

CHAPTER IV

FINDING AND RESULTS

4.1: Introduction

This chapter discusses the analysis of the data produced from the quantitative part of this study with the use of questionnaire. The results were based on the collection of pre and post questionnaire obtained from the participants. Also, the evaluation of the training materials took place in the post questionnaire. The strategy of this study is as drawn in the figure 3.



Figure: 3 Research Planned Strategy

The reported findings are categorized into four main sections; that are:

- 1- Demographic information and general information security questions
- 2- Security awareness
- 3- Security practices
- 4- Personal opinion

Section five was designed especially to evaluate the training materials based on secondary school students' perspective in the post questionnaire.

4.2: Information Security Awareness (ISA) “Training Tools”

The aim of this section is to provide an overview of the available security awareness training tools. The source of these tools is cyber portals and CERTs of South-East Asia.

4.2.1: Method

The Internet security or commonly known as “Cyber-security”, makes an important aspect in how the governments could educate end-users about the security issues. Following this, South-East Asia countries provide a cyber security portal to innovate a new way in creating awareness towards the risks that they will face while using the Internet. Some of the South-East Asia countries did not provide any cyber portal to date, but as far as the study conducted, there was a review in case any new cyber portal created. Table 5 lists availability of cyber-security portals in South East Asia.

Table: 5 Available -Non Available Cyber Security Portals

Country	Available cyber Security portal	Non-available cyber Security portal
Brunei	√	-
East Timor	-	√
Cambodia	√	-
Indonesia	-	√
Laos	-	-
Malaysia	√	-
Myanmar	-	-
Philippines	-	-
Singapore	-	-
Thailand	-	√
Vietnam	-	√

From table 5, it is clear that only Malaysia, Singapore, Cambodia, and Brunei have setup a security cyber portal. For more results to find out a new way to evaluate the security awareness tools for South-East Asia countries, another searching for the websites that provide security awareness training tools is done on the CERTs website for each country.

The CERT is The Internet official emergency team, which stands for (computer emergency readiness team) which was formed by the Defence Advanced Research

Projects Agency (DARPA) in November 1988 after the Internet was assaulted in the Internet worm incident. Today, CERT focuses on security breach and denial of service incidents, providing alerts, incident-handling, and avoidance guidelines. CERT also conducts an ongoing public awareness campaign and engages in research aimed at improving security system. (Rouse, 2011)

As listed in table 6, it can be reported that few countries of South-East Asia did not provide a security awareness tool for the public.

Table: 6 Available CERTs and Security Program

Country	Available CERT	No-Security Awareness program for Public
Philippine (PH-CERT)	√	√
Thailand (TH-CERT)	√	
Indonesia (ID-CERT)	√	√
Cambodia (COM-CERT)	√	√
Taiwan (TW-CERT)	√	√
Vietnam (VN-CERT)	√	√
Laos (LAO-CERT)	√	√
Myanmar (MM-CERT)	√	√
Brunei (BRU-CERT)	√	√
East-Timor	*	*
Singapore (SING-CERT)	√	-
Malaysia (MY-CERT)	√	√

4.2.2: Review and Results

From the section 4.2.1, we can state that countries who own a security portal for the users, they do provide awareness training tools, tips for cyber security, news, as well as contact information; in the case of any emergencies in the future, such as spam attack. The available security awareness training tools that are usable and in these websites are presented in table 7.

Table: 7 Security Awareness Tools

Cyber portal	Video	Poster	Game	Newsletters
Malaysia (Cyber-safe)	√	√	√	√
Singapore (Go safe online)	√	√	√	√
Singapore (Cyber-wellness)	-	-	-	√
Brunei (Secure verify connect)	√	-	-	-
Cambodia (Secudemy)	√	√	-	-

Website such as (Go safe online) contains video and games that are available, but more likely for the use of organizational level. Moreover, the video game is limited to the citizen students as you have to enter your citizen school to start playing the game.

Another problem associated with the website with (Cyber-wellness), as the news latter cannot be found when you search for any articles in any years. Brunei cyber security (Secure Verify Connect) contains cyber security awareness for the public, some problem on this website related to the video available on social networks was in the citizen language, games also cannot be played as they open only as an interface in some cases or not available.

4.2.3: Discussion

After this searching on the security awareness tools on the South-East Asia was completed, an actual employing to these materials that summarized from theses portals took place. The posters, videos, and games that were designed for this age based on “cyber safe and cyber wellness” were conducted in a real security training program for secondary school students.

4.3: Pre-Questionnaire Results

The first step in this study is submitting the pre-questionnaire to students. This action was to collect more details about the current information security awareness among students. The next subsections discussed in details students’ feedback on the presented issues of this study in the given questionnaire.

4.3.1: Demographic and General Security Information

Based on the results of the participants as shown in figure 4, it was found that the majority of 68% (34 of the respondent were female), with 32% (16 male).

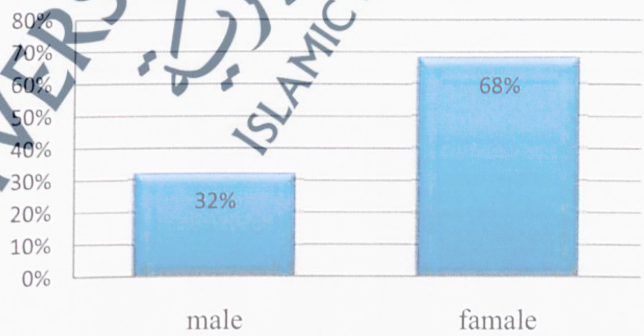


Figure: 4 Gender Frequency of the Respondents (x= gender, y= percentage)

The age of students varied as the sample was chosen randomly, as in figure 5, 16% (8 respondents) were at the age of thirteen, 18% (9 respondents) were at the age of fourteen, 18% (9 respondents) in the age of fifteen, 18% (9 respondents) in the age of sixteen, 18% (9 respondents) in the age seventeen, and finally, 12% (6 respondents) were at the age of eighteen.

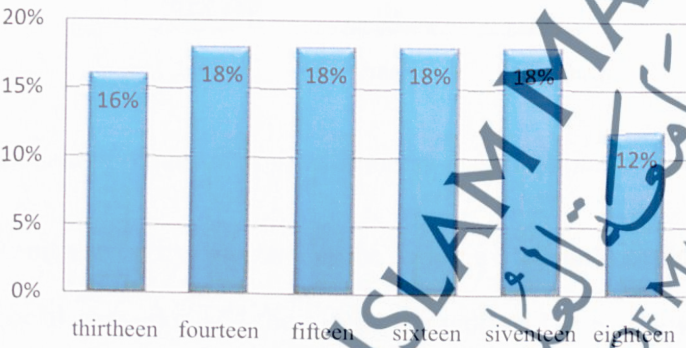


Figure: 5 Respondents Age Categories (x= age, y= percentage)

The students' education level is presented in figure 6. The majority of them are 16% (8 respondents) are at seven grade, 16% (8 respondents) at eight grade, 16% (8 respondents) at ninth grade, 18% (9 respondents) at ten grade, 18% (9 respondents) at eleventh grade, and 16% (8 respondents) at twelve grade.

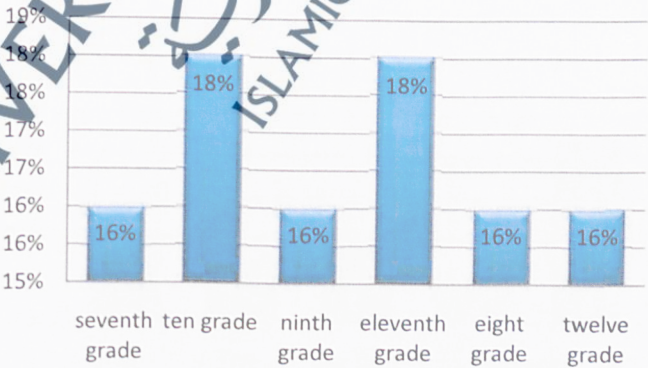


Figure: 8 Students' Educational Level (x= grade, y= percentage)

Figure 7 draws the sample nationality as 90% (45 respondents) Libyan, 6% (3 respondents) were Iraqi, while 4% (2 respondents) were Palestinian see section 3.3.3.

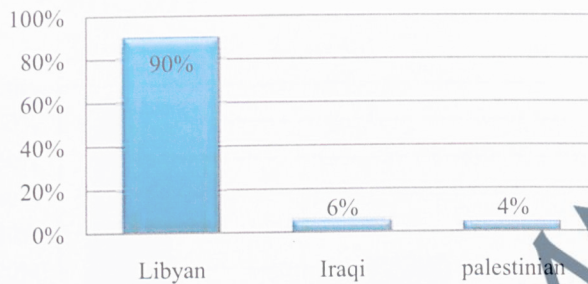


Figure: 7 Nationality Frequency of the Respondents (x= nationality, y= percentage)

In the part of general security information the author asked students about when they started using social networks, and the results are indicated as shown in figure 8. From figure 8, 18% stated that they start visiting it since one year, 14% five months, 16% two months, 8% two years, and 44% more than two years. For further information we asked students about how many social networks they have, there were 48% (or 24 respondents) have four social networks, 18% (9 respondents) have one only, 12% (six respondents) have three social networks, and 22% (11 respondents) have two. This can lead us to further information about the security practices by the students.



Figure: 8 Social Networks Usages (x= start using social networks, y= percentage)

The influence of the students’ friends can be seen when 66% of them hear about social networks through their friends, 2% by classmates, 22%by siblings, and 8% through media as drawn in figure and frequency in table8.

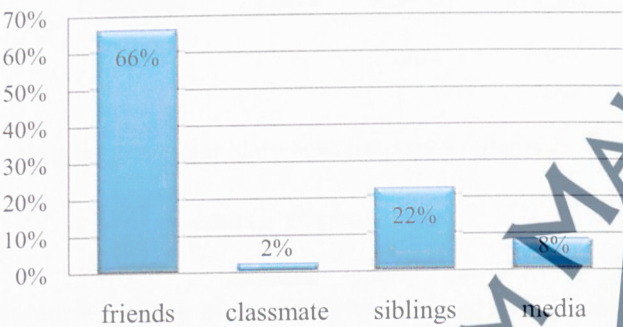


Figure: 9 Source of Knowledge about Social Networks indicated by Students
(x= source, y= percentage)

Table: 8 Frequency by Source of Knowledge about Social Networks

	Frequency	Percent
Friends	33	66%
Classmates	2	4%
Siblings	11	22%
Media	4	8%

Another concern where based on how many social networks students have, in order to stand on the range of risk regarding their multi accounts. The finding listed in figure 10 and the frequency in table 9, reported that 18% (9 respondents) has only one, 22% (11 of the respondents have two), 12% (6 of respondents) have three, and 48% (24 of respondents) have four social networks.

