Sexuality & Culture (2018) 22:1205–1229
https://doi.org/10.1007/s12119-018-9522-6

ORIGINAL PAPER

A Model of Online Protection to Reduce Children's Online Risk Exposure: Empirical Evidence From Asia

Misha Teimouri[1] · Seyed Rahim Benrazavi[2] · Mark D. Griffiths[3] · Md Salleh Hassan[4]

Published online: 27 April 2018

Abstract Children are surrounded by a variety of digital media and are exposed to potential risks that come with such easy accessibility. Learning how to be safe online is an important consideration for both children and their caregivers. The present study proposes an integrated model of online safety based on constructs from protection motivation theory and the health belief model, namely perceived severity of (and susceptibility to) risk, online self-efficacy, online privacy concern, and digital literacy. The study comprised a survey conducted among 420 schoolchildren aged 9–16 years. Using partial least squares-structural equation modelling, the results illustrated the presence of a negative effect of 'perceived severity of online risk' toward online risks, whereas the effect of 'digital literacy' was found to be positive. Children whose perception of online risks was more severe were less exposed to online risks if they had higher 'online privacy concerns' than the children with

✉ Misha Teimouri
misha.teimoury@gmail.com

Seyed Rahim Benrazavi
rahim.benrazavi@gmail.com

Mark D. Griffiths
mark.griffiths@ntu.ac.uk

Md Salleh Hassan
salleh5045@gmail.com

[1] Faculty of Communication, Islamic Azad University E-Campus, Sarv, Tehran, Tehran Province, Iran

[2] Faculty of Philology, Institute for Media Studies, Ruhr University Bochum, Bochum Süd, Universitätsstraße 150, 44801 Bochum, Germany

[3] International Gaming Research Unit, Psychology Department, Nottingham Trent University, Burton Street, Nottingham NG1 4FQ, UK

[4] Faculty of Modern Languages and Communication, Department of Communication, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia

higher ‘digital literacy’ who are more exposed to online risk. Results of the study show that engaging in safe online behaviour requires children to have a high perception regarding severity of online risks as well as knowledge of online privacy concerns. Online risks and opportunities occur in parallel. Consequently, the factors that increase or decrease risk may also increase or decrease the benefits.

Keywords Children’s online risk exposure · Online risk perception · Self-efficacy online · Online privacy concerns · Digital literacy

Introduction

For a period of time, television and film were the only audio-visual medium to which most children were exposed (Clark 2011). The risks associated with children’s television viewing were primarily limited to exposure to sexual content (Peterson 1991) and violent content (Goldstein 1998), the nature of which were known and relatively easy to control. Today, children are surrounded by a variety of digital media content, and therefore they are exposed to many risks that have not yet been fully identified or quantified. Within the academic literature, studies indicate the risks of online activities for children have escalated substantively but that it is difficult to obtain an accurate picture of online risks and harms (Lareki et al. 2017; Slavtcheva-Petkova et al. 2015).

The existing literature claims protection practices have substantial effects on the negative consequences of Internet usage, depending on how much (1) individuals believe in their vulnerability to (and severity of) online risks (Camacho et al. 2014; Chen et al. 2016a; Yau et al. 2014), (2) individuals believe in their ability to tackle online protective practices (Chen et al. 2016b; Görzig 2016), and (3) their knowledge of Internet safety and safe behaviours online (Farrukh et al. 2014).

Despite the high possibility of encountering online risk, there is no universally accepted definition of online risks or the best way to keep children safe online. However, it is possible to reduce unpleasant consequences experienced by children by providing them with educational strategies alongside training concerning self-protection techniques. Risk perception mediated by protective action, together with children’s beliefs about their ability to perform risk-reducing behaviour, are likely to help children to engage in coping behaviour and therefore protecting themselves (Youn 2009). Empirical research examining the effects of protection motivation constructs (e.g., self-efficacy, perceived severity, and susceptibility) and safety behaviour in reducing risks are inconclusive. While some researchers have found a significant relationship between self-efficacy and protective behaviour (Feng and Xie 2014), others have not (Mohamed and Hawa 2012).

Studying the global concern of youth protection against potential threats of digital media requires evaluation of international studies in the field. A German media initiative by the National Center for Media Communication (Südwest 2017) asserted that effective promotion of media competences, and cooperation in this field are essential beyond national boundaries. This organisation cooperates with various media institutions and companies across borders to provide a safer online experience for the children and young adults (Südwest 2017). Likewise, Siero (2017) in Dutch guidelines for supporting teachers in teaching digital literacy, indicated that, students are in a great need of education about the proper application of digital media. This research notes that only 30% of students in secondary education are able to gather and process digital information without additional guidance. Therefore, schools have to reconsider what and how teachers should prepare their students for the twenty-first century. A report by UNICEF (2017) points out that even the present generation of children are digital natives, that does not mean they do not require guidance and support to make the most of connectivity. Similarly, they do not automatically understand their vulnerability to online risks or take their own responsibility to be good digital citizens. Digital literacy—whether coming from teachers, parents or the media—increases children's ability to protect themselves against online risks. This includes teaching children how to protect themselves from online dangers including cyberbullying, sextortion, and loss of privacy, as well as teaching concerning reputational risk, utilizing safety and protection features, solving related problems, and building up efficiency in doing so (UNICEF 2017).

Although studies defining the risks of online activity for children have increased substantially, within the academic literature, it is difficult to get a clear picture of online risks and safety practices. Risks and harms caused by using the Internet are varied and rather unidentified, as are safety practices (Dönmez et al. 2017; Farrukh et al. 2014; Slavtcheva-Petkova et al. 2015). Considering this gap, the present study aims to identify the influence of children's self-protection techniques against online risks, in an attempt to contribute to a deeper perspective on the nature of the risks associated with Internet usage among children. More specifically this study is conducted to determine the effect of (1) "perceived severity of (and susceptibility to) online risk", (2) "online self-efficacy", (3) "digital literacy", and (5) "online privacy concerns" on "online risk" as well as testing the mediation effect of (6) "online privacy concerns" on the relationship between "perceived severity of (and susceptibility to) online risk" and "online risk".

Definitions of Online Risk

There is a broad range of possible risks to children from online activities. Countries' definition of risks and means of protecting children against these risks are different according to culture, legal framework, and style of government. Little research has examined online risk using a standard measurement. However, as discussed by Organisation for Economic Co-operation and Development (OECD 2012), a systematic approach to the classification of online risks to children has been developed by OSTWG, Internet Safety Technical Task Force (ISTTF), European Youth Protection Roundtable Toolkit (YPRT), and the Family Online Safety Institute (FOSI). The OSTWG defines the categories of online risks as predator danger, cyberbullying, sexting, and inappropriate content (OSTWG 2010). The ISTTF identifies sexual solicitation, online harassment, and problematic content as a subgroup of online risks (Berkman Center for Internet and Society 2008). Based on the same context 'perceived severity of online risk' is defined as the partisipants understanding of the gravity and the concequences of exposure to online riskd whereas 'perceived susceptibility to online risk' is defined as the perception of a child from the probability of exposure to online risks. The YPRT establishes the types of risks related to online content (e.g., violent/illegal content, racism, child pornography, etc.) (YPRT Toolkit 2008). Finally, the FOSI introduced the classifications of teen identity theft, fraud, being tracked for marketing, being bullied, ugly/unflattering pictures posted, and security issues on the Internet (Family Online Safety Institute 2013).

Another systematic study into online risk, which is repeated every 5 years in the United States, is conducted by the Youth Internet Safety Survey (YISS) in order to quantify the unwanted or problematic experiences of younger Internet users, including unwanted exposure to pornography, and sexual solicitation/harassment (Jones et al. 2013; Ybarra and Mitchell 2005).

The European Kids Online survey, was a research network, and utilized interviews with 25,000 children and their parents in 25 European countries from 2006 to 2009, and aimed to study the Internet and new online technologies and identify findings across Europe, with a view to evaluating online opportunities and risks for children, their responses along with parents' involvement (Livingstone et al. 2011b). EU Kids Online developed a classification of child-related online risks including content risks (whereby the child is a recipient of unwelcome or inappropriate contents), contact risks (whereby the child participates in risky peer or personal communication), and conduct risks (whereby the child acts themselves to contribute to risky content or contact).

Although many studies have been conducted in various countries, Malaysia-specific classification of online risks have yet to be identified. While surveys have been conducted by the Ministry of Science, Technology and Innovation, MCMC, and the Women, Family and Community Development Ministry, most of them only share descriptive-based results (Salman and Hasim 2011; MCMC 2011, 2012). Furthermore, in Malaysia, children are limited when it comes to talking about the sex-related issues they may face online. Consequently, studies on these topics are rare, and many issues remain unexplored, such as those concerning the definition of online risk and measurement.

