International Journal of Information Technology and Language Studies (IJITLS)

Effectiveness of Cyber Security Awareness Program for young children: A Case Study in UAE

Arwa A. Al Shamsi
arawee_a@yahoo.com

Faculty of Engineering and IT, The British University in Dubai, Dubai, UAE

Abstract. Children are an important element of the community; they represent the hope of a bright future. The safety of our children is priceless. Nowadays children are using the internet on a daily basis for many reasons; playing online games, social media or even for doing their school works. The internet takes a huge part of their times and unfortunately, most of these children are not aware of online risks and how they should respond properly to online risks. Moreover, children may have unlimited access to the internet without any control or supervision. The cybercrimes are increasing year after a year and the government of UAE considers the safety of the citizens as one of the most priorities to achieve. As the safety of our children is a priority, the Ministry of Education in UAE provided a cyber security awareness program for children in order to raise their security awareness level about online risks and online best practices. The objective of this research is to investigate the effectiveness of the cyber security awareness program offered by the Ministry of Education in UAE to students aged 8 to 10 years old. This research paper methodology based on qualitative methods for collecting data in which data were collected from interviews conducted with both the trainers of the program and students who attended the program. It was found that the children may expose to different online risks and the topics included in the cyber security awareness program were effective and aligned along with possible online risks children may expose to. Both the trainers and the students agreed on the efficiency of the cyber security awareness program and students believed that the awareness program influenced their online behavior. Although the interviews provided valuable findings, the real effectiveness of the cyber security awareness program hard to be measured as it depends on how students will behave online.

Keywords: *cyber security; awareness; children; Ministry of Education; and Online risks.*

1. Introduction

The internet has become an important element in our lives, the use of the internet takes huge parts of people's time. Children as well as use the internet daily. Children use the internet in their spare time as well as at studying time. In fact, children use the internet at schools and at homes, as many schools applied the use of technology in teaching and doing homework. Gemma Pons-Salvador, Xud Zubieta-Méndez, Dolores Frias-Navarro, (2018) stated that children start using the internet in very young age and they may have access to the internet without any supervision even without any use time limit or restrictions. The use of the internet can be very beneficial for children as it considered as a valuable source of information, children can get great knowledge and it can be used for education and communication. On the other side, the use of the internet can be risky for children especially if they are not aware of online risks and how they should respond to each of online risks. Children need to learn how they should behave online and what are the internet best practices. Children as well need to be aware of how to protect themselves online. Gemma Pons-Salvador, Xud Zubieta-Méndez, Dolores Frias-Navarro, (2018) believed that the risks online that children may face are huge and recommend the parents participation in protecting their children online.

Cybercrimes indicator worldwide are rising year after year, this increase may result in increasing the risks that our children may face online. George Tsakalidis, Kostas Vergidis, (2017) stated that a worldwide study was released in which it was found that the number of information crimes incidents that have been reported all around the world were increased of about 48%. They stated as well that the cybercrimes have negative impacts on the global economy, people and citizens safety, the society well-being and it may involve negative effects on our children's safety. The government of the United Arab Emirates puts the safety of the citizens as a priority and always takes the proper steps in order to achieve that goal. As the safety of our children is priceless, the Ministry of Education in UAE provided cyber security awareness training as a compulsory module for students in grade 4 at government preliminary schools. This module is a comprehensive training of online risks and the proper response for each of these online risks. The training as well as involves teaching the students how to protect themselves online and the best online behavior.

The aim of this research is to investigate the effectiveness of cyber security awareness program that is offered by the Ministry of Education and targeted students aged 8 to 10 years old in raising the cyber security awareness level among children and influence their online behavior. This investigation is important for both the Ministry of Education and our children. It is important to investigate whether these awareness programs are efficient, or it is just a waste of time and money.

This research applied qualitative methods for collecting data based upon conducting a number of interviews with both the trainers of the cyber security program and the students who attended the program.

Study design: The first section of this research is the introduction that identifies the topic and the purpose of the research. The second section is the research problem statement. The third section is the literature review in which similar topics of the research that have been addressed by other researchers will be highlighted. The fourth section is the research question in which the three research questions will be identified. The fifth section is the research methodology in which the research questions will be converted into interview questions, then the interviews will be designed and then will be carried out. The sixth section includes the interview findings. The seventh part includes qualitative data analysis and discussions. Finally, the eighth section provides the summary and conclusion.

2. Research justification/theoretical background

2.1. Cyber Security

It is essential to address the concept of cyber security. The term of cyber security has been addressed by a number of research papers. Rossouw von Solms, Johan van Niekerk, (2013) defined the cyber security as the protection of the user and its assets from any online threats, while Lene Hansen and Helen Nissenbaum, (2009) stated that in the early 1990s, the concept of cyber security appeared to be related to the lack of security in computer networks. Nowadays, however, the concept of cyber security has become much more than mere insecurity to become a real problem requiring attention and taking appropriate measures to ensure the safety of Internet users. Cyber security transcended technical problems and became the cause of many social problems. Dan Craigen, Nadia Diakun-Thibault, Randy Purse, (2014) reviewed a number of literature reviews that discussed the concept of cyber security and comes up with the following definition; Cyber security involves all the procedures and resources that are used to ensure the safety of the cyberspace and systems connected to the cyberspace from incidents that are illegal and considered to break the law.

Most European Union countries, America, Australia, and other countries have defined the concept of cybersecurity, Eric Luiijf, Kim Besseling and Patrick de Graaf, (2013) discussed that fact that different countries have a different definition for cyber security concept. For example, Australia defined cyber security as the measures that applied to information assets to ensure its confidentiality, availability, and integrity. India definition of cyber security involves the protection of both the information and the information system. While France defined the cyber security as the resistance of any break to the confidentiality, integrity, and availability of information.

When we go over the concept of cybersecurity as defined earlier, we find that the concept of cybersecurity involves the protection of online end-users as well as all the procedures that are used to ensure the confidentiality, integrity, and availability of systems and data assets.

2.2. Cyber security risks children may face online

Children may face different kinds of dangers while using the Internet. The world of the Internet is a dynamic world; it is difficult to specify all the risks our children may be exposed to when using the Internet. Many research papers have discussed the risks children may face while using the Internet; in this section number of research papers that discussed the online risks children may face will be reviewed to identify some of the important and common online risks.

M. Valcke, B. De Wever, H. Van Keer, T. Schellens, (2011) discussed the online risks children may face. The online risks divided into three basic kinds of risk. First is content risks and example of content risks the online wrong information. Second is the contact risks such as cyber bullying and privacy risks. The third is the commercial risks such as collecting personal data. On the other hand, Sonia Livingstone, Giovanna Mascheroni and Elisabeth Staksrud, (2015) studied different types of online risks by classifying the online risks into content risks, contact risks and conduct risks. Researchers found that the younger the child, the higher the chance to exposed to online risks such as stalking, grooming, and bullying.

Slavtcheva-Petkova, Vera; Nash, Victoria Jane; Bulger, Monica, (2014) stated that the risks that children may experience when using the internet are very great, some of these risks, which are classified as very serious, may be a small percentage compared to other risks, which are also serious and have significant dimensions and negative effects. While reviewing research papers that studied the online risks, it was found that the main online risks that were mentioned are pornography, cyberbullying, sending and receiving sexual messages, identity theft, and phishing.

Bőthe, B., Tóth-Király, I., Zsila, Á., Demetrovics, Z., Griffiths, M.D., Orosz, G, (2017) defined online pornography as all materials on websites that are indecent and contain sexual thoughts or views. Livingstone, Sonia, and Haddon, Leslie and Görzig, Anke and Ólafsson, Kjartan, (2011) stated that children at any age should not be exposed to pornographic materials due to its harm on the children thought and minds. Karen Brown, Margaret Jackson & Wanda Cassidy, (2006) stated that cyberbullying involves secret psychological bullying conducted through a technological medium such as websites, cell phone, and chat rooms. cyberbullying can be verbal or written. Rahat Ibn Rafiq, Homa Hosseinmardi, Richard Han, Qin Lv, Shivakant Mishra, Sabrina Arredondo Mattson, (2015) defined cyberbullying as the aggression online that is repeated and intended. Cyberbullying can be through instant messaging, hurtful comments, recording and sharing videos without taking permission.

Livingstone, Sonia, and Haddon, Leslie and Görzig, Anke and Ólafsson, Kjartan, (2011) mentioned critical online risk which is sending and receiving sexual messages (sexting), number of cases were recorded in which adults communicate with children through online games and social networking sites and try to gain their trust in order to attract and meet them without the knowledge of their parents. Anna Sevcíkova, (2016) stated that sending and receiving sexual messages (sexting) involves the electronic exchange of sexual materials such as video and pictures.

Nazura Abdul Manap, Anita Abdul Rahim, Hossein Taji, (2015) refer to identity theft as the stealing of private information such as the name, Date of Birth, address, etc. using technological-based methods via the internet in order to commit crime or fraud, while Gila Cohen Zilka, (2017) defined identity theft as using victim's private information that has been stolen online to impersonate him then conduct crimes and cause troubles.

Elmer Lastdrager, Inés Carvajal Gallardo, Pieter Hartel, Marianne Junger, (2017) stated that phishing involves tricking the victim to reveal his personal information most likely credentials to access online accounts most likely bank accounts and misuse them. Online phishing commonly happened to reveal bank account credentials, but recent phishing incidents reported from retailers and service companies. Komal Bansal, (2016) found that phishing involves tricking the online user to reveal his sensitive information. Phishing commonly happened using fake websites.