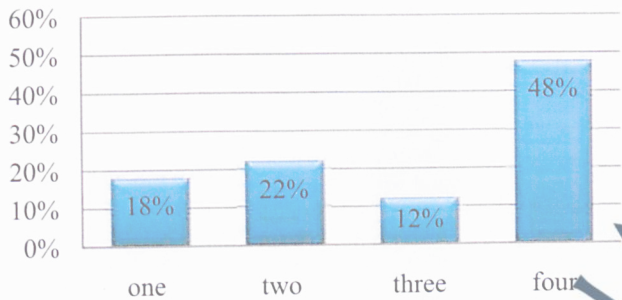


Figure: 10 The Number of Social Networks used by Students (x= number of used accounts, y= percentage)

Table: 9 Number of Social Networks used by Students

	Frequency	Percent %
One	9	18%
Two	11	22%
Three	6	12%
Four	24	48%

In the aspect of asking secondary school students about kinds of passwords they are using as in figure 11 and table 10, they indicated that 82% (41 of respondents) used their date of birth as a password, 14% (7 respondents) used three letters, 2% (1 respondents) used part of song password, 2% (1 respondents) used blank password. This can be suggested as that students do not consider the real dangers of using this kind of passwords as it is easy to attacker to break same passwords.

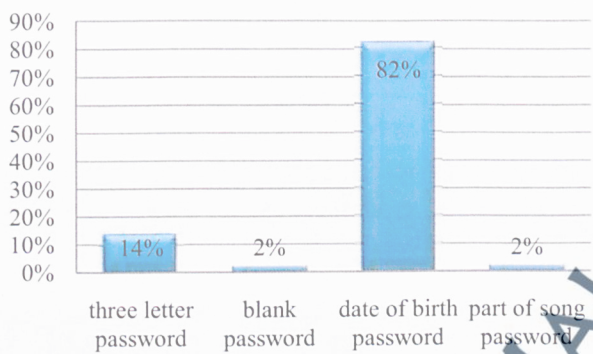


Figure: 11 Passwords Habits of Students (x= kind of password, y= percentage)

Another risk discovered in the way they are changing their passwords as presented in figure 12 and the frequency composition in the table 10. Students' risky behaviour can be seen as shown in the percentage of 52% (26 respondents) did not change their passwords as this can be combined with the risk of using their date of birth as a password to show clearly the high level of risk presented by students. Followed by 18% (9 respondents) change it once a year, while 24% (12 respondents) indicated that they changed it once a month, and 6% (3 respondents) change their passwords twice a year.



Figure: 12 Changing Passwords by Students (x= times of changing passwords,

y= percentage)

Table: 10 General Security Information

Frequency & Valid percent							
What kind of passwords did you use?							
A blank password		Three letters		Date of birth		Part of song	
1	2%	7	14%	41	82%	1	2%
How many times did you change your passwords?							
I did not change my passwords		Once a month		Once a year		Twice a year	
26	52%	12	24%	9	18%	3	6%

Cyberbullying is a new form of misuse of technology. Based on this we take part of each section on this questionnaire to assess students awareness and practices with this phenomena. Figure 13 reflects students’ performance on cyberbullying and table 11 presents the frequency The majority of 46% (23 respondent) have been bullied by emails, 38% (19 of respondents) by text messages, 2% (1 respondent) by phone call, and 10% (5 respondents) by using chatting rooms. This can clearly show that bullying by using emails was the most popular among students.

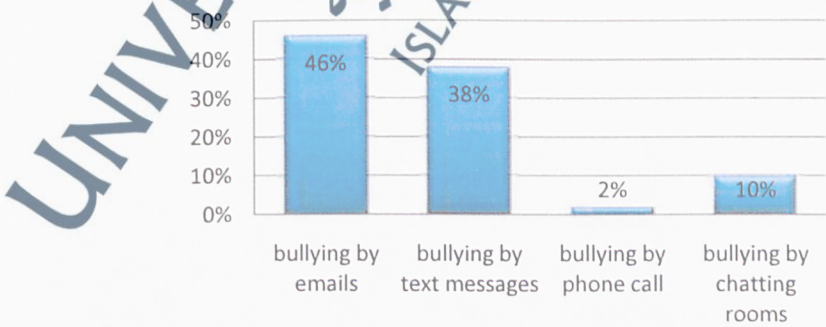


Figure: 13 Technology used to Bully Students (x= kind of bullying, y= percentage)

Table: 11 CyberBullying Forms between Students

Method of Bullying	Frequency	Percent %
Bullying by using emails	23	46%
Bullying by using text messages	19	38%
Bullying by using phone call	1	2%
Bullying by using chatting rooms	5	10%

For further information about the effects resulted from bullying we asked the students about their emotions when they were put in a position as a victim of cyberbullying. Figure 14 presents the percentage and composition in the table 12. The majority of 40% (or 20 respondents) clearly answered that they feel angry and this can be considered as a dangerous effect of bullying with the concern of the danger that can be caused from similar situations.16% (8 respondents) felt sad, 34% (17 respondents) indicated that they feel it is hard to trust others, and 6% (3 respondents) answered that do not want to go to school as a result of being bullied. This result clearly states, what have presented in the Farvadi's, (2011) report, as he stated that cyberbullying has a high damage on students' emotions.



Figure: 14 Effect Caused by the Cyberbullying Utilities (x= kind of effect, y= percentage)

The interaction of students who are being bullied by others can be described as in figure 15 and the composition of the table 12. The high risk presented in the percentage of 36% (18 respondents) bully the bullier, 30% (15 respondents) they simply pretend to ignore it, 18% (9 respondents) have good reaction as they chose to “talk to others about it”, and only 12% (6 respondents) indicated that they delete all the bullier messages.

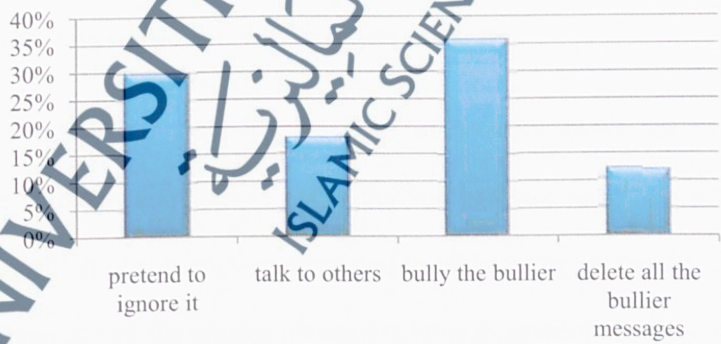


Figure: 15 Actions Taken by Students when Victimized in Cyberbullying (x= kind of action, y= percentage)

Table: 12 Cyberbullying Related Issues

Frequency &Valid Percent							
Are you aware about Cyberbullying category?							
Emails		Text Messages		Phone Call		Chatting Rooms	
23	46%	19	38%	1	2%	5	10%
How you feel when you been bullied via Internet?							
Angry		Sad		Difficult to trust others		Do not go to school	
20	40%	8	16%	17	34%	3	6%
What did you do when you are bullied?							
Pretend to ignore it		Talk to others		Bully the bullier		Delete all the bullier messages	
15	30%	9	18%	18	36%	6	12%

4.3.2: Security Awareness for the Pre-Questionnaire

This section focuses on assessing the level of security awareness in three areas, namely (Password, social networks, cyber-bullying) among secondary school students and the composition of this section presented in table A “see appendix C”. Figure 16 draws the percentage of the current awareness level as presented by secondary school students. Students showed a risky behavior when they were asked about posting personal information via social networks as 30% (or 15 respondent) answered they did not consider posting personal information via social networks as dangerous, while

28% (14 respondents) they did not know about this issue, and 42% (21 of respondents) they agree that posting personal information is risky.

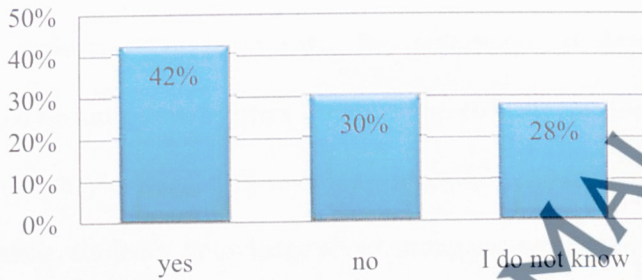


Figure: 16 Posting Personal Information via Social Networks Sites

Another question was considered with the privacy sitting on social networks and these expected to be with the general information on the participants' perspectives as a formal user to the social network sites. Figure 17 shows students' polls in this issue. 44% (or 22 respondents) know how to deal with the privacy sitting on social networks, while 26% (13 respondents) answered with no, and 30% (15 respondents) they did not know about the privacy setting provided by social network sites. This question leads us to consider how this could affect students when someone get their phone number or even control the list of who can look for their profiles and somehow post in their profiles.

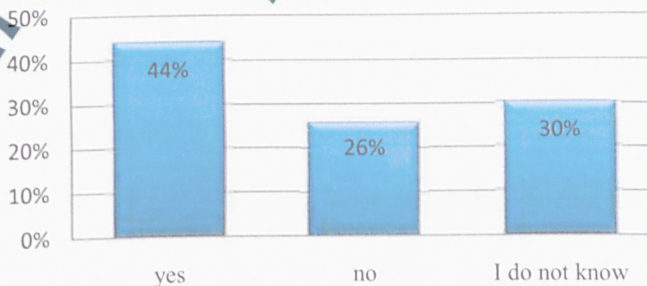


Figure: 17 Dealing with the Privacy Setting in Social Network Sites

The passwords have an important aspect in strengthening the security of different accounts of users. The general security awareness was asked to students in order to measure their awareness level based on passwords habits. Figure 18 presents the knowledge of students about passwords. The percentage of 64% indicated that passwords should be more than 8 letters length, while 20% are not sure about that, and 16% indicated that they did not know about this regulation. As it summarized from the previous statements, students' knowledge about strong passwords is very limited, even there are some websites enforce users to use passwords that more than 8 letters length there is still a lack in their awareness level. This finding is also resented in Padric, (2012).