As the number of children who access and use the Internet increases, the exposure to various forms of online risks also increases (Lareki et al. 2017; Teimouri et al. 2016). Conceptualized in prior studies outlined above, online risks refer to a set of wanted or unwanted inappropriate activities by children (as an actor, a receiver, or a participant), which includes (1) *unwanted sexual solicitation*, such as requests to be exposed to unwanted sexual activities/sexual talk/divulging sexual information against their will (Chang et al. 2016; Lareki et al. 2017); (2) *risky sexual online behaviour*, in which children participate in sexual behaviour online (Moore et al. 2017; Teimouri et al. 2014); (3) *potentially harmful content*, where children are exposed to online violent content such as self-harm, suicide, pro-anorexia, drugs, hate/racism (Schilder et al. 2016); *sexting,* which refers to sending/receiving sexual images/videos/texts online (Samimi and Alderson 2014); (5) *cyber-bullying,* which refers to children being the victim of aggressive behaviour in the cyberspace (Vaillancourt et al. 2017), and (6) *personal data misuse,* whereby children's information is misused or they are a victim of Internet fraud or theft (Teimouri et al. 2016). Online risks that children are exposed to, could generally be defined as any wanted or unwanted inappropriate activities by children (as an actor, a receiver, or a participant) which in the present study are specified as: unwanted sexual solicitation, risky sexual behaviour, potential harmful content, sexting, bullying, and personal data misuse.

Online Risk and Protection Motivation Behaviour

A review of the theoretical literature demonstrates that a reduction in risky online behaviour requires an individual to assess the severity of online risks, the probability of the occurrence of online risks caused by unsafe Internet usage, self-efficacy of protective action to prevent the threat, and the ability to perform protection behaviours while online. Theories of behaviour change to promote healthy behaviour have considered three main areas: (1) individual as a unit of change, (2) changing with the family, and (3) changing with the community (Glanz and Rimer 2005). These types of theories that have been borrowed from healthcare are known as the expectancy-value approaches that examine: (1) how well a person can perform a task, and (2) the reason for performing a task or change (e.g., health belief model; protection motivation theory) (Ng et al. 2009). In order to change some aspect of behaviour or take a healthy action, individuals need to be assured of the benefits they will get or the risks they may avoid. Few studies have focused on children's online protecting behaviours. Considering these issues and potential online risks outlined above, the purpose of the present study was to (1) identify the level of online risks that children are exposed to, (2) identify their perception of online risks, and (3) determine how children protect their privacy online.

The literature claims protection practices have substantial effects on the negative consequences of Internet usage, and it depends on the level of (1) individuals' belief in their vulnerability to (and severity of) online risks (Taddei and Contena 2013), (2) individuals belief in their ability to take protective practices, and (3) their knowledge about safety behaviours (Shillair et al. 2015; Waddell et al. 2014). One of the factors that may influence willingness to adopt protective actions is risk perception. The perceived vulnerability or likelihood of encountering online risk combined with perceived severity can be viewed as online perceived risk (Zwart et al. 2009). Young Internet users are not always concerned about the negative consequences caused by online high-risk activities such as sharing information or making friends online. Higher perceived severity of (and susceptibility to) online risk clearly advocates that children need to protect themselves from online risks such as cyber-bullying (Camacho et al. 2014), unwanted online sexual solicitation, and risky online sexual behaviour (Baumgartner et al. 2010).

Although the awareness of privacy protection is raised by increasing Internet usage, children appear to have a different sense of privacy, subject to factors such as age and gender (Livingstone and Görzig 2012). Most studies investigating online protection behaviour mainly focuses on disseminating information, but fail to consider how to protect oneself in a high-risk situation such as an online sexually-related threat. Together with beliefs about being vulnerable to risk and taking protected action, children need to acquire skills in dealing with high-risk situations while online. These skills are known as digital literacy (OECD 2012; Wisniewski et al. 2014). Digital literacy refers to a combination of knowledge, skills, and ability to use the Internet and being aware of the consequences. Children's level of digital literacy is highly associated with the way they use the internet (Livingstone and Görzig 2012). While many children establish digital literacy skills, a lack of risk awareness may explain negligence regarding information security (OECD 2012). This means that digital literacy may boost and improve children's online experience. However, it does not seem to increase awareness by itself.

To promote online protection behaviour, researchers have used the construct of online self-efficacy (Ekizoglu and Ozcinar 2010). Online self-efficacy is an individual's belief that they are capable and confident of recognizing and dealing with the risky situation (Lee et al. 2008). Computer self-efficacy is increased by increasing computer use and could be improved by training (Chen 2017). It was also debated that by increasing self-efficacy, individuals can deal with some forms of online threats such as cyberbullying (Cross and Barnes 2015). At the same time, a user's sense of personal responsibility has positive effects on online safety interventions (Shillair et al. 2015). Overall, children's online protection behaviour has been found to be an effective safeguard for children to be aware, prepared, and safe in the case of undesired, unpleasant, and/or hurtful experiences when using the Internet.

Theoretical Perspectives

While there is no specific theory underlying how online safety should be implemented, researchers have borrowed constructs from theories that focus on health behaviour in order to generate models for promoting safe online behaviour. Hence, the theoretical framework for this study is based on aspects of the protection motivation theory (PMT) and the health belief model (HBM). The present authors specifically applied the constructs of perceived severity of (and susceptibility to) online risk, or how likely it is for a youth to be exposed to online threats such as cyberbullying, self-efficacy in relation to online safety concerns, and how efficient young people regard themselves in safeguarding themselves against exposure to online threats, as well as theories of behaviour change to promote healthy behaviour. These theories have considered three main areas: (1) individuals as a unit of change whereby, planners tend to explain and influence the behaviour of individuals with regards to self-protection and prevention of exposure to online threats, (2) changing the family, whereby, planners try to explain and influence the role of family in protection and prevention of exposure to online threats, and (3) changing the community, whereby, planners take on explaining and influencing communities with regards to youth protection and prevention of exposure to online threats (Glanz and Rimer 2005). These types of theories have been borrowed from healthcare and they are known as the 'expectancy-value approach' that examine: (1) how well a person can perform a task, and (2) the reason for performing a task or change (e.g., health belief model; protection motivation theory) (Ng et al. 2009). In order to change some aspect of behaviour or carry out a healthy action, individuals need to be assured of the benefits they will get or the risks they may avoid.

The PMT was initially formulated by Rogers (1975). Later, Rogers et al. (1983) extended the theory by highlighting cognitive processes to a general scheme of persuasive communication for behavioural change. In some studies, PMT was initiated as a result of two appraisal processes of health threat in adaptive and maladaptive coping behaviour. PMT originally proposed to share the HBM emphasis on the cognitive processes mediating attitudinal and behavioural change (Prentice-Dunn and Rogers 1986). The HBM is one of the primary theories of health behaviour and is widely recognized in the field. It was developed in the 1950s by a group of U.S. Public Health Service social psychologists who wanted to explain why so few people were participating in tuberculosis detection and prevention programs (Janz and Becker 1984). The HBM initially offered four key concepts (perceived susceptibility, perceived severity, perceived benefits, and perceived barriers). The concept of 'self-efficacy' was added to meet the challenges of unhealthy behaviours such as smoking and overeating. The PMT was an extension and re-working of HBM Intention to protect individuals from risky health behaviours by educating them about the threat appraisal (severity and susceptibility), and coping (response efficacy, self-efficacy) (Rosenstock et al. 1988).

The PMT model is widely employed as a model for safe decision-making and taking actions regarding health behaviour. Likewise, researchers have begun utilizing PMT to predict and identify online threats and suggest protective actions to understand children's perception of risks safeguards. Some examples of such predictive, preventive, and comprehensive behaviours could be (1) identifying online security behaviour such as password management and obtaining security training (Stanton et al. 2004); (2) proposing a conceptual model of user security behaviour based on risk perception (Aytes and Conolly 2003); (3) attitudes towards online gambling and player protection (Wijesingha et al. 2017); (4) examining online privacy concern in *Facebook* users (Saeri et al. 2014) and teens' online privacy protection and subsequent online information disclosure on social network sites (Chen et al. 2016b); and (5) understanding individual email protection (Herath et al. 2014). The HBM has also been utilized to explore users' perceptions of being safe and secure online (Davinson and Sillence 2014), and the impact of online and offline friendship networks on adolescent smoking and alcohol use (Huang et al. 2014). Youn (2005), tested the threat appraisal component of PMT to examine the context of online safety and found that higher levels of risk perception motivate teenagers to protect themselves from online privacy threats.

Drawing from a number of related theories, the present study assessed children's level of privacy concerns, children's perception of exposure to online risks, safety in taking online protection behaviour, and online self-efficacy. Research has demonstrated that a reduction in risky online behaviour requires an individual to assess the severity of online risks, the probability of the occurrence of online risks caused by unsafe Internet usage, self-efficacy of protective action to prevent the threat, and the ability to perform protection behaviours while online. In the present study, online protection behaviour (motivation) refers to risk perception and protection action. Risk perception is defined by two concepts: (1) *perceived susceptibility to online* *risk* (referring to a child's perception of the potentiality of harm or abuse) and (2) *perceived severity of online risk* (referring to a child's perception of how serious an online risk is and what its consequences are) (Glanz and Rimer 2005). Protection action is defined by three concepts: (1) *online privacy concern* (referring to when a child knows how to protect themselves from the potential risks posed by the Internet, and has the basic knowledge and skills to protect themselves during their online activities), (2) *online self-efficacy* (referring to a child's perception of how capable they are of understanding the risk caused by the Internet and their ability to take protective action against negative outcomes), and (3) *digital literacy* (referring to a child's knowledge about and capability of using the Internet and dealing with possible risks.

