ENHANCEMENT OF CYBERSECURITY AWARENESS PROGRAM ON PERSONAL DATA PROTECTION AMONG YOUNGSTERS IN MALAYSIA: AN ASSESSMENT

Noor Hayani Abd Rahim[1] , Suraya Hamid[2], Miss Laiha Mat Kiah[3]

[1,2,3]Faculty of Computer Science and Information Technology, University of Malaya
50603 Kuala Lumpur, Malaysia
[1]International Islamic University of Malaysia, Kuliyyah of Information Communication Technology,
Department of Information System P.O Box 10, 50728 Kuala Lumpur, Malaysia

Email: noorhayani@iium.edu.my[1*] (corresponding author); suraya_hamid@um.edu.my[2*] (corresponding author); misslaiha@um.edu.my[3]

DOI: https://doi.org/10.22452/mjcs.vol32no3.4

ABSTRACT

Cybersecurity awareness program has been used as a medium to educate and make awareness among youngsters on personal data protection. However, it is still unclear the extent to which the effectiveness of this cybersecurity awareness program among youngsters require an assessment. This to ensure the current content of cybersecurity awareness program is consistently updated and aligned with current Internet usage among youngsters. Our assessment was systematically conducted using Kirkpatrick's Four Learning Evaluation Model as conceptual framework; which consists of four phases of sequential assessment; Phase 1 –Reaction, Phase 2- Learning, Phase 3 – Behavior and Phase 4-Result. This study used mixed method research methodology in conducting the assessment and the instruments used in Phases 1 until 4 respectively were survey, pre-test and post-test survey, observation of web recording and focus group interview. The findings from this study revealed that youngsters do have positive reaction towards the program content, reported to have changes in terms of their knowledge and skills and practice of desired behavior on personal data protection. However, the undesired behavior also revealed practiced among youngsters and this suggest improvement required to the current module used to educate youngsters. The improvements include i) Decision making process in using personal data, ii) Management of online application iii)Management of online contents iv)Management of password and username. The result of this assessment is significant to the stakeholders in terms of providing insight into the effectiveness level of current module used to educate youngsters and assist them to decide better module.

Keywords: cybersecurity awareness, program assessment, youngsters, personal data protection, Kirkpatrick's Four Learning Evaluation Model.

1.0 INTRODUCTION

The Internet has inevitably affected the youngsters' daily activities. As early adopters, youngsters are more open to explore and using new technologies inclusive of the Internet [12], [41], [49]. Youngsters or millennials are categorized as individuals aged between 12 and 19 years old [8], [28], [38]. Often labelled with term NetGen, youngsters who were born surrounded by Internet technologies and smart devices are among the most active Internet users [28], [44]. They are highly involved with social media and Internet applications such as YouTube, WeChat, WhatsApp and also gaming applications. Youngsters nowadays are fully equipped with gadgets like mobile telephony and smartphones which enable them to get Internet access. This is one of the contributing factors for youngsters to have high involvement in Internet usage [12], [39], [35]. Youngsters normally use the Internet for social media opportunities as well as entertainment, which is mostly done via the use of smartphones and computer tablets [39], [41]. Youngsters in particular, have unique characteristics in browsing the Internet due to their attitude that is keen to explore and discover new things [38], [45], [58]. They also have a high degree of enthusiasm and belief that whatever information available on the Internet is considered genuine and trustworthy. To a certain degree, youngsters sometimes overshare their personal data over the Internet. Using social media for instance, youngsters who have their personal information available on the Internet opens windows to vulnerabilities. Due to this attitude, they are becoming so vulnerable in the cyber environment and can become an easy target for cyber criminals to take advantage over them. Therefore, it is required to educate youngsters on personal data protection as their extensive use of the Internet may cause vulnerabilities and attract attacks by cyber criminals. The understanding of youngsters on personal data protection is deemed important due to their extensive Internet usage.

1.1 The characteristics of youngsters while using the Internet

The consistent finding of high Internet literacy among youngsters as compared to the elderly in studies [31], [38], is another element that justifies the focus required toward youngsters for them to gain the appropriate security awareness. Their enthusiasm in exploring the Internet often exposes them to risks of cyber threats, such as phishing and identity theft [11], [58]. The other reason for conducting assessments among youngsters is due to the lack of awareness of safety measures, security practices, and reliability of Internet applications used [17], [38]. In addition, youngsters have an oversharing attitude with online media, thus encouraging third parties or intruders to stalk or steal personal information. Further investigation on youngsters reveals that popularity, or being famous in the digital world, has also encouraged youngsters to get connected to the Internet and try uploading videos, profile or materials which attract other Internet users to view and share [34], [36], [41], [51]. At a young age, youngsters often lack self-monitoring skills, and have difficulty filtering unpleasant online material such as sexual content and misleading communication [58]. Because of these characteristics, the digital environment becomes unsafe for them, especially in terms of their personal data. Thus cybersecurity awareness is considered an appropriate platform to educate and keep reminding them of the risks. However, it is still unclear the extent to which the effectiveness of this cybersecurity awareness program among youngsters require an assessment to be conducted. The review of current assessment method is presented in the next section.

2.0 RELATED LITERATURE

2.1 Current approaches used to assess cybersecurity awareness program

The investigation on the assessment strategies for cybersecurity awareness programs revealed a lack of attempt to conduct the assessment via a systematic technique. The systematic technique addressed here is an evaluation method which involves a systematic procedure of performing evaluation, judgment, investigation, decision making, improvement, upgrading and assessment of any social intervention program [46], [47], [59]. In the study done by [2] on the assessment of human factors, they suggested the use of a specific systematic technique namely Kirkpatrick's Four Learning Evaluation Model (reaction, learning, behavior and result) to evaluate the effectiveness of the cybersecurity awareness program. However, the former literature shown the actual use of this technique is less considered for an assessment of cybersecurity awareness programs. Most of the current assessment methods were merely for determining certain criteria such as the general experience and usage of security measures, the attitude while accessing the Internet, and security perception [20], [21]. In the study conducted by [7], the assessment was made on the following criteria: information security in general, and understanding of a few topics concerning security. Other studies were only focused on the user behavior without looking at other components of assessment as per Kirkpatrick's Four Learning Evaluation Model [42], [54].

Literature on the assessment of cybersecurity awareness programs also revealed that the focus groups mainly targeted for assessment were organizations and home Internet users [19], [22], [32]. It seems that the scope of these two contexts is too broad and requires proper segmentation during assessment due to the fact that Internet communities vary and possess different understanding and unequal level of security awareness among different age groups [2], [48]. There were attempts made by [20], [21] to assess the security perception and find the security belief of personal Internet users. However, the study randomly focused on general Internet users without segregation in terms of age segmentation, especially with youngsters. Thus the need for assessment according to age segmentation is warranted particularly is assessing youngsters due to their characteristics previously discussed.

The extended investigation on the assessment of cybersecurity awareness programs in relation to the risk of personal data protection among youngsters revealed that they were found to have a lack of understanding, and poor security behavior with regards to personal data protection, in this case as prevention from being seen by others while accessing the Internet [21], [48]. Also in an analysis done by [56], it was discovered that personal data such as real names, email addresses, real dates of birth and full addresses were made available on the Internet. This has made it easy for identity thieves to capture this information and use it for illegal means [5]. Youngsters can easily become a victim due to their ill equipped nature with regards to the practice of Internet safety [19]. Thus, whether personal data protection components were focused during assessment is examined. Based on the literature, it was found that most of the assessment of cybersecurity awareness sessions available was generally focused on a broad security concern but with less focus specifically on creating awareness of personal data protection.

In summary, the literature of current assessment approach is done by investigating the current methodology used, focused target audience as well as whether the issues of personal data protection were focused during an assessment. The previous assessment approaches lack of consideration to use program evaluation technique. Also, little attention

has been given on the assessment among youngsters and personal data protection. Therefore, this study attempts to fill in the gaps in assessment of cybersecurity awareness research by embarking on Kirkpatrick's Four Learning Evaluation Model as a proposed framework which includes assessment on the four components; i) reaction ii) learning iii) behavior and iv) result. This study is conducted through step-by-step assessments based on the four mentioned components, conducted among youngsters to gain their feedback on the effectiveness of current cybersecurity awareness module used. The instruments used within this study were designed and tailored to the issue of personal data protection. The output of this study consists of a proposal of systematic assessment approach using Kirkpatrick's Four Learning Evaluation Model with identification of an additional assessment component on IT Literacy and parental guide and control. The systematic assessment approach is beneficial to facilitate stakeholders such as Cybersecurity Malaysia, parents and management of schools to decide for a better module to convey the message on personal data protection.

2.2 Cybersecurity awareness program

A cybersecurity awareness program is defined as a way to educate and increase alertness about computer threats and vulnerabilities with regard to IT usage [50]. Another purpose of this program is to increase the level of understanding about self-responsibility and the necessary action required while engaging in digital activities. Various methods can be used to promote cybersecurity awareness regardless of the age of the individual, for example, classroom-based training sessions, educational videos, seminars, workshops, pamphlet distribution, online advertisement, and e-learning [1], [14], [16], [56]. A cybersecurity awareness program should be conducted frequently to remind and update Internet users about new potential Internet threats [14], [32]. In Malaysia, there is one agency established as a reliable organization to conduct and manage cybersecurity awareness among Malaysia citizens. It is known as Cybersecurity Malaysia (CSM). This study is conducted based on the cybersecurity awareness program module known as CyberSAFE program conducted by CSM.

CSM uses a few approaches in conducting awareness to Malaysian citizens. Among the approaches are having an online portal which includes necessary tips, advices, videos, games, quizzes and newsletters. Various approaches have been to attract the audience to the importance of the cybersecurity message. Apart from the online portal, CSM has also conducted a series of cybersecurity awareness program all over Malaysia to different types of Internet users as way to be a step closer in educating and improving cybersecurity.