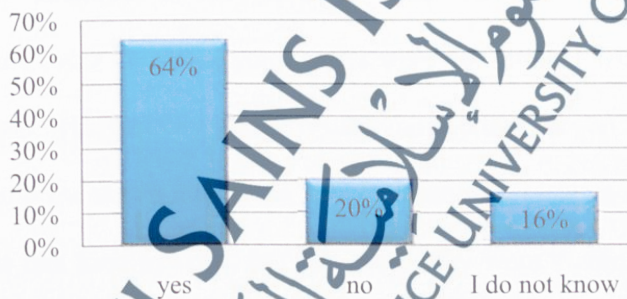


Figure: 18 Knowledge about Passwords Length

The role of changing passwords has a strong strategy of defence against security risks. A part of this section on assessing the awareness asked students about changing the passwords. Figure 19 shows students' answers. The majority of 40% indicated that they know passwords should be changed regularly, while 40% indicated no, and 20% did not have any idea about this issue. This also refers to the awareness issue in presenting the highest risk occurred, when they may face multi attacks without taking in mind that their passwords are the important key in preventing the attacker and

reduce the risks. Padric (2012) also stated that students appeared risky behaviour in the way they never change their passwords.

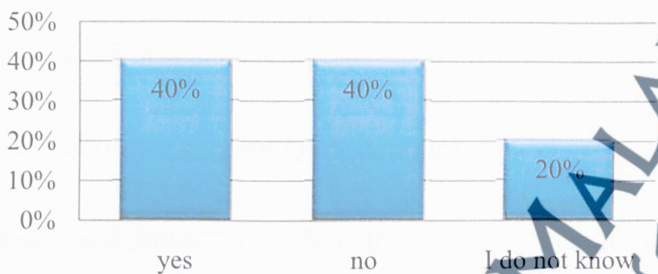


Figure: 19 Changing Passwords based on Students' Indication

Cyberbullying has increased in its severity based on the literature findings. Figure 20 drawn students' attention to the word of cyberbullying. Nearly 84% (42 of respondents) know what Cyberbullying is, 8% were not familiar with this word, and 8% unaware about cyberbullying. These results showed that Libyan secondary school students are also presented in this issue, although there were some students who are not aware about this kind of risks, but somehow they were victims of its forms as found in the results.

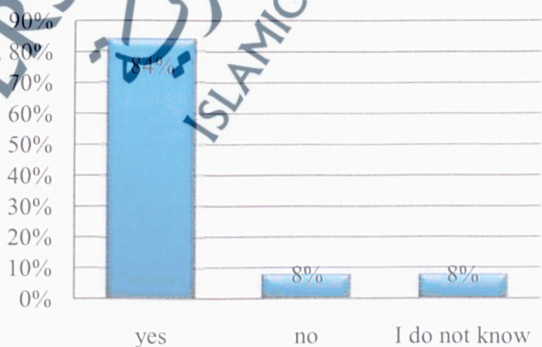


Figure: 20 Cyberbullying Awareness among Students

From the results we can clearly identify that security awareness level is slightly high in ethical issue, and when asked students about their answer, we clearly observed that students take this practice from creating new accounts, as the program used to ask them to enter more than 8 letters in length.

4.3.3: Security Practices for the Pre-Questionnaire

The security practice is a critical part of how the secondary school students are really aware about security risks and they apply their knowledge in their daily life. Based on the students' performance in answering this section we summarized that students did not apply the security rule to avoid any possible risks. Table B presents the illustration of this section as presented in appendix C

Each security issue considered in this study has four questions in this section in order to obtain students' attitude and behaviour. As seen in section one the influences of friends as they have a vast majority of spreading the knowledge about social networks, figure 21 drawn the students' readiness to share their daily activities with friends via social networks. The results showed that 4% strongly disagree to share their daily activities with friends, 16% disagree, while 22% were neutral and did not like to appear any opinion about this section, 32% respondents agreed, and 26% strongly agree. This can clearly show to us that students did not consider the danger of this habit as they indicated that they do not organize the list of their friends or who can see the contain of their profiles.

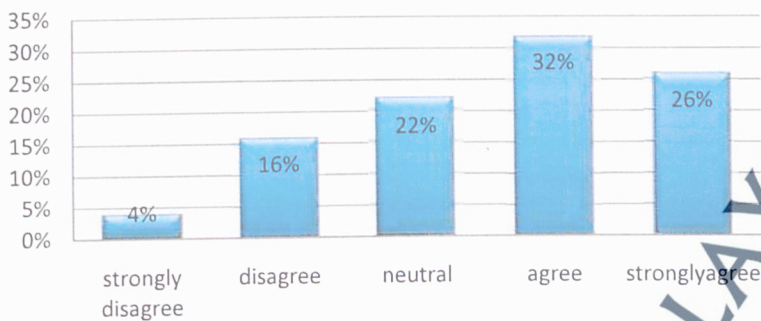


Figure: 21 Sharing Daily Activities with Friends via Social Networks

An example was given to students as a part of the question if they post their personal information “as their city”. Figure 22 gives the percentage of students’ performance, as 4% strongly disagreed to have the same action, 8% disagreed, while 14% respondents were neutral, but the risks start appearing in the percent of 38% agreed and 36% strongly agreed on posting personal information via social networks. Students did not recognize what are the consequences of the same behaviour as they did not mind to post it and give the details about their living place as they think the other person can not cause any real danger to them.



Figure: 22 Posting Personal Information via Social Networks

The stringers played an important role in threatening others as a part of the risk caused by bad security practices in social networks. Figure 23 presents the percentage of

students' answers. A majority of 14% (or 7 respondents) strongly disagreed to accept friend request from people they did not know, 8% disagreed, while 30% neutral, 32% agreed and 16% strongly agreed to accept invitation from people they did not know. As a result, students' behaviour in this case can lead them to face even cyberbullying as it results from strangers in many cases of bullying.

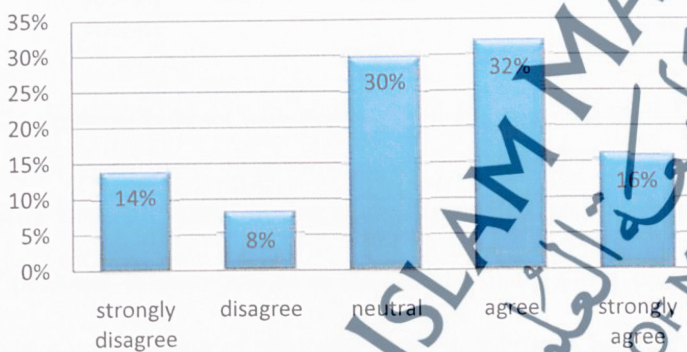


Figure: 23 Accepting Friends' Request from other People

The more advance service provided by social networks is the location. For some people it is interesting to send your location and make people know where are you know, but this can be a high risk in unexpected ways. Figure 24 shows the students' interaction with this phenomenon. We found that 24% strongly agreed and 16% agreed to send their location through social network sites, while 34% of respondents were neutral, 6% strongly disagree, 20% disagreed to post their location via social networks. Students did not believe that posting of their location can cause any risk to them. They also believe themselves to be far from being followed by criminals or any risks that could result from posting their location.

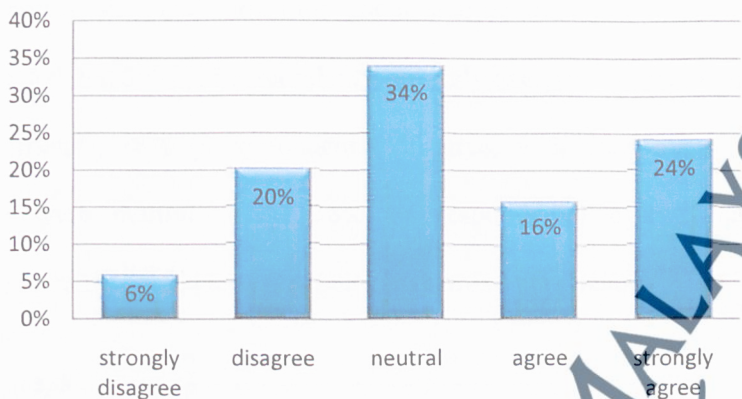


Figure: 24 Students Interact with Posting their Location via Social Networks

Another security issue presented in this study considered passwords as it can have a huge loss of personal information as it targeted to many kinds of security attacks. Figure 25 gives a presentation of students’ performance with holding the passwords. 48% (24 respondents) of respondents strongly agreed and 14% (7 respondents) agreed that passwords should contain “letters, characters, and numbers”, while 18% (9 respondents) neutral, 8% (4 respondents) strongly disagreed, and 12% (6 respondents) disagree in term of building the passwords. This issue reflects the risk presented by students when they use their date of birth as a password that makes it contains numbers only.

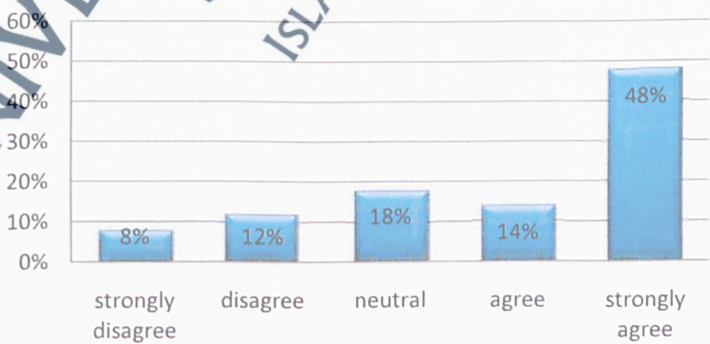


Figure: 25 Students Attitude about the Contents of their Passwords

Figure 26 showed students' indication about sharing their passwords with friends. Results indicated that 30% (15 respondents) strongly disagree to share their passwords words with friends, 18% (9 respondents) disagree, with the percent of 22% (11 respondents) were neutral, while 18% (9 respondents) agreed, and 12% (6 respondents) strongly agreed to share their passwords with friends.

