used to select the respondents. Muslim students who spent most of their time with parents after school were selected for data collection. The respondents should have at least one social media ID used in the last 12 months. Lastly, only students who felt comfortable providing data were selected as respondents. As this study aimed to test the cyber risk classification, the intensity of intent usage was not considered. Counsellors suggested the children at their respective schools. Empirical data were gathered with a classroom-administered survey method. Each session lasted for approximately one hour, during which students were accompanied by two researchers who assisted and guided them.

The researchers were required to substitute explicit terms in their study questions pre-data collection in adherence to Malaysian cultural appropriation. In Malaysian culture (specifically in Muslim families), some cyberbullying terms were deemed inappropriate while conversing with someone. The respondents may feel shy to use them directly. Hence, these words were rephrased without altering the original meaning. The sexually-explicit language was replaced for questionnaire validation. For example, the phrase "having sex" was replaced with "having an inappropriate intimate relationship, while "showing sexual actions and content" and "naked photos" were substituted with "obscene pictures" and "obscene acts or materials," respectively. The data collected was classified into three levels ranging from 1 (low) to 3 (high).

The demographic results revealed that most students (66 %) were females and Malay Muslims from 9 to 16 years old (74 %). Statistically, children frequently used the Internet after school (80%) or under

parental supervision (79 %). Male students were more susceptible to cyber threats compared to their female counterparts.

Findings

This study performed a descriptive analysis to confirm the cyber risk classification. Resultantly, over 36% of the students encountered something on the Internet that “made them feel uncomfortable, upset, or that they shouldn’t have seen it”, while almost 58 % of them indicated having not experienced unfavourable scenarios. Meanwhile, 6 % did not respond to the question. Additionally, 61 % agreed on being exposed to unsuitable content, while 32 % disagreed and 7 % did not respond to the questions.

Most of the respondents (82.6%) reported a low level of exposure to “unwanted exposure to pornography,” while 17.4% of them denoted a high level of exposure. Meanwhile, 91% encountered low exposure to “potentially hazardous user-generated material”, whereas 9% accounted for excessive exposure. Many adolescents (91.2%) demonstrated low exposure to “sexting,” while 8.8% reflected significant exposure. Personal data abuse accounted for 93.6% and 6.4% of low-exposure and high-exposure cases, respectively. Most of the young adults (96.7%) engaged in low-level sexual online activity, while a mere 3.3% engaged in high-level sexual online behaviour. A majority of the adolescents (98.3%) experienced modest levels of “cyberbullying”, while only 1.7% experienced severe levels of “cyberbullying”.

Table 1: Descriptive report of child cyber risks exposure

Constructs/indicators		% of frequency			M	S.D	% of high-low rate	
		1	2	3			L	H
Unwanted exposure to pornography							82.6	17.4
1	Unwanted obscene materials on the web	45	47	8	1.62	0.62		
2	Unwanted e-mail or IM	69	26	5	1.35	0.57		
3	Unwanted obscene materials on messages or links	67	31	2	1.35	0.52		
4	Naked picture/inappropriate intimate relationship on message/link	80	19	1	1.20	0.43		
5	Anyone asks to talk about inappropriate acts	82	17	1	1.18	0.40		
6	Anyone asks to do inappropriate acts	91	9	0	1.09	0.30		
	Overall mean				1.30	0.47		

Potentially harmful user-generated content							91.0	9
1	Seen bloody movies or photos	40	54	6	1.66	0.62		
2	Seen people beaten up	64	31	5	1.65	0.58		
3	Seen hate messages	80	18	2	1.40	0.58		
4	Seen anorexia or bulimic	94	6	0	1.22	0.45		
5	Talk about drugs	95	5	0	1.06	0.25		
6	Ways of physical harming	95	5	0	1.05	0.21		
7	Ways of committing suicide	97	3	0	1.03	0.19		
	Overall mean				1.30	0.41		
Sexting							91.2	8.8
1	Received inappropriate messages (words, pictures, and videos)	80	20	0	1.20	0.41		
2	Being posted inappropriate materials	80	20	0	1.20	0.41		
3	Being sent inappropriate messages	85	15	0	1.15	0.38		
4	Seen obscene images or videos	86	14	0	1.14	0.35		
5	Seen other people perform obscene acts	86	14	0	1.14	0.35		
6	Seen intimate images or videos in a violent way	87	13	0	1.13	0.34		
7	Seen someone's obscene images or videos	89	11	0	1.11	0.32		
8	Seen obscene images or videos about private parts	90	10	0	1.10	0.29		
	Overall mean				1.15	0.36		
Personal data misuse							93.6	6.4
1	Misuse of password	81	18	1	1.30	0.57		
2	Misuse of personal information you didn't like	90	10	0	1.08	0.29		
3	Being hacked	92	8	0	1.05	0.22		
4	Misuse of personal information	95	5	0	1.05	0.23		
5	Lost money by being cheated online	97	3	0	1.03	0.20		
	Overall mean				1.10	0.30		
Risky online conversation							96.7	3.3
1	Sent address or phone number to someone you only knew online	75	19	5	1.30	0.3		
2	Search for someone to talk about intimate relationship	92	7	0	1.08	0.29		
3	Search for someone to do intimate relationship	96	4	0	1.05	0.22		
4	Sent obscene photos to someone you only knew online	98	2	0	1.02	0.17		
Overall mean					1.10	0.30		