The content of the CyberSAFE program is specifically designed towards meeting different types of Internet users such as kids, youths, parents and organizations. A different approach is used for each type of user. Specifically, the cyber tips for children include messages on basic security protection such as managing cyber friends and safeguarding personal information. Particularly for youngsters, the cyber tips given to them covers information protection, spyware watch, emails and spams, chat safety, blog safety, cyber bullying, password protection, P2P sharing and downloading, making friends online, cyberstalk, cyber harassment, virus, worms and general safety computing tips. On the other hand, cyber tips for parents are more towards how to observe their children while using the Internet. Meanwhile, for organizations, the cyber tips given are mainly on business continuity and disaster discovery. In this study, the subject of interest is on youngsters and personal data protection. Based on the cybersecurity awareness message conveyed via the CyberSAFE program, personal data protection is highlighted in almost every cyber tips. Therefore, it is suitable for this study to leverage on the CyberSAFE program in order to perform the assessment on personal data protection among youngsters in Malaysia.

2.3 Kirkpatrick's Four Learning Evaluation Components

The four learning evaluation model was introduced by Donald Kirkpatrick in 1975 as a way to evaluate a program [30]. Kirkpatrick's Four Learning Evaluation Model consists of four levels of evaluation namely Level 1 – Reaction, Level 2- Learning, Level 3- Behavior and Level 4 – Result. The evaluation procedure of using this model is conducted in sequence. The valuable information is gathered from all level of assessments.

There are different reasons to embark on evaluation of a program. According to [30], the specific aims could be to justify the contribution of a particular training, decision making purpose on continuation or discontinuation and finally for making improvement to a program. In the context of this research, the Kirkpatrick's Four Learning Evaluation Model is used to make improvement to the current state of the cybersecurity awareness program. The assessment in this study is conducted after the program, by utilizing several methods of collecting information pertaining to reaction, learning, behavior and impact of the program. The target of this study is to propose a framework through the use of program evaluation technique in order to explore the effectiveness of the

cybersecurity awareness program in giving education pertaining to personal data protection among youngsters. Thus, the sequential methodology used in collecting information from the participants starts with quantitative basis and followed by qualitative methodologies.

2.3.1 Level 1 – Reaction

The assessment of reaction means to identify the participant reaction towards the program content. The general rules of reaction assessment are that it must ensure that the participant acts favorably towards the program content which would then motivate them to learn more. [30] underline several reasons for measuring reaction which are first, to provide beneficial feedback, comments and suggestion for program improvement. Secondly to assess the credibility of program coordinator and thirdly as a way to provide quantitative measurement for the program stakeholders. Lastly, help to outline the program standards for future programs. In the context of this study, assessment of reaction is meant to identify the general view of participants who attended the cybersecurity awareness program with regard to the program content, understanding the concept of personal data protection, as well as the effectiveness of the methodology used to convey the security awareness message.

2.3.2 Level 2- Learning

The assessment of learning among participants is composed of three branches, which include knowledge, skills and attitudes. The importance of having this assessment level is that it stands as a predecessor for the next assessment on behavior. This is due to the fact that there must be changes in one of the three branches listed above to give an effect in changing behavior. In the context of this study, participants are expected to gain knowledge on security threats, understanding a few actions to be taken while dealing with security threats and having a positive attitude in keeping personal information while engaging in online activities.

2.3.3 Level 3- Behavior

The third assessment level is more complicated due to the fact that the measurement of knowledge transfer from the previous level is determined in this stage. The measurement of behavior is subjective and varies to each individual. Therefore, in the context of this study, the assessment of behavior takes place in a special session of observation that records the participants' activities while engaging in online activities. Behavioral change is a complex process and often requires a wide time frame to observe whether the changes have occurred. This study was conducted based on two cybersecurity awareness programs only and time was limited for behavior observation. Therefore, in order to justify the behavioral change, the data was collected using other methodologies such as surveys, pre and post-test surveys, as well as interviews. The recorded observation data was compared against other data collected and determination was made whether the observed behavior is real.

2.3.4 Level 4- Result

This is the final assessment level which informs the quality of the cybersecurity awareness program. The determination of quality is the most difficult part of the assessment. However, it can be shown by analyzing the data collected in the previous level. The actual change in behavior determines whether the cybersecurity awareness program had met its objectives. Figure 2.1 shows the conceptual framework for this research.

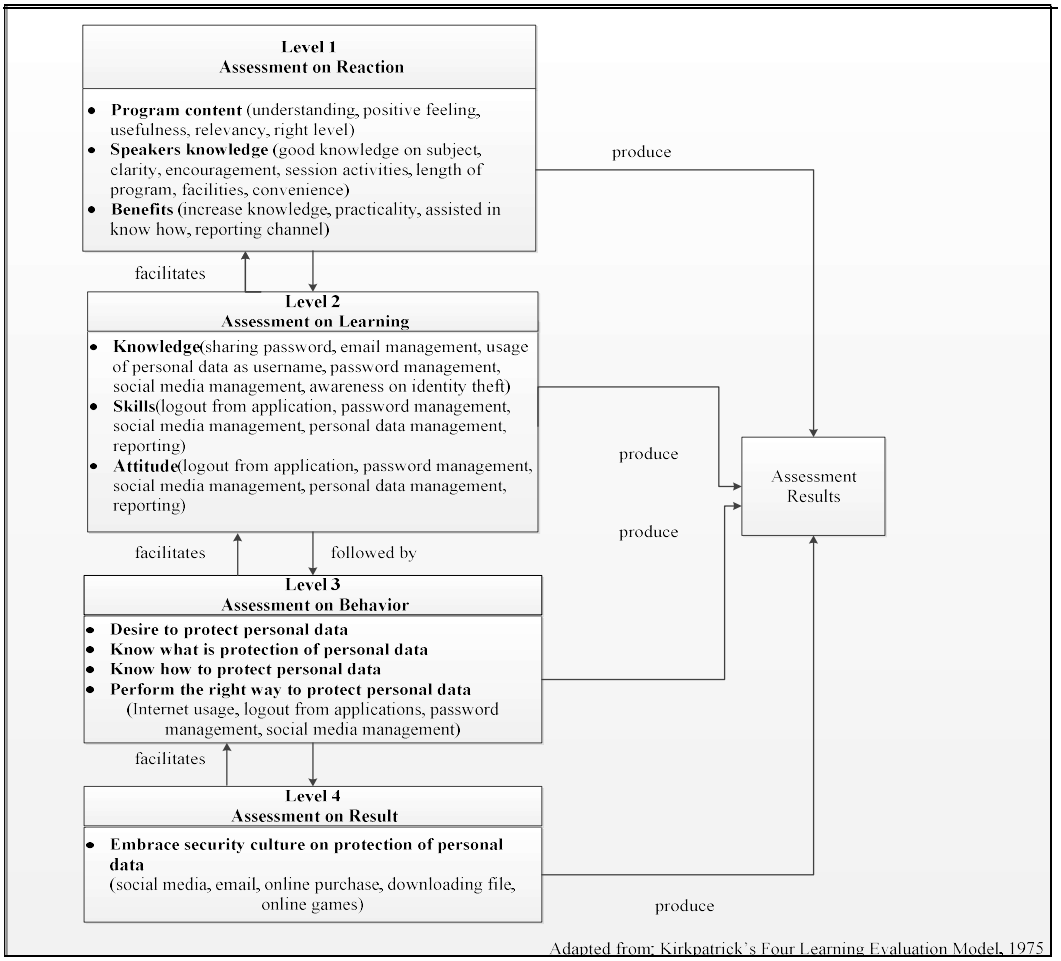

Fig 2.1 Conceptual Framework

This framework depicts major levels adapted from Kirkpatrick's Four Learning Evaluation Model; Level 1- Reaction, Level 2- Learning, Level 3- Behavior and Level 4- Result. These levels are later translated into steps in performing data collection. Basically, the assessment of the cybersecurity awareness program is conducted in sequence which examines the feedback gathered from the attended participants of the cybersecurity awareness program.

Level 1- assessment on reaction involves three sub categories of assessments which are assessment towards the program content, features and benefit. The elements for assessment on reaction are derived from the original model proposed by Kirkpatrick 1975. Level 2- assessment on the level of change in learning which involves sub-assessments on knowledge, skills and attitude. For knowledge, the elements on personal data protection were examined through developing questions based on sharing passwords, email management, usage of personal data such as username, password management, social media management, awareness on identity theft. Meanwhile, for skills and attitude, the elements on personal data protection were asked based on logout from application, password management, social media management, personal data management, reporting. For each level presented in the conceptual framework, there are elements that involve personal data protection. For Level 3 assessment on behavior, the assessment was based on the desire to protect personal data, knowing what protection of personal data is, knowing how to protect personal data and performing the right way to protect personal data. This involves the observation of the following: Internet usage, logout from applications, password management, and social media management. The final level is Level 4, which is assessment on result, includes an examination on how the youngsters embrace the security culture on protection of personal data which involve the usage of social media, email, online purchase, downloading file, online games.

3.0 RESEARCH DESIGN AND METHODOLOGY

The research design presents the flow of research activities from beginning until the end. This study uses research design from [37]. There are four main steps namely analysis, design, development and evaluation. Each main step consisted of several tasks that have to be completed prior to proceeding to the next step.

Here are the detailed steps for the research design:

3.1 Step 1: Analysis

- Task 1: Introduction and research background

This is the most important part in this study in which the problem analysis was identified in the current assessment of cybersecurity awareness programs. It was done through finding related literature to increase the understanding and justify the problems.

- Task 2: Defining gaps

The second important step in this study was to clearly define the gaps. This study was able to define the following gaps:

Gap 1: Fewer attempts found from the literature that used program evaluation technique in assessing cybersecurity awareness program.
Gap 2: Lack of studies that focused on assessment of cybersecurity awareness programs among youngsters.
Gap 3: Lack of studies that assessed the cybersecurity awareness programs that focused on personal data protection among youngsters.

- Task 3: Literature review

Based on the defined problem statements, further investigations were conducted through literature review analysis. This was also an important step taken in order to propose a solution to the problems. The literature review were focus upon the assessment of cybersecurity awareness session in term of existing research on assessment approaches, previous technique or model applied in assessment and relevant model of assessment. Besides, there were other studies reviewed with regard to cybersecurity awareness programs, personal data protection and Kirkpatrick's Four Learning Evaluation Model.