When reviewing the online risks as mentioned above, it is noticeable how great is the threat that our children may face when using the internet, especially if they are unaware of the extent of the negative effects of risks online and how they could respond properly.

2.3. Cyber Security awareness

Cyber Security awareness training has become an urgent necessity as cyber incidents caused by human factor achieve the largest percentage of cyber security incidents causes. This is the reason behind focusing attention on cyber security awareness program to reduce cyber security attacks and incidents. In this section, a number of research paper has been reviewed to investigate how cyber security awareness was defined.

Jemal Abawajy, (2014) defined the security awareness as how much the user is aware of the online best practices. Jemal Abawajy, (2014) stated that the security awareness campaigns mainly focus on raising the cyber security awareness level for the online end users and the success of these awareness campaigns depend basically on the delivery methods of the security awareness information. On the other hand, Bilal Khan, Khaled S. Alghathbar, Syed Irfan Nabi and Muhammad Khurram Khan, (2011) stated that information security awareness involves assuring that users are aware of information security rules and behave accordingly. Maria Bada, Angela M. Sasse and Jason R.C. Nurse, (2019) refer to NIST publication 800.16 to define the security awareness term as the process of focusing the attention on cyber security with aim to understand the cyber security concerns and react properly, while Gila Cohen Zilka, (2017) stated that cyber security awareness involves raising the knowledge level of the online risks and the practices online by children and teenagers to stay safe online.

Bilal Khan, Khaled S. Alghathbar, Syed Irfan Nabi and Muhammad Khurram Khan, (2011) stated that security awareness considers assuring the knowledge of security rules and regulations and behave accordingly. Mackenzie Adams, Maged Makramalla, (2015) found that security awareness training is essential to provide a higher security level.

From all definitions of cyber security awareness mentioned above; cyber security awareness can be identified as all the steps that are taken to raise the cyber security knowledge level at the end-users and direct them to react properly online.

2.4. Effectiveness of cyber security awareness programs

There are many ways and concepts for evaluating the effectiveness of cyber security awareness program and assessing how good is the security awareness program.

Jemal Abawajy (2014) investigated the security awareness program delivery methods; which delivery method is effective and which delivery method users preferred. The researcher found that the security awareness program is very effective in raising the awareness level on the best practices while using the internet. The researcher concluded that the video-based method in delivering the security awareness program is the preferred security awareness method.

Tonia SanNicolas-Rocca, Benjamin Schooley and Janine L. Spears, (2014) demonstrated that end-user of the Internet is the weakest point in the system of cyber security protection in organizations. Hence the researcher explained the importance of cyber security awareness training for internet end-users on the optimal use of the Internet. The researchers concluded after conducting a case study that the cyber security awareness training programs are very effective in raising the security awareness level and improving the end-user online practices. Researchers proofed that the participation of internet end-users in the cyber security awareness training led to the spread the culture of cyber security best practices.

Fadi A. Aloul. (2012) studied the security awareness importance and need in improving the cyber security level. The researcher found that cyber security awareness program and training is essential for internet end-users in everywhere. Cyber security awareness training is essential in governments institutes, schools, universities, and organizations.

Jun Zhao, GeWang, Carys Dally, Petr Slovak, Julian Edbrooke-Childs, Max Van Kleek, and Nigel Shadbolt (2019) investigated whether children online able to recognize the online risks and what are the best methods for reducing the risks online that children may be exposed to. Researchers found that the cyber security awareness program is essential and beneficial in educating children about online safety.

Maria Bada, Angela M. Sasse and Jason R.C. Nurse (2019) investigated a number of cyber security awareness campaigns to discover the reasons of security awareness campaign's success or failure. Researchers reported the following suggestions that may lead to cyber security awareness campaign success. Security awareness program should be well prepared. It should be actionable and targeted. Cyber security awareness program should be flexible to be accepted by different cultures.

2.5. Programs Cyber security awareness in the United Arab Emirates

The Internet is one of the most important aspects of life in the United Arab Emirates since the United Arab Emirates has become one of the highest countries in the individuals' use of the Internet. Fadi A. Aloul (2012) stated that statistics indicated an increase in the number of Internet users in recent years in middle east countries, and the number of internet users in UAE has shown a sharp increase as UAE government's always questing to achieve the highest levels of the technological progress. The Government of the United Arab Emirates has supported the transition to intelligent systems in all ministries and government institutions. The Government of the United Arab Emirates has become a smart government, smart systems have been activated in healthcare institutions, intelligent learning has been activated in all government schools in the United Arab Emirates under the name of smart education. United Arab Emirates government aims to achieve world-class standards in IT environment hence the United Arab Emirates gives electronic security a great deal of attention as the UAE is keen to achieve the highest standards of safety and security for citizens. In this regard, the Government of the United Arab Emirates has taken many steps and procedures to achieve the highest cyber safety standards:

- United Arab Emirates government issued federal law No. 5 of 2012 known as Cyber Crime Law in order to regulate all the cyber transactions in the UAE and provides for all cyber offenses, and penalties resulting from them. This Cyber Crime law has been slightly modified in 2016.

- Hamad O. Al Mansoori, (2015) stated that aeCERT was established in 2008 with the aim to raise the cyber security awareness level in UAE society and protect the Information Technology infrastructure from being compromised. aeCERT stands for Computer Emergency Response Team, aeCERT goal is to establish safer ICT community and the best way to achieve this goal is by security awareness among society and cyber security education in schools and universities. eaCERT is computer emergency response team that is a department of Telecommunication Regulatory Authority.

- Two major telecommunication companies Etisalat and Du focused on the end-user awareness through SMS, emails and short videos through TV channels and social media.

- The Ministry of Education focused on training and educating students about the cyber security and Internet best practices. This research paper studied the effectiveness of the security awareness education for students aged 8 to 10 years old; i.e. students at grade 4. During term two of the academic year students of grade 4 learn about Internet safety as the major topic of Design and Technology subject. Internet safety is the topic of Design and Technology of term 2 which is focusing basically on internet best practices and aims to educate students about the cyber security and internet safety. In this compulsory module that lasts for about three months students educated about the internet usages, online risks, how students can protect themselves online and how they respond to online risks properly.

3. Research questions

As been discussed in the previous sections, the research gap is to evaluate the effectiveness of the cyber security awareness programs delivered to young children. The objective of this research paper is to investigate the effectiveness of the cyber security awareness program adopted by the Ministry of Education in the United Arab Emirates in training and educating students aged 8 to 10 years old about online best practices.

The main research question to fulfill the gap is "How effective is the cyber security awareness programs adopted by the Ministry of Education in the United Arab Emirates in training and educating students aged 8 to 10 years old about internet safety and to raise the cyber security awareness level among young children?". This main research question will be addressed through the following three research questions:

1. What online risks children may expose to?

2. How cyber security awareness training influences student's online behavior?

3. How effective is the Cyber Security Awareness program adopted by the Ministry of Education in UAE in educating students aged 8 to 10 about the safe use of the internet?

4. Research methodology (interview protocol etc.)

4.1. Converting research questions into interview questions

The aim of this research is investigating the effectiveness of the cyber security awareness program adopted by the Ministry of education for young children. This research is qualitative research in which interviews were prepared and conducted. Semi-structured interviews questions were designed and conducted. The interviews targeted children at grade 4 from government schools in the UAE and trainer of the cyber security awareness programs, i.e. teachers of Design and Technology in government schools. The research main question was converted into three research questions; then these research questions were converted into interview questions for young children and trainers of the cyber security awareness program.

Research main question	Interview sub-question	Purpose of interview question
1. What online risks children may expose to?	1.1 What online risks you learn about?	To discover the ability of the child to identify different online risks.
	1.2 What online risks you may expose to?	To investigate the ability of children to identify online risks they may expose to.
2. How cyber security awareness training influences student's online behavior?	2.1 Can you give an example to show how the awareness program influenced your online behavior?	To investigate how the cyber security awareness program influenced children's behavior online.
3. How effective is the Cyber Security Awareness program adopted by the Ministry of Education in UAE in educating students aged 8 to 10 about the safe use of the internet?	3.1 Do you think that this awareness program is effective? To what extent?	To find out the children opinion about the benefits of the cyber security awareness program.

Table 1. The link between the research main questions and the young children interview questions.

Research main question	Interview sub-question	Purpose of interview question
1. What online risks children may expose to?	1.1 What online risk children may expose to?	To discover the teacher's and trainer's opinion about the online risks the children may expose to.
	1.2 What are the topics of the security awareness that children learn about?	To collect information about sections of cyber security awareness program.
2. How cyber security awareness training influences student's online behavior?	2.1 Can you give an example to show how the awareness program influenced children's online behavior?	To investigate how the cyber security awareness program influenced children's behavior online from the teacher's point of view.
3. How effective is the Cyber Security Awareness program adopted by the Ministry of Education in UAE in educating students aged 8 to 10 about the safe use of the internet?	3.1 Do you think that this awareness program is effective? To what extent?	To find out the teacher's opinion about the benefits of the cyber security awareness program.
	3.2 What are the limitations in the cyber security awareness program?	To investigate the limitations of the cyber security awareness program from the teacher's point of view.
	3.3 What are your suggestions to increase the effectiveness of the cyber security awareness program?	To collect suggestions from teachers to improve the cyber security awareness program.