Method

Participants and Procedure

A total of 420 Malaysian primary and secondary school students aged 9–16 years in eight schools participated in this study. The population comprised children living in the Malaysian state of Selangor, which has the highest rate of Internet use in Malaysia's 13 states for the last 10 years. Two of these were randomly selected to be the sampling location. Then, the two selected districts were divided according to urban and rural areas. Four pairs of national primary and regular secondary schools in rural and urban (in both districts) areas were randomly selected, based from the list of schools available in Education Management Information System online portal. The researcher needed to meet the children several times to gather data from them and also to collect the response from their respective parents/guardian'. This is the reason that making the schools the perfect place from which to collect data. The schools were asked to disclose the total number of their student populations. The total population was 6671 across the eight selected schools. A sample size of 420 was required based on the assumption of the partial least square application. The children were stratified according to their age-group categories, and those students who returned the signed consent letter from their parents participated in the survey. The sample comprised 34% boys and 66% girls with the mean age of 12.6 years. The participants were asked to provide their feedback based on their personal experience online rather than placing themselves in a hypothetical situation.

Materials

The survey was completed offline using a 'paper and pencil' method. Children's exposure to online risks were assessed using items from the final reports of two national studies in Europe (EU Kids Online Survey, among 25,142 children aged 9–16 and their parent/guardians in 25 European Countries 2006–9) and the United States [Youth Internet Safety Survey (YISS-1, 2000; YISS-2, 2005; YISS-3, 2010)]. A total of 39 items across six constructs were adapted. Due to the sensitivity of the topic, the Malaysian Ministry of Education required sensitive words to be replaced and/or removed from the children's questionnaire in order to be approved for data collection. Thus, "having sex" was replaced by "having an inappropriate intimate relationship"; "naked pictures" and "showing sexual acts and content" were replaced by "obscene pictures" and "obscene acts or materials" respectively.

Children were asked to answer 39 questions concerning exposure to online risks with 12 questions assessing perceived online safety, and 22 items assessing online protection motivation. The children's questionnaire displayed cartoon characters that are popular with Malaysian children to engage them in completing the survey. The six constructs of exposure to online risks used in the study were: (1) a six-item scale for assessing 'unwanted exposure to pornography'; (2) a four-item scale assessing 'risky sexual online behaviour' adapted from Youth Internet Safety Survey 1, 2, and 3 (Finkelhor et al. 2008, 2011; Jones et al. 2012); (3) an eight-item scale assessing 'sexting', (4) a seven-item scale assessing 'potentially harmful user-generated content, (5) a nine-item scale assessing bullying, and (6) a five-item scale assessing personal data misuse adapted from EU Kids Online Survey (Livingstone et al. 2011a, b).

Five constructs were identified to assess the level of children's online self-protection behaviour: (1) perceived severity of exposure to online risk was assessed by seven items adapted from EU Kids Online, (2) perceived susceptibility of exposure to online risk was assessed by five items from Wirth et al. (2008) and Youn (2010), (3) online self-efficacy was assessed using two questions addressing 'privacy self-efficacy' adapted from Youn (2009); furthermore, four questions from Ng et al. (2009) were used to address user's self-confidence in their ability to practice computer security, together with two items of Internet self-efficacy adapted from EU Kids Online Survey were used; (4) online safety concern was assessed using the six-scale adopting from Youn (2009) which addresses the level of concerns for online privacy, and (5) for assessing digital literacy, eight items of children's digital literacy and safety skills adopted from EU Kids Online was used. The six constructs of children's exposure to online risks and five constructs of the level of children's online self-protection behaviour are presented in Table 1.

In the present study, data were analyzed using partial least square-structural equation modeling (PLS-SEM) with SmartPLS, 3. PLS-SEM was used because the model is less developed and is complex with many latent variables and indicators. Furthermore, the data are not normally distributed with a combination of formative and reflective measurement models (Hair et al. 2013). First, the measurement model including the convergent and discriminant validity was assessed. This was followed by a structural model to test the hypothesized paths between latent constructs.

Measurement Model-PLS Procedure

In order to assess the validity and reliability of measurement model, the reflective constructs were evaluated [i.e., perceived severity of (and susceptibility to) exposure to online risk, online self-efficacy, online safety concerns, and digital literacy], followed by the formative constructs (children's exposure to online

Table 1 Constructs examined in the present study

Variables	Constructs
Children's exposure to online risks (adopted from EU Kids Online) (six constructs)	
	Unwanted exposure to pornography
	Risky sexual online behaviour
	Potential harmful user-generated content
	Sexting
	Cyberbullying
	Personal data misuse
Level of children's online self-protection behaviour (five constructs)	
Perceived online safety	
	Perceived severity of exposure to online risk (EU Kids Online)
	Perceived susceptibility of exposure to online risk (Wirth et al. 2008; Youn 2010)
Online protection motivation (level of children's online self-protection behavior)	
	Online self-efficacy (Youn 2009; Ng et al. 2009)
	Online safety concern (adopted from EU Kids Online)
	Digital literacy (adopted from EU Kids Online)

risks). To check the validity of reflective measurement, the results for the outer loadings, composite reliability, and AVE were presented. Convergent validity and cross loading were checked applying Fornell–Larker criteria (Table 2). Based on Fornell–Larker criteria (Hair et al. 2014, p. 111), the square root of AVE for each construct was higher than the construct's highest correlation with other constructs, which indicates the achievement of convergent validity. During the modification of the reflective measurement model, two indicators with lower loading were excluded for further procedures. The following (1) 'I am able to use a false name or false ID' from online privacy concerns; and (2) 'I am able to find information to use the Internet safely' from digital literacy. The other indicators with loadings of between 0.4 and 0.7 were retained in the construct given that the

Table 2 Reflective discriminant validity (Fornell–Larker criterrium)

Constructs		1	2	3	4	5
1	Digital literacy	0.72				
2	Online protective behaviour	0.63	0.73			
3	Online self-efficacy	0.56	0.44	0.84		
4	Perceived severity of exposure to online risk	0.4	0.49	0.47	0.87	
5	Perceived susceptibility to online risk	0.19	0.22	0.23	0.58	0.9

deleting indicators did not significantly increase AVE and composite reliability of constructs (Figs. 1 and 2, Table 3).

For the evaluation of the formative measurement model, convergent validity, collinearity assessment, and significant of indicators were assessed. Exposure to online risks was defined as the higher-component formative measurement with six constructs. Firstly, convergent validity was examined using redundancy analysis by correlating indicators of each formative construct with a 'global item/measure' for that construct. Global item is summarized as the essence of the construct and the researcher can develop it (Hair et al. 2014), in the present study, all six formative constructs were tested by redundancy analyses and met the criteria of convergent validity since all exceeded the threshold (path coefficient above 0.8) (Table 4).

Next, collinearity of the indicators was detected by evaluating variance inflation factor (VIF). All VIF values were less than 0.5, which demonstrated there was no multicollinearity issue. High correlations are not expected among indicators since they are not interchangeable (Hair et al. 2014). Following this, the statistical significance of the outer weights was assessed using a bootstrapping option. The results of the exposure to online risk to children's construct show that all formative indicators were significant except the "Seen anorexia or bulimia" indicator which has been deleted (Fig. 3, Table 5).

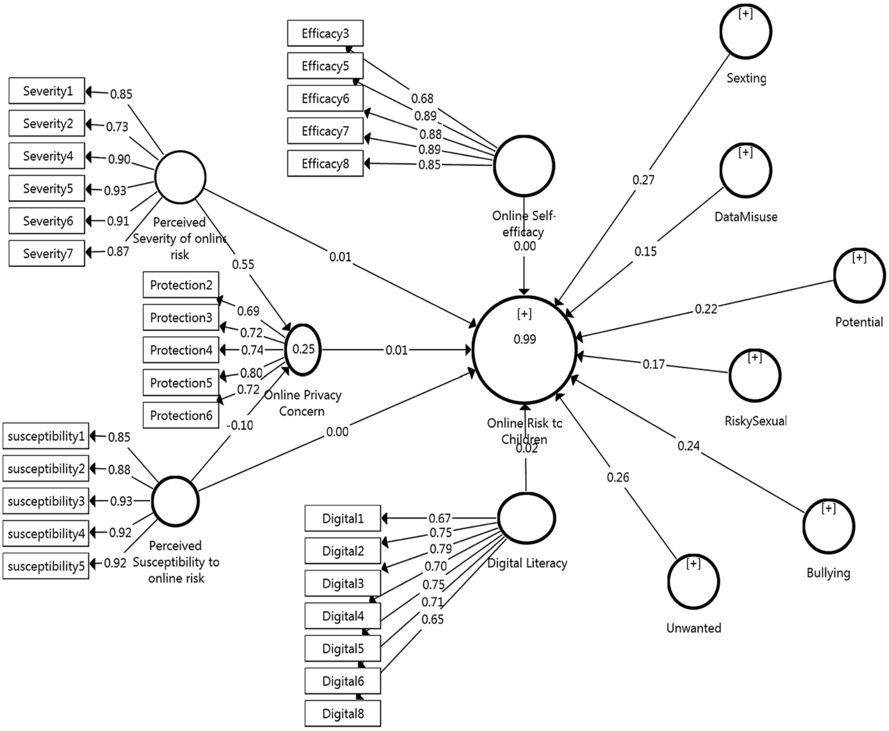

Fig. 1 Reflective measurement model (initial)