3.2 Step 2: Design

- Task 1: Propose conceptual framework for assessment of the cybersecurity awareness program using the selected program evaluation technique
  The first three steps mentioned above were used as an input for constructing the conceptual framework. The components and its relationship were presented in detail via the conceptual framework diagram.

- Task 2: Data collection (Quantitative method: survey, pre-test and post-test survey)
  Based on the conceptual framework constructed in the previous step, the instruments were designed in order to examine the components and its relationship through quantitative methods (survey, pre-test and post-test surveys). There were two different sets of surveys prepared for different purposes. The first set was used to assess the reaction of participants. Another set was used to assess the level of knowledge gained by participants before and after they attended the cybersecurity awareness program.

- Task 3: Data collection (Qualitative methods: focus group interview and web recording observation)
  The conceptual framework also guided the design of instruments used in the focus group interview session and web recording observation. The focus group interview protocol was prepared prior to the interview session. Randomly selected participants were drawn from the same participant pool who answered the surveys. After finishing the interview session, the same randomly selected participants was next asked to participate in a free Internet browsing session. A web recording observation application, namely Camtasia Studio, was installed in every laptop used during the session. Their online activities were recorded and checked against an observation checklist that was prepared prior to the field work.

3.3 Step 3: Development

Development involved a data collection stage which was conducted over four distinct yet sequential phases. The whole data collection process was held at two OUTREACH CyberSAFE programs conducted by Cybersecurity Malaysia. Firstly, at Bahagian Teknologi Pendidikan Negeri Johor which involved youngsters from all over Malaysia, and secondly at Sekolah Seri Puteri Kuala Lumpur which involved only youngsters who studied in this particular school. The following tasks were involved in the development step.

- Task 1: Develop and conduct data collection using surveys. 400 sets of surveys were prepared for participants who attended the cybersecurity awareness program by Cybersecurity Malaysia, divided into 2 cohorts.
- Task 2: Develop and conduct data collection through pre and post-test surveys. 400 sets of pre-test and post-test surveys were prepared for participants who attended the cybersecurity awareness program by Cybersecurity Malaysia, divided into 2 cohorts.
- Task 3: Develop and conduct data collection using focus group interviews with 12 randomly selected participants who attended the cybersecurity awareness program by Cybersecurity Malaysia.
- Task 4: Develop and conduct data collection through web recording observation of online behaviour with 12 randomly selected participants who attended cybersecurity awareness program by Cybersecurity Malaysia.

3.4 Step 4: Evaluation

- Task 1: Data analysis for quantitative methods
  The results of surveys were gathered and analyzed using Statistical Software Package (SPSS) Version 22, and further analysis involved the use of Smart PLS Version 3.0.
- Task 2: Data analysis for qualitative methods
  The finding from the focus group interview was transcribed from each participant while recording observation was recoded based on the earlier prepared observation checklist.
- Task 3: Final framework for assessment of the cybersecurity awareness program
  The expected output from this research was to propose a final framework for assessment of cybersecurity awareness programs.

4.0 FINDINGS

4.1 FINDING FOR PHASE 1

The finding starts with the descriptive analysis of the demographic profile of the sample. The finding is for Section 1 (Question 1-7). The demographic profile consists of gender, age, access to the Internet, usage of the Internet, duration of Internet usage, attendance to any cybersecurity awareness program previously and awareness on identity theft. The summary of the descriptive analysis in terms of frequency for each question asked for demographic profile is as per Table 4.1 below:

Table Error! No text of specified style in document.**.1: Summary of Descriptive Analysis in Term of Frequency for Each Question asked for Demographic Profile**

Demographic Profile (n=384)		Responses (N)	Percentage %
Gender	Male	36	90.6
	Female	348	9.4
Age	12 years old	0	0
	13 years old	51	13.3
	14 years old	99	25.8
	15 years old	134	34.9
	16 years old	38	9.9
	17 years old	60	15.6
	18 years old	1	0.3
	19 years old	1	0.3
Access to the Internet	Yes	379	98.7
	No	5	1.3
Internet Usage	Social Media	351 – Yes 33 – No	Yes (91.4%) No (8.6%)
	Sending and reading email	359 – Yes 25 – No	Yes -93.5 No - 6.5
	Watching online video	351 – Yes 33 – No	Yes - 91.4 No - 8.6

From table 4.1, based on the descriptive analysis made on the demographic profile, the majority of participants were female; this is because cohort 2 involved a cybersecurity awareness program conducted at an all-female school. The sample consists of 12-19 year olds in which this study managed to get participants from all ages in the stated range, except for 12 years old. For the Internet usage, the majority of participants were involved in the usage of social media, sending and reading email, watching online videos, downloading, while less participants used Internet for playing games and online shopping. Almost half of the youngsters used the Internet daily while others used the Internet only during weekends. From the descriptive finding, the percentage of those who have attended, and those who have never attended any cybersecurity awareness program is approximately equivalent. A majority of participants realised the risk of identity theft of their personal data. In Section 2 of the data collection, which is still within Phase 1, the items asked were pertaining to the feedback from youngsters regarding the program content. The summary of findings for Section 2 of the data collection is presented as per table 4.2:

Table Error! No text of specified style in document.**.2: Summary of Findings for Section 2 Data Collection Phase 1**

Items ID	Items asked	Mean
PC1	I understand the program objective is to educate youngsters about safety in cyber world	4.53
PC2	I found this program is joyful and attractive.	4.15
PC3	I found the material used is useful to enhance the practice of personal data protection.	4.38
PC4	I found the program content is relevance for me to enhance the practice of personal data protection.	4.42
PC5	I felt this program has been presented at the right level to enhance the practice of personal data protection.	4.30
PC6	I understood the importance of protecting personal data.	4.38

Based on table 4.2, there were six items asked in Section 2. Each of the item was given an item ID for easy reference. Each item was analysed based on the mean score of 3 (neutral). From the result each item asked has a mean score above 3. Therefore it can be said that the content presented during cybersecurity awareness program on personal data protection were understood by the participants.

In section 3 of the data collection, which is still within Phase 1, the items asked were pertaining to the quality of speakers and the program features. The summary of findings for Section 3 of the data collection is depicted as per table 4.3:

Table Error! No text of specified style in document.**.3: Summary of Finding for Section 3 Data Collection Phase 1**

Items ID	Items asked	Mean
PPC1	The presenter has good knowledge about personal data protection.	4.46
PPC2	The presenter has explained clearly about personal data protection.	4.44
PPC3	The presenter has given example about personal data protection.	4.46
PPC4	The presenter has encouraged the participants to have better understanding about personal data protection.	4.48
PPC5	I found the activities during the session help me to have better understanding about personal data protection.	4.38
PPC6	I found the session about personal data protection is too long.	3.71
PPC7	I found that session about personal data protection require additional content.	3.73
PPC8	I found the session about personal data protection is useful.	4.35

Based on table 4.3, there were 8 items asked and comparisons were made based on the mean score values. The mean score values were above 3 (neutral). Overall, the participants found that the presenter had good capability in giving awareness on personal data protection. However, the participants found that the session was too long and required additional content.

Table Error! No text of specified style in document.**.4: Summary of Finding for Section 4 Data Collection Phase 1**

Items ID	Items asked	Mean
PB1	My knowledge about personal data protection has increased.	4.42
PB2	I'll practice the knowledge gained through this session to protect my personal data protection.	4.39
PB3	Now, I know how to protect my personal data.	4.41
PB4	Now, I know how to contact the responsible party if any third party ask or steal my personal data.	4.39
PB5	Now, I know how to act if any third party ask or steal my personal data.	4.36
PB6	Now, I know the importance to protect personal data protection.	4.43

In section 4 of the data collection, which is still within Phase 1, the items asked were pertaining to the benefit gained from the cybersecurity awareness program. The analysis is presented in table 4.4, which is also based from the mean value score, all items asked recorded of score above 3 (neutral). Overall, the participants found that the session gave them benefits, and their knowledge on personal data protection had increased.

Further analysis was made to determine the validity through path analysis in Smart PLS 3. The purpose of this analysis is to ensure only valid items in the survey were used to determine participants' reaction based on the item loading value. This is to ensure only applicable items were included, and any redundancies and items measuring same scenario is disregarded. The first step of path analysis involved drawing a diagram as per Figure 4.1. The diagram represented by the oval shape is a section as developed in the survey. Each oval has items represented by arrows and rectangle shape. The path analysis was conducted through path algorithm in Smart PLS which results in the items loading at each arrow. To be considered as valid, the items' score must be > 0.2. Overall, each item's loading was found to be > 0.2. However there were 2 items that scored at lower values as relative to the other items. Thus, the item loading for PPC6 and PPC7 is disregarded.