Cyberbullying							98.3	1.7
1	Received inappropriate messages that bothered you	80	19	1	1.20	0.42		
2	Received nasty or hurtful messages	84	16	0	1.17	0.38		
3	Received another nasty message that hurt you	89	11	0	1.12	0.33		
4	Being left out or excluded	90	10	0	1.10	0.32		
5	Received nasty or hurtful messages about yourself	92	8	0	1.08	0.29		
6	Being threatened online	94	6	0	1.06	0.25		
7	Being asked to talk about nasty acts	95	5	0	1.05	0.21		
8	Being asked to show your private part	96	4	0	1.04	0.21		
9	Received inappropriate messages encourage you to run away	97	3	0	1.03	0.16		
Overall score					1.09	0.28		

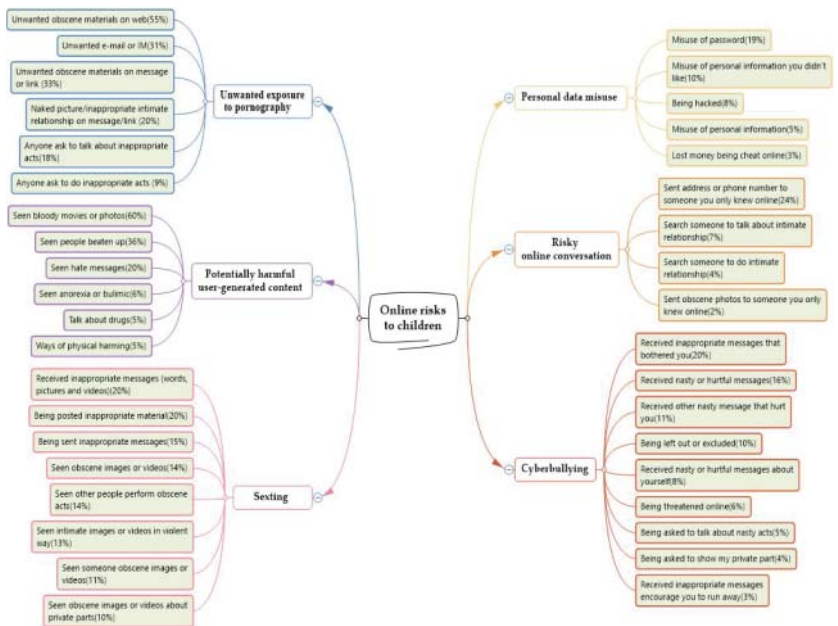


Figure 1: Malaysian classification of online risks model

Discussion

This study pioneers the purposing of cyber risk categories, all of which were confirmed based on the research outcome. Most of the

respondents reported encountering unwanted exposure to pornography, followed by sexting, and personal data misuse. Regardless, very few of them experienced risky online conversations and cyberbullying. As such, the study outcome confirmed six cyber risk categories as follows: unwanted exposure to pornography, potentially harmful user-generated content, sexting, personal data misuse, risky online conversation, and cyberbullying.

#### *Unwanted exposure to pornography*

This study considered unwanted exposure to pornography as unwanted material sent or received over the Internet. Empirically, 17.4% of the respondents encountered unwanted exposure to pornography following existing works on unwanted exposure to pornography (Henry, 2023; Kumar et al., 2016), which documented a high number of respondents encountering unwanted exposure to pornography. Despite a paucity of local studies on unwanted exposure to pornography, these empirical works underscored unwanted exposure as a primary issue (Teimouri et al., 2014). This problem may result from ineffective internet regulation and monitoring measures. Although the Malaysian government has enforced laws to regulate online content, these regulations are frequently disregarded. Many websites and online platforms continue operating without proper supervision. Unwanted exposure to pornography could significantly impact young people and increase their vulnerability to the adverse effects of exposure to explicit materials. Following past literature, exposure to pornography could instigate various problems, including addiction, desensitisation to sexual content, and distorted views of sexuality and relationships.