Table 2. The link between the research main questions and the trainers' interview questions.

4.2. Designing interviews and data recording protocols

Designing and conducting semi-structured interviews in this research paper influenced by steps identified by Jacob, S. A and Furgerson, S. P, (2012) ; 1) Select your topic, 2) Identify research question, 3) Define the interviewee, 4) Define interview settings, 5) Collect consents, 6) Design interview protocol 7) Record the interview,8) Questions should be open-ended, 9) Listen carefully. The following points illustrate how these steps are fulfilled:

1. The topic of this research paper is about the effectiveness of the cyber security programs targeting young children.

2. As been discussed earlier, the research questions specified in this research paper are: (A) what online risks children may expose to? (B) How the cyber security awareness training influences student's online behavior? (C) How effective is the Cyber Security Awareness program adopted by the Ministry of Education in UAE in educating students aged 8 to 10 about the safe use of the internet?

3. The research paper is qualitative research to investigate the effectiveness of the cyber security awareness program. Semi-structured interviews have been conducted. The interviewees are (A) Children who attended the cyber security awareness program, (B) Teachers and Trainers of the cyber security awareness program.

4. The place in which all the interviews are conducted are government schools. The interviews were held in classrooms in which the interviewee and the interviewer are sitting in front of each other and there is a small table between them.

5. Consents were prepared as it is essential before conducting the interviews to collect consents from all the interviewee.

6. Interview protocol has been set and designed to include: (A) Information about the interviews date, location and time, (B) interviewee general information, (C) interviewer information.

Date: ……………………………………………………………………………………
Time: ………………………………………………………………………………
Location: ………………………………………………………………………………
Interviewee Name: ……………………………………………………………………
Title: (student / Teacher / Trainer)
Experience (For Teacher and Trainer): ……………………………………
Organization (For Teacher and Trainer): …………………………………
Interviewer: …………………………………………………………………………

7. The interviewee must agree to record the interview before conducting the interview. All of the interviewees refused to record the interview.

8. Interview questions were prepared to be open-ended.

9. The interviewer should listen carefully to the interviewee; listening carefully with eye contact shows to the interviewee how you value the information provided and how much you respect him.

4.3. Carrying out interviews and recording data

The three interviews were conducted with Design and Technology teachers who are the trainers of the cyber security awareness program and twelve interviews were conducted with students aged 8 to 10 years old who attended the cyber security awareness program.

5. Interviews Findings

Table 3 summarizes the trainer (teachers) interviews findings:

Table 5: Trainer (teachers) interview findings:

Interview Question	Interview No. 1	Interview No. 2	Interview No. 3
1.1 What online risks children may expose to?	-Cyber Bullying -Identity Theft -Online Phishing -Pornography	-cyber bullying -pornography -break to privacy -sharing personal information.	-online bullying -viruses that may destroy the computers -break to the privacy of children -Identity theft
1.2 What are the topics of the security awareness that children learn about?	-Cyber Bullying -Privacy -Password - Online safety -Online protection -phishing -Identity theft -online strangers	-Identity theft -cyber bullying -online protection -phishing -securing private information -password security	-Identity theft - password protection -Internet safety best practices -cyber bulling -privacy
2.1 Can you give an example to show how the awareness program influenced children's online behavior?	- more secure while playing online games - aware of phishing - transfer their knowledge to their family members	-students became more cautious when using the Internet -students become more caring about their personal information -Students become more aware while playing online games to some issues such as pornography	-students become more aware -students create strong passwords and they don't use the same password for all of their accounts -students stop giving their private information online
3.1 Do you think that this awareness program is effective? To what extent?	Yes, very effective in raising the cyber security awareness level among students	-Too effective to raise sufficient awareness among students and to sensitize them not to share their personal information -Students learned to protect themselves and be more aware while using the internet.	Yes, cyber security awareness is very effective in raising the awareness level and affecting student's behavior online
3.2 What are the limitations in the cyber security awareness program?	Too narrative, more awareness videos should be added as well as training offered through video games	narrative more videos should be added -the curriculum should include more video games and hands-on activities about the topics.	-more narrative, tends to be somewhat static -more short films and video clips should be added to the Cyber Security Awareness program

3.3 What are your suggestions to increase the effectiveness of the cyber security awareness program?	Society engagement in awareness to build security culture among society.	-awareness training for parents to recognize online risks and then engage in educating their children and protect them. -all society should be aware of internet best practices in order to achieve a more secure society. -Media should participate in the awareness program and telecommunication companies as well.	-parent's engagement in cyber security awareness training -society should be engaged in the cyber security awareness programs especially the media. -Awareness posters should be set in public places -awareness messages should be sent to citizens to build strong security culture among society
Main Themes that have emerged out of the interview	-Cyber Bullying -Identity Theft -Online Phishing -Pornography -phishing -password -privacy -Effective -narrative training -social engagement	-cyber bullying -pornography -break to privacy -privacy -password -effective -narrative training -phishing Identity theft -parents awareness -media engagement	-Identity theft - password protection -Internet safety best practices -cyber bulling -privacy -phishing -viruses -effective -narrative training -parents' engagements Awareness posters and messages

Table 3. Summarizes the students (children) interviews findings.

Interviewee No.	1.1 What online risks you learned about?	1.2 What online risks you may expose to?	1.3 How security awareness training materials were presented?	2.1 Can you give an example to show how the awareness program influenced your online behavior?	3.1 Do you think that this awareness program is effective? To what extent?
1	-Cyber bullying -Phishing, Identity theft -how to make a strong password -how to act properly online -not to share personal information online	-cyber Bullying -break to privacy	-lectures -awareness videos -creating awareness poster	Good behavior while playing online games	Yes, very effective
2	-Cyber bullying -Identity theft -Internet safety -Online strangers -How to create a strong password	-Identity theft -password break	-lectures -awareness videos -creating awareness poster	-Not sharing personal information -Good behavior while playing online games	Yes, very effective

3	-Cyber Bullying -Identity theft -Password protection -online strangers	Online Phishing	-lectures -awareness videos -creating awareness poster	-make strong password -protect personal information -email security	Yes, very effective
4	-phishing -identity theft -cyber bullying - passwords	-Identity theft -cyber bullying -accessing my account	-lectures -awareness videos -creating awareness poster	-Act carefully online -I don’t talk to strangers -I don’t say my private information -Use strong password	Yes, very effective
5	-password -Identity theft -phishing online strangers -cyber bullying	-Break to privacy -cyber bullying	-lectures -awareness videos -creating awareness poster	Good behavior while playing online games	Yes, very effective
6	-secure websites -online privacy - cyber bullying	-Cyber bullying -Identity theft -phishing	-lectures -awareness videos -creating awareness poster	Good behavior while playing online games	Yes, very effective
7	-Online strangers -Identity theft -cyber bullying	-cyber bullying -Identity theft	-lectures -awareness videos -creating awareness poster	-Good behavior while playing online games -not respond online to anyone I don’t know	Yes, very effective
8	cyber bullying - password -email protection -online phishing	-cyber bullying -phishing	-lectures -awareness videos -creating awareness poster	Good behavior while playing online games -privacy	Yes, very effective
9	-online phishing -password -online protection -cyber bullying	cyber bullying	-lectures -awareness videos -creating awareness poster	Recognize phishing email and act properly	Yes, very effective
10	internet safety -identity theft -online bullying -online strangers -online phishing -passwords	cyber bullying	-lectures -awareness videos -creating awareness poster	Using a strong password and different passwords for different accounts	Yes, very effective
11	-Passwords -cyber bullying - online phishing	-cyber bullying -online phishing	-lectures -awareness videos -creating awareness poster	-Use strong password -privacy	Yes, very effective
12	-cyber bullying -secure websites -Identity theft -passwords	-cyber bullying -Identity theft	-lectures -awareness videos -creating awareness poster	Not respond to strangers online	Yes, very effective

Main things emerged	-Cyber bullying -Identity theft -Internet safety -Online strangers -How to create a strong password -phishing -privacy -secure websites -protection and safety	-cyber bullying -Identity theft -online phishing -break to privacy -password break	-lectures -awareness videos -creating awareness poster	-Use strong password -privacy - Not respond to strangers online -Recognize phishing email and act properly - Good behavior while playing online games -Not share personal information	Effective awareness program

Table 4. Students (children) interview findings.

The main themes that are repeated through the interviews with the trainer (Design and Technology Teachers) of the cyber security awareness program are:

1. Online risks
2. Content of awareness program
3. Effectiveness
4. Effects
5. Limitations
6. Suggestions

Table 5 illustrates the main themes and their constructs and dimensions.