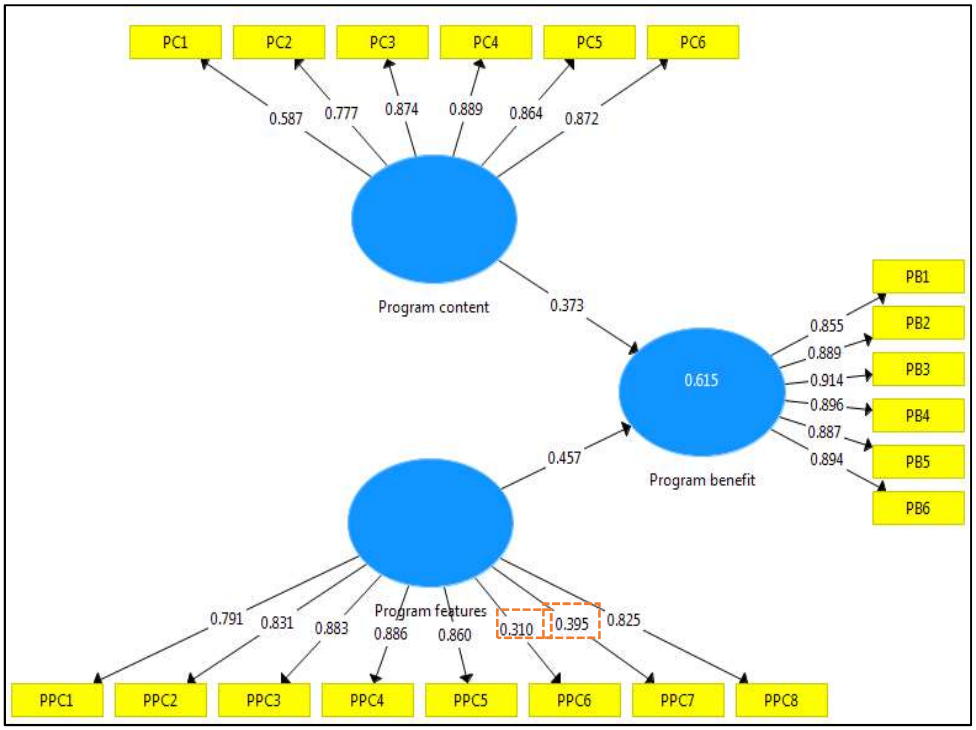

Fig Error! No text of specified style in document.**.1: Path Analysis**

The acceptable item loading value is - Loading, r^2 is between 0.5 and 0.7 to ensure reliability. Thus, the remaining items loading based on the path algorithm are considered reliable. The next analysis, using Smart PLS, was meant to show the convergent validity and discriminant validity of each item. Convergent validity and discriminant validity is meant to measure the construct as in the data collection Phase 1, the program content, program benefits and program features which theoretically should be related to each other. The measurement model is used in order to specify the type of relationship between construct and item involved. Table 4.5 shows the model measurement for this study.

Table Error! No text of specified style in document.**.5: Model Measurement for Data Collection Phase 1 – Convergent Validity**

Construct	Item	Loadings	AVE	CR
PC1 <- Program content	PC1	0.587	0.668	0.922
PC2 <- Program content	PC2	0.777	0.668	0.922
PC3 <- Program content	PC3	0.874	0.668	0.922
PC4 <- Program content	PC4	0.889	0.668	0.922
PC5 <- Program content	PC5	0.864	0.668	0.922
PC6 <- Program content	PC6	0.872	0.668	0.922
PPC1 <- Program features	PPC1	0.791	0.569	0.905
PPC2 <- Program features	PPC2	0.831	0.569	0.905
PPC3 <- Program features	PPC3	0.883	0.569	0.905
PPC4 <- Program features	PPC4	0.886	0.569	0.905
PPC5 <- Program features	PPC5	0.86	0.569	0.905
PPC8 <- Program features	PPC8	0.825	0.569	0.905
PB1 <- Program benefit	PB1	0.855	0.79	0.957
PB2 <- Program benefit	PB2	0.889	0.790	0.957
PB3 <- Program benefit	PB3	0.914	0.790	0.957
PB4 <- Program benefit	PB4	0.896	0.790	0.957
PB5 <- Program benefit	PB6	0.887	0.790	0.957

PB6 <- Program benefit	PB6	0.894	0.790	0.957

Legend:
AVE: average variance extracted
CR: Composite Reliability
Note: PPC6 and PPC 7 were deleted due to low loading.

[11], suggested using the square root of AVE to establish the discriminant validity if this value is larger than other correlation values among the items. From table 4.5, in summary, all the measurements of items met the criteria of convergent and discriminant validity. For convergent validity, the AVE value in this study was all above 0.5 which indicates sufficient convergent validity except for PPC6 and PPC7. For discriminant validity, it is a prerequisite for analysing the relationship between latent (items) variables [23]. Thus, to ensure that the discriminant validity is met, the AVE of each latent (item) variable should be higher than the squared correlations with all other latent (items) variables. In this study, the square root of AVE met the criteria of discriminant validity. Based on the result of the path analysis, the discriminant validity and convergent validity of all items used during the survey were reliable to explain on positive reaction among participants who attended cybersecurity awareness program.

4.2 FINDING FOR PHASE 2

The finding for data collection Phase 2 for the pre-test and post-test survey was started by analysing the type of data collected. This is important to identify whether the data collected is normally distributed or non-normally distributed. In SPSS, the normally distributed data is commonly known as parametric data and non-normally distributed data is commonly known as non-parametric data. According to [24], the normality of data is based on the skewness and kurtosis values which formed the *z* value. If the calculated *z* value exceeds -1.96 to +1.96 the normality of data is rejected. In this study, the *z* value was calculated at Skewness: 1.877/0.123 = 15.26, and Kurtosis = 1.530/0.246 = 6.22, which exceeded +1.96, thus the data is considered not normally distributed.

The first step in determining the type of data collected is important because it would identify a suitable statistical test to be used in comparing the pre-test and post-test result. Also, according to [24], if a violation of the normality data occurs, the suitable type of statistical test to be used for comparison between pre-test and post-test score would be the Wilcoxon test. The Wilcoxon test is suitable to analyse a set of data collected from the same individuals as in this study. Cumulative scores derived from the pre-test and post-test scores were compared using the Wilcoxon test. The result from the Wilcoxon test was tested against the following assumptions: These assumptions were developed based on the conceptual framework for Level 2 assessment to measure changes in knowledge, skills and attitude.

i. The knowledge of participants does not change after attending the cybersecurity awareness program.
ii. The skill of participants does not change after attending the cybersecurity awareness program.
iii. The attitude of participants does not change after attending the cybersecurity awareness program.

The comparison between the pre-test and post-test is as in Table 4.6.

Table Error! No text of specified style in document.**.6: Comparison Table between Pre-test and Post-test Result**

Data were compared using the Wilcoxon Signed Rank Test				
Ranks				
		N	**Mean Rank**	**Sum of Ranks**
The total score of post-test knowledge - The total score of pre-test knowledge	Negative Ranks	181[a]	173.79	31456.50
	Positive Ranks	210[b]	215.14	45179.50
	Ties	0[c]		
	Total	391		
The total score of post-test skills - The total score of pre-test skills	Negative Ranks	132[d]	158.13	20873.50
	Positive Ranks	197[e]	169.60	33411.50
	Ties	62[f]		
	Total	391		
The total score of post-test attitude - The total score of pre-test attitude	Negative Ranks	152[g]	185.58	28208.50
	Positive Ranks	198[h]	167.76	33216.50
	Ties	41[i]		

	Total	391

a. The total score of post-test knowledge < The total score of pre-test knowledge
b. The total score of post-test knowledge > The total score of pre-test knowledge
c. The total score of post-test knowledge = The total score of pre-test knowledge
d. The total score of post-test skills < The total score of pre-test skills
e. The total score of post-test skills > The total score of pre-test skills
f. The total score of post-test skills = The total score of pre-test skills
g. The total score of post-test attitude < The total score of pre-test attitude
h. The total score of post-test attitude > The total score of pre-test attitude
i. The total score of post-test attitude = The total score of pre-test attitude

Table Error! No text of specified style in document..17**: Wilcoxon Test for Data Collection 2 (Pre-test and Post-test)**

Test Statistics[a]			
	The total score of post-test knowledge - The total score of pre-test knowledge	The total score of post-test skills - The total score of pre-test skills	The total score of post-test attitude - The total score of pre-test attitude
Z	-3.105[b]	-3.678[b]	-1.324[b]
Asymp. Sig. (2-tailed)	.002	.000	.186

a. Wilcoxon Signed Ranks Test
b. Based on negative ranks.

Based on the Wilcoxon test, the statistical result is as in Table 4.7, the p>0.05 was used to determine the level of significance. The critical value of *z* must be within -1.96 and +1.96. In SPSS, the Wilcoxon statistic is converted into a *z*-value which can be tested for significance under the normal curve of data distribution [24]. Since the obtained *z* value were *z* (-3.105) for measuring knowledge, and *z* (-3.678) for measuring skills, the assumptions (i) and (ii) are rejected. Thus shown after attending cybersecurity awareness program, knowledge and skills of participants changed. It is different with the result for attitude, where *z* (-1.324) was found to support the assumption no (iii). Thus, the attitude of participants did not change after attending the cybersecurity awareness program. This result could be disputed as only knowledge and skills were reported to change as compared to attitude. Attitude requires time to change. Thus a continuous effort in making cybersecurity awareness is deemed essential in order to result in changing of the participants' attitude.

4.3 FINDINGS FOR PHASE 3

The findings for data collection Phase 3 were derived from five important steps in the thematic analysis. This section briefly discusses each step taken before the final finding from the observation of web recording was derived. The steps in thematic analysis involved:

i. Becoming familiar with the data

In this step, the process of transcribing and combining the collected data through the observation checklist and notes taken during the observation session was done. Then, the data was read by a researcher many times in order to understand the flow and pattern, and the initial idea was then noted. It was necessary to read the data repeatedly before starting with the coding process in order to identify the pattern of collected data. To ensure the accuracy of the pattern, the collected data was checked against the observation checklist.

ii. Generating initial codes

To generate initial ideas, notes were written manually beside the collected data and retyped in Microsoft Word for easy reference. The code was meant to identify the feature of the data and to organise them into categories. Each category of codes is given its own definition. It is important to work systematically on the collected data by giving equal attention to each data. The initial codes were gained based on the following aspect of observation which were components of suspicious behaviour among participants, attitude in browsing the Internet, behaviour practiced after attending the cybersecurity awareness program and additional elements required to make the participants aware on the importance of protecting personal data. The sample of initial codes gathered is presented as per the following

figure 4.2. This table consists of three columns, data extract is for the actual data collected, coded for is for the initial coding and definition column is meant to provide clear definition of the codes. [Y0] indicates the identification number assigned to participant.