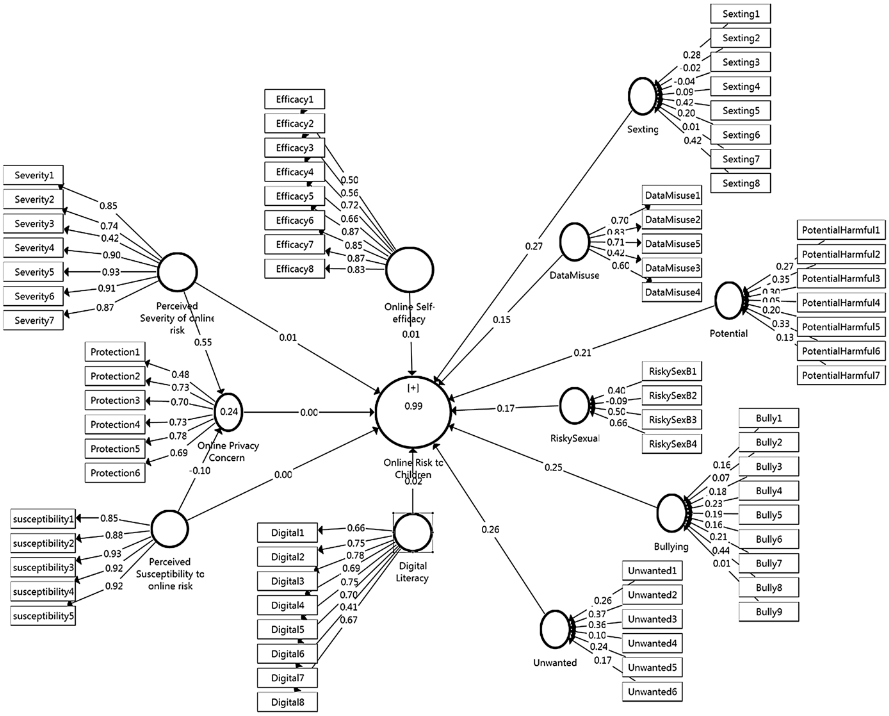

Fig. 2 Reflective measurement model (modified)

Results of Structural Model-PLS Procedure

The relationships between latent variables were assessed by running a PLS algorithm. The structural model result is presented in Table 6. To test the mediation effect, a common method of direct–indirect effect suggested by Hair et al. (2014) was used through the relationship between independent and dependent variables with/without including the mediator (Table 6, Fig. 4). The result of hypothesis testing showed that while perceived severity of an online risk reduced exposure to online risks to children ($\beta = -0.16$, $p = 0.01$), perceived susceptibility to online risk was not significant predictor in reducing children's exposure to online risks ($\beta = 0.088$, $p = 0.07$). The effects of online self-efficacy were not significant in reducing exposure to online risks ($\beta = 0.06$, $p = 0.2$) and online privacy concerns ($\beta = -0.00$, $p = 0.9$).

In order to test the mediation effects, the indirect models were assessed separately and were compared with the direct model. The direct effect of perceived susceptibility to online risk was not significant ($\beta = 0.05$, $p = 0.1$), therefore the mediation effects of this predictor was not absorbed. The direct effect of perceived severity of online risk on exposure to online risks was significant ($\beta = -0.12$, $p = 0.0$), the indirect effects mediated by online privacy concern on exposure to online risks was also significant ($\beta = -0.16$, $p = 0.0$). Consequently, VIF for mediation effects "online privacy concern" was $[-0.16/(-0.16 + -0.12)] = 0.58$. The VIF for mediation

Table 3 Reflective measurement model assessment

Constructs (indicators)	Loading (initial)	Loading (modified)
Perceived severity of exposure to online risk		
It is risky if I received inappropriate message	0.85	N.C
Upset about nasty or hurtful messages	0.74	N.C
Bothered if meeting someone I knew only online	0.42	N.C
It is risky if searched for someone online to talk about inappropriate relationship	0.90	N.C
It is risky if searched for someone online to do inappropriate intimate relationship	0.93	N.C
It is risky if I sent my naked photos to someone I knew online	0.91	N.C
It is risky if I sent my address or phone number to someone knew online	0.87	N.C
Composite reliability	0.93	N.C
AVE	0.67	N.C
Perceived susceptibility to exposure to online risk (It is risky if…)		
Having conflict with parents	0.85	N.C
Getting junk or unwanted mail	0.88	N.C
Your personal information being misused	0.93	N.C
You experienced financial loss	0.93	N.C
You experienced identity theft	0.92	N.C
Composite reliability	0.96	N.C
AVE	0.81	N.C
Online privacy concern		
I am able to use a false name or false ID	0.48	Del
I am able to provide incomplete information about myself	0.73	0.69
I ask somebody (e.g., parents and teachers) what I should do	0.70	0.72
I am able to read the privacy statement provided by the site	0.73	0.74
I go to other websites that do not ask for my personal information	0.78	0.80
Usually, I do nothing and leave the website	0.69	0.72
Composite reliability	0.84	0.85
AVE	0.48	0.54
Digital literacy		
I am able to bookmark a website	0.66	0.67
I am able to block messages from someone unwanted	0.75	0.75
I am able to change privacy settings for my social networking profile	0.77	0.79
I am able to delete a record of websites visited	0.66	0.70
I am able to block unwanted ads or junk mail/spam	0.75	0.75
I am able to change filter preferences	0.67	0.71
I am able to find information on how to use the Internet safely	0.45	Del
I am able to compare websites to decide if information is true	0.71	0.64
C.R	0.87	0.88
AVE	0.47	0.52

Table 3 (continued)

Constructs (indicators)	Loading (initial)	Loading (modified)
Online self-efficacy		
I feel confident dealing with the ways companies collect my personal information	0.50	N.C
I feel confident learning skills that protect my privacy online	0.56	N.C
I know more about the Internet than my parents	0.72	N.C
I know lots of things about the Internet	0.66	N.C
I am confident of recognizing a suspicious email	0.87	N.C
I am confident of recognizing suspicious email headers	0.86	N.C
I am confident of recognizing suspicious email attachment filename	0.87	N.C
I can recognize a suspicious email attachment even if there was no-one around to help me	0.83	N.C
Composite reliability	0.91	N.C
AVE	0.56	N.C

Loading modified: factor loading after delete item with loaded less than 0.5; Del: item which has been deleted; *N.C* no change: loading is not changed after item has been deleted; *AVE* average variance extracted (AVE is higher than 0.5 but 0.4 is also acceptable (Huang et al. 2013); *CR* construct reliability

Table 4 Global item for formative construct

Construct global item	Single global item	Coefficient
Unwanted sexual solicitation	Seen/talked about obscene materials	0.88
Risky sexual behaviour	Talk/act intimately	0.89
Potential harmful content	Seen violent/aggressive materials	0.8
Sexting	Send/received obscene massage	0.8
Bullying	Experienced bullying online	0.8
Misuse of personal data	Personal information has been misused online	0.87

effects were between 0.20 and 0.80, which indicates online privacy concern partially mediate the effect of "perceived severity of online risk" on exposure to online risks (Table 7). Overall, the proposed model was supported by the data showing that the model predicted a reduction in exposure to online risks even though it was not strong. The coefficient of determination r^2 showed that the proposed model predicted 21% of the risk involved ($r^2 = 0.21$).