Main constructs	Main Dimensions
Online risks	O1: Cyber Bullying O2: Pornography O3: Identity theft O4: Online Phishing O5: Break to privacy
Content of awareness program	C1: Internet Safety C2: Cyber Bullying C3: Identity theft C4: Online Phishing C5: Privacy C6: Password C7: securing private information C8: Internet Strangers
Effectiveness of cyber security awareness program	E1: Positively affects children's behavior online E2: effective in raising cyber security awareness level among students E3: efficient in helping students to protect themselves online
Effects on students	EF1: protect their personal information EF2: use strong passwords EF3: respond properly to different incidents online EF4: more cautious while playing online games EF5: keep their parents aware if they feel uncomfortable online EF6: aware of phishing emails and messages. EF7: Transfer the knowledge their family members
Limitations	L1: narrative L2: little awareness videos, more should be included L3: little hands-on activities, more should be included
Suggestions	S1: society engagement S2: cyber security training for parents

	S3: media participation in the awareness campaign S4: cyber security awareness posters in public places S5: awareness messages for all citizens

Table 5. Main constructs and main dimensions resulted from the three interviews.

Twelve interviews were conducted with students aged 8 to 10 years old who attended the cyber security awareness.

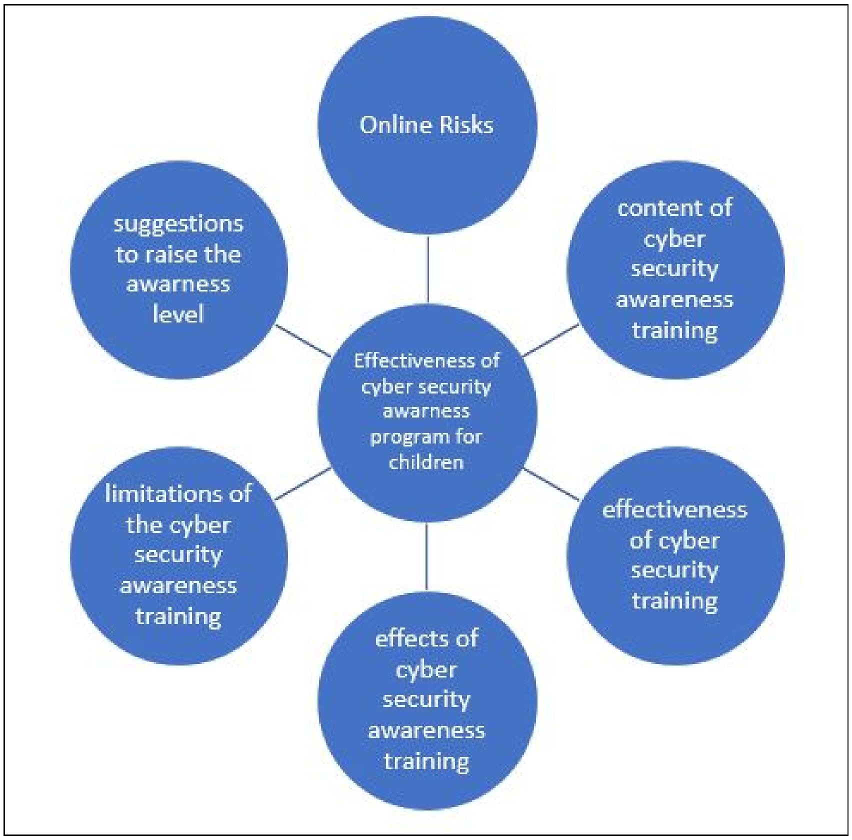
Online Risks
suggestions to raise the awarness level
content of cyber security awareness training
Effectiveness of cyber security awarness program for children
limitations of the cyber security awareness training
effectiveness of cyber security training
effects of cyber security awareness training

Figure 1. Illustration of the main constructs resulted from the trainer interviews.

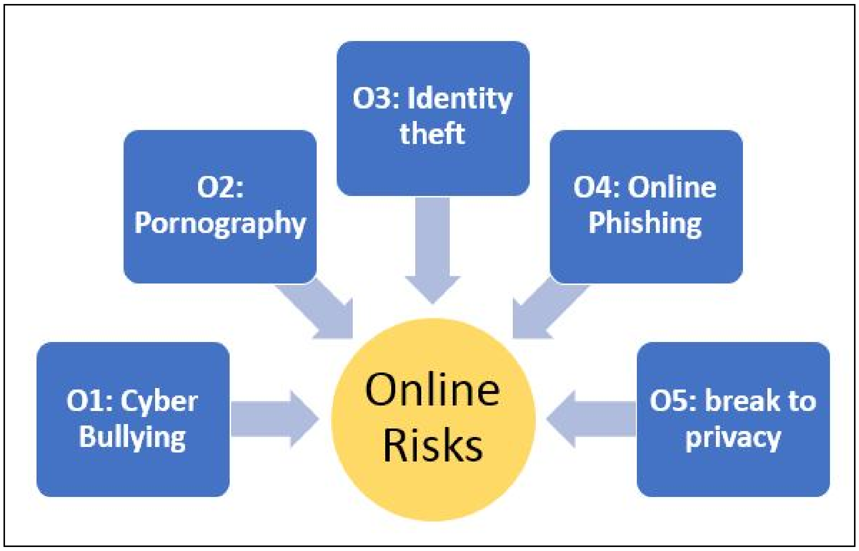

Figure 2. Illustration of the main dimensions for the Online Risks construct.

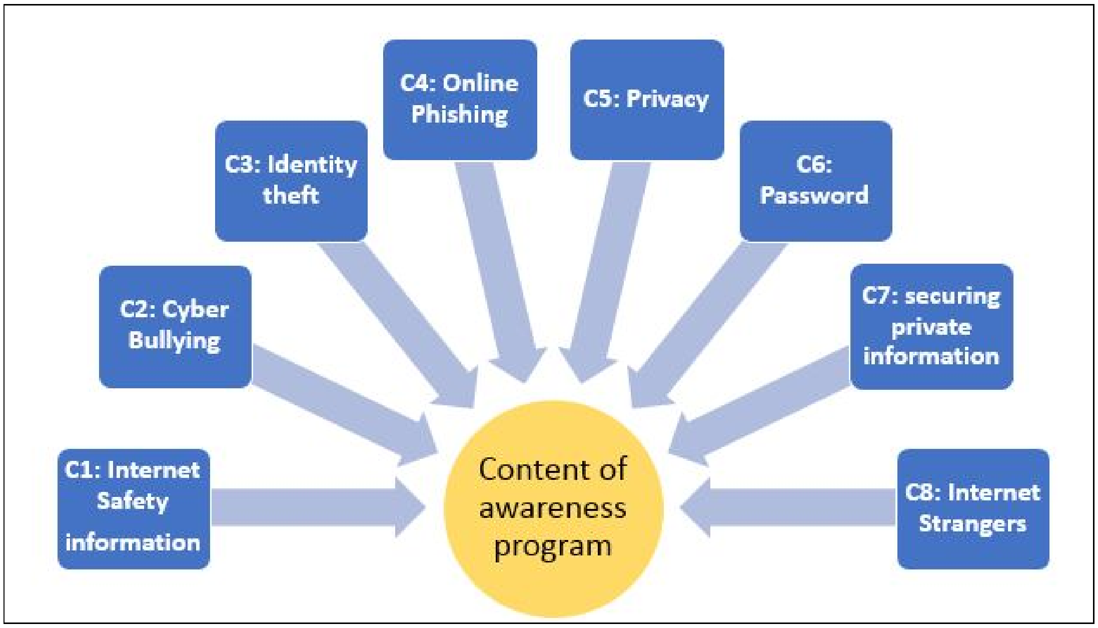

Figure 3. Illustration of the main dimensions for the Content of the awareness program construct.

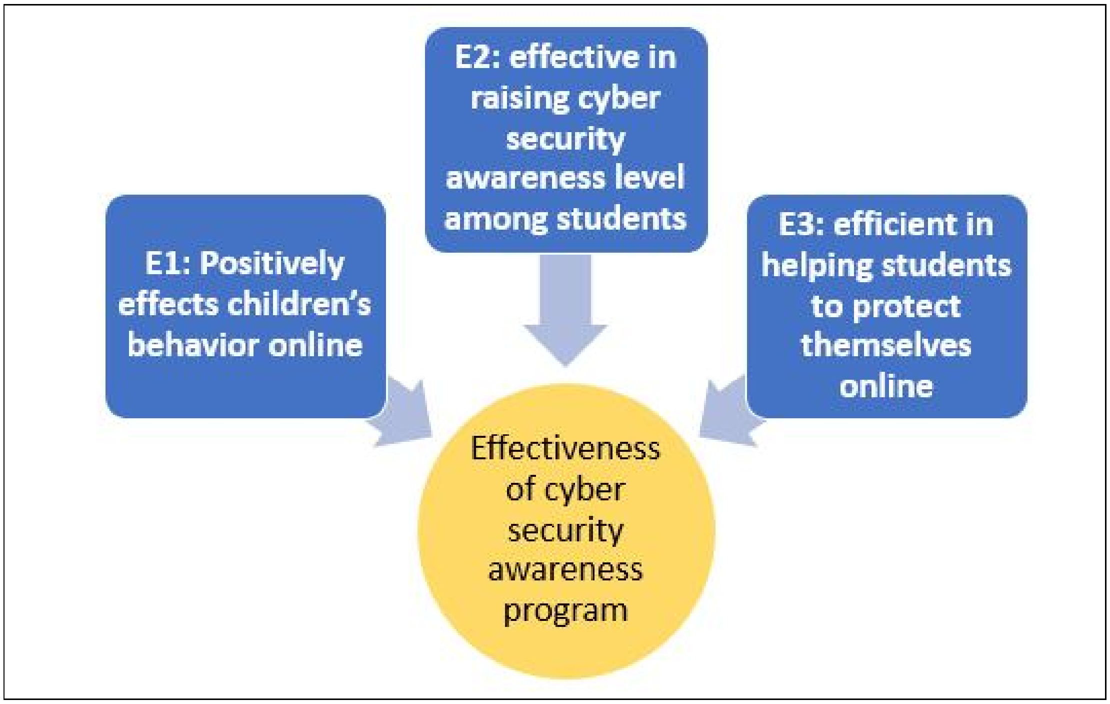
E1: Positively effects children's behavior online
E2: effective in raising cyber security awareness level among students
E3: efficient in helping students to protect themselves online
Effectiveness of cyber security awareness program

Figure 4. Illustration of the main dimensions for the Effectiveness construct.