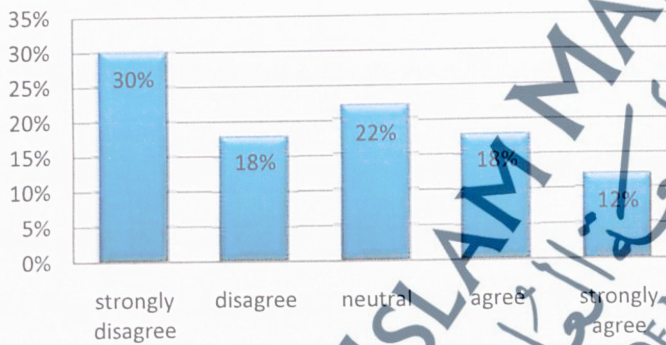


Figure: 26 Sharing Passwords with Friends

The way of remembering passwords draws another risk toward students as drawn in figure 27. The majority of 24% (12 respondents) of respondents strongly disagreed to write their passwords down in order to remember, 20% (10 respondents) disagree, while 20% (10 respondents) were neutral, 28% (14 respondents) agree to write their passwords, and 8% (4 respondents) strongly agree. This could result in violating of their personal information, when someone can easily take this information illegally and use it to violate their personal accounts.

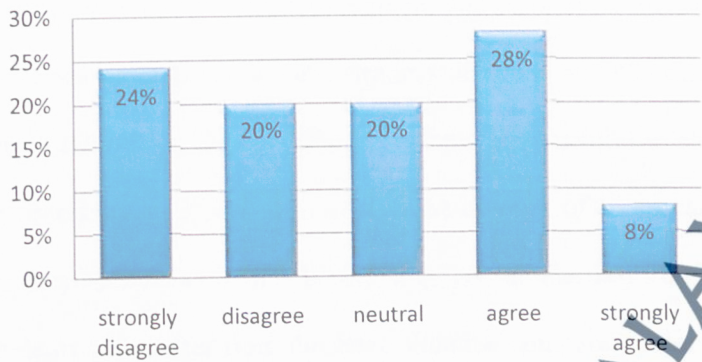


Figure: 27 Writing down the Password to Remember it

What students’ passwords include where another plane to draw students’ performance. The question was considered if students include their personal information in building their passwords. Figure 28 gives a presentation of students’ practices in holding their passwords. 36% (18 respondents) strongly agree, and 30% (15 respondents) agree that their passwords contain their personal information. 12% (6 respondents) strongly disagree, 2% (1 respondent) disagree, and 20% (10 respondents) were neutral in using their personal information as a part of their password.

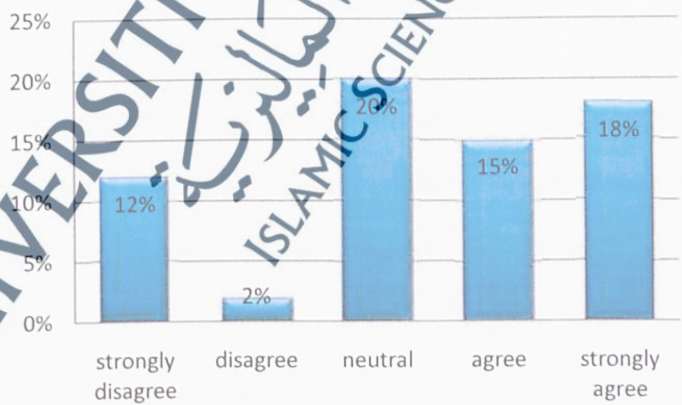


Figure: 28 Passwords Contain Personal Information

The last part of this section focused on Cyberbullying. The action of being a victim of cyberbullying and what students should do in the same situation was presented in

figure 29. The majority of 18% strongly agreed, and 32% agree to tell someone in case they have been bullied. While 16% strongly disagree, and 4% disagree to have any indication to tell others. Nearly 30% of students were neutral to show anything. This practice presented by students illustrates the amount of harm can occur upon students when they been a victim of cyberbullying. As summarized from the literature, there were students who suffer from the same situation compared to the case of other students who tell others “parents or teachers” to help them avoid same danger.

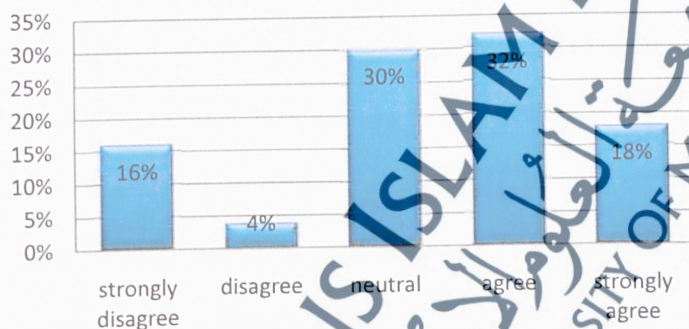


Figure: 29 Telling Others about Being Bullied

Figure 30 shows the percentage of students who have involved in some forms of cyberbullying. 18% of respondents strongly disagree and 6% disagree in receiving a hate message from someone, while 38% were neutral. 18% strongly agreed and 22% agree as they received a hate message from someone. These results show the spread of cyberbullying between students, although the high majority did not indicate any but the threat still present.

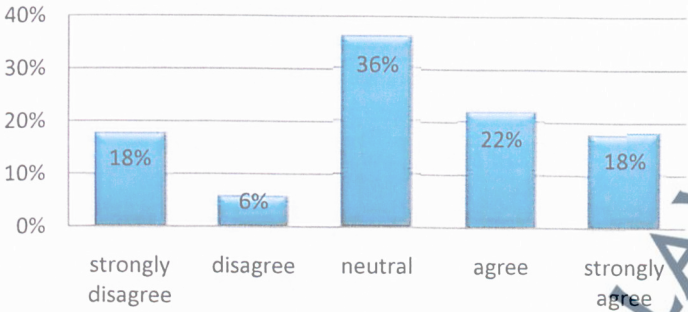


Figure: 30 Receiving a Hate Message from Someone

To measure the spread of cyberbullying between students, we asked them if they have engaged in cyberbullying. Figure 31 draws the percentage of students who bullied others. The total of 28% (14 respondents) strongly disagree, and 22% (11 respondents) disagree to bully someone, while 10% (5 respondents) strongly agree, and 24% (12 respondents) agree to bully someone. The majority of 16% (8 respondents) were neutral on this issue. The action of bullying others can indicate the severity of cyberbullying caused by students. With the result of students who answer to bully the bullier, cyberbullying will spread among students and based on this the schools need to hold the action among students to prevent cyberbullying in the early stage.

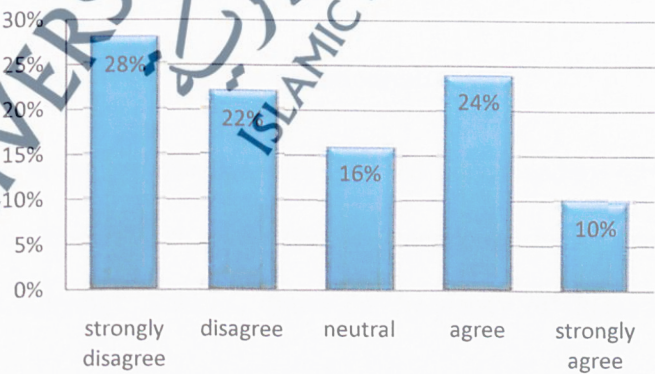


Figure: 31 Majority of Students Bullying Others

To measure the effects of cyberbullying on students’ behavior, we ask them if they can go to school in case they were bullied. Respondents interaction presented in figure 32. Nearly 38% (19 respondents) strongly disagree, and 26% (13 respondents) disagree as cyberbullying will not impact on them and they can go to their schools. On the other hand, 8% (4 respondents) strongly agree, and 14% (7 respondents) agree as they will not go to school in case they bullied. Finally, 14% (7 respondents) were neutral about their situation. The result of students who will not be able to go to their school reflects the bad effect of bullying and this will result in their academic performance as presented in faryadi (2011) report.

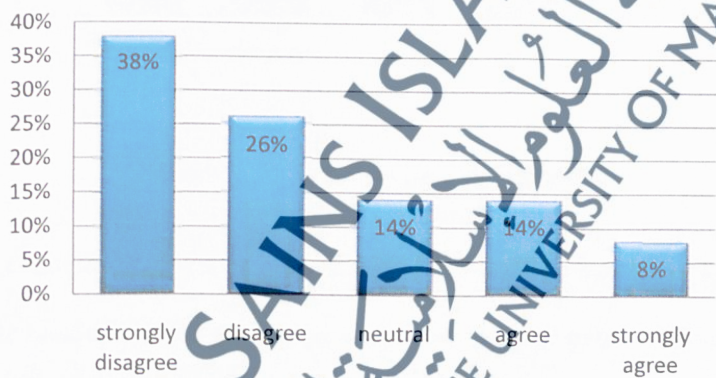


Figure: 32 Cyberbullying Impact on Students Ability on Going to School

4.3.4: Personal Opinion for the Pre-Questionnaire

The last section in the pre-questionnaire is asked the secondary school students on their personal opinion related to the previous mentioned issues “passwords, social networks, cyberbullying”. Table C draws the frequency of students’ answers “see appendix C”.

From the results of the students’ personal opinion, figure 3 draws students’ personal opinion on a sample of password. The total of 40% disagree (20 respondents) while

46% (23 respondents) agree that “123” is a good password. Only 14% (or 7 respondents) were neutral on this issue. The simplicity of this issue presents the limited knowledge of students about the structure of strong passwords. It is hoped to enhance students' performance after the training program which presents the importance of passwords.

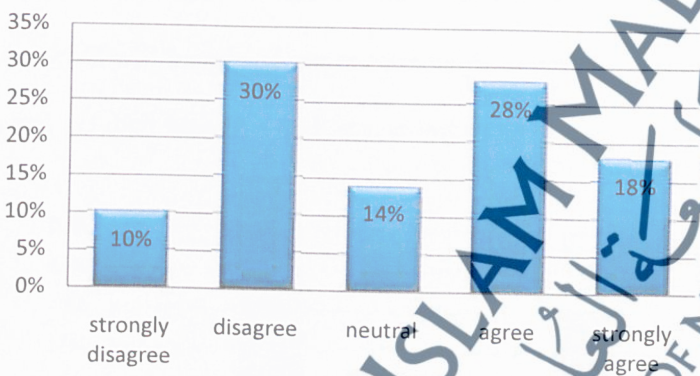


Figure: 33 Is “123” a Good Password?