Discussion

The present study suggests that although children who take exposure to online risks seriously are less exposed to those risks, there is no association between perceived susceptibility to online risks and exposure to online risk to children. The result of

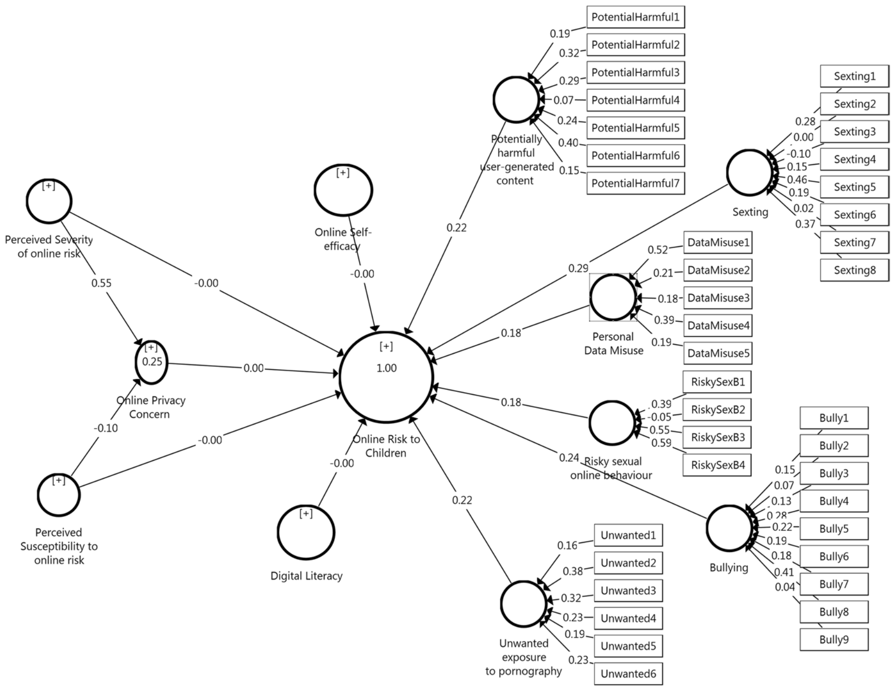

Fig. 3 Formative measurement model

this study is similar to studies by Lareki et al. (2017) and Saeri et al. (2014) which illustrated perceived severity of online risks related to posting data and photos, and increased intentions to protect one's privacy online. In the PMT, perceived susceptibility and perceived severity are part of a first appraisal (threat) after exposure to a fear appeal message. If threat perception is relatively high for individuals, they will engage in a second appraisal (coping) attempt (Rogers et al. 1983). As mentioned, perceived susceptibility to online risks did not reduce the likelihood of children's exposure to risk in this study. A possible reason is found in an early argument by Ronis (1992), who distinguished between 'conditional susceptibility' versus 'unconditional susceptibility'. Unconditional susceptibility is when an individual does not experience a situation (e.g., non-smokers) while conditional susceptibility includes measuring a conditional behaviour of the form (e.g., smokers). Ronis (1992) argued the effect of conditional perceived susceptibility is higher than unconditional susceptibility (non-smokers) as a conditional behaviour. In the present study, given that children's level of exposure to online risks were reported to be low (unconditional behaviour), the effects of susceptibility were not found to be significant.

The present study also found that children's greater digital literacy and safety skills were associated with riskier online activities, which may cause them more risk. However, it must be noted that the effect of new media literacy on online risk is challenging because it increases the risks as well as the benefits of Internet use. Children were asked questions about their ability to use the Internet safely, deal

Table 5 Formative measurement model assessment

	Constructs and its indicators	OW	t	*p*	OL	*p*
Unwanted exposure to pornography						
1	Unwanted obscene materials on web	0.26	3.85	0	0.65	0.00
2	Unwanted obscene materials on message or link	0.37	4.17	0	0.75	0.00
3	Unwanted e-mail or IM	0.35	4.31	0	0.7	0.00
4	Naked picture or inappropriate intimate relationship on message or link	0.1	0.92	0.3	0.63	0.00
5	Anyone asked to talk about inappropriate acts	0.24	2.72	0.01	0.62	0.00
6	Anyone asked to do inappropriate acts	0.17	1.67	0.1	0.53	0.00
Risky sexual online behaviour						
1	Searched for someone to talk about intimate relationship	0.39	2.33	0.02	0.56	0.00
2	Searched for someone to have an intimate relationship	−0.09	0.55	0.6	0.42	0.00
3	Sent obscene photos to someone you only knew online	0.5	3.76	0	0.62	0.00
4	Sent address or phone number to someone you only knew online	0.66	5.91	0	0.77	0.00
Sexting						
1	Seen obscene images or videos	0.29	2.91	0	0.65	0.00
2	Seen obscene images or videos about private parts	−0.02	0.29	0.7	0.5	0.00
3	Seen someone obscene images or videos	−0.04	0.52	0.6	0.51	0.00
4	Seen intimate images or videos in violent way	0.08	1.15	0.2	0.5	0.00
5	Been sent inappropriate messages	0.42	6.23	0	0.77	0.00
6	Posted inappropriate material	0.21	3.01	0	0.6	0.00
7	Seen other people perform obscene acts	0.01	0.2	0.8	0.41	0.00
8	Received inappropriate messages (words, pictures and videos)	0.42	4.43	0	0.83	0.00
Potentially harmful user-generated content						
1	Seen bloody movies or photos	0.28	3.08	0	0.68	0.00
2	Seen people beaten up	0.35	4.39	0	0.71	0.00
3	Seen hate messages	0.3	3.59	0	0.61	0.00
4	Seen anorexia or bulimic images	0.05	0.56	0.6	0.21	0.07
5	Talked about drugs	0.21	1.63	0.1	0.54	0.00
6	Seen ways of physical harming	0.32	3.92	0	0.68	0.00
7	Ways of committing suicide	0.13	1.12	0.3	0.31	0.01
Bullying						
1	Been asked to show my private part	0.16	2.33	0.02	0.34	0.00
2	Been asked to talk about nasty acts	0.07	0.82	0.41	0.42	0.00
3	Received nasty or hurtful messages	0.18	2.33	0.02	0.69	0.00
4	Received nasty or hurtful messages about yourself	0.24	2.74	0.01	0.66	0.00
5	Received other nasty or hurtful messages	0.18	1.98	0.05	0.68	0.00
6	Been threatened online	0.16	2.39	0.02	0.39	0.00
7	Been left out or excluded	0.21	3.22	0	0.52	0.00
8	Received inappropriate messages that bothered you	0.44	5.3	0	0.78	0.00
9	Received inappropriate messages that encourage you to run away	0.01	0.09	0.93	0.25	0.02
Personal data misuse						
1	Misused password	0.57	4.28	0	0.81	0.00
2	Misused personal information you didn't like	0.2	1.17	0.24	0.75	0.00
3	Lost money and been cheated online	0.13	1.28	0.2	0.37	0.00
4	Misused personal information	0.34	1.99	0.05	0.61	0.00
5	Been hacked	0.21	1.58	0.12	0.62	0.00

OW, outer weights; t, t value; OL, outer loading; *p*, *p* value

Table 6 Structural model

Name of constructs	Effect	t value	*p* value
Digital literacy → children's exposure to online risks	0.46*	8.52	0
Online privacy concern → children's exposure to online risks	– 0.00	0.05	0.96
Online self-efficacy → children's exposure to online risks	0.06	1.26	0.21
Perceived severity of online risk → online privacy concern	0.55*	10.98	0
Perceived severity of online risk → children's exposure to online risks	– 0.16*	2.63	0.01
Perceived susceptibility to online risk → online privacy concern	– 0.10	1.87	0.06
Perceived susceptibility to online risk → children's exposure to online risks	0.09	1.81	0.07

*Statistically significant ($p < 0.05$)

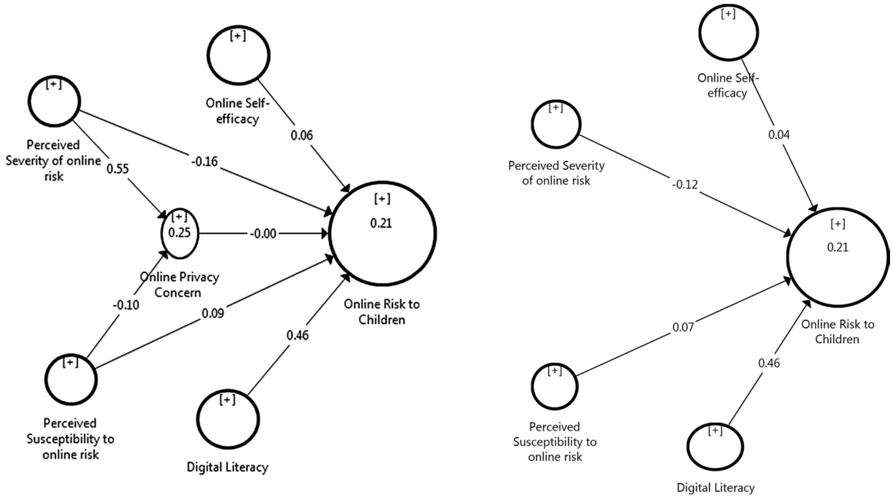

Fig. 4 Mediation effect (direct–indirect model)

Table 7 Mediation effect

Hypothesis	Direct effect	Indirect effect	VAF	Result
Mediating effect of online privacy concern				
Perceived severity of online risk > children's exposure to online risks	– 0.12*	– 0.16*	0.58	Partial mediation
Perceived Susceptibility to online risk > children's exposure to online risks	0.05	0.09		No mediation

*Statistically significant ($p < 0.05$)

with unpleasant/unsafe content, and protect their information. The results showed that children who have a higher level of digital literacy might be exposed to greater online risk because when they know more about the Internet, they use it more and therefore have a higher chance of encountering risk. The concept of media literacy has been long addressed. The term has been used within media education, and studies concerning the topic can be found in disciplines from education to communication, and psychology to sociology. However, some common ground for researchers was established in 1992 at the National Leadership Conference on Media Literacy. At this event, media literacy was defined as the ability to access, analyse, evaluate, and communicate messages in a variety of forms (Aufderheide 1993).