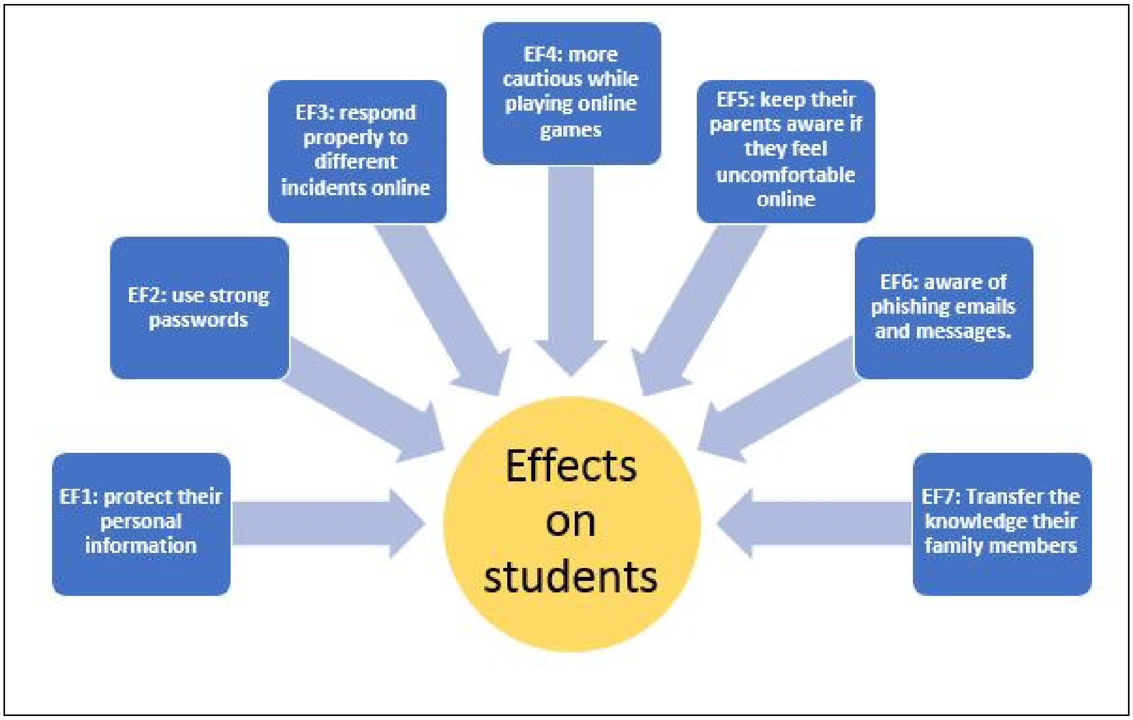
EF4: more cautious while playing online games
EF3: respond properly to different incidents online
EF5: keep their parents aware if they feel uncomfortable online
EF2: use strong passwords
EF6: aware of phishing emails and messages.
EF1: protect their personal information
Effects on students
EF7: Transfer the knowledge their family members

Figure 5. Illustration of the main dimensions for the Effects on students construct.

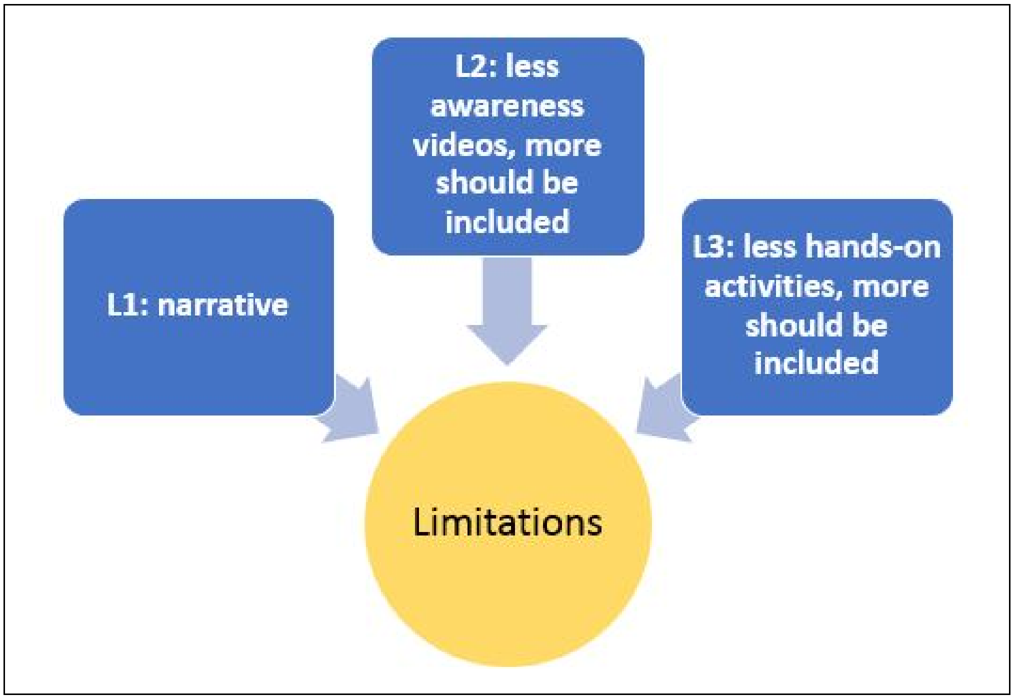
L2: less awareness videos, more should be included
L1: narrative
L3: less hands-on activities, more should be included
Limitations

Figure 6. Illustration of the main dimensions for the limitations construct.

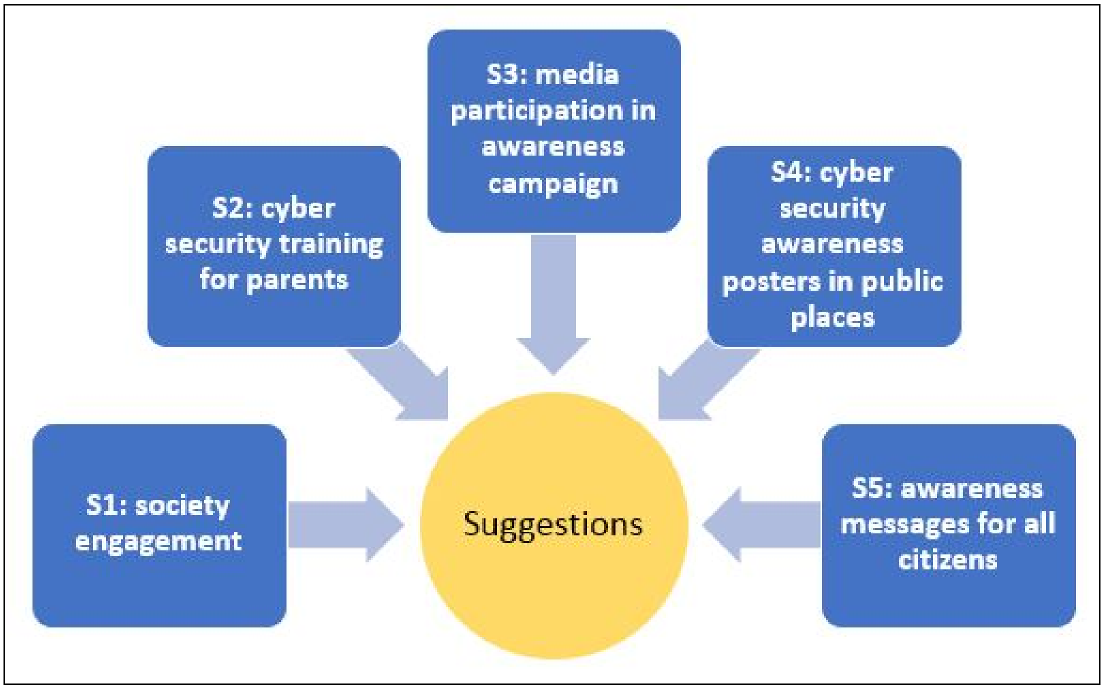
S3: media participation in awareness campaign
S2: cyber security training for parents
S4: cyber security awareness posters in public places
S1: society engagement
Suggestions
S5: awareness messages for all citizens

Figure 7. Illustration of the main dimensions for the suggestions construct.

The main themes that are repeated through the interviews with the students aged 8 to 10 years old that attended the cyber security awareness program are:

1. Online risks students may expose to
2. Content of awareness program
3. Effectiveness
4. Effects

Table 6 illustrates the main themes and their constructs and dimensions.