The way of changing passwords after sharing was another concern as presented in figure 34. The total of (40% strongly agree, and 14% agree) to change their passwords after sharing it. While (22% disagree, 2% strongly disagree) to change their passwords, and 22% did not indicate any at a neutral level.

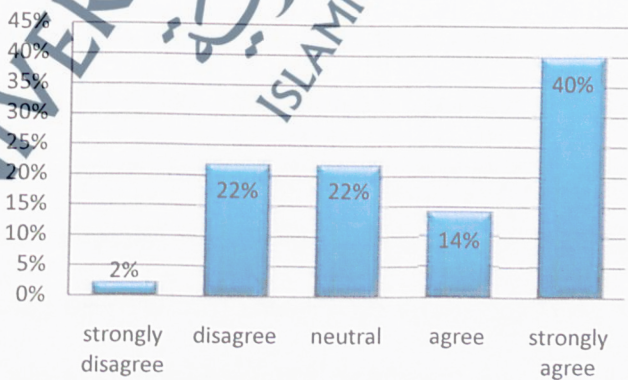


Figure: 34 Changing Passwords after Sharing them

Some people prefer to use the same password for all of their accounts, figure 35 shows the results of students personal opinion on this issue, it was found that 40% strongly agree, 20% agree that it is easier for them to use the same password for all of their accounts. On the other hand, 4% of respondents were strongly disagreed, 24% disagree to use the same password. Nearly 12% were neutral. Students think in a simple way which make them remember their passwords by just using one only without thinking what will happen if someone manage to get this password and broke their accounts and get their sensitive and private information.

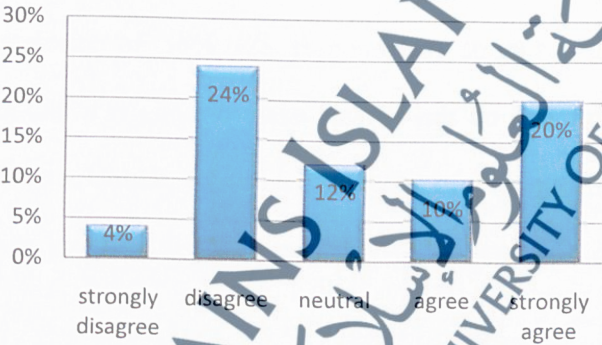


Figure: 35 Using the Same Password for all Accounts

Posting personal photos present a real risk to people. Students dealing with their personal photos on social network sites reported in Figure 36. The total of 38% (12% strongly disagree and 26% disagree) to share their personal photos with others via social networks. The total of 54% (24% strongly agree and 30% agree) to share their personal photos. Finally, 8% (or 4 respondents) were neutral. When comparing the negative and positive results, we clearly summarize that students appear a risky behaviour in sharing their personal photos without thinking about who can use this photo in a sleazy way or even to be harassed by others.

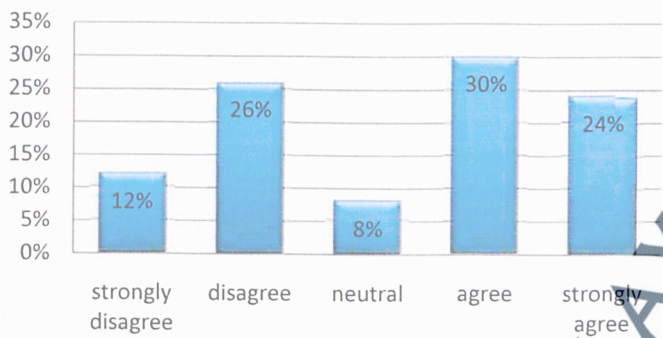


Figure: 36 Posting Personal Photos via Social Networks

Making new friends sounds attractive for students, but in the case of social networks they will not be able to identify who is the second part. Figure 37 draws students' indication. The majority of 56% (28 respondents) strongly agree and 10% (5 respondents) agree that it is good to make new friends on social network sites even they did not know them. Unlike, 16% (8 respondents) of respondents were neutral, 4% (2 respondents) was strongly disagree and 14% (7 respondents) disagree with this term.



Figure: 37 Good to Make New Friends via Social Networks

Figure 38 showed the percentage of students in accepting friend request from unknown people. The total of 60 % (38% strongly agree and 22% agree) to accept the invitation, while 28% (22% disagree and 6% strongly disagree) to accept the

invitation. Followed by 22% (11 respondents) were neutral on this issue. This question stands as the key of the risks students face while using social networks, as this presents the effect and the role of attacker, bullyier and harasser to target such case of students who did not know them in person.

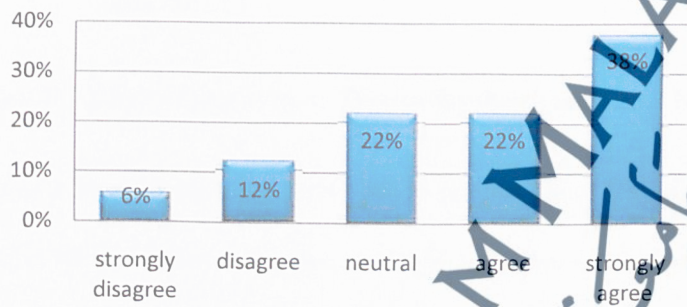


Figure: 38 Accept Friends' Request from Unknown People

Students are familiar with the term of bullying and with the spread of technology cyberbullying starts appearing. We asked the students about their opinion, if cyberbullying is more dangerous than the normal bullying, and figure 39 draws students' opinions on this concept. In the percent of 48% (24 of respondents) strongly agree, 18% (9 respondents) agree as cyberbullying is more dangerous than the normal bullying. While 8% (4 respondents) strongly disagree, 8% (4 respondents) disagree, and 18 % (9 respondents) neutral in this term. Although some male students indicated that they prefer to be bullied "traditional bullying" as they can present themselves and react to the action, but the results of students' opinion that cyberbullying is more dangerous than normal bullying.

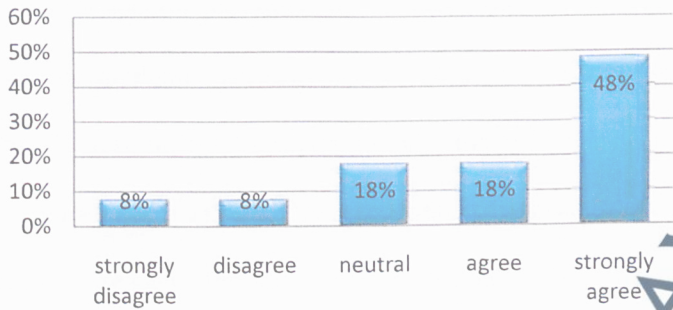


Figure: 39 Cyberbullying is more Dangerous than Traditional Bullying

The effects caused by cyberbullying, and how to prevent this risk make the bullying action a crime in itself. Figure 40 draws students’ answers. 12% (6 of respondents) strongly disagree and 34% (17 respondents) disagree in term of “is not a crime if I bully someone”, followed by 20% (10 respondents) strongly agree and 18% (9 respondents) agree about this issue. Nearly 16% (8 respondents) were neutral from any indications. From the results it is obtained that students did not take the action of bullying as a serious problem, and in this case students should be educated as well as provided with the real life stories about students who suffer from being bullied and the judgment caused to the bullier. These actions can provide students with the real knowledge about cyberbullying and its effects.

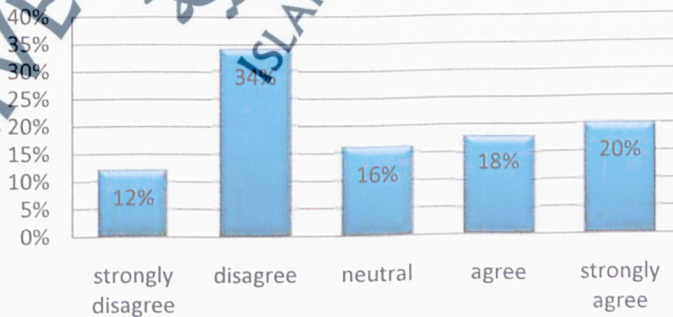


Figure: 40 It is a Crime when Bullying Someone

The last issue of this section presented in students' interaction when they bullied. Figure 41 shows the students' performance at 14% (7 respondents) were strongly disagreeing, 26% (13 respondents) disagree to bully the bullier in case they bullied by someone. The majority of 18% (9 respondents) strongly agree and 22% (11 respondents) agree to react in the same way. However, 20% (10 respondents) were neutral.

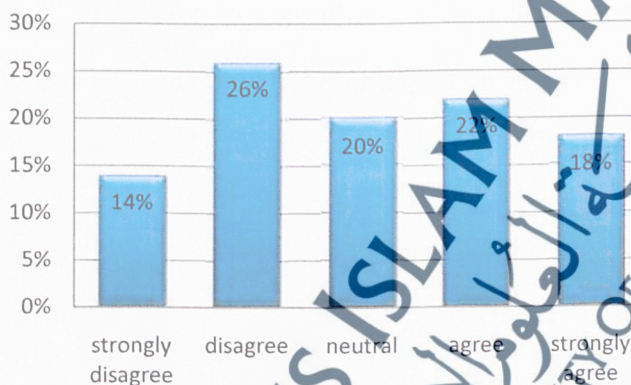


Figure: 41 Repeating the Action of Bullying to the Bullier

4.4: Post-Questionnaire Results

Based on the planned strategy of this study, the second part after the pre questionnaire was conducting a training program to the same participants. The post-questionnaire was given to students to assess their awareness, practices, and opinion based on what they have participated in the training program. The part of evaluating the security awareness training tools took place in the section five of this questionnaire.

4.4.1: Demographic and General Security Information for Post-Questionnaire

In this section as the participants are the same as those who have done the pre questionnaire almost all the answer of this section were the same as the pre

questionnaire except some of the questions that the students obtained the answers from what they have learned from the training program.