Media literacy was developed to express the accomplishment of the skills and ability to access, analyse, and appraise different forms of media. Today, children are growing up with much greater access to new forms media. They spend a great amount of time screening digital media even before they enter kindergarten. Digital literacy is usually associated with the positive side of media use, and users are encouraged to enjoy the maximum benefits of using new media. However, when it comes to the Internet, researchers are interested in investigating whether they can also minimize the risky consequences. As the present study demonstrates, digital literacy increases the online risks that children are exposed to. Yet, it must be stressed that most scientific research, including the present study, assess the self-acquired digital literacy which is more risk exploratory and less protective or preventive. Therefore, it can be concluded that the positive view over digital literacy or self-acquired digital literacy is not absolute, whereas it can potentially increase both benefits and the likelihood of exposure to online risks.

The present study rejected the idea that higher online self-efficacy predicted fewer online risks as well as online privacy concerns. The findings of the study suggest that the ability to recognize and deal with unpleasant/disturbing experiences online is not a predictor for reducing exposure to online risks. This is in contrary to many past findings in the literature, which posit that using virus protection has a positive impact on information security (Lee et al. 2008), or that privacy concerns have a positive impact on coping behaviours in preventing exposure to online risk (Youn 2009). These studies provide evidence that Internet users who are concerned with information privacy can maintain their online privacy. However, the study did not find any association between privacy protection and exposure to online risk. Several alternative explanations are possible. First, it might be affected by the low level of exposure to online risks among children in this study (unconditional behaviour), discussed earlier. Self-confidence in the ability to protect oneself from undesired experience online might be stronger among children with higher levels of self-efficacy and perhaps self-assumed digital literacy. However; they might have little perception about the threats of information disclosure. This is perhaps because children think they are in control of their information privacy and online safety. As a result, their perception of privacy self-efficacy may not lead to reducing exposure to online risks. However, it may be questionable whether children are actually capable of coping with and averting privacy risks. Given that children are still at the earlier stages of forming and developing their online safety skills, it is be important to examine possible erroneous beliefs held by the vulnerable applicants.

The mediation effect test shows that online privacy concern had a partial mediation effect of ‘perceived severity of online risk’ on exposure to online risks. The present study filled this knowledge gap by examining the mediation role of online privacy concerns concerning the association between perceived online risks and actual exposure to online risks. Given this expectation, it was hypothesized that individuals with the strongest perceived severity of online risk would be exposed to fewer online risks mediated by online privacy concerns. However, the study failed to find any association between perceived susceptibility to online risks and children's exposure to online risks. The results suggest that in order to reduce exposure to online risks among children, children need to have a strong perception of the severity of risks in relation to their concerns about privacy protection rather than susceptibility. In studies such as that of Yau et al. (2014), it is shown that perceived severity of online risk has controlling effects on exposure to online risks, in cases of online gambling. However, contrary to a promising theoretical framework by Lee et al. (2008) and Youn (2008), the findings of the present study demonstrated that there was no significant correlation between children with a high perception of susceptibility to risks and experiencing exposure to online risks. Consequently, this study suggests that in order to control exposure to online risks there is a greater need for the attention on the severity of online risks rather than perception of susceptibility to them.

The present study demonstrated that (1) online self-efficacy negatively influences the children's exposure to online risks; (2) digital literacy is positively associated with children's exposure to online risks; and (3) online privacy concerns mediated the negative effects of perceived severity to online risks on children's exposure to online risks. The results of this study confirm that an integrated model based on PMT and HBM can be a promising theoretical framework to decrease children's exposure to online risks. The model presented in this study contributes to the understanding of the factors affecting children's engagement in appropriate protection behaviour while using the Internet. Hence, children are advised to increase their level of awareness about the negative consequences of risky online behaviour as well as their risk perception and online safety knowledge.

In summary, PMT and HBM suggest that in order to take positive action, people need to believe in both severity and susceptibility of the threats caused by ignoring safe use. It is also important to improve recommendation efficacy once it comes to promoting coping behaviours and protective action. Using the notion of these theoretical perspectives, the present study attempted to predict an online protection motivation method which specifically refers to the attenuation to exposure to online risks. It is also worth mentioning that while risk perceptions (severity and susceptibility) have been studied intensively in health research (Zwart et al. 2009), little is known about risk perception of recently emerging new media. The present study demonstrates the need for increasing insight regarding risk perception and online privacy concern to reducing children's exposure to online risks.

The findings of this study provide a number of implications. Firstly, the true form of digital literacy for children is about being conscious of the possible online risks and learn how to be safe while using the Internet. Secondly, it is necessary to raise awareness among children regarding the negative consequences of risky online behaviour as well as teaching them how to cope with risky situations online. For policymakers, this will encourage continuous innovation and development of online safety strategies. For academicians, this study contributes to the application of PMT and HBM regarding children's new media application.

The study confirmed that a combination of digital literacy, self-protection, and awareness among children is effective in reducing the negative consequences of undesired online experiences, which is helpful for patrons in charge of policymaking. Policymakers are recommended to provide teaching materials for parents as well as updating services and guidelines for using the Internet safely. Digital natives can easily share their personal information, start friendships over a social network, conduct online shopping without concern for financial information safety, and visit inappropriate websites with minimal concern towards safety and security. Promoting online safety depends on the cooperation of policymakers, practitioners, society, and family to pay greater attention to children's Internet usage. This study suggests that children need to be educated about how to use the Internet with a greater level of self-protection and awareness of online risks.

Furthermore, the study contributes to the literature concerning the measurement of Internet usage and exposure to online risks among children and young adults. It helps to increase children's awareness of the possible threats of online activities. It could also improve children's online protection and safety skills. In addition, the study presents the latest data on risk patterns of Internet usage among children. In terms of theoretical contributions, this study extends the application of health belief model (HBM) and protection motivation theory (PMT) to the area of digital risk protection and prevention. The study also suggests that integration between PMT and HBM functions more effectively in promotion of online risk protection behaviour among children. Health behaviour and health promotion theories have been applied to identify factors influencing individual's healthy behaviour adoption. These theories are proposed as explaining the behavioural changes for an individual (e.g., PMT and HBM) (Glanz and Rimer 2005; Prentice-Dunn and Rogers 1986; Rogers 1975). The PMT is suggested to be one of the most applicable and influential risk learning theories, which helps to identify how people choose to behave when faced with various threats. The HBM also emphasizes individuals' perception of threats or actions to prevent the threats (Janz and Becker 1984; Ronis 1992; Rosenstock 1974). Consequently, these two theories, initiated in health promotion context, proved to be applicable for practicing online safety or to prevent the exposure to online risks, and needs to be integrated with mediation effects of protection action.

Previous studies concerning exposure to online risks have used classical measurement approaches to estimate the relationship between latent constructs. Unlike the classical measurement methods, which measure a latent variable by effective (reflective) indicators, modern methods deal with the latent constructs which involve causal (formative) indicators. The application of causal indicators as formative measures has become a solution for researchers who are struggling with the implications of reflective indicators. In the present study, the researchers measured exposure to online risks latent variables by formative indicators given (1) the indicators are causes of constructs, (2) indicators are a characteristic explaining construct, and (3) indicators are not interchangeable (Hair et al. 2014). For example, for measuring the 'personal data misuse' indicator 'have you ever been hacked?' cannot be changed by the indicator 'have you ever lost money online?'. Consequently, the present study contributes to the application of partial least squares to process the statistical analyses for the study.

The present study has several limitations. The participants comprised a Malaysian convenience sample which was approximately two-third female and did not cover all the years from 9 to 16 years old. Therefore, other studies with more representative samples from both within and outside of Malaysia are needed to confirm the findings here. The self-report instrument assessing children's exposure to online risks was adapted from a study conducted on children in Europe and the US. In terms of instruments used, there were sensitive words and phrases in the questions, such as "sexual content" or "having sex", and the researchers were required to replace them with other words or phrases (e.g., "inappropriate intimate relationship"). Research into sensitive topics (i.e., sexual content) are likely to increase social desirability (one of the major biases of self-report data alongside memory recall biases). However, changing some of the wording in the adapted questionnaire may be one of the reasons that the children included in this study were found to have had less online experience than those of European countries or the US when it came to exposure to online risks.

Another possible issue with assessing exposure to online risks is that the risks caused by using the Internet are not specific or well defined. It is impossible to have a clear and defined designation of online risks; the changes caused in new media can be just as fast and reckless as their consequences. Even though researchers might have a common definition of online risks, parents, government and children might well view risk differently. Asian countries face challenges with conflicting context diversity when it comes to adoption of new media by children. The number of studies on this topic in the Asian context is minimal and there is a need for further extensive research. Another point that is worth noting is that most of the questions assessing exposure to online risks considered children being exposed to risks, or showing risky behaving against their will. However, the risks that children become deliberately involved in remain unexamined.

The other major challenge and concern about research regarding children and their Internet usage is the fact that online risks and opportunities are parallel. This study is limited due to the fact that it focuses only on risk due to typical research limitations (time, cost, etc.). The factors that reduce/increase risk may also reduce/increase benefits. For example, apart from negative consequences of children's participation in sex-related activities online, "it is developmentally appropriate for teenagers to be sexually curious and to be eager to know how sex works", and such exploration could provide the possibility of promoting growth and positive development (O'Sullivan 2014, p. 38).