Main constructs	Main Dimensions
Online risks students may expose to	O1: Cyber Bullying O2: break of password O3: Identity theft O4: Online Phishing O5: break to privacy
Content of awareness program	C1: Internet Safety C2: Cyber Bullying C3: Identity theft C4: Online Phishing C5: Privacy C6: Password C7: secure websites C8: Online Strangers C9: protection
Effectiveness of cyber security awareness program	E1: very effective E2: positively influence their online behavior
Effects on students	EF1: protect their personal information EF2: use strong passwords EF3: respond properly to different incidents online EF4: more cautious while playing online games EF5: keep their parents aware if they feel uncomfortable online

	EF6: aware of phishing emails and messages EF7: Not respond to strangers online

Table 6. Main constructs and main dimensions resulted from the three interviews.

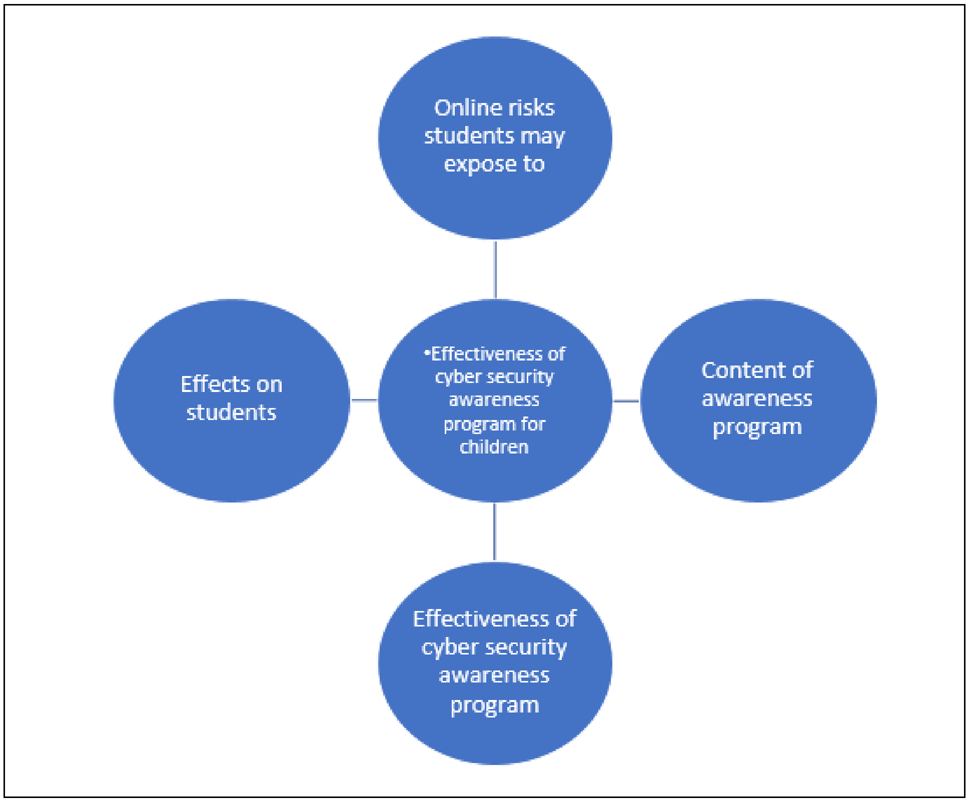
Online risks students may expose to
Effects on students
•Effectiveness of cyber security awareness program for children
Content of awareness program
Effectiveness of cyber security awareness program

Figure 8. Illustration of the main constructs resulted from the students' interviews.

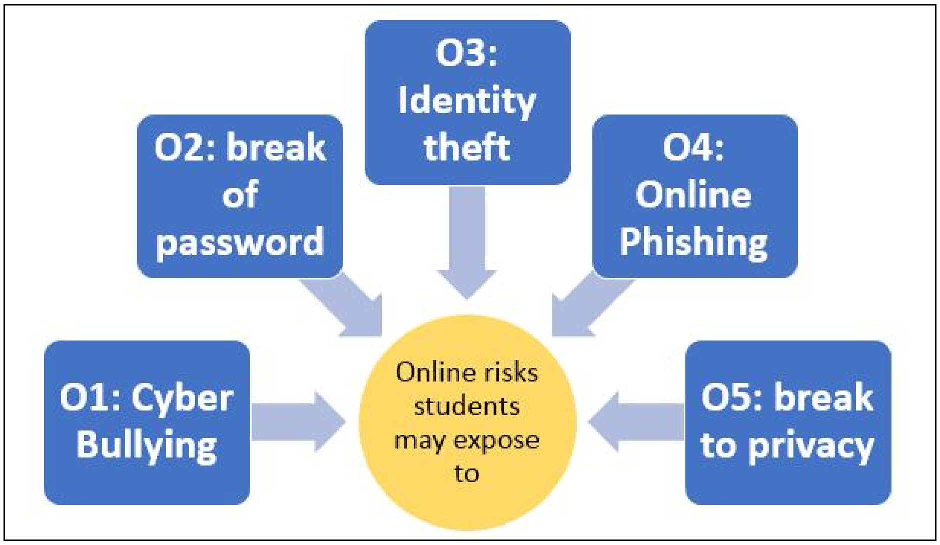

Figure 9. Illustration of the main dimensions for the Online Risks construct.

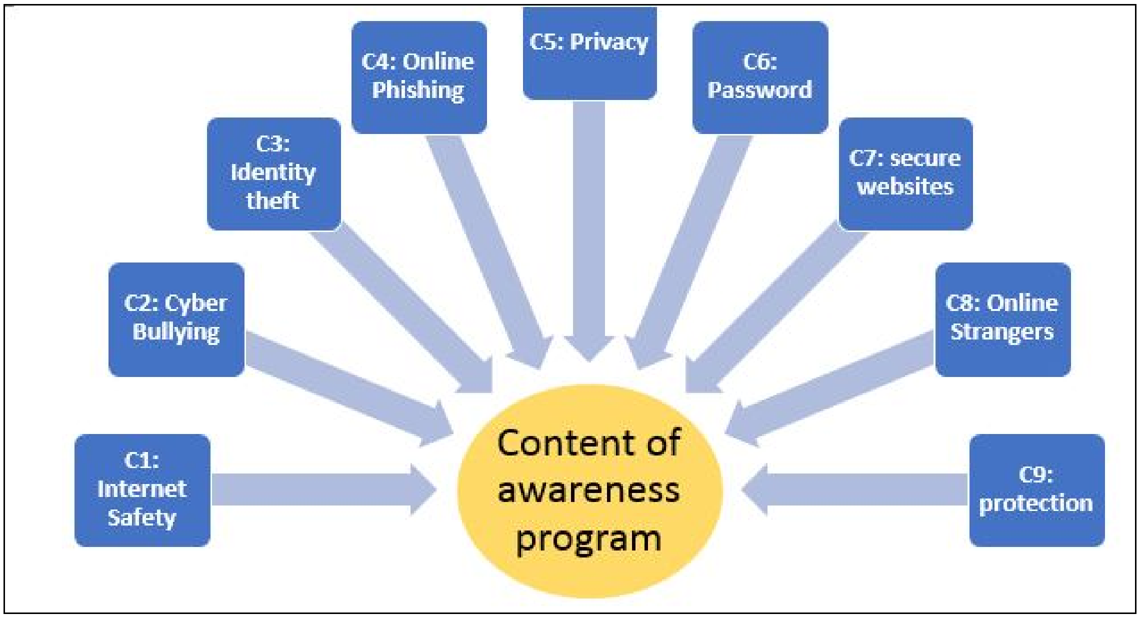

Figure 10. Illustration of the main dimensions for the content of the awareness program construct.

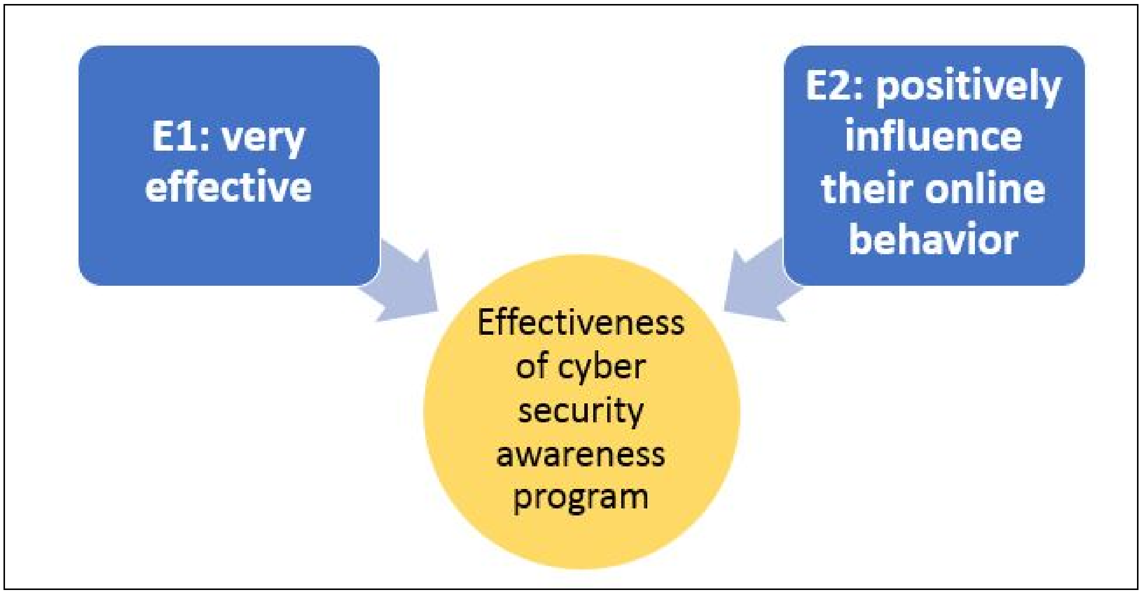
E1: very effective
E2: positively influence their online behavior
Effectiveness of cyber security awareness program

Figure 11. Illustration of the main dimensions for the effectiveness of the awareness program construct.