#### *Potentially harmful user-generated content*

In line with the study outcomes, only 9% of the respondents encountered potentially harmful user-generated content. Notwithstanding, past Malaysian studies revealed that most of the respondents encountered such content (Sofee et al., 2022). This contradiction may result from variances in the research definition and context. Following Sofee et al. (2022), user-generated content on social media encompassed harmful and fear-inducing elements. Nonetheless, the study did not incorporate other cyber risk materials, such as sexting and pornography. Hence, the results depended on the study definition and context. It is deemed necessary to increase public awareness of and education on responsible

online behaviour and the implications of online content by educating content creators and consumers on the significance of validating information pre-sharing, avoiding hate speech, and respecting people's privacy and dignity.

### *Sexting*

Resultantly, only 8.8% of the children encountered sexting issues. This finding contradicted past studies, which highlighted sexting as a primary construct of cyber risk (Goh et al., 2022). This inconsistency could be attributed to the study respondents (children), who might have been hesitant to discuss such topics. Sexting could instigate content-sharing without consent, which could induce humiliation, embarrassment, and cyberbullying or harassment in some cases. Such content could lead to further harm or exploitation when manipulated by strangers or criminals. Sexting could also be used as a form of coercion or grooming. For example, an individual may be pressured into sending explicit photos or videos to someone in a position of authority (teacher or employer), who could then use the materials for exploitation purposes.

### *Personal data misuse*

Only 6.4% of students encountered issues with personal data misuse. The current study results varied from past literature, where many people experienced data misuse (Sudarwanto & Kharisma, 2022). This contradiction could result from differences in terms of definition and context. In Malaysia, data misuse incidents in the context of cyber risk for children proved to be lower.

### *Cyberbullying and Risky Online Communication*

Relevant literature considers risky online communication as cyberbullying (Yusop & Al-Shami, 2021). Notwithstanding, this study regarded the concept from different categories. The results revealed a minimal number of students who encountered cyberbullying. Regardless, past literature posited cyberbullying as one of the key concerns in Malaysia (ASANAN et al., 2016). The current study outcomes may be different, as cyberbullying was considered separately with lesser factors. Nevertheless, relevant literature regarded more factors under cyberbullying. Overall, this study proposed cyberbullying as a cyber risk category to attract researchers' and government bodies' attention towards this issue.

## Conclusion

The Internet has become part of children's daily life following rapid advancements in digital technology, which may present new digital risks or threats. The current work expanded the current body of knowledge by proposing six cyber risk categories. Regardless, the risk associated with these categories is yet to be categorised. Researchers placed much emphasis on sex-related risks, sharing personal information with strangers, and cyberbullying as a range of online risks encountered by internet-using children. It is deemed crucial to categorise these activities for the government and regulatory bodies to undertake preventive measures and implement optimal strategies. For example, research by the Ministry of Science, Technology and Innovation, MCMC, and the Women, Family and Community Development Ministry, and Digi Telecommunication Sdn. Bhd provide useful insights into cyber risk among the target groups (Ahmad et al., 2019). The survey results revealed the need to extensively examine cyber risk and its associated categories for a sound understanding of the issue.

The Internet exposes children to both risks and opportunities. Based on the study finding, online risk exposure towards children between 9 and 16 years old in Malaysia was not very high as they "never or seldom experienced risks online". Although the situation is not alarming, parents and society should seriously consider the online risks of "unwanted exposure to pornography" and "potentially harmful user-generated content" towards children. Over 50% of the current study respondents had been exposed to unwanted obscene materials (sexual content) on websites, while almost 60% had seen gory movies or photos and people being beaten up online. In addressing the concerns of family members, practitioners, and policymakers about the negative consequences of the online risks faced by children, it is deemed crucial to classify these risks: not all children feel uncomfortable, upset, or troubled upon encountering them (Zlamal et al., 2020). Strategies to mitigate such risks remain unexplored despite the digital threats encountered by internet-using children.

Due to sensitivity issues, the Malaysian Ministry of Education required the removal of some inappropriate or explicit words from the study questionnaire pre-data collection. For example, the phrase "having sex" was replaced with "having an inappropriate intimate relationship,"

while “naked pictures” and “showing sexual acts and content” were substituted with “obscene pictures” and “obscene acts or materials,” respectively. Hypothetically, the children may not have derived the actual meaning of the classified risks owing to the word replacements. Malaysian parents should be more realistic and open-minded as children-parent discussions on sexual matters remain taboo. Parents should face reality and initiate conversations with their children to create an awareness of online hazards and potential consequences. During data collection, the researchers observed the children’s reluctance to share their exposure to sexual content with parents and teachers. Visiting children at school in an isolated environment could also have influenced their responses. Future works could utilise different data collection methods to minimise the online risks encountered by children.