When it comes to defining online risks, there is no clear literal or operational definition that all scholars agree upon. In fact, the nature of online risk is unclear, and the assessment of exposure to online risk is empirically difficult to develop (Livingstone et al. 2012). Since no validated instrument was found to assess exposure to online risks among children in the Asian context, the present study applied an instrument developed in Europe and the US. Consequently, there is a great need to explore the overall risks children are exposed to as an actor, recipient, and participant in the Asian context.

Some earlier findings suggest that it is unlikely for most risky behaviours to lead to negative consequences, unless children engage in such behaviours frequently

(Baumgartner et al. 2010). The diversity of online-related risks and the different consequences that Internet use may cause suggest that there can be no one solution that promises to help overcoming the risks. In addition, the present study focused primarily on risks of which children are victims; risks that are perpetrated by children were of lesser concern in this study. At the same time, the available literature mostly concerns the major online risks that children are exposed to such as cyber-bullying, while there is minimal stress on the long-term effects of such threats (Slavtcheva-Petkova et al. 2015). Long-term effects of exposure to online risks demand further attention because exposure to an online risk might not instantly or even directly harm the child but it might traumatize the child or trigger long-term side effects that deserve greater attention from researchers.

References

Aufderheide, P. (1993). *Media literacy. A report of the national leadership conference on media literacy*. Washington, DC: Aspen Inst.

Aytes, K., & Conolly, T. (2003). A research model for investigating human behavior related to computer security. In *9th Americas conference on information systems* (pp. 2027–2031). Florida, USA: Tampa.

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.

Berkman Center for Internet & Society. (2008). Enhancing child safety & online technologies. Cambridge, US. Retrieved from http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf.

Camacho, S., Hassanein, K., & Head, M. (2014). Understanding the factors that influence the perceived severity of cyber-bullying. *HCI in business* (pp. 133–144). Hamilton, Canada: Springer International Publishing.

Chang, F.-C., Chiu, C.-H., Miao, N.-F., Chen, P.-H., Lee, C.-M., & Chiang, J.-T. (2016). Predictors of unwanted exposure to online pornography and online sexual solicitation of youth. *Journal of Health Psychology, 21*(6), 1107–1118. https://doi.org/10.1177/1359105314546775.

Chen, I.-S. (2017). Computer self-efficacy, learning performance, and the mediating role of learning engagement. *Computers in Human Behavior, 72,* 362–370.

Chen, H., Beaudoin, C. E., & Hong, T. (2016a). Protecting oneself online: The effects of negative privacy experiences on privacy protective behaviors. *Journalism and Mass Communication Quarterly*. https://doi.org/10.1177/1077699016640224.

Chen, H., Beaudoin, C. E., & Hong, T. (2016b). Teen online information disclosure: Empirical testing of a protection motivation and social capital model. *Journal of the Association for Information Science and Technology, 67*(12), 2871–2881.

Clark, L. S. (2011). Parental mediation theory for the digital age. *Communication Theory, 21*(4), 323–343. https://doi.org/10.1111/j.1468-2885.2011.01391.x.

Cross, D., & Barnes, A. (2015). Protecting and promoting young people's social and emotional health in online and offline contexts. In J. Wyn & H. Cahill (Eds.), *Handbook of children and youth studies* (pp. 115–126). Melbourne: Springer.

Davinson, N., & Sillence, E. (2014). Using the health belief model to explore users' perceptions of "being safe and secure" in the world of technology mediated financial transactions. *International Journal of Human-Computer Studies, 72*(2), 154–168. https://doi.org/10.1016/j.ijhcs.2013.10.003.

Dönmez, O., Ferhan Odabaşı, H., Kabakçı Yurdakul, I., Kuzu, A., & Girgin, Ü. (2017). Development of a scale to address perceptions of pre-service teachers regarding online risks for children. *Educational Sciences: Theory and Practice, 17*(3), 923–943.

Ekizoglu, N., & Ozcinar, Z. (2010). The relationship between the teacher candidates' computer and internet based anxiety and perceived self-efficacy. *Procedia Social and Behavioral Sciences, 2*(2), 5881–5890. https://doi.org/10.1016/j.sbspro.2010.03.962.

Family Online Safety Institute. (2013). Teen identity theft. Resource document. Family Online Safety Institute Retrieved April 3, 2018, from www.fosi.org/files/Teen-Identity-Theft-online.pd.

Farrukh, A., Sadwick, R., & Villasenor, J. (2014). Youth Internet safety: Risks, responses, and research recommendations. Retrieved April 3, 2018, from http://www.brookings.edu/~/media/research/files/papers/2014/10/21-youth-internet-safety-farrukh-sadwick-villasenor/youth-internet-safety_v07.pdf.

Feng, Y., & Xie, W. (2014). Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors. *Computers in Human Behavior, 33,* 153–162.

Finkelhor, D., Mitchell, K. J., & Wolak, J. (2008). First Youth Internet Safety Survey (YISS-1). Retrieved April 3, 2018, from http://www.ndacan.cornell.edu/datasets/pdfs_user_guides/134user.pdf.

Finkelhor, D., Mitchell, K. J., & Wolak, J. (2011). Second Youth Internet Safety Survey (YISS-2). Retrieved April 3, 2018, from http://www.ndacan.cornell.edu/datasets/pdfs_user_guides/159user.pdf.

Glanz, K., & Rimer, B. K. (2005). Theory at a glance: A guide for health promotion practice (2nd ed.). Bethesda MD: U.S. Department of Health And Human Services National Institutes of Health. Retrieved April 3, 2018, from http://www.cancer.gov/PDF/481f5d53-63df-41bc-bfaf-5aa48ee1da4d/TAAG3.pdf.

Goldstein, J. (1998). *Why we watch: The attractions of violent entertainment*. Oxford: Oxford University Press.

Görzig, A. (2016). Adolescents' experience of offline and online risks: Separate and joint propensities. *Computers in Human Behavior, 56,* 9–13. https://doi.org/10.1016/j.chb.2015.11.006.

Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2014). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Thousand Oaks: Sage Publications Inc.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2013). Partial least squares structural equation modeling: Rigorous applications, better results and higher acceptance. *Long Range Planning, 46,* 1–12.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service. *Information Systems Journal, 24*(1), 61–84. https://doi.org/10.1111/j.1365-2575.2012.00420.x.

Huang, G. C., Unger, J. B., Soto, D., Fujimoto, K., Pentz, M. A., Jordan-Marsh, M., et al. (2014). Peer influences: The impact of online and offline friendship networks on adolescent smoking and alcohol use. *Journal of Adolescent Health, 54*(5), 508–514. https://doi.org/10.1016/j.jadohealth.2013.07.001.

Huang, C. C., Wang, Y. M., Wu, T. W., & Wang, P. A. (2013). An empirical analysis of the antecedents and performance consequences of using the moodle platform. *International Journal of Information and Education Technology, 3*(2), 217.

Janz, N. K., & Becker, M. H. (1984). The health belief model: A decade later. *Health Education and Behavior, 11*(1), 1–47. https://doi.org/10.1177/109019818401100101.

Jones, L. M., Mitchell, K. J., & Finkelhor, D. (2012). Trends in youth internet victimization: Findings from three youth internet safety surveys 2000–2010. *Journal of Adolescent Health, 50*(2), 179–186. https://doi.org/10.1016/j.jadohealth.2011.09.015.

Jones, L. M., Mitchell, K. J., & Finkelhor, D. (2013). Online harassment in context: Trends from three Youth Internet Safety Surveys (2000, 2005, 2010). *Psychology of Violence, 3*(1), 53–69. https://doi.org/10.1037/a0030309.

Lareki, A., Martínez de Morentin, J. I., Altuna, J., & Amenabar, N. (2017). Teenagers, perception of risk behaviors regarding digital technologies. *Computers in Human Behavior, 68,* 395–402. https://doi.org/10.1016/j.chb.2016.12.004.

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behaviour and Information Technology, 27*(5), 445–454. https://doi.org/10.1080/01449290600879344.

Livingstone, S., & Görzig, A. (2012). Sexting: The exchange of sexual messages online among European youth. In S. Livingstone, L. Haddon, & A. Görzig (Eds.), *Children, risk and safety on the Internet: Kids online in comparative perspective* (pp. 151–164). Bristol: The Policy Press.

Livingstone, S., Haddon, L., Görzig, A., & Olafsson, K. (2011a). Risks and safety on the Internet: The perspective of European children Kids Online network. London, UK. Retrieved April 3, 2018, from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CB8QFjAA&url=http%3A%2F%2Fwww.lse.ac.uk%2Fmedia%40lse%2Fresearch%2FEUKidsOnline%2FEU%2520Kids%2520II%2520(2009-11)%2FSurvey%2FTechnical%2520report.PDF&ei=A_0lVMbpEdSgugTMkIG4BA&usg=AFQjC.

Livingstone, S., Haddon, L., Görzig, A., & Olafsson, K. (2011b). Technical report and user guide: The 2010 EU kids online survey their parents in 25 countries kids online network. LSD, London, UK.

Livingstone, S., Haddon, L., & Gorzig, A. (2012). Children, risk and safety on the Internet: Research and policy challenges in comparative perspective. London: The Policy Press.