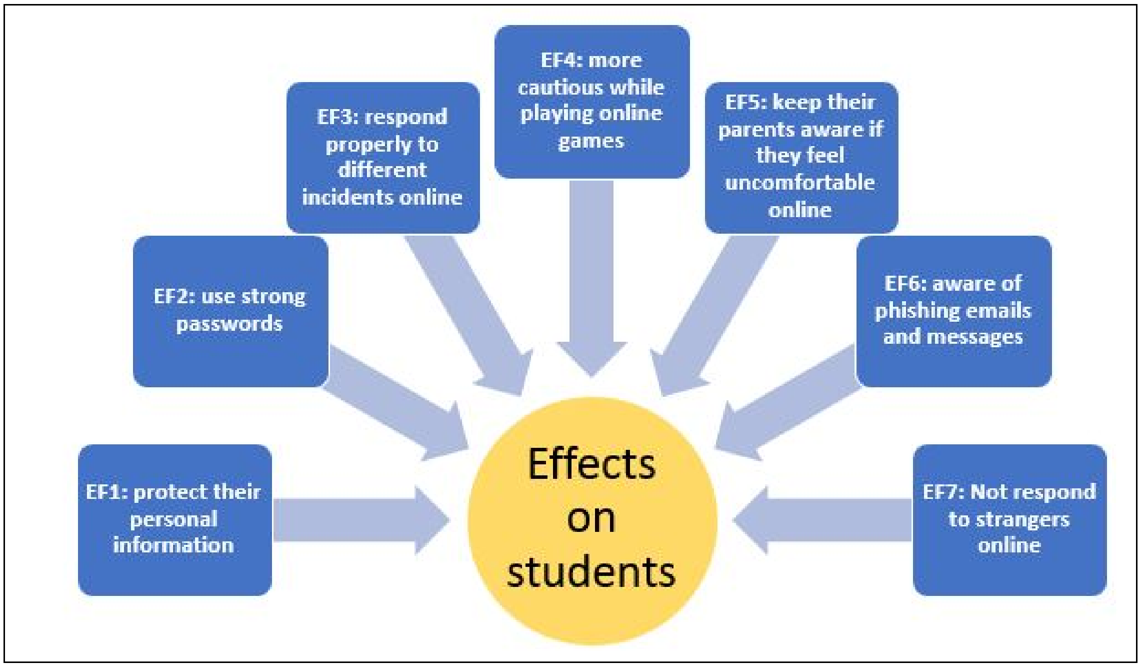
EF4: more cautious while playing online games
EF3: respond properly to different incidents online
EF5: keep their parents aware if they feel uncomfortable online
EF2: use strong passwords
EF6: aware of phishing emails and messages
EF1: protect their personal information
Effects on students
EF7: Not respond to strangers online

Figure 12. Illustration of the main dimensions for the effects on students construct.

The data collected from the three interviews with the trainers of the cyber security awareness program as well as the data collected from the twelve interviews with the students who attended the cyber security awareness program were organized as illustrated above to be able to answer the three research questions; (1) What online risks children may expose to? (2) How cyber security awareness training influences student's online behavior? (3) How effective is the Cyber Security Awareness program adopted by the Ministry of Education in UAE in educating students aged 8 to 10 about the safe use of the internet? The results based upon the three interviews with the trainers (Design and Technology teachers) of the cyber security awareness program and the students who attended the awareness program to answer the first research question: what online risks children may expose to, both the trainer of the program (Design and Technology teachers) and students agreed that the online risks that children may expose to are cyber bullying, online phishing, identity theft, break to the privacy of the children. The trainer of the program considered pornography as an online risk that children may face online while children didn't mention anything related to pornography. On the other hand, children considered the password break as an online risk that they may face online.

The second question in this research was about "How the cyber security awareness training influences student's online behavior", both the trainer of the program and the students who attended the cyber security awareness training agreed that the cyber security awareness training positively influenced the student's behavior online, students become more cautious while they are using the internet especially when they are playing online games, students as well start using strong passwords for their accounts and they stop sharing their personal information.

The third research question in this research paper was "How effective is the Cyber Security Awareness program adopted by the Ministry of Education in UAE in educating students aged 8 to 10 about the safe use of the internet?", both the trainer of the cyber security awareness program and the students who attended the training agreed that this training is very effective, essential and very beneficial, both trainer of the program and the students identified how this training benefit them, the trainer of the awareness program stated that students after the training tend to protect their personal information, use strong passwords, respond properly to different incidents online, become more cautious while playing online games, keep their parents aware if they feel uncomfortable online, become more aware of phishing emails and messages, moreover they tend to transfer the knowledge they gained to their family members. Students who attended the cyber security awareness training as well agreed to what the trainer said above and they added one more point that they wouldn't respond to strangers online.

6. Results discussions and the implications

In this research paper, three interviews were conducted with the trainers of the cyber security awareness program that targeted students aged 8 to 10 years old, and twelve interviews were conducted with students who attended the awareness program. Although the number of interviews is little, the effectiveness of the cyber security awareness program was examined by two points of view; the trainers of the program and the children who attended the program. The discussion section consists of two parts; part one will be based upon the main themes that were identified in the previous section from the interviews, part two will focus on the interview's outcomes in order to answer the three research questions, finally, the conclusion will be delivered.

Part One: discussions based on the six themes (Online risks, Content of awareness program, Effectiveness of the awareness program, Effects of the training of the students, Limitations of the awareness training and Suggestions)**.**

1. Both the trainers of the cyber security awareness program and the students who attended the awareness program identified online risks that children may face while they use the internet, it was noticeable that the interviewee agreed on most of the common online risks. The trainers of the program believed that the most common online risks for the children at the age of 8 to 10 years old is the cyber bullying, students as well believed that it is likely that they may expose to cyber bullying. Many other online risks identified by both the trainers and the students such as identity theft, online phishing, and the break to the privacy. Trainers of the program identified the pornography as a common online risk that children may expose to, but students didn't mention anything related to pornography.

2. The content of the cyber security awareness program focused on the identification of different online risks and how students should respond to each of them. The topics of the awareness training as well discussed the protection online; how students protect themselves and their digital devices, how they create strong passwords, how they differentiate between secure and insecure websites and how they can differentiate the phishing emails. If we compare the online risks that were identified earlier and considered as common, it is clear that these online risks were covered in the content of the cyber security awareness program and children trained about them. This can be considered as a positive strong indicator of the efficiency of the cyber security awareness program.

3. Both the trainers of the cyber security awareness (Design and technology teachers) and the students agreed on the effectiveness of the awareness program. They both stated that the awareness program is very effective and beneficial. It is noticeable that most of the students said that awareness is very effective without explaining the reasons and this is due to their age; they are young to give a full explanation. On the other side, the trainers of the program are teachers who know the students and deals with them in a daily manner, they explained how the students benefit from the awareness program. At the end of the awareness program students become more cautious while they are online, they tend to protect their personal information and start using strong passwords. Students noticed that they shouldn't agree to meet any online stranger. Students speak to the teachers on how they react to different incidents online and how they keep their parents aware of anything makes them uncomfortable while they are online.

4. The cyber security awareness training has great effects on students as both the trainers and the students said. The students tend to protect their personal information and use strong passwords. Students respond properly to different incidents online and they become more cautious while playing online games. Students keep their parents aware if they feel uncomfortable online and they transferred the knowledge they gained to their family members. These great effects on the student's behavior online is a positive indicator of the effectiveness of the cyber security awareness program on the children.

5. The cyber security awareness program was delivered to students through lectures about different topics of online risks and online protection, some short awareness videos were included and at the end of the awareness program, each student created an awareness poster about internet safety. The trainers believed that the awareness program is narrative, and the content of

the awareness program should include more awareness videos as they believed that the videos have a great impact on the children. Trainers as well suggest that the awareness program should include more hands-on activities as the involvement of children in creating something has great effects on assuring the concepts on their minds.

6. The trainers of the awareness program provide the following suggestions that they believe in their important role in raising the awareness level among children. The engagement of the society in the cyber security awareness training is essential to build cyber security culture among society. The cyber security awareness training for parents is crucial as the parent's recognition of different online risks and the best online practices will have great effects on their children moreover it will help to protect their children online. The participation of all the media in the cyber security awareness would create great knowledge among society. Awareness posters in public places are recommended as well as awareness messages for all citizens.

Part Two: discussions based on interviews results to answer the research three main questions.

The data collected from the three interviews with the trainers of the cyber security awareness program as well as the data collected from the twelve interviews with the students who attended the cyber security awareness program to answer the three research questions; (1) What online risks children may expose to? (2) How the cyber security awareness training influences student's online behavior? (3) How effective is the Cyber Security Awareness program adopted by the Ministry of Education in UAE in educating students aged 8 to 10 about the safe use of the internet?