### **Limitations and Recommendations**

The current work proposed six cyber risk categories that could be empirically examined. For example, potential researchers could investigate the intensity of these categories across multiple age groups. As this study did not investigate the risks associated with these categories, further research may analyse these risks in relation to various activities and their prevention. The present research only presented six cyber risk categories. As such, future works could introduce new classifications based on the Malaysian context and might use these classifications in a research framework. Given the current study limitations, which conducted a purposive study by confirming the cyber risk categories, further research may be performed to investigate these categories in different contexts and incorporate them into the research model. This empirical work proposed six broad categories of cyber risk. Hence, potential scholars could be more specific in considering these categories. As cyberbullying varies following the research context, each category should be sub-categorised based on future study contexts and aims. Prospective studies could perform sub-categorisation based on a country’s norms and culture, which was not included in this research.

### **Acknowledgement**

Authors of this article would like to extend their utmost appreciation and gratitude to the Research Management and Innovation Centre of University Pendidikan Sultan Idris and the Ministry of Higher Education for funding the research project under the Fundamental Research Grant



Scheme (FRGS), code: FRGS/1/2021/SSO/UPSI/02/3 (2021-0137-106-02) that has led to the production of this article. The authors also wish to appreciate the continuance of support and unending guidance given that has led toward the success of the publication of this article.

## References

- Abd Rahman, M., Jaafar, N. H., Ismail, Z., Khalid, R. M., Saúdah, N., Zamani, N. D., & Mokhtar, R. (2022). Children's Online Safety: Literature Review. *International Journal of Technology Management and Information System*, 4(3), 17-25.
- Adebayo, D. O., Ninggal, M. T., & Bolu-Steve, F. N. (2020). Relationship between Demographic Factors and Undergraduates' Cyberbullying Experiences in Public Universities in Malaysia. *International Journal of Instruction*, 13(1), 901-914.
- Ahmad, N., Arifin, A., Asma'Mokhtar, U., Hood, Z., Tiun, S., & Jambari, D. I. (2019). Parental awareness on cyber threats using social media. *Jurnal Komunikasi: Malaysian Journal of Communication*, 35(2).
- ASANAN, Z. Z. B. T., Hussain, I. A., & Laidey, N. M. (2016). *A study on cyberbullying: Its forms, awareness and moral reasoning among youth Asia Pacific University*.
- Bakar, H. S. A., Yusof, N., & Budiman, A. M. (2018). The Paradigm Model of Cyberbullying Phenomenon. *GSTF Journal on Media and Communications (JMC)*, 1(1).
- Baumgartner, S. E., Valkenburg, P. M., & Peter, J. (2010). Unwanted online sexual solicitation and risky sexual online behavior across the lifespan. *Journal of Applied Developmental Psychology*, 31(6), 439-447. <https://doi.org/10.1016/j.appdev.2010.07.005>
- Bevan Jones, R., Stallard, P., Agha, S. S., Rice, S., Werner-Seidler, A., Stasiak, K., ... & Merry, S. (2020). Practitioner review: Co-design of digital mental health technologies with children and young people. *Journal of child psychology and psychiatry*, 61(8), 928-940.
- Blaya, C., Audrin, C., & Skrzypiec, G. (2020). School Bullying, Perpetration, and Cyberhate: Overlapping Issues. *Contemporary School Psychology*, 1-9.
- Costello, M., Barrett-Fox, R., Bernatzky, C., Hawdon, J., & Mendes, K. (2020). Predictors of viewing online extremism among America's youth. *Youth & Society*, 52(5), 710-727.