Data Extract (Skills)	Coded for	Definition
Not clear cache not shut the screen. [Y1]	Gets thing done in rush	Youngsters tend to be forgetful and lack of focus during engaging in online activities.
Respondent immediately "click" at the email "to confirm email address. The early evaluation is required before clicking the email. [Y10]	Think before act	Individual judgement is important role in protecting personal data.
Do not close the screen. [Y10]	Gets thing done in rush	Youngsters tend to be forgetful and lack of focus during engaging in online activities.
Open gay song. [Y6]	Enthusiast feeling to discover	The discovery will among youngsters is high. They are free to browse sometimes without restriction.
He just watched YouTube by opening two songs. The song source looks genuine.[Y4]	No restriction in Internet browsing	They are free to browse sometimes without restriction.
No clear cookies. Not logout twitter just click close. Same password used within various applications. [Y9]	Gets thing done in rush The risk of password	Youngsters tend to be forgetful and lack of focus during engaging in online activities. The awareness about using password in online activities is lack.
Data Extract (Attitude)	**Coded for**	**Definition**
Too fast. Sometimes less thought were given. He used different password for different application. Less risk if someone wants to hack his personal account. [Y10]	Think before act The risk of password	Individual judgement is important role in protecting personal information. Certain youngster has awareness upon how to manage password in online activities.
Practiced security culture by having the following. Logout after used his email. Removed his email account from the stored email list inside the computer. He seems understand the concept of security while using an Internet. [Y2]	Clean cookies after browsing the Internet	Has awareness on how to clear trace after using the computer.

Fig Error! No text of specified style in document.**.2: Sample of Generated Initial Codes at the Early Stage of Data Analysis**

iii. Searching for themes

The third process involved looking at the initial codes in a bigger picture, which is also known as a theme. In order to identify the themes, line-by-line analysis of the collected data were done manually and the different codes were sorted into potential themes. The process of collating and combining different codes also occurred here which eliminates any redundancies which were found to be unrelated to the study. The line-by-line analysis was important because it allows for rich and complex narratives. The process of determining the themes was done manually. When the line-by-line analyses had been done, the notes on the texts were analysed by using highlighter pens to identify potential patterns. This is because, this kind of technique is suited for rich and complex narratives. A technique to discover themes in qualitative data is important to describe, compare, and explain about the data. The themes identified in this step were gathered and illustrated using the thematic map. The purpose of having the thematic map is to show the relationship of each theme and sub-themes. The thematic map was developed based on the list of initial codes categorised into three main themes which were behaviour outcome, undesirable behaviour and desirable behaviour together with their sub-themes. A sample of initially identified themes using the thematic map is presented as per the following figure 4.3.

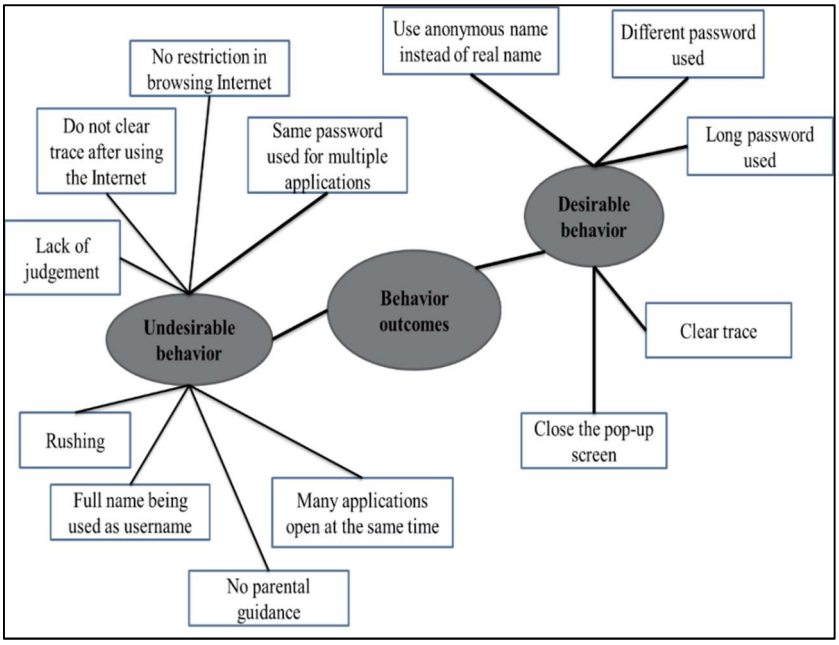

Fig Error! No text of specified style in document.**.3: Sample of Initial Identified Themes Using Thematic Map**

The list of initial codes based on behaviour outcomes were further categorised into undesirable behaviour and desirable behaviour. The undesirable behaviours that were found were; same password used for multiple applications, no restriction in browsing the Internet, do not clear trace after using the Internet, lack of judgement, rushing, full name being used as username, no parental guide and many applications open at the same time. The desirable behaviours that were found were; close the pop-up screen, clear trace after using the Internet, long password used, different password used for different applications and use anonymous name as username. These themes were further reviewed and refined many times in order to select the best themes to answer the developed research question.

iv. Reviewing themes

Step 4 involves reviewing the themes gathered as above. During this step, the initial themes were checked against its relationship to personal data protection. This was to ensure that only themes and sub-themes which were related to personal data protection remained. Based on figure 4.4, the two finalised themes were undesirable behaviour and desirable behaviour. The theme of behaviour outcome was disregarded because it was considered too general to be considered as a theme. There were also sub-themes that were removed because they were found to be irrelevant to personal data protection. Each finalised theme had its own sub-themes. For undesirable behaviour, the sub themes were; same password used for multiple applications, no restriction in browsing the Internet, do not clear trace after using the Internet and lack of judgement. For desirable behaviour, the sub-themes were clear trace after using the Internet, different and long password used, use anonymous name for username and close the pop-up screen.

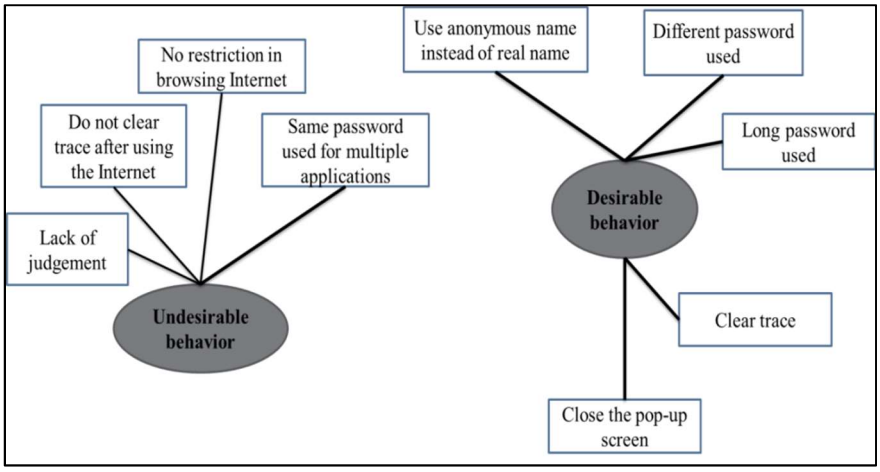

Fig Error! No text of specified style in document.**.4: Sample of Reviewed Theme**

v. Defining and naming themes

In this step, each theme and its sub-themes were gathered in one table as per figure 4.5. This table also includes real observation data as well as supporting literature to ensure the identified themes were valid to be considered as a theme. The process of reviewing the themes involved cross-checking those with data extracted during the observation of web recording. This was to ensure consistency and provide evidence to support each theme. The sample of identified themes together with its sub-themes and real observation is presented as per figure 4.5.

Themes	Sub-themes	Real observation	Related Literature Review
Undesirable behavior **Definition:** Not favorable actions	Do not clear trace after using the Internet **Definition:** The browsing history remain	Not clear cache, not shut the screen **[Y12]**	*"An advertiser can track a user's movements between Web sites because the first banner advertisement presented can set a cookie containing a unique identifier. As subsequent advertisements are read, the advertiser can construct a profile about a user based on the cookies it receives from the user"* (Sit & Fu, 2001)
	Lack of judgement **Definition:** Capability of making decision	Respondent immediately "click" at the email "to confirm email address. The early evaluation is required before clicking the email **[Y10]**	*"Substantial proportion of young Internet users may lack the good judgment"* (Beebe, Asche, Harrison & Quinlan, 2004)
	No restriction in browsing the Internet **Definition:** Free browsing of the Internet	Open gay song. **[Y6]**	*"Those aged 15 and 16 reported to surf the Internet without any restrictions being placed"* (Álvarez, Torres, Rodríguez, Padilla & Rodrigo, 2013)
	Same password used for multiple applications **Definition:** One password used for all	Same password used within various applications. **[Y9]**	*"They also used the same password and username to other social networking website accounts"* (Haron & Yusof, 2010)

Fig Error! No text of specified style in document.**.5: Sample of Themes and its Definition and Supporting Literature**

vi. Producing a report.

The final step was to produce a report of complete analysis of the data collected from the observation of web recording. Thus, this section briefly reports on the processes involved.

4.4 FINDINGS FOR PHASE 4

Findings for the data collection Phase 4 were also derived from five important steps of the thematic analysis. This section briefly discusses each step taken before the final finding from interview was derived. The steps in the thematic analysis involved:

i. Becoming familiar with the data

In this step, the process of transcribing data for each focus group interview was based on recorded audio and video. The transcribed data was repeatedly read in order to understand the flow and pattern, as well as to find initial ideas which later formed the themes. It was necessary to read the data repeatedly before it starts with finding initial coding. At this stage, it was also important to identify patterns in the collected data. To ensure the accuracy of the patterns, the collected data was checked against the audio and video recording of the interview. The transcribed data was systematically arranged based on the same questioned asked to each focus group. These were important steps before starting to generate initial ideas. A sample interview transcription is presented as per the following figure 6.6. [Y0] indicates the identification number assigned to a participant. Figure 4.6 presents the interview transcriptions arranged according to the focus groups.