In this section, the discussion will highlight the research three questions:

1. "What online risks children may expose to?" the interview conducted with both the trainers of the cyber security awareness program "Design and Technology teachers" and the students who attended the cyber security awareness program identified the most common online risks that children may expose to are cyber bullying, online phishing, identity theft, break to the privacy of the children and pornography. This finding can be proved through the work of Slavtcheva-Petkova, Vera; Nash, Victoria Jane; Bulger, Monica, (2014); they stated that the risks that children may experience when using the internet are very great, and the most common online risks are pornography, cyberbullying, sending and receiving sexual messages, identity theft, and phishing.

2. "How the cyber security awareness training influences student's online behavior?" all the interviews agreed that the cyber security awareness program positively influenced student's online behavior. Number of research papers discussed whether the awareness program affects children online behaviour or not; Jun Zhao, GeWang, Carys Dally, Petr Slovak, Julian Edbrooke-Childs, Max Van Kleek and Nigel Shadbolt, (2019) stated that the cyber security awareness program is essential and beneficial in educating children about the online risks and internet best practices and this result can be aligned along with the results found from the interviews in which all of the interviewees agreed that the awareness program positively affects children's online behavior.

3. "How effective is the Cyber Security Awareness program adopted by the Ministry of Education in UAE in educating students aged 8 to 10 about the safe use of the internet?" Although all of the interviewees agreed that the cyber security awareness program that the provided by the Ministry of Education in UAE for students aged 8 to 10 years old is effective in raising the cyber security awareness level among students and educate them about different online risks and how they should respond to each of these online risks, there is no any approved model or framework that can be used to evaluate the effectiveness of these awareness programs for student's online behaviour.

7. Conclusion

As the internet takes a huge part of our children's lives, it is essential to ensure that they are safe and to protect them while they are online. This research paper focused on investigating the effectiveness of the cyber security awareness program that is provided by the Ministry of Education in UAE in training and educating the students aged 8 to 10 years old about online risks and how they should respond properly to each of these risks. To investigate this, data were collected from interviews conducted with three of the trainers of the cyber security awareness program "Design and Technology teachers" and twelve students who attended the awareness program. All the participants agreed that the children are at risk while they are online, and the cyber security awareness is essential. The participants as well agreed that the cyber security awareness program is effective and influenced student's online behavior. Although all the students who attended the cyber security awareness program agreed that it was effective, and they benefit from it, the real effectiveness is measured in reality and how they behave online, and this is hard to measure. Children due to their young age may forget some of the skill they gain from the program, that's why the regular cyber security awareness for children and all society is essential. It is recommended for future research to apply observation on a group of students who attended the awareness program to observe how they behave online. The participation of parents in future research is recommended as it will provide valuable findings.

References

Anna Sevcíkova. (2016). *Girls' and boys' experience with teen sexting in early and late Adolescence*. Journal of Adolescence 51 (2016) 156e162

Avtcheva-Petkova, Vera; Nash, Victoria Jane; Bulger, Monica (2014). *Evidence on the extent of harms experienced by children as a result of online risks: implications for policy and research.* Information, Communication & Society, 2014, 18(1), pp. 48-62

Bilal Khan, Khaled S. Alghathbar, Syed Irfan Nabi and Muhammad Khurram Khan, 2011. *Effectiveness of information security awareness methods based on psychological theories.* African Journal of Business Management Vol. 5(26), pp. 10862-10868, 28 October, 2011.

Bőthe, B., Tóth-Király, I., Zsila, Á., Demetrovics, Z., Griffiths, M.D., Orosz, G. (2017). *The development of the Problematic Pornography Consumption Scale (PPCS)*. Journal of Sex Research. 2018

Dan Craigen, Nadia Diakun-Thibault, Randy Purse (2014). *Defining Cybersecurity*. Technology Innovation Management Review. October 2014.

Elmer Lastdrager, Inés Carvajal Gallardo, Pieter Hartel, Marianne Junger. (2017). *How Effective is Anti-Phishing Training for Children?.* Proceedings of the Thirteenth symposium on Usable Privacy and Security (SOUPS 2017). July 12–14, 2017 • Santa Clara, CA, USA. ISBN 978-1-931971-39-3

Eric Luiijf, Kim Besseling and Patrick de Graaf (2013*). Nineteen national cyber security strategies*. Int. J. Critical Infrastructures, Vol. 9, Nos. 1/2, 2013

Fadi A. Aloul. (2010). *Information Security Awareness in UAE: A Survey Paper*. JOURNAL OF ADVANCES IN INFORMATION TECHNOLOGY, VOL. 3, NO. 3, AUGUST 2012

Felix Haeussinger, Johann Kranz, 2013. *Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior*. ICIS.

Gemma Pons-Salvador, Xud Zubieta-Méndez, Dolores Frias-Navarro, (2018). *Internet Use by Children Aged six to nine: Parents' Beliefs and Knowledge about Risk Prevention*. Volume 11, Issue 6, pp 1983–2000

George Tsakalidis, Kostas Vergidis, 2017. *A Systematic Approach Toward Description and Classification of Cybercrime Incidents.* IEEE Transactions on Systems, Man, and Cybernetics: Systems (Volume: 49 , Issue: 4). Pages: 710 - 729

Gila Cohen Zilka. (2017). *AWARENESS OF ESAFETY AND POTENTIAL ONLINE DANGERS AMONG CHILDREN AND TEENAGERS*. Journal of Information Technology Education Research. Volume 16, 2017.

HAMAD OBAID AL MANSOORI. (2015). *TOWARDS A SAFER CYBER CULTURE. Telecommunication Regulatory Authority official website*. https://www.tra.gov.ae/aecert/en/about-us/director-generals-message.aspx

Jacob, S. A., & Furgerson, S. P. (2012). *Writing Interview Protocols and Conducting Interviews: Tips for Students New to the Field of Qualitative Research*.The Qualitative Report, 17(42), 1-10.

Jemal Abawajy. (2014). *User preference of cyber security awareness delivery methods*. Behaviour & Information Technology, 2014. Vol. 33, No. 3, 236–247

Jun Zhao, GeWang, Carys Dally, Petr Slovak, Julian Edbrooke-Childs, Max Van Kleek and Nigel Shadbolt. (2019). *'I make up a silly name': Understanding Children's Perception of Privacy Risks Online*. arXiv.1901.10245.

Karen Brown, Margaret Jackson & Wanda Cassidy. (2006). Cyber-Bullying: *Developing Policy to Direct Responses that are Equitable and Effective in Addressing this Special Form of Bullying. Canadian Journal of Educational Administration and Policy*, Issue #57, December 18, 2006

Komal Bansal. (2016). *Effectiveness of Children Online Privacy Strategies*. The 16th Winona Computer Science Undergraduate Research Symposium. April 27, 2016

Lene Hansen and Helen Nissenbaum (2009). *Digital Disaster, Cyber Security, and the Copenhagen School*. International Studies Quarterly (2009) 53, 1155–1175

Livingstone, Sonia and Haddon, Leslie and Görzig, Anke and Ólafsson, Kjartan (2011) *Risks and safety on the internet*. LSE Research Online, August 2012.

M. Valcke, B. De Wever, H. Van Keer, T. Schellens (2011). *Long-term study of safe Internet use of young children*. Computers & Education 57 (2011) 1292–1305

Mackenzie Adams, Maged Makramalla. (2015). *Cybersecurity Skills Training: An Attacker-Centric Gamified Approach*. Technology Innovation Management Review. January 2015.

Maria Bada, Angela M. Sasse and Jason R.C. Nurse, 2019. Cyber Security Awareness Campaigns: Why do they fail to change behavior?. *Arxiv*. arXiv: 1901.02672.

Mehmet Tekerek, Adem Tekerek, 2013. A Research on Students' Information Security Awareness. *Turkish Journal of Education*. Volume 2 Issue 3.

Nazura Abdul Manap, Anita Abdul Rahim, Hossein Taji. (2015). *Cyberspace Identity Theft: The Conceptual Framework. Mediterranean Journal of Social Sciences*. Vol 6 No 4 S3. August 2015.

Rahat Ibn Rafiq, Homa Hosseinmardi, Richard Han, Qin Lv, Shivakant Mishra, Sabrina Arredondo Mattson. (2015). *Careful what you share in six seconds: Detecting cyberbullying instances in Vine.* IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. (2015).

Rossouw von Solms, Johan van Niekerk, 2013. *From information security to cyber security*. Computer and Security. Volume 38, October 2013, Pages 97-102

Sonia Livingstone, Giovanna Mascheroni and Elisabeth Staksrud (2015). *Developing a framework for researching children's online risks and opportunities in Europe.* London: EU Kids Online. ISSN 2045-256X

Tania Cabello-Hutt, Patricio Cabello and Magdalena Claro (2017). *Online opportunities and risks for children and adolescents: The role of digital skills, age, gender and parental mediation in Brazil*. SAGE Journals. Volume: 20 issue: 7, page(s): 2411-2431.Sl

Tonia SanNicolas-Rocca, Benjamin Schooley and Janine L. Spears. (2014). *Designing Effective Knowledge Transfer Practices to Improve IS Security Awareness and Compliance*. 2014 47th Hawaii International Conference on System Science.