- Daud, A., Omar, S. Z., Hassan, M. S., Bolong, J., & Teimouri, M. (2014). Parental Mediation of children's positive use of the Internet Azlina. *Life Science Journal*, 11(8), 360–369.
- DGInstitute. (2020). *2020 child online safety*. <https://www.dqinstitute.org/wp-content/uploads/2020/02/2020COSIReport.pdf>
- Digital, M. o. C. a. (2020). *Govt To Draft Law Specific To Combat Cyberbullying - Cybersecurity*. <https://www.kkd.gov.my/en/public/news/19761-govt-to-draft-law-specific-to-combat-cyberbullying-cybersecurity>
- Dinakar, K., Reichart, R., & Lieberman, H. (2011). Modeling the detection of textual cyberbullying. In *Proceedings of the International AAAI Conference on Web and Social Media* (Vol. 5, No. 3, pp. 11-17).
- Family Online Safety Institute. (2013). *Teen Identity Theft*. [www.fosi.org/files/Teen-Identity-Theft-online.pdf](http://www.fosi.org/files/Teen-Identity-Theft-online.pdf)
- Finkelhor, D., Mitchell, K. J., & Wolak, J. (2011). *Second Youth Internet Safety Survey (YISS-2)*. [http://www.ndacan.cornell.edu/datasets/pdfs\\_user\\_guides/159user.pdf](http://www.ndacan.cornell.edu/datasets/pdfs_user_guides/159user.pdf)
- Goh, Y. S., Tan, S. A., & Gan, S. W. (2022). Sexting motives and sexting behavior among emerging adults in Malaysia during the COVID-19 pandemic lockdown. *Gender, Technology and Development*, 1-21.
- Graham, A. (2023). *Cybercrime: Traditional Problems and Modern Solutions* Open Access Te Herenga Waka-Victoria University of Wellington].
- Henry, B. (2023). *The Correlation of Adverse Childhood Experiences and Pornography Consumption in Adulthood* Walden University].
- Hinduja, S., & Patchin, J. W. (2013). Social influences on cyberbullying behaviors among middle and high school students. *Journal of youth and adolescence*, 42, 711-722.
- Hua, T. K., Hamid, B. A., & So'od, S. M. (2019). Linguistic features of Cyberbullying. *International Conference on Advanced Research in Social Sciences*,
- HWEE, L. S. (2009). *Cyber Risk Insurance Policy: a Proposed Framework for E-Business in Malaysia*. Universiti Teknologi Malaysia.
- Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. *Complex & Intelligent Systems*, 7(5), 2157-2177.
- Kamaruddin, I. K., Ma'rof, A. M., Mohd Nazan, A. I. N., & Ab Jalil, H. (2023). A systematic review and meta-analysis of interventions to decrease cyberbullying perpetration and victimization: An in-depth analysis within the Asia Pacific region. *Frontiers in psychiatry*, 14, 1014258.

- Karadimce, A., & Bukalevska, M. (2023). Threats Targeting Children on Online Social Networks. *WSEAS Transactions on Advances in Engineering Education*, 20, 25-31.
- Kee, D. M. H., Al-Anesi, M. A. L., & Al-Anesi, S. A. L. (2022). Cyberbullying on social media under the influence of COVID-19. *Global Business and Organizational Excellence*, 41(6), 11-22.
- Keen, C., France, A., & Kramer, R. (2020). Exposing children to pornography: How competing constructions of childhood shape state regulation of online pornographic material. *New Media & Society*, 22(5), 857-874.
- Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: a critical review and meta-analysis of cyberbullying research among youth. *Psychological bulletin*, 140(4), 1073.
- Kumar, S., Pallathadka, H., & Pallathadka, L. K. (2016). Exposure to Pornography and Harmful Materials against Children: An Analysis.
- Kwan, I., Dickson, K., Richardson, M., MacDowall, W., Burchett, H., Stansfield, C., Brunton, G., Sutcliffe, K., & Thomas, J. (2020). Cyberbullying and children and young people's mental health: a systematic map of systematic reviews. *Cyberpsychology, Behavior, and Social Networking*, 23(2), 72-82.
- Lamsal, B. (2022). Exploring issues surrounding a safe and conducive digital learning space in Nepal: A preparation for online education in the post-pandemic era. In *Socioeconomic Inclusion During an Era of Online Education* (pp. 246-263). IGI Global.
- Landripet, I., Buško, V., & Štulhofer, A. (2019). Testing the content progression thesis: a longitudinal assessment of pornography use and preference for coercive and violent content among male adolescents. *Social Science Research*, 81, 32-41.
- Livingstone, S., Haddon, L., & Gorzig, A. (2012). *Children, risk and safety on the Internet: Research and policy challenges in comparative perspective*. The Policy Press.
- Mitchell, K. J. (2020). *The Fourth National Survey of Internet & Technology Facilitated Child Exploitation*.
- Mkhize, S., & Gopal, N. (2021). Cyberbullying perpetration: Children and youth at risk of victimization during Covid-19 lockdown. *International Journal of Criminology and Sociology*, 10, 525-537.
- Nascimbeni, F., & Vosloo, S. (2019). Digital literacy for children: Exploring definitions and frameworks. *Scoping Paper*, 1.
- Noor, N., & Hamid, B. A. (2021). Cyberbullying in the Name of God: Critical Discourse Analysis of Online Responses to the Act of De-hijabbing in