115 Researcher: Do you know about the threat called identity theft or you just have heard it from the
116 session just now.
117 [Y5]: Definitely. Especially in the reality TV made in the America. Catfish TV. I'm not sure
118 about it talk about the threat identity theft they took the trick become someone else and do frank
119 to other people.
120 Researcher: Ok. How about [Y6]?
121 [Y6]: What is identity theft?
122 Researcher: is actually someone steal you identity and use it for any illegal used, so you have
123 make sure that your identity is not being available too much over the Internet. How about [Y7]?
124 [Y7]: Yes I know identity theft.
125 Researcher: and [Y8]?
126 [Y8]: I knew this because when I was started using Facebook but I plan to take it seriously when
127 I join this discourse about the danger of it.
128 Researcher: Ok. The last question for this section is having you ever attended any cyber security
129 awareness session instead of this one. So [Y5]
130 [Y5]: Oh no. This is the first one. Initially
131 Researcher: Ok next question is about problem that you've faced before you attending this cyber
132 security awareness session. Can you share with me any problem that you have faced when you
133 browsing the Internet. Start with [Y5]. Anything's that border you

Focus group 1	Focus group 2`	Focus group 3
Question 2: So how many times do you use Internet in a day? Ryan: No limitation because they think I big and able to differentiate. [Y2]: It depends actually if I'm free it like use all day and if I have homework or other stuffs there will be like 2-3 hours [Y3]: 3 hours, 4 hours [Y4]: Yes, it all depends like 1 to 3	Question 2: So how many times do you use Internet in a day? [Y5]: Erm depend on the situation, if I were giving project to do based on using the Internet and then I have to used it but then but in normal days I don't because in normal days because I don't have any social media. [Y6]: There wasn't a single day that I didn't use the Internet. [Y7]: If there is Internet connection I'll be using. [Y8]: Arr. Internet usage depend on the situation let for example if I had a competition and I need a lot of points normally it could even take one whole day. 24hrs but let say I've nothing to do I just go and check my social media to find what post they have.	Question 2: So how many times do you use Internet in a day? [Y9]: : If it is weekend maybe around 10 it depends I play games online so ya if during weekdays around 3-5 [Y10]: I periodically used the Internet rr I'm not erm I don't really use it every day but once I have a need to used it like let say I have a tough question that I couldn't answer in my homework I'll used the internet. Sometimes in a day I don't use it sometime in a day I use it. [Y12]: The same with [Y11] and [Y9] [Y11]: I also play games but during weekdays since we have school we basically at the school like since 6 till 6 so.

Fig Error! No text of specified style in document.**.6: Sample of Interview Transcriptions**

ii. Generating initial codes

In order to generate the initial codes, the interview transcription was manually printed and initial ideas were noted down and later transferred into Microsoft Word to be used for the next step. Equal attention was given to each collected data. The initial codes were gained based on the following aspect of information required which were desired behaviour on protecting personal data among participants, security culture on protecting personal data, management of behaviour in the digital world and assessment component required. The sample of initial codes gathered is presented as per figure 4.7. This table consists of three columns, data extract is for the actual data collected, coded for is for the initial coding and definition column is meant to provide clear definition of the initial code.

Data Extract	Coded for	Definition
Question 11: can you share any problem that you face while engaging to the online activities. [Y1]: Problems. I think the most obvious one is slow internet connection. Security aspect, well occasionally there will be some spam, stuff coming in like ads like you are getting 100000 so I don't really buy it. [Y2]: Sometimes when they are using your laptop or your computer it will come the advertisement that sometimes might border you right so with inappropriate stuff so [Y3]: advertisement scam [Y6]: The Internet connection. And sometimes the videos in you tube not available in your country. [Y7]: Ad and crash. The software crash. [Y8]: It is always the advertisement and the so every time I need to get a particular things that I need installing software or patch, it happen when the entire website is not secured and safe.	Self-realization about the harmful effect. Think before act. Trust Self-realization about the harmful effect Realized but wanted to try Love to trial Know how to differentiate the legitimate and illegitimate Problem: Slow internet connection Ads (mostly about ads) YouTube not available in Malaysia Software crash Waste of time Chat room/massager	List of identified problem faced by participants.

Fig Error! No text of specified style in document.**.7: Sample of Initial Codes from each Interview Question**

iii. Searching for themes

The third process involved looking at the initial codes in a bigger picture, which is known as themes. There were 4 main themes and 43 sub-themes developed initially. The main theme was desired behaviour, security culture, management of behaviour and assessment component as presented in figure 4.8. Unlike the same step in data analysis of Phase 3, the presentation of themes and its sub-themes in this analysis was in a form of a table due to a number of sub-themes which couldn't be presented in the form of a thematic map.

Main themes	Desired behavior	Security Culture	Management of behavior	Assessment component
1	Think before act	Extra precaution	Managing peer influence	Level of IT Literacy
2	Determine the level of trust	Self-realization about the harmful effect	Managing time in accessing the Internet	Personality background
3	Think about privacy	Differentiate between legitimate and illegitimate	Managing social interaction in online environment	Perception of individual
4	Not trusting outsider or stranger	Double checking strategies	Level of sharing information	Parenting guidance and level of control
5	Trust common sense	Reliability concept	Managing discovery will to try on something	
6	Belief the uncertainty in social media activities	Alternative thinker	Managing advertisement	
7	Seeking verification before proceed	Never underestimate	Managing perception	
8	Just delete the unnecessary		Understanding of process	
9	Changing the setting		Clear trace of activity	
10	Logout for every application		Early evaluation before action	
11	Password combination of more than 8 characters		No rushing	
12	Responsible for reporting unusual activities		Managing multiple website	
13	Recognition about something		Managing password	
14	Refusal		Managing inappropriate content	
15	Spontaneous decision making			
16	Clear trace after use			
17	Shut or close the pop-up screen			
18	Use anonymous name for online gaming.			

Fig Error! No text of specified style in document.**.8: List of Initial Themes and its Sub-themes**

iv.Reviewing themes

Step 4 involved reviewing the themes gathered from the previous step. In this step, the initial themes were checked against its relationship to personal data protection. This was to ensure that only themes and sub-themes which were related to personal data protection remained. The themes and sub-themes were also checked against redundancy, and then rearranged and renamed accordingly. The outcome from this step was the list of final themes and its sub-themes as per figure 4.9 below.

Themes	Sub themes	Real interview scripts	List of participants ID	Related Literature Review
Desired behavior **Definition:** Good behavior which result in positive outcome.	**Password – Creation of password must be long and having combination of characters. (derived from quantitative study & observation)** - **Definition:** A combination of characters to be used for verification online application. **Thinking – Belief the uncertainty, think before act, refusal** **Definition:** The act of producing thought about something. **Trust – Common sense, Do not trust outsider and strangers, privacy** **Definition:** Degree of reliance about something.	"The thing is we need to meet them outside and they give their Facebook then only we can accept" "First of all I won't open the email. Because I won't recognized them" "He is opening multiple web pages inclusive of YouTube, Facebook, and Twitter and online shopping at the same time. He forgot to logout his twitter. Opening multiple web page make you forget to logout especially when you are rushing" "I'll only accept the one that I know	Y3, Y4, Y6, Y9, Y12	*"Prior work has shown that password-composition policies requiring more characters or more character classes can improve resistance to automated guessing attacks, many passwords that meet common policies remain vulnerable"* (Ur et al. 2013) *"System administrators typically require that users select passwords according to a password-composition policy designed to make users' passwords harder to predict. Such a policy may require, for example, that passwords exceed a minimum length, that they contain uppercase letters and symbols, and that they do not contain dictionary words"* (Komanduri et al. 2011) *"It feels heartless to think that way when you know some of the nice sorts of techies who thrive in our computation centric times. But we have to do our best at thinking dark thoughts if we are to have any forethought about technology at all"* (Lanier, 2013) *"An individual (trustor) will therefore concentrate on a limited set of information cues – including trust signals from the technology service (trustee) – which are important or relevant to them, to ascertain the ability and motivation (or willingness) of the trustee to safeguard their personal information"* (Morton, 2014

Fig **Error! No text of specified style in document.**.9: Sample of Defining Themes

v.Defining and naming themes

In this step, the finalised themes were derived based on the initial themes that have been reduced. For each theme and sub-themes, its definition, real quotation from interview script, participants' ID and related literature were given. This is to provide consistency and evidence in order to ensure validity of the theme selection. The finalised themes were, firstly, desired behaviour and its sub-themes include password, thinking, trust, information security actions and responsibility. The second theme was security culture and its sub-themes include never underestimate, self-realisation of harmful effect, differentiate between legitimate and illegitimate, and reliability. The next identified theme was program content and its sub-themes include management of discovery will, social interaction, information sharing, management of password and understanding processes involved in online activities. The final main theme derived was assessment component and it sub-themes include Internet literacy.

vi. Producing a report.

The final step was to produce a report of complete analysis of the data collected for the interview. This section briefly reports the processes involved.

5.0 DISCUSSION

The identification of enhancements is meant to improve the current module of the cybersecurity awareness program used to convey a message on personal data protection among youngsters. The proposed enhancement components were made based on the understanding derived from the research findings. In previous assessments, personal data protection was not given a focus, as most assessments of cybersecurity awareness programs were concerned with understanding security in general without specifically emphasizing on personal data protection as with the assessment conducted by [10],[18],[40]. By focusing on personal data protection during the assessment, this study found evidences on components of personal data protection that require attention from stakeholders such as CSM, parents, management of schools and responsible institutions for conducting cybersecurity awareness among youngsters. The proposal for enhancement components with regard to personal data protection was motivated by present concerns over protecting personal data as highlighted in [25], [60]. A lack in personal data protection was found to be among the cause of other cyber threat problems among youngsters. By empirically investigating the current state of the cybersecurity awareness program through the assessment conducted to measure youngsters' reaction, learning, behavior and result, this study proposed enhancement to the current cybersecurity awareness module which specifically focused on personal data protection. Throughout the analysis, by comparing result in each phases of data collection the following emerged components derived. Each emerged component was discussed one by one together with its supporting literature and justification.