The reaction of cyber bullying is presented in figure 42 while table 13 described the frequency. The action of bullying the bullier decreased at the percent of 4% (or 2 respondents only), followed by deleting all the bullier messages at 20% (or 10 respondents), and “talk to others about it” at 30% (or 15 respondents). Finally, “pretend to ignore it” at 46% (or 23 respondents). This showed a real enhancement on students’ behaviour as this can have a positive impact on students’ life and reduce the effect caused of being bullied.

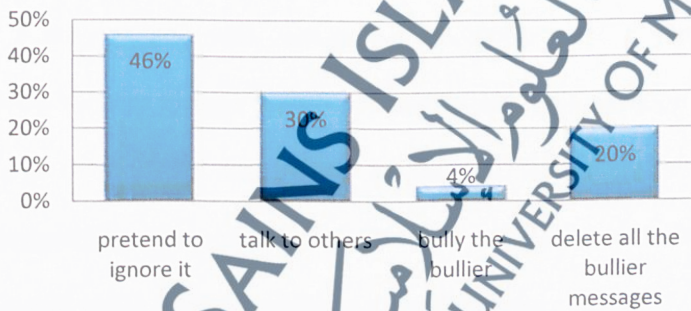


Figure: 42 Action will be Taken by Students when Bullied

In the statement of asking students about how many passwords they will have, figure 43 presents students’ results and table 13 detailed the results. 76% of respondents indicated that they will use one for each account, followed by 12% of them will use one only, and 12% of respondents will use three passwords. Students’ knowledge about the risk that could be caused in case of using one password for all of their accounts as they indicated in the pre-questionnaire, have been reduced as a result of the training program students have had in previous stages of the research. This practice should continue with students in order to prevent any future risks.

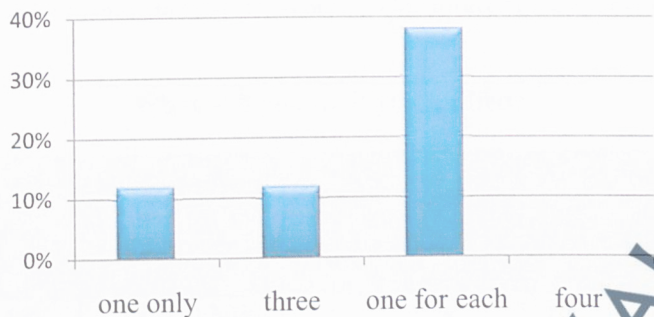


Figure: 43 Number of Passwords will be used by Students

Figure 44 illustrates the enhancement in students’ habits on changing their passwords and the composition in table 13. 82% (or 41 respondents) choose to change their passwords once a month, followed by 8% (or 4 respondents) will change it twice a year, 4% (or 2 respondents) will change the passwords once a year, and 6% (3 respondents) they will not change their passwords at all. This question clearly shows the enhancement of students’ knowledge as resulted from the training program. Students are suggested to keep practicing what they have learned during the training program as this will guide them to reduce any possible risks.

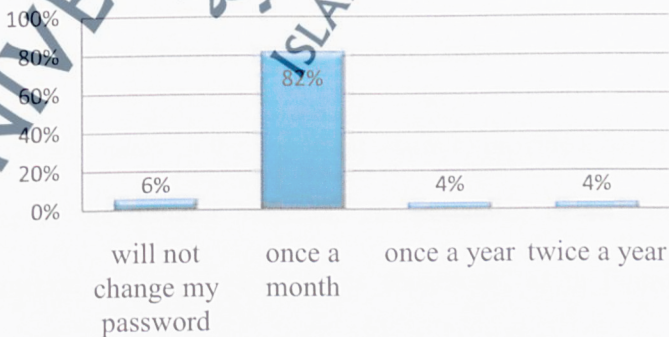


Figure: 44 Times Students will Change their Passwords

Table: 13 General Information Security Questions “Post-Questionnaire”

What will you do if you bullied?							
Pretend to ignore it		Talk to others about it		Bully the bullier		Delete all the bullier messages	
23	46%	15	30%	2	4%	10	20%
How many passwords will you use for all your accounts?							
One only		Three		One for each		Four	
6	12%	6	12%	38	76%	0	0
How many times will you change your passwords?							
Once a month		Once a year		Twice a year		I will not change my passwords	
41	82%	2	4%	4	8%	3	6%

Basically from this section there was an enhancement in students’ performance on the critical issues as this could result in reducing the risks to them, as this reflects the importance of the training program in making the change on students’ behaviour.

4.4.2: Security Awareness for the Post-Questionnaire

In this section we will focus on the important issues to provide a better understanding of the outcome of the training program. The responses of students on “posting personal information via social networks is dangerous” as in figure 45: 96% (48 respondents) yes, 2% (one respondents) no, 2% (one respondents) I do not know. This clearly shows students’ awareness about posting their personal information compared to their results on the pre questionnaire as in figure 15. Enhancing students’

knowledge about posting personal information will limit other possible risks can caused from the same habit and this also reflect the positive outcome from the training program.

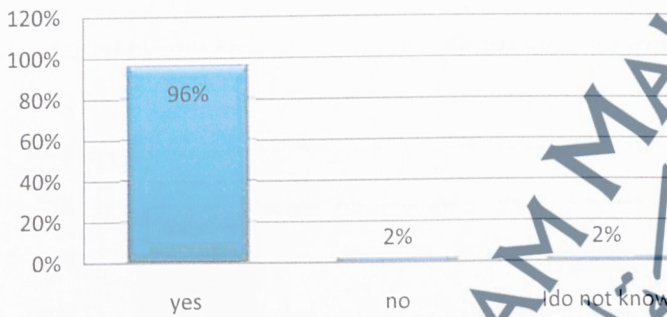


Figure: 45 Post-Questionnaire Results about Posting Personal Information

Dealing with privacy setting is an important aspect to protect students against unsuitable use of their information. Figure 46 draws the results for the term of dealing with the privacy setting on social networks, 74% (or 37 respondents) yes, 16% (or 8 respondents) no, while 10% (or 5 respondents) they still did not know about it. From the results it could be stated that dealing with the privacy setting means to prevent any possible risk. As mentioned in the question of who can see the contact number, this lead students to manage their profile and limiting the unwanted contact with strangers.

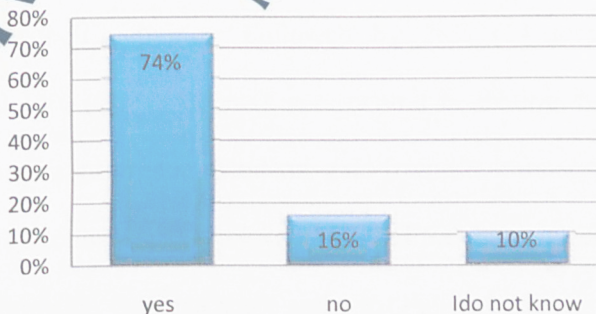


Figure: 46 Dealing with Privacy Setting on Social Network Sites

In the statement of “I should change my passwords regularly”, figure 47 presents the respondents’ performance. Totally 82% (41 respondents) answered with yes, 10% (5 respondents) no, followed by 8% (4 respondents) did not know. This considered as an important finding of straightening the password protection between students and to reduce the risks caused by any kind of misuse of their personal information.

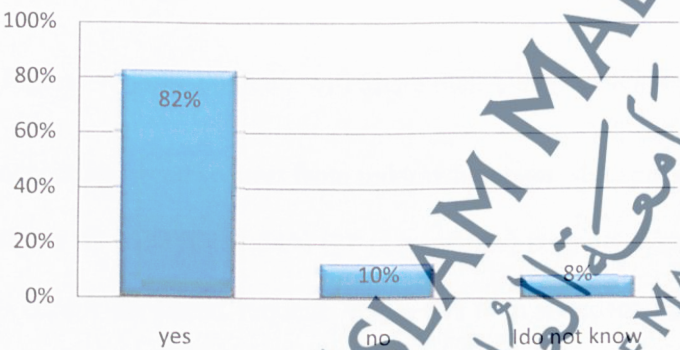


Figure: 47 Changing Passwords based on the Post-Questionnaire

4.4.3: Security Practices for the Post-Questionnaire

The main purpose of this section to stand further on how students going to apply what they have learned from the training program. First step presented in figure 48 to show how students share their daily activities via social networks from strongly disagree to strongly agree. The majority of 38% (19 respondents) strongly disagrees, 12% disagree to share their activities. Followed by 28% (14 respondents), 4% (2 respondents), and 18% (9 respondents) were neutral in sharing their activities. This result is passed on the information students gain from the training program, although some students still standing in the negative side but the threats decreased with taking in mind what information they can share and what they need to think carefully before sharing them.

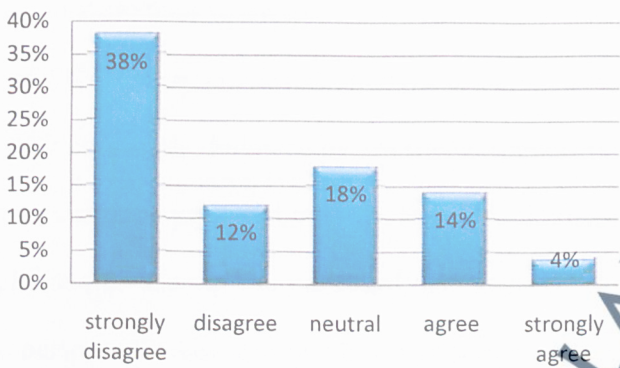


Figure: 48 How Students will Share their Daily Activities

In the state of accepting friend request from unknown person, students showed a good practice as in figure 49. Starting at 54% (27 respondents) strongly disagree, 26% (13 respondents) to accept the friend request. While 8% (4 respondents) strongly agree, 4% (two respondents) agree to accept the invitation. Lastly, 8% (4 respondents) were neutral. Therefore, students can prevent any misuse of their profiles, information and any unexpected threat as cyberbullying to occur if they apply the roles of accepting the invitation “friends’ request”. Also, students need to think before chatting with a new friend or any request of viewing their personal photos, and in the case of similar action they strongly recommended to delete the unwanted friend.