- Malaysia. *3L: Southeast Asian Journal of English Language Studies*, 27(4).
- NST. (2019). Ensuring a safer Internet for children. *NST*. <https://www.nst.com.my/lifestyle/bots/2019/11/540437/ensuring-safer-internet-children>
- Ooi, P. B., Ahrumugam, P., Teh, P. L., & Chan, N. N. (2022, October). Factors Associated with Adolescent Cyberbullying Perpetration and Victimization in Malaysia. In *Proceedings* (Vol. 82, No. 1, p. 109). MDPI.
- Online Safety and Technology Working Group Online Safety and Technology Working Group (OSTWG). (2010). *Youth safety on a living Internet: Report of the online safety and technology working group*. [http://www.ntia.doc.gov/legacy/reports/2010/OSTWG\\_Final\\_Report\\_060410.pdf](http://www.ntia.doc.gov/legacy/reports/2010/OSTWG_Final_Report_060410.pdf)
- Ptaszynski, M., Masui, F., Nitta, T., Hatakeyama, S., Kimura, Y., Rzepka, R., & Araki, K. (2016). Sustainable cyberbullying detection with category-maximized relevance of harmful phrases and double-filtered automatic optimization. *International Journal of Child-Computer Interaction*, 8, 15-30.
- Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, 30, 100343.
- Sivabalan, T. V., Zaki, R. A., & Yuen, C. W. (2020). The prevalence of cyberbullying and its associated factors among young adolescents in Penang, Malaysia. *Journal of Health and Translational Medicine*, 202-211.
- Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., & Hasebrink, U. (2020). *EU Kids Online 2020: Survey results from 19 countries*. *EU Kids Online*.
- Smith, P. K., & Berkun, F. (2017). How research on cyberbullying has developed. *Bullying and cyberbullying: Prevalence, psychological impacts and intervention strategies*, 11-27.
- Smith, P. K., Görzig, A., & Robinson, S. (2018). Issues of cross-cultural variations in cyber bullying across Europe and beyond.
- Smith, P. K., Görzig, A., & Robinson, S. (2019). Cyberbullying in schools: Cross-cultural issues. In *Cyberbullying in schools, workplaces, and romantic relationships* (pp. 49-68). Routledge.
- Sofee, S. F. M., Aziz, A. A., & Mohamed, S. (2022). Redefining Social Activism through the Transition towards User Generated Content in Malaysia. *Journal of Media and Information Warfare Vol*, 15(3), 54-67.
- Statista. (2023). Global social media users by platform 2023. Statista. <https://www.statista.com/statistics/1109866/number-social-media-users-worldwide-select-platforms/>

- Star, t. (2022). Malaysia is 2nd in Asia for youth cyberbullying. <https://www.thestar.com.my/news/nation/2022/01/14/malaysia-is-2nd-in-asia-for-youth-cyberbullying>
- Sudarwanto, A. S., & Kharisma, D. B. B. (2022). Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia. *Journal of Financial Crime*, 29(4), 1443-1457.
- Teimouri, M., Hassan, M. S., Bolong, J., Daud, A., Yussuf, S., & Adzharuddin, N. A. (2014). What is Upsetting Our Children Online? *Procedia - Social and Behavioral Sciences*, 155(October), 411–416. <https://doi.org/10.1016/j.sbspro.2014.10.314>
- Teimouri, M., Hassan, M. S., Griffiths, M., Benrazavi, S. R., Bolong, J., Daud, A., & Adzharuddin, N. A. (2016). Assessing the Validity of Western Measurement of Online Risks to Children in an Asian Context. *Child Indicators Research*, 9(2), 407–428. <https://doi.org/10.1007/s12187-015-9316-4>
- UNICEF. (2020). *Keeping children safe online during the COVID-19 pandemic*. UNISEF Malaysia. <https://www.unicef.org/malaysia/reports/keeping-children-safe-online-during-covid-19-pandemic>
- Vogels, E. A., & O'Sullivan, L. F. (2019). The relationship among online sexually explicit material exposure to, desire for, and participation in rough sex. *Archives of Sexual Behavior*, 48(2), 653–665.
- Willard, N. E. (2007). *Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress*. Research press.
- Wireless Malaysian. (2014, September 8). DiGi CyberSAFE in Schools report: 83% of Malaysians school children are vulnerable to online risks. [https://www.malaysianwireless.com/wp-content/uploads/2014/09/DiGi-CyberSAFE\\_Survey\\_Report\\_2014.pdf](https://www.malaysianwireless.com/wp-content/uploads/2014/09/DiGi-CyberSAFE_Survey_Report_2014.pdf)
- Wolak, J., Mitchell, K., & Finkelhor, D. (2007). Unwanted and wanted exposure to online pornography in a national sample of youth Internet users. *Pediatrics*, 119(2), 247–257. <https://doi.org/10.1542/peds.2006-1891>
- YaM. (2020). *Digital citizenship*. <https://doi.org/http://youthandmedia.org/digital-citizenship/>
- Yusop, N., & Al-Shami, S. A. (2021). Risk and Protecting Factors of Cyberbullying in Malaysia: A Comparative Analysis. *Ulum Islamiyyah*, 33(S5), 101-112.
- Yusuf, S., Osman, M. N., Hassan, M. S. H., & Teimoury, M. (2014). Parents' Influence on Children's Online Usage. *Procedia - Social and Behavioral Sciences*, 155, 81–86. <https://doi.org/10.1016/j.sbspro.2014.10.260>