5.1 Decision making process in using personal data

The requirement to educate youngsters on the decision making process in the cybersecurity awareness program is deemed necessary to minimize the risk of their personal data being available to third parties. The proposal to educate youngsters on the decision making process in using personal data is aligned to various studies that are concerned on the capacity of youngsters or adolescents in making matured decision. [6], [33], [55] specifically suggested that youngsters require guidance in their Internet usage as they were found to be lacking in self-regulation. This proposed enhancement was consistent with findings recorded during the focus group interview session which revealed that youngsters lacked judgement especially in differentiating between legitimate and illegitimate applications available over the web. Initial judgement and individual evaluation is important to be stressed on during the cybersecurity awareness program because it helps to increase the cognitive process among youngsters to think twice and realize the negative consequences of their decision. This statement is supported by [38] who mentioned that youngsters are in the process of building their cognitive ability which requires continuous guidance in order to increase their degree of maturity. However, the current cybersecurity awareness program module does not include decision making as part of the cybersecurity awareness content. This proposed enhancement component was acknowledged by CSM as it could add value to their current module used to convey the message on personal data protection among youngsters in Malaysia. Practically, by adding decision making process as part of the cybersecurity awareness message, youngsters could have insights on how better decisions could be made on filtration and sharing of their personal data in digital world.

5.2 Management of online application

Based on the survey conducted in this study, youngsters were found to actively use the Internet for social media, email, watching online videos and also for downloading songs, drama, films or software. The confirmation of various Internet applications used among youngsters is supported based on the findings from the focus group interview. It was found that the majority of youngsters who participated in this study had at least one online social media account. In accordance to [3], [4], [53] social media has given tremendous impact to personal data protection as it involved extensive use of personal data. Additionally, [34] mentioned that youngsters often left their digital footprint available over the web. Furthermore, [36] added that the usage of smartphone devices gave youngsters an easy platform to access their online social media account. Even though the findings in this study confirm youngsters as skillful and advanced Internet users, they need to be educated on the aspect of managing their online applications. This is because as mentioned by [27], online social media provide an unsafe environment as personal data were made to be online and available publicly. This could encourage cyber criminals to get details of youngsters' social media accounts and use it to hack other online applications used by the same youngsters. The proposal of enhancement components on the management of online activities is supported by [12] who claimed that youngsters shall be made to know how to manage their online applications and determine the authenticity of applications that they used in order to minimize their personal data from being stolen. Therefore, this study suggests the current cybersecurity awareness module to include awareness on how to manage online applications used by the youngsters. For instance, education on which type of personal data could be revealed and how it is prompted by the online application.

5.3 Management of online contents

The next enhancement component proposed is to include management of online content among youngsters. Based on the understanding observed through conducting the observation of web recording, youngsters were found to have freedom while browsing the Internet. Similarly, the finding from the interview showed that there were youngsters who claimed that they could freely browse Internet without supervision by their parents. Online content could sometimes be tricky and require judgement from the youngsters on which content is applicable to them as the Internet contains inappropriate content and advertisements which sometimes prompt them to provide their personal data [15], [43]. Because of the availability of free content, youngsters often browse without thinking that the content could lead to harmful effects on their personal data. Due to this reason, this study proposes to include management of online content in order to assist youngsters to differentiate between appropriate and inappropriate content. This suggestion is aligned with who performed longitudinal study on the nature of internet usage and parental supervision among young children and stressed the importance to educate young Internet users on Internet content.

5.4 Management of password and username

The importance of protecting passwords and usernames from being stolen and used by third parties should be made clear to the youngsters. This includes characteristics of a good password, where a combination of characters, symbols and numbers produce good passwords, and sharing policy of passwords [26]. It could be observed from the findings that there were youngsters who used simple passwords and admitted sharing passwords among their friends and family. In addition, there were also youngsters who chose to paste their passwords at places that could be easily remembered. All these actions were found to pose risk to their personal data. Therefore, it is proposed to include knowledge on how to protect their password as well as to avoid using their full name as for the username. This suggestion is consistent with [35], [52], [60] who highlighted the need for education on password management among youngsters as a way to protect their personal data from being unintentionally revealed to strangers. For that reason, this study reinforces the need to include management of passwords and usernames as part of the cybersecurity awareness program.

5.5 Comparisons of propose content on personal data protection among other countries

The emerged components as enhancement proposed to the current module of cybersecurity awareness program were further compared with the other cybersecurity contents from other countries. In this comparison, the contents from Singapore and Australia were used. The comparison is to provide conclusive result rather than an indicative result as derived from the data analysis. In Singapore the responsible organization to provide cybersecurity awareness program to their public citizens is Cyber Security Agency of Singapore. They are conducting online and series of awareness among youth particularly on risk of online applications. This content is found to be aligned with our emerged components to include management of online content and applications in conducting cybersecurity

awareness program. Their awareness include advices to only use latest technology, reliable and reputable content of the applications [13]. Beside they also give awareness to ensure username and password created which can't easily be guessed. In Australia, the responsible organization to govern cybersecurity is an Australian Cyber Security Center. Particularly for youth they do provide awareness on identity theft and preventing exposure to inappropriate online content [9]. This is because the risk of identity theft and inappropriate online content could bring harmful effect to the youngsters. In relation to our propose content, the management of password and username is found to be important to avoid identity theft cases. Thus, we can say that the proposed enhancement content of cybersecurity awareness program is accordance with the developed countries such as Singapore and Australia in governing their digital world.

6.0 CONCLUSION

The main focus of this study was to perform an assessment on youngsters by getting their feedback after attending a cybersecurity awareness program. The feedback recorded their reaction, learning outcomes, behaviour and results particularly on personal data protection. The study was carried out due to the fact that previously assessments were lacking in performing a systematic assessment, having little focus on youngsters and little emphasis on personal data protection. This study started with the development of the conceptual framework which guided the construction of instruments and selection of sample. The real field work then took place by systematically conducting a survey session, pre-test and post-test surveys, focus interview and observation of web recording session. It was done in sequence and data was collected and recorded. It was followed by a data analysis step for each type of data. The finding was built upon the results gained from quantitative and qualitative data analysis. Through the steps, some conclusions were drawn. The topic addressed in this study is novel as it sought to perform systematic assessment on a cybersecurity awareness program particularly on youngsters. Multiple components of assessments offered a complete view and alternative findings on the effectiveness level of the current cybersecurity awareness module on personal data protection. This study also offered a novel way in assessing cybersecurity awareness programs by proposing an assessment framework that can be used and replicated to assess other cybersecurity awareness programs. By identifying enhancement components on personal data protection to the current module of the cybersecurity awareness program, this study offered another novelty as this enhancement can be a valuable input for better modules. In conclusion, the cybersecurity awareness program involving youngsters needs to be continuously assessed and updated with new information as Internet technology evolves fast and offers new security risks.

ACKNOWLEDGEMENT

This project was funded by the Ministry of Higher Education and International Islamic University of Malaysia

REFERENCES

[1] Abawajy, J., "User preference of cyber security awareness delivery methods". *Behaviour & Information Technology*, Vol. 33 No. 3, 2014, 237–248. https://doi.org/10.1080/0144929X.2012.708787

[2] Abawajy, J., Thatcher, K., & Kim, T."Investigation of stakeholders commitment to information security awareness programs", in *2008 International Conference on Information Security and Assurance (isa 2008)* 2008, pp. 472–476. https://doi.org/10.1109/ISA.2008.25

[3] Acquisti, A., Brandimarte, L., & Loewenstein, G.,"Privacy and human behavior in the age of information". *Science*, Vol. 347 No.(6221), 2015, 509–514. https://doi.org/10.1126/science.aaa1465

[4] Ahmad, R., & Bakar, Z. A., "Information systems skills requirements in Malaysia". *Malaysian Journal of Computer Science*, Vol. 13 No.2, 2000, 64–69.

[5] Aimeur, E., & Schonfeld, D., "The ultimate invasion of privacy: Identity theft", in *2011 Ninth Annual International Conference on Privacy, Security and Trust,* IEEE 2008, pp. 24–31. https://doi.org/10.1109/PST.2011.5971959

[6] Albert, D., Chein, J., & Steinberg, L., "The teenage brain peer influences on adolescent decision making". *Current Directions in Psychological Science*, Vol. 22 No.(2), 2013, 114–120. https://doi.org/10.1177/0963721412471347

[7] Al-Hamdani, W. A., "Assessment of need and method of delivery for information security awareness program", in *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development - InfoSecCD '06*, 2006, p.102. https://doi.org/10.1145/1231047.1231069

[8] Atkinson, S., Furnell, S., & Phippen, A., "Securing the next generation: enhancing e-safety awareness among young people". *Computer Fraud & Security*, Vol. July, 2009, pp.13–19. https://doi.org/10.1016/S1361-3723(09)70088-0

[9] Australian Cybercrime Online Reporting Network. Australian Cyber Security Center. Retrieved April 3, 2017, from https://www.acorn.gov.au/

[10] Baek, Y. M., Kim, E. M., & Bae, Y., "My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns". *Computers in Human Behavior*, Vol .31, 2014, pp.48–56. https://doi.org/10.1016/j.chb.2013.10.010

[11] Christodoulaki, M., & Fragopoulou, P., "SafeLine: reporting illegal internet content". *Information Management & Computer Security*, Vol 18 No 1, 2010, pp. 54–65. https://doi.org/10.1108/09685221011035269

[12] Correa, T., Straubhaar, J. D., Chen, W., & Spence, J., "Brokering new technologies: The role of children in their parents' usage of the internet". *New Media & Society*, Vol 1461444813,2013. https://doi.org/1461444813506975.

[13] Cyber Security Awareness Alliance. Cyber Security Agency of Singapore. Retrieved April 3, 2017, from https://www.csa.gov.sg/gosafeonline/go-safe-for-me/for-students

[14] Da Veiga, A., "An information security training and awareness approach (ISTAAP) to instil an information security-positive culture", in *Proceedings of the ninth international symposium on human aspects of information security and assurance (HAISA 20150,* 2015.

[15] De Moor, S., Dock, M., Gallez, S., Lenaerts, S., Scholler, C., & Vleugels, C. Teens and ICT: Risks and opportunities, 2008. Retrieved November, 6, 2016.