MCMC. (2011). Statistical brief number thirteen household use of the internet survey. Retrieved from http://www1.skmm.gov.my/skmmgovmy/media/General/pdf/SKMM_2011.pdf.

MCMC. (2012). Internet Users Survey. Retrieved from https://www.google.com/url?sa=t&rct=j&amp;q=&amp;esrc=s&amp;source=web&amp;cd=1&amp;ved=0CB4QFjAA&amp;url=http://www.skmm.gov.my/skmmgovmy/media/General/pdf/InternetUsersSurvey2012.pdf&amp;ei=9hbGU6p4ice4BMnDgsgM&amp;usg=AFQjCNEQNNN3JQVQtdzGUMgc597UQwciBQ&amp;SzdQ.

Mohamed, N., & Hawa, I. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior, 28,* 2366–2375.

Moore, A. A., Overstreet, C., Kendler, K. S., Dick, D. M., Adkins, A., & Amstadter, A. B. (2017). Potentially traumatic events, personality, and risky sexual behavior in undergraduate college students. *Psychological Trauma: Theory, Research, Practice, and Policy, 9*(1), 105.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815–825.

Online Safety and Technology Working Group (OSTWG). (2010). Youth safety on a living Internet: Report of the online safety and technology working group. Retrieved from http://www.ntia.doc.gov/legacy/reports/2010/OSTWG_Final_Report_060410.pdf.

Organisation for Economic Co-operation and Development. (2012). *The protection of children online*. Paris: Organisation for Economic Co-operation and Development.

O'Sullivan, L. F. (2014). Linking online sexual activities to health outcomes among teens. *New Directions for Child and Adolescent Development, 2014*(144), 37–51. https://doi.org/10.1002/cad.20059.

Peterson, J. L. (1991). Televsion viewing and early initiation of sexual intercourse: Is there a link? *Journal of Homosexuality, 21*(1–2), 93–118.

Prentice-Dunn, S., & Rogers, R. W. (1986). Protection motivation theory and preventive health: Beyond the health belief model. *Health Education Research, 1*(3), 153–161. https://doi.org/10.1093/her/1.3.153.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *Journal of Psychology, 91*(1), 93–114.

Rogers, R. W., Cacioppo, J. T., & Petty, R. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153–177). New York: Guilford Press.

Ronis, D. L. (1992). Conditional health threats: Health beliefs, decisions, and behaviors among adults. *Health Psychology, 11*(2), 127.

Rosenstock, I. M. (1974). Historical origins of the health belief model. *Health Education and Behavior, 2*(4), 328–335. https://doi.org/10.1177/109019817400200403.

Rosenstock, I. M., Strecher, V. J., & Becker, M. H. (1988). Social learning theory and the health belief model. *Health Education Quarterly, 15*(2), 175–183. https://doi.org/10.1177/109019818801500203.

Saeri, A. K., Ogilvie, C., La Macchia, S. T., Smith, J. R., & Louis, W. R. (2014). Predicting facebook users' online privacy protection: Risk, trust, norm focus theory, and the theory of planned Behavior. *Journal of Social Psychology, 154*(4), 352–369. https://doi.org/10.1080/00224545.2014.914881.

Salman, A., & Hasim, M. S. (2011). Internet usage in a malaysian sub-urban community: A study of diffusion of ict innovation. *The Innovation Journal, 16*(2), 8.

Samimi, P., & Alderson, K. G. (2014). Sexting among undergraduate students. *Computers in Human Behavior, 31,* 230–241. https://doi.org/10.1016/j.chb.2013.10.027.

Schilder, J. D., Brusselaers, M. B. J., & Bogaerts, S. (2016). The effectiveness of an intervention to promote awareness and reduce online risk behavior in early adolescence. *Journal of Youth and Adolescence, 45*(2), 286–300. https://doi.org/10.1007/s10964-015-0401-2.

Shillair, R., Cotten, S. R., Tsai, H. S., Alhabash, S., Larose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior, 48,* 199–207.

Siero, N. B. (2017). *Guidelines for supporting teachers in teaching digital literacy*. Master's thesis, University of Twente, The Netherlands.

Slavtcheva-Petkova, V., Nash, V. J., & Bulger, M. (2015). Evidence on the extent of harms experienced by children as a result of online risks: Implications for policy and research. *Information, Communication and Society, 18*(1), 48–62. https://doi.org/10.1080/1369118X.2014.934387.

Stanton, J., Mastrangelo, P., Stam, K., & Jolton, J. (2004). Behavioral information security: Two end user survey studies of motivation and security practices. In *AMCIS 2004 proceedings* (pp. 175). New York, NY: Association for Information Systems.

Südwest, M. (2017). Aktuelle Basisdaten zu TV, Hörfunk, Print, Film und Internet. Retrieved April 3, 2018, from http://www.mediendaten.de/medienthemen/medienstandort-rheinland-pfalz/medienkompetenz/.

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior, 29,* 821–826. https://doi.org/10.1016/j.chb.2012.11.022.

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,* 411–416. https://doi.org/10.1016/j.sbspro.2014.10.314.

Teimouri, M., Hassan, M., Griffiths, M., Benrazavi, S., Bolong, J., Daud, A., et al. (2016). Assessing the validity of western measurement of online risks to children in an Asian context. *Child Indicators Research, 9,* 407–428. https://doi.org/10.1007/s12187-015-9316-4.

UNICEF. (2017). *The state of the world's children 2017: Children in a digital World*. New York: UNICEF.

Vaillancourt, T., Faris, R., & Mishna, F. (2017). Cyberbullying in children and youth: Implications for health and clinical practice. *Canadian Journal of Psychiatry, 62,* 368–373. https://doi.org/10.1177/0706743716684791.

Waddell, J. C., McLaughlin, C., LaRose, R., Rifon, N., Wirth-Hawkins, C., Crouse, J., et al. (2014). Promoting online safety among adolescents: Eancing coping self-efficacy and protective behaviors through enactive mastery. *Communication and Information Technologies Annual, 8,* 133–157.

Wijesingha, R., Leatherdale, S. T., Turner, N. E., & Elton-Marshall, T. (2017). Factors associated with adolescent online and land-based gambling in Canada. *Addiction Research and Theory, 25,* 525–532.

Wirth, C. B., Rifon, N. J., Larose, R. & Lewis, M. Lewis. (2008). Promoting teenage online safety with an i-safety intervention: Enhancing self-efficacy and protective behaviors. *Paper presented at the annual meeting of the international communication association, TBA, Montreal, Quebec, Canada Online, 2008-05-21.* http://citation.allacademic.com/meta/p233579_index.html.

Wisniewski, P., Xu, H., Rosson, M. B., & Carroll, J. M. (2014). Adolescent online safety: The "moral" of the story. In: *Proceedings of the 17th ACM conference on computer supported cooperative work and social computing* (pp. 1258–1271). Baltimore, MD: ACM.

Yau, Y. H. C., Pilver, C. E., Steinberg, M. A., Rugle, L. J., Hoff, R. A., Krishnan-Sarin, S., et al. (2014). Relationships between problematic Internet use and problem-gambling severity: Findings from a high-school survey. *Addictive Behaviors, 39*(1), 13–21. https://doi.org/10.1016/j.addbeh.2013.09.003.

Ybarra, M. L., & Mitchell, K. J. (2005). Exposure to internet pornography among children and adolescents: A national survey. *CyberPsychology and Behavior, 8*(5), 473–486. https://doi.org/10.1089/cpb.2005.8.473.

Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviours: A risk-benefit appraisal approach. *Journal of Broadcasting & Electronic Media, 49(*1), 86–110.

Youn, S. (2008). Parental influence and teens' attitude toward online privacy protection. *The Journal of Consumer Affairs, 42*(3), 362–388.

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs, 43*(3), 389–418.

Youn, S. (2010). Teenagers' perceptions of online privacy and coping behaviors: A risk–benefit appraisal approach. *Journal of Broadcasting and Electronic Media, 49*(1), 37–41.

YPRT Toolkit. (2008). Youth Protection Roundtable. Retrieved from https://www.google.com/url?sa=t&amp;rct=j&amp;q=&amp;esrc=s&amp;source=web&amp;cd=2&amp;ved=0CCQQFjAB&amp;url=http%3A%2F%2Fec.europa.eu%2Finformation_society%2Fapps%2Fprojects%2Flogos%2F7%2FSIP-2005-UE-518747%2F080%2Fpublishing%2Freadmore%2FYPRT%2520Toolkit.pdf&amp;ei=zfQlVICAPMGgugSaiYCQDw&usg=AFQjCNH1QH9CceXrI_V4rfYzfVr_M_-ENA&amp;sig2=oicL_CoQK6NLAnkQOaONhg.

Zwart, O., Veldhuijzen, I. K., Elam, G., Aro, A. R., Abraham, T., Bishop, G. D., et al. (2009). Perceived threat, risk perception, and efficacy beliefs related to SARS and other (emerging) infectious diseases: results of an international survey. *International Journal of Behavioral Medicine, 16*(1), 30–40. https://doi.org/10.1007/s12529-008-9008-2.