- Zhao, R., Zhou, A., & Mao, K. (2016, January). Automatic detection of cyberbullying on social networks based on bullying features. In *Proceedings of the 17th international conference on distributed computing and networking* (pp. 1-6).
- Zhong, M., Huang, X., Huebner, E. S., & Tian, L. (2021). Association between bullying victimization and depressive symptoms in children: The mediating role of self-esteem. *Journal of affective disorders*, 294, 322-328.
- Zhong, Jinping, Jing Qiu, Min Sun, Xiunan Jin, Junyi Zhang, Yidong Guo, Xinxin Qiu, Yujie Xu, Jingxiu Huang, and Yunxiang Zheng. "To Be Ethical and Responsible Digital Citizens or Not: A Linguistic Analysis of Cyberbullying on Social Media." *Frontiers in Psychology* (2022): 2203.
- Zlamal, R., Machackova, H., Smahel, D., Abramczuk, K., Ólafsson, K., & Staksrud, E. (2020). *EU Kids online 2020: Technical report*.



# In This Issue

## *Note from the Editor*

## *Research Articles*

**Muhammad Faris Abdullah, Mohamad Sahari bin Nordin, Suhailah binti Hussien, Norhayati Mohd. Alwi & Noor Suzilawati binti Rabe**

Validation of a *Sejahtera* Living Index Using the Rasch Model

**Fatmir Shehu**

Investigating Ismā'īl Rājī al-Fārūqī's Methodology in the Study of Christianity through Selected Textual Analysis from His *Christian Ethics*

**Mirsad Karić, Šejma Aydin, Huseyin Korkut & Muhidin Mulalić**

Paradoxical and Insufficient? Gender Quotas and Placement Mandates in Bosnia and Herzegovina's 2020 Local Elections

**Aida Mokhtar & Faiswal Kasirye**

Gestalt and Semiotic Analyses of Brand Communication on Disability Inclusion: The Case of Malaysia and the US

**Roy Anthony Rogers, Noraiz Arshad & Iftikhar Ali**

Understanding the Decline of Pakistan-US Alliance and the Growing Influence of China in Pakistan

**Sarina Yusuf, Misha Teimouri, Muhamad Shamsul Ibrahim, Nan Zakiah**

**Megat Ibrahim, Syahida Mohd Nazri & Stephanie Ann Victor**

Let's Think They are Safe Online! A Malaysian Perspective on The Classification of Children's Cyber Risks

**Farah Fazlinda Mohamad, Khazaila bt Zaini & Nur Syahidatul Idany**

Social Media Use for English Learning in Southeast Asia: A Systematic Review

**Ali Mehellou, Mohamad Saifudin Mohamad Saleh & Bahiyah Omar**

*Maqāṣid al-Sharī'ah* as Goal Framing for Sustainable Behaviours: A Conceptual Framework

**Siti Aisha Joharry**

Faith in The Time of Coronavirus: A Corpus-assisted Discourse Analysis

**Abdul Manan Ismail, Ahmad Syukran Baharuddin & Muhammad Hazim Ahmad**

COVID-19: Analysing the Principle and Application of *I'tibār Ma'ālāt* in the Selected *Fatwas* Issued by the Malaysian National Council for Islamic Religious Affairs (MKI)

**Sharifah Nursyahidah Syed Annuar & Muhamad Takiyudin Ismail**

The Challenges of Civil Society Organisations: NGO-isation of Resistance in Malaysia?

**Anhar Anshory, Ahmad Faizuddin Ramli & Ramli Awang**

The Authenticity of Theology in Scientific and Technological Thinking

## *Research Notes*

**Alwi Alatas, Agus Setiawan, Achmad Sunjayadi & Yunadi Ramlan**

The Seminar on *Da'wah* in Kuala Lumpur in 1977 and the Emergence of *Hijab* Awareness in Indonesia

## *Book Review*

ISSN 0128-4878 (Print)

ISSN 2289-5639 (Online)





[Back to results](#) | 1 of 1[Download](#) [Print](#) [Save to PDF](#) [Add to List](#) [Create bibliography](#)**Intellectual Discourse** • Volume 31, Issue 1, Pages 139 - 160 • 2023**Document type**

Article

**Source type**

Journal

**ISSN**

01284878

[View more](#)