[16] Farooq, A., Isoaho, J., Virtanen, S., & Isoaho, J., "Information Security Awareness in Educational Institution: An Analysis of Students' Individual Factors", in *2015 IEEE Trustcom/BigDataSE/ISPA.* IEEE, 2015, pp. 352–359. https://doi.org/10.1109/Trustcom.2015.394

[17] Fornell, C., & Bookstein, F., "Two structural equation models: LISREL and PLS applied to consumer exit-voice theory". *Journal of Marketing Research*, Vol.19 No.4, 1982, pp. 440–452. https://doi.org/10.1177/002224378201900406

[18] Furman, S., Theofanos, M. F., Choong, Y. Y., & Stanton, B.,"Basing cybersecurity training on user perceptions". *IEEE Security and Privacy*, Vol. 10 No.2, 2012, pp. 40–49. https://doi.org/10.1109/MSP.2011.180

[19] Furnell, S., " Jumping security hurdles". *Computer Fraud & Security*, Vol. 2010 No.6, 2010, pp. 10–14. https://doi.org/10.1016/S1361-3723(10)70067-1

[20] Furnell, S. M., Bryant, P., & Phippen, A., "Assessing the security perceptions of personal Internet users". *Computers & Security*, Vol.26 No.5, 2007, pp. 410–417. https://doi.org/10.1016/j.cose.2007.03.001

[21] Furnell, S., Tsaganidi, V., & Phippen, A.,"Security beliefs and barriers for novice Internet users". *Computers & Security*, Vol. 27 No.7–8, 2008, pp. 235–240. https://doi.org/10.1016/j.cose.2008.01.001

[22] Gross, J. B., & Rosson, M. B. (2007).,"Looking for trouble", in *Proceedings of the 2007 symposium on Computer human interaction for the management of information technology - CHIMIT '07* (p. 10). New York, New York, USA: ACM Press, 2007. https://doi.org/10.1145/1234772.1234786

[23] Henseler, J., Ringle, C., & Sarstedt, M.,"A new criterion for assessing discrimant validity in varience-based structural equation modeling". *Journal of the Academy Marketing Science*, Vol.43 No.1, 2014, pp.115-135. https://doi.org/10.1007/s11747-014-0403-8

[24] Ho, R, *Second Edition: Handbook of Univariate and Multivariate Data Analysis eith IBM SPSS*. CRC Press, 2014. https://doi.org/10.1201/b15605

[25] Hong, W., & Thong, J. Y.,"Internet privacy concerns: an integrated conceptualization and four empirical studies". *MIS Quaterly*, Vol.37 No.1, 2013, pp.275–298. https://doi.org/10.25300/MISQ/2013/37.1.12

[26] Humaidi, N., & Balakrishnan, V.,"The moderating effect of working experience on health information system security policies compliance behaviour". *Malaysian Journal of Computer Science*, Vol.28 No.2 2015.

[27] Joe, M. M., & Ramakrishnan, D. B.,"A survey of various security issues in online social networks". *International Journal of Computer Networks and Applications*, Vol. 1 No.1, 2014, pp.11–14.

[28] Johansson, A., & Götestam, K. G.,"Internet addiction: characteristics of a questionnaire and prevalence in Norwegian youth (12-18 years)". *Scandinavian Journal of Psychology*, Vol. 45 No.3, 2004, pp. 223–229. https://doi.org/10.1111/j.1467-9450.2004.00398.x

[29] Johnson, E. C.,"Security awareness : Switch to a better programme". *Network Security*, Vol. February,2006, pp. 15–18. https://doi.org/10.1016/S1353-4858(06)70337-3

[30] Kirkpatrick, D, *Evaluating training programs: four levels*. San Francisco: Berrett-Koehler, 1994.

[31] Kok, E. T., Ng, M. L. Y., & Kim, G. S.,"Online activities and writing practices of urban Malaysian adolescents". *System*, Vol. 38 No.4,2010, pp. 548–559. https://doi.org/10.1016/j.system.2010.09.014

[32] Kruger, H., & Kearney, W. D.," A prototype for assessing information security awareness. *Computers & Security*, Vol.25 No.4, 2006, pp.289–296. https://doi.org/10.1016/j.cose.2006.02.008

[33] LaRose, R., Lin, C. A., & Eastin, M. S., "Unregulated Internet usage: Addiction, habit, or deficient self-regulation?". *Media Psychology*, Vol. 5 No. 3, 2003, pp. 225–253. https://doi.org/10.1207/S1532785XMEP0503_01

[34] Lenhart, A, *Teens, smartphones & texting*. Pew Internet & American Life Project, 2012, pp.1-34.

[35] Lenhart, A., Madden, M., Smith, A., Purcell, K., Zickhur, K., & Rainie, L.,*Teens, kindness and cruelty on social network sites*. Pew Internet and American Life Project, 2011, p.28.

[36] Lenhart, A., Purcell, K., Smith, A., & Zickhur, K, *Social media and mobile internet use among teens and youngs adults*. Pew Internet and American Life Project, 2010.

[37] Lewis, M.,"Iterative tringulation: A theory development process using existing case studies". *Journal of Operation Managements*, Vol.16 No.4, 1998, pp.455–469. https://doi.org/10.1016/S02726963(98)00024-2

[38] Livingstone, S., Bober, M., & Helsper, E, *Internet literacy among children and young people : findings from the UK children go online project Internet literacy among children and young people*. Findings from the UK Children Go Online Project, 2005.

[39] Madden, M., Lenhart, A., Duggan, M., Cortesi, S., & Grasser, U,. *Teen and technology 2013*. Washington, DC: Pew Internet & American Life Project.,2013.

[40] Mani, D., Choo, R., & Mubarak, S.,"Information security in the South Australian real estate industry: A study of 40 real estate organisations". *Information Management & Computer Security*, Vol.22 No.1, 2014, pp.24–41. https://doi.org/10.1108/IMCS-10-2012-0060

[41] Micheli, M., "What is new in the digital divide? Understanding internet use by teenagers from different social

backgrounds", in Communication and Information Technologies Annual. Emerald Group Publishing Limited, 2015 pp. 55-87. https://doi.org/10.1108/S2050-206020150000010003

[42] Ng, B.-Y., Kankanhalli, A., & Xu, Y. (Calvin).,"Studying users' computer security behavior: A health belief perspective". *Decision Support Systems*, Vol.46 No.4, 2009, pp.815–825. https://doi.org/10.1016/j.dss.2008.11.010

[43] O'Keeffe, G. S., Clarke-Pearson, K., & Council on Communications and Media.,"The impact of social media on children, adolescents, and families. *Pediatrics*, Vol. 127 No.4, 2011, pp. 800–804. https://doi.org/10.1542/peds.2011-0054

[44] Oblinger, D., & Oblinger, J.," Is it age or IT: First steps toward understanding the net generation". *Educating the Net Generation*, Vol. 2 No.1–2, 2005, p. 20.

[45] Ramli, N. S., Hassan, M., Osman, M. N., Shaffril, M., & Azril, H.,"Qualitative findings on youths views on the internet and mobile phone: the case of university students in Malaysia". *The Social Sciences*, Vol.9 No.3,2014, pp. 239–243.

[46] Rossi, P. H., Lipsey, M. W., & Freeman, H. E, *Evaluation: A systematic approach*. USA: Sage Publications Inc, 2004.

[47] Royse, D., Thyer, B. A., Padgett, D. K., & Logan, T. K, *Program evaluation an introduction*. Cengage Learning, 2001.

[48] Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J.,"The impact of information richness on information security awareness training effectiveness". *Computers & Education*, Vol. 52 No.1, 2009, pp.92–100. https://doi.org/10.1016/j.compedu.2008.06.011

[49] Sieber, S., & Sabatie, J. V.,"Uses and attitudes of young people toward technology and mobile telephony", in *16th Bled eCommerce Conference eTransformation 2003,* pp. 773–787. Bled, Slovenia.

[50] Siponen, M. T., "A conceptual foundation for organizational information security awareness". *Information Management & Computer Security*, Vol.8 No.(Table I), 2000 31–41. https://doi.org/10.1108/09685220010371394

[51] Sithira, V., & Nguwi, Y., "A study on the adolescent online security issues". *International Journal of Multidisciplinary and Current Research*, Vol.2 No. June, 2014, pp.596–601.

[52] Smahel, D., Helsper, E., Green, L., Kalmus, V., Blinka, L., & Ólafsson, K.,"Excessive internet use among European children". *Research and policy challenges in comparative perspective*, 2012, pp. 191-204. https://doi.org/10.1332/policypress/9781847428837.003.0015

[53] Spiekermann, S., Acquisti, A., Böhme, R., & Hui, K. L.,"The challenges of personal data markets and privacy". *Electronic Markets*, Vol. 25 No.2, 2015, pp.161–167. https://doi.org/10.1007/s12525-015-0191-0

[54] Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J.,"Analysis of end user security behaviors". *Computers & Security*, Vol.24 No.2, 2005, pp. 124–133. https://doi.org/10.1016/j.cose.2004.07.001

[55] Steinberg, L., & Cauffman, E.,"Maturity of judgment in adolescence: Psychosocial factors in adolescent decision making". *Law and Human Behavior*, Vol. *20 No.* 3, 1996, p. 249. https://doi.org/10.1007/BF01499023

[56] Talib, S., Clarke, N. L., & Furnell, S. M., "An analysis of information security awareness within home and work environments", in *2010 International Conference on Availability, Reliability and Security.* 2010, pp. 196–203). Ieee. https://doi.org/10.1109/ARES.2010.27

[57] Valcke, M., De Wever, B., Van Keer, H., & Schellens, T., " Long-term study of safe Internet use of young children". *Computers & Education*, Vol.57 No.1, 2011, pp. 1292–1305. https://doi.org/10.1016/j.compedu.2011.01.010

[58] Vandoninck, S., D'Haenens, L., & Smahel, D. *Preventive measures – how youngsters avoid online risks*. 2014. Retrieved April 3, 2016, from www.eukidsonline.net

[59] Yarbrough, D. B., Shulha, L. M., Hopson, R. K., & Caruthers, F. A, *The program evaluation standards: A guide for evalators and evaluation users*. California: Sage Publications, Inc. 2011.

[60] Young, A. L., & Quan-Haase, A., "Privacy protection strategies on Facebook: The Internet privacy paradox revisited". *Information, Communication & Society*, Vol. 16 No.4, 2013, pp.479–500. https://doi.org/10.1080/1369118X.2013.777757