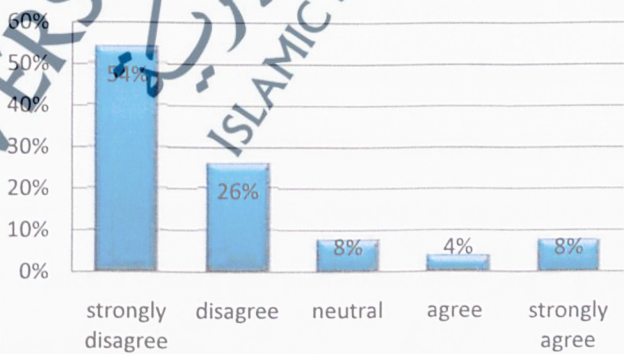


Figure: 49 Future Dealing with Friends Request

Students’ readiness to share their passwords with friends illustrated good results as in figure 50. Total of 76% (38 respondents) strongly disagree, 18% (9 respondents) disagree to share their passwords, followed by 4% (two respondents) neutral, 2% (one respondent) agree to share the password with friends. This finding presents students’ attitude in critical issue as sharing the password, and reduce the violence of their accounts even the person who they share with it may seems trusted, but they need to be aware of any action that may cost them extensively in the future.

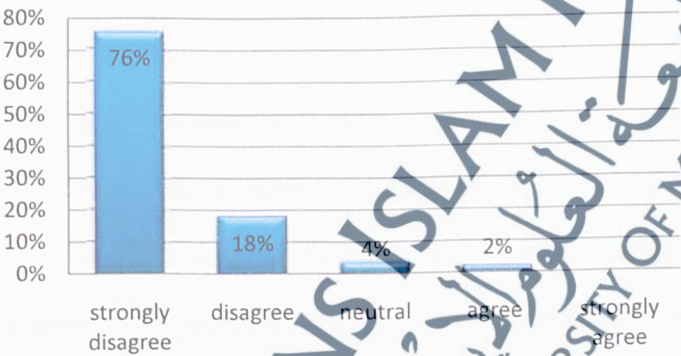


Figure: 50 How Students will Share their Passwords

How students will remember their passwords draw a good finding as presented in the figure 51, when 30% (15 respondents) strongly agree, 30% (15 respondents) agree as they will not write their password in order to remember it. Followed by 20% (10 respondents) strongly disagree, 8% (4 respondents) disagree with this term, while 12% (6 respondents) were neutral. Comparing to the results of students’ indication in the pre-questionnaire, a real improvement presented in the post-questionnaire. As they learned to have a good a memorable passwords which did not need to save them anywhere else except their minds.

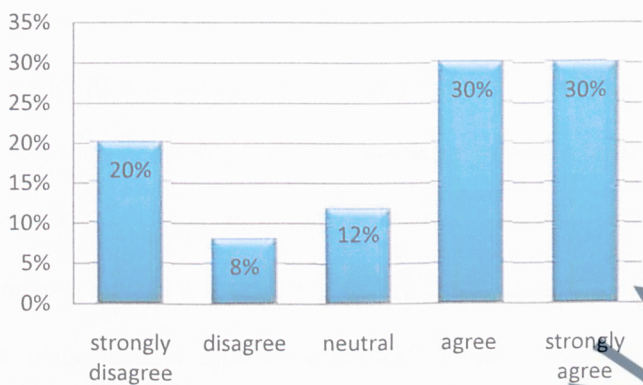


Figure: 51 Students' Interaction in Writing their Passwords Down

Two important issues presented in this section referred to cyberbullying, the first one presented in figure 52, as it showed will students bully someone by using the Internet. 66% (33 respondents) strongly disagree, 26% (13 respondents) disagree to bully any, while 2% (one respondents) neutral, 6% (three respondents) strongly agree on this term. This considered as an acceptable enhancement on students' behavior based on their performance. It is really needed to have this kind of awareness program to reduce the spread of cyberbullying as the results of the post-questionnaire shows how students change their attitude in bullying others.

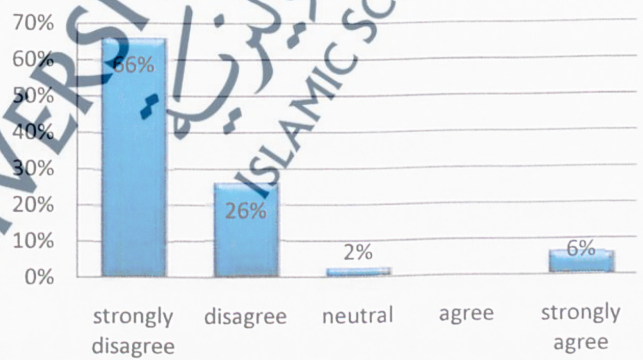


Figure: 52 Bullying Someone by Internet

The second issue reflected is one of the bad effects of cyberbullying when students could not go to school as a result of being bullied. Figure 53 showed the frequency of students in this issue as 60% (30 respondents) strongly disagree, 24% (12 respondents) disagree to will not be able to go to their schools if they bullied, while 2% (one respondent) strongly agree, 6% (three respondents) agree on this term, followed by 8% (four respondents) were neutral. Students showed in the previous sections in a high majority they will tell others in case they have been a victim of cyberbullying and in this section, they answer in the majority of 84% as they will be attending their classes even under the action of bullying. These results can reduce the negative effect on their academic performance as well as their emotions.



Figure: 53 Reduce the Negative Effect Caused by the Bullier

4.4.4: Personal Opinion for the Post-Questionnaire

In order to stand on the change that occurred after the training program, assessing students' personal opinion is important. It is important to have a change on students' personal opinion as this will be reflected on their awareness level as well as their security practices on the three security issues "passwords, social networks, and cyberbullying".

Figure 54 presents students' indications of the kind of password contain "123" as a good password. The total of 38% (or 19 respondents) strongly disagree, 38% (19

respondents) disagree with this term. Followed by 22% (11 respondents) neutral, 2% (one respondent) agree. This result reflects the change in students' opinion on what can be considered as a good password.

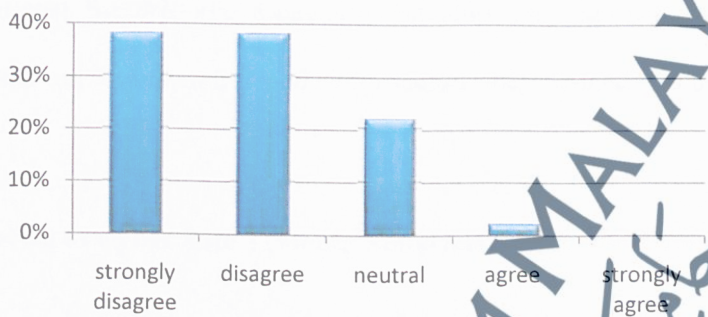


Figure: 54 Considering “123” as a Good Password

Figure 55 shows the students’ interaction on sharing their personal photos via social networks. The majority of 46% (23 respondents) strongly disagree, 44% (22 respondents) disagree to share their personal photos. Followed by 8% (4 respondents) neutral, and 2% (one respondent) agree on this term. This finding strongly approves the enhancement on the students’ personal opinion, although there were still a few students insisted to share their photos, but the idea of having personal privacy occurred.

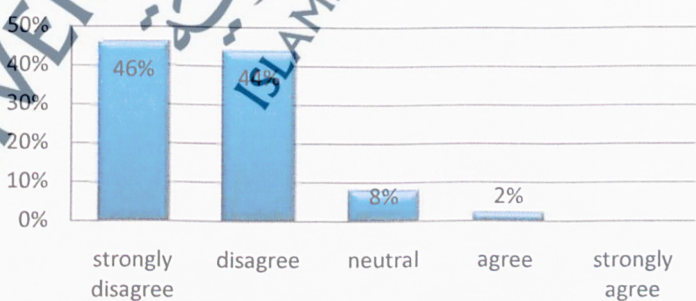


Figure: 55 How Students will Share their Daily Activities via Social Networks

4.5: Training Program Evaluation “Post-Questionnaire”

Based on secondary school students' practices on the training program, they are required to evaluate the materials based on what they have exercised as these chosen tools were almost for this age especially. Students are required to measure the materials based on the benefits and information they gained from the training program.

4.5.1: Evaluation of Cyber Safe Training Materials

For each cyber portal presented to students, they are required to evaluate these materials based on the outcome they have gained. This section provides the evaluation of Malaysia cyber portal “Cyber Safe” for all the materials practiced by students. Each tool requires students to answer two relevant questions to assess its effectiveness. Figure 56 draws students' evaluation on posters of cyber safe. The majority of 16% (8 respondents) disagree, 42% (21 respondents) neutral, 36% (18 respondents) agree, and 6% (three respondents) strongly agree in the term “posters are easy to understand”. Furthermore, another question considered the simplicity of the posters in explaining the security issue as in figure 57. Students showed that 6% (three respondents) strongly disagree, 20% (10 respondents) disagree, 22% (11 respondents) neutral, 40% (20 respondents) agree, and 12% (six respondents) with this term.

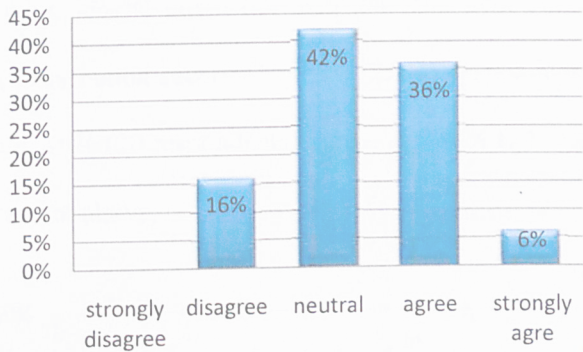


Figure: 56 Students Indication on Posters

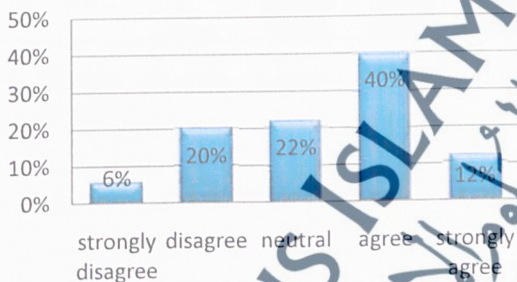


Figure: 57 Students Evaluation to the Value of Posters

The next material is a video which is presented in figure 58. In the statement of “the video explains the security risk very well”, students stated in the percent of 12% (or 6 respondents) disagree, 14% (7 respondents) neutral, 52% (26 respondents) agree, 22% (11 respondents) strongly agree with this statement.