# Let's Think They are Safe Online! A Malaysian Perspective on The Classification of Children's Cyber Risks

[Yusuf, Sarina<sup>a</sup>](#) ; [Teimouri, Misha<sup>b</sup>](#) ; [Ibrahim, Muhamad Shamsul<sup>c</sup>](#) ;[Ibrahim, Nan Zakiah Megat<sup>d</sup>](#) ; [Nazri, Syahida Mohd<sup>e</sup>](#) ; [Victor, Stephanie Ann<sup>a</sup>](#) [Save all to author list](#)<sup>a</sup> Department of Communication and Media, Faculty of Languages and Communication, Universiti Pendidikan Sultan Idris, Malaysia<sup>b</sup> Department of Public Relation, University of Applied Science and Technology, Tehran, Iran<sup>c</sup> Department of Media and Communication Studies, Faculty of Arts and Social Sciences, University Malaya, Malaysia<sup>d</sup> Universiti Poly-Tech Malaysia, Malaysia[View additional affiliations](#) [View PDF](#) [Full text options](#) [Export](#)

Cited by 0 documents

Inform me when this document is cited in Scopus:

[Set citation alert >](#)**Related documents**[A Model of Online Protection to Reduce Children's Online Risk Exposure: Empirical Evidence From Asia](#)[Teimouri, M. , Benrazavi, S.R. , Griffiths, M.D. \(2018\) \*Sexuality and Culture\*](#)[Effects of Cybervictimization on the Mental Health of Primary School Students](#)[Sidera, F. , Serrat, E. , Rostan, C. \(2021\) \*Frontiers in Public Health\*](#)[The Amplification of Cyberhate Victimization by Discrimination and Low Life Satisfaction: Can Supportive Environments Mitigate the Risks?](#)[Görzig, A. , Blaya, C. , Bedrosova, M. \(2023\) \*Journal of Early Adolescence\*](#)[View all related documents based on references](#)[Find more related documents in Scopus based on:](#)[Authors >](#) [Keywords >](#)**Abstract**

Author keywords

Sustainable Development Goals 2023

SciVal Topics

Funding details

**Abstract**


Children currently spend more time on the Internet and corresponding technologies to socialise virtually and play video games. Scholars have not reached a consensus on whether children's participation in such recreational activities is beneficial or detrimental. Although Malaysian parents are concerned about the digital threats that may be encountered by their children, most of the detriments remain unknown. Children still hesitate to inform their families about their online exposure to inappropriate content, such as cybersex and pornography, which remain taboo subjects in Malaysian households. This study performed a descriptive analysis to determine the risk factors associated with

children's internet use with 420 school-going children aged from 9 to 16 years around Selangor. Resultantly, children were highly exposed to unwanted exposure to pornography (17.4 %), potentially dangerous user-generated content (9 %), sexting (8.8 %), personal data misuse (6.4 %), cyber grooming (3.3 %), and cyberbullying (1.7 %) in the past 12 months of using the Internet. © IIUM Press.

## Author keywords

cyberbullying; digital generation; personal data misuse; sexting; unwanted exposure to pornography

---

Sustainable Development Goals 2023 

New



---

SciVal Topics 



---

Funding details



## References (64)

[View in search results format >](#)

☐ All

[Export](#)



[Print](#)



[E-mail](#)



[Save to PDF](#)

[Create bibliography](#)

- 
- ☐ 1 Abd Rahman, M., Jaafar, N. H., Ismail, Z., Khalid, R. M., Saúdah, N., Zamani, N. D., Mokhtar, R.  
Children's Online Safety: Literature Review  
(2022) *International Journal of Technology Management and Information System*, 4 (3), pp. 17-25.

- 
- ☐ 2 Adebayo, D.O., Ninggal, M.T., Bolu-Steve, F.N.  
**Relationship between demographic factors and undergraduates' cyberbullying experiences in public universities in Malaysia**  
  
(2020) *International Journal of Instruction*, 13 (1), pp. 901-914. Cited 11 times.  
[http://www.e-iji.net/dosyalar/iji\\_2020\\_1\\_58.pdf](http://www.e-iji.net/dosyalar/iji_2020_1_58.pdf)  
doi: 10.29333/iji.2020.13158a

[View at Publisher](#)

- 
- ☐ 3 Arifin, N.A., Mokhtar, U.A., Hood, Z., Tiun, S., Jambari, D.I.  
**Parental awareness on cyber threats using social media**  
  
(2019) *Jurnal Komunikasi: Malaysian Journal of Communication*, 35 (2), pp. 485-498. Cited 18 times.  
<http://ejournal.ukm.my/mjc/article/download/33515/9624>  
doi: 10.17576/JKMJC-2019-3502-29

[View at Publisher](#)

- 
- ☐ 4 ASANAN, Z. Z. B. T., Hussain, I. A., Laidey, N. M.  
(2016) *A study on cyberbullying: Its forms, awareness and moral reasoning among youth Asia Pacific University*
-