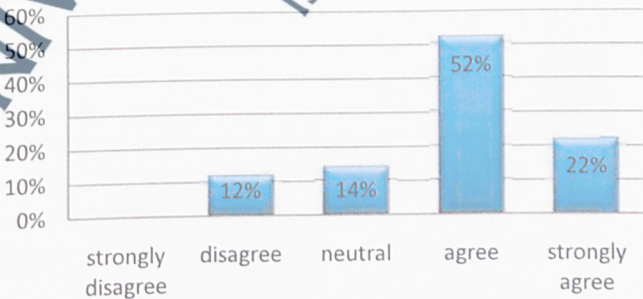


Figure: 58 The Video Explains the risk very Well

Figure 59 draws the students’ interaction with the statement “video make me know what I need about information security”. Nearly 2% (1 respondent) disagree, 10% (5 respondents) neutral, 40% (20 respondents) agree, and 48% (24 respondents) strongly agree with the statement above.

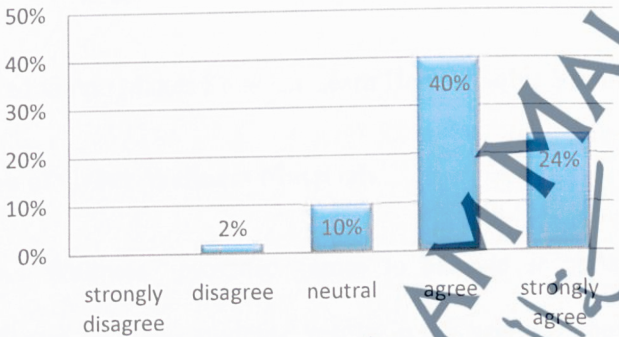


Figure: 59 How Video Provides the Knowledge about Information Security

Last evaluation is for the games as illustrated in figure 60. Students’ understanding of the issue is presented in the game indicated that 2% (one respondent) neutral, 32% (16 respondents) agree, and 66% (33 respondents) strongly agree on this term. While the statement of “the game makes me learn how to solve the security problem” is presented in figure 61. The total of 34% (11 respondents) agree, and 66% (33 respondents) strongly agree with the statement.



Figure: 60 Students Understanding of the issue Presented in the Game

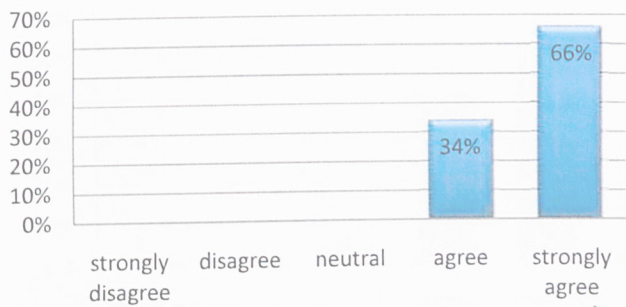


Figure: 61 Game Makes Students Learn How to Solve Security Risk

4.5.2: Evaluation of Cyber Wellness Materials

Singapore “Cyber Wellness” provides games to educate secondary school about security issues. Figure 62 draws students’ results in this section. The majority of 60% (or 30 respondents) strongly agree, 36% (18 respondents) agree, 2% (one respondent) neutral, and 2% (one respondent) strongly disagree as the game makes them understand the problem.

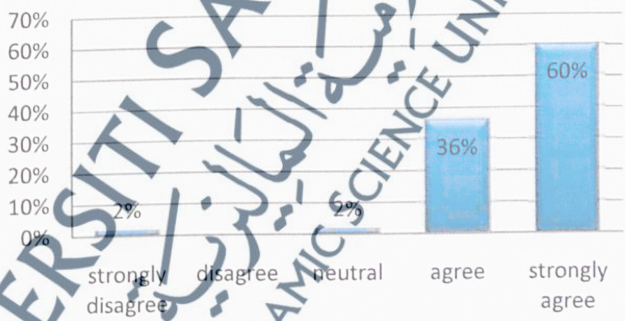


Figure: 62 Students Evaluation on Game of Cyber-Wellness

In the statement of “game makes me learn how to solve the security issue” figure 63 illustrates students’ indication. 2% (one respondent) strongly disagree, 4% (two respondents) neutral, 40% (20 respondents) agree, 54% (27 respondents) strongly agree with this statement.

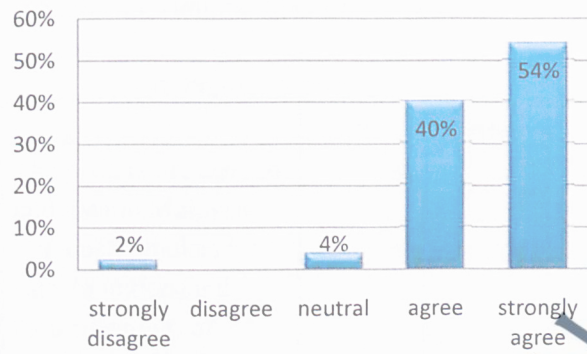


Figure: 63 The Percentage of Game Benefits

4.6: Finding and Results of the Pre and Post Questionnaire

As listed in the section 1.4, all the training materials are required to be evaluated by students in order to measure their effectiveness. Section 4.5.1 and section 4.5.2 represents respondents' polls on these materials. After this step, we need to identify what is the ideal tool for the age of secondary school students. Descriptive statistic by the function of "Mean" is deployed to declare what tool has the higher value. As summarized from the table 14 that games have the highest mean, followed by videos and posters respectively.

Table: 14 Training Materials Evaluation

Descriptive Statistics		
	N	Mean
The posters are easy to understand Malaysia	50	3.32
The poster makes it easy to understand their meaning of security Malaysia	50	3.32
The video explains the risk very well Malaysia	50	3.84
The video makes me know what I need to know about information security Malaysia	50	4.34
The game makes me understand the issue Malaysia	50	4.64
The game makes me learn how to solve the security issue Malaysia	50	4.66
The game makes me understand the issue Singapore wellness	50	4.52
The game makes me learn how to solve the security risk Singapore wellness	50	4.44
Valid N (listwise)	50	

Another concern is based on assessing the current level of awareness among secondary school students regarding their polls in the pre-questionnaire and comparing it with the results on the section of security awareness in the post questionnaire by using “Crosstab Function” in SPSS which helps in providing the values of multi choices separately. The results after calculating the values in the table

15 is summarized that the majority of 38% (or 19 respondents) has a slight level of awareness, compared to 62% (or 31 respondents) unaware. This result illustrated the need for security awareness training program for students. After conducting the training program the post-questionnaire submitted to students in order to stand in its effectiveness in enhancing the students' security awareness level. Table 16 showed the results of the “Crosstab Function” and after solving the percentage for each value “negative and positive” we found that 86% (or 43 respondents) aware, and 14% (7 respondents) unaware. From these results we clearly summarize that the training program has a positive impact on secondary school students' behaviour.

Table: 15 Crosstab Values for Security Awareness in the Pre-Questionnaire

awareness_mean * gender Crosstabulation

		Gender		
		Male	Female	Total
awareness_mean	Yes	3	0	3
	1	3	6	9
	1	5	2	7
	2	4	6	10
	2	1	9	10
	No	0	3	3
	2	0	6	6
	I do not know	0	2	2
Total		16	34	50

Table: 16 Crosstab Values for Post-Questionnaire
AWARENESSMEAN * gender Crosstabulation

	Gender		Total
	Male	Female	
AWARENESSMEAN 1	10	18	28
1	1	10	11
1	1	3	4
2	1	1	2
2	0	1	1
2	1	0	1
2	2	0	2
3	0	1	1
Total	16	34	50

As far as this work was done, the part of observation was done by the researcher. The researcher found that students in the first time when invited to involve within a science research were very excited as they started asking which kind of researches they have to take part. After the instructions on how the students are required to answer the questionnaire some of them ask "Why do we need to answer these questions". When the students finished answering on the pre questionnaire they set for a training program. At first, we showed the posters to all students and gave them the brief for a while. The students responded very positively when they started playing the games compared to their case when they watched the videos. Most of the students showed real attention on the subject of the games, and they took some kind of competition for the games when asked to answer questions. Finally, the post questionnaire was given to students and some of them suffered boredom as they ask "Why we need to answer the same questionnaire for the second time".

All the students’ questions were answered by the researcher as the subject of this study required. Another point mentioned by a female student when she asked about cyberbullying “if someone bully her,” she indicated “I will be neutral as I send but I did not receive any bullying messages”. Some of younger teen aged from 17 to 18 showed acceptance of the content of posters as they interested in getting brief information. Moreover, female students were more careful in posting their personal photos than male students and this could be clearly referred back to the culture of Islam between students, as female students especially need to keep their photos private from the stranger which could affect their personality or can be used in unrespectable ways.

Finally, to find if there are any differences in the level of security awareness and practices between students in term of gender, the one way ANOVA deployed in this study. Table 17 illustrates the impact of gender difference on the level of security awareness and security practices. The results indicated that there is a relationship between the level of awareness and security practices based on students, gender.

Table: 17 The Significant Value for Security Awareness and Practices

Coefficients ^a					
Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	.307	.369		.833	.409
1 awareness	.488	.133	.459	3.679	.001
practice	.176	.091	.242	1.938	.059

Furthermore, the results showed the significance level at 0.001 for ANOVA test as in table 18.

Table 18: ANOVA Test for Significant

ANOVA ^a						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	2.932	2	1.466	8.668	.001 ^b
	Residual	7.948	47	.169		
	Total	10.880	49			

4.7: Summary

This chapter presents the results of the research methodology. The finding of fulfilling the first objective of this study “to identify and evaluate available security awareness training tools used for secondary school students”, based on the results of South East Asia cyber-portals, two cyber portals were deployed and the materials were “games, videos, and posters”. The result of the first objective showed that game is the best tool as reported from students indication from the post-questionnaire. The second objective of this study focuses on “assessing the level of security awareness among secondary school students related to social networks, passwords, and cyberbullying”. The results were obtained from the analysis showed that students’ knowledge in the presented risks of this study very limited, and their awareness level was very low. After conducting the training program, students showed improvement in their behaviour as reported from the post-questionnaire results. The overall objectives of this study toward Libyan secondary school students were investigated.