CHAPTER I

INTRODUCTION

1.1: Background

New development in information security raises many responsibilities, and many organizations attempt different solutions to safeguard their sensitive information. Starting from the idea of spreading the awareness about the importance of the information security, all organizations have to work together to ensure people are aware about the challenges that they might face in their daily life.

The enormous connections and usages of communication and information between the organization and the system requires high quality of safety use as well as the detection of the risks and security gaps in any systems. Shaw et al., (2009) stated that the increase progress of the use of the Internet has negative effects on the organizations budgets due to the lack of security. This requires a review of the threats from both outside and inside the organization. Therefore, there is an increase to apply the security on the Internet by using risk analysis, and risk management to provide the safety and security in the network (Saleh et al., 2011).

Nowadays, the information security awareness is becoming a big issue. Although organizations spend high cost to secure their information, the threats are still a big challenge. Peltier (2005) stated that no one can apply information security without applying the security awareness and training program that will provide the real result of information security in an organization. Information security means protecting information from unauthorized access, use, disclosure, disruption, modification, or destruction (Salter, 2013).

The concatenation of information security requests deep view on the principle of information security awareness among different users. Albrechtsen and Hovden (2010) stated that the crucial execution in an organization is the awareness and the behaviour of all kinds of users, as this execution of the information security awareness will exit the real needs of any organizations in the strength of the security of their sensitive information. This can clearly show us that even employees still do not recognize the risks associated with their Internet usages.

Information security awareness means to provide information to all authorized users, and to identify the role for each user to ensure how they can raise the level of information security and in the same time, to present the users with the rules and regulation that they have to accept and follow (Korovessis, 2011).

The role of information technology, (i.e Internet) is not circumscribed to one age group, and because of this explosion of the new smart technology, teens are more exposed to the role of the Internet in everyday life. Brady (2010) stated that, as the Internet meets an increasingly higher role in the daily lives of our children. As a learning and communication tool, it offers a broad scope of opportunities for people of all ages.

According to the Pew Research Internet Project, "teens registered an Internet use growth at 95% consistent since 2006, as teens age of (12-17) lead the age of the connection with Smartphone and Internet browsing" (Madden et al., 2013).

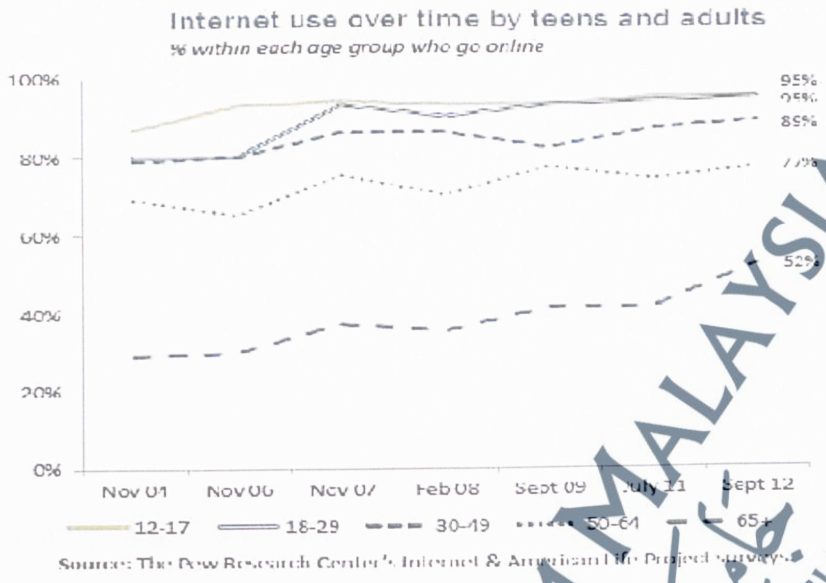

Figure: 1 The Internet use by age group: (2013)

There are some risks associated with this powerful source of knowledge toward students. Secondary school students, especially, are considered as the core ages, which recorded a significant use of the Internet and with all of the risks. The National Security Criminal Investigations Program in a report of "Youth online and at risk" stated that the Internet became widely accessible by youth in their classrooms, libraries, and bedrooms, as well as the fast spread of the cell phones" (NSCIP, 2011).

Bintziou et al., (1999) stated that it is necessary for secondary school students to be aware of information security issues in Greek education as the violation of personal information increase gradually.

Tekerek and Tekerek (2013) found that students are connected to the Internet at home or at Internet café, and they use Internet for education. As a result, students' awareness level was very low in many aspect of security. The authors showed that many students start using the Internet, but they skip many important things related

to security of their personal information. As those students will build the future of the new technology knowledge, there must be a concern to investigate their awareness toward securing their privacy.

Brady (2010) showed that schools are a universal point where students can get the knowledge and recognize the possible effect and risks associated with the use of the Internet, as they can get them to be safer, wiser and more responsible cyber users.

Falque (2012) stated that researchers found that the most "expensive" data were linked to the user's real identity (age, gender, address, etc.) and those relating to social or financial issues: on average, web users were prepared to sell those data for three times as much as their browsing data.

Another risk that was determined by Watson (2005) is the psychological effects of Internet on children. Thus, children who overuse computers isolate themselves from the society, lack self confidence, have depression, and social problems.

The use of communication influences Libyan young people as they are the generation who have the advantages of this era of technology. According to the Global information technology report, Libya recoded a growth of information technology about 2.77%, and rank of 119 out of the general ranking of 142 (Bilboa et al., 2013).

According to the Internet world state, the rank of young people who use the Facebook in Libya recorded about 781,700 Facebook users on December 2012, with a 13.9% percentage. Libya registered 954,275 Internet users as on June 2012

was around 17.0% of the total population (5,613,380 populations, 2012) (Miniwatts, 2012).

To raise the security awareness among secondary school students there must be a security awareness training program to educate those students about the risks that they may face in their cyber life. The security awareness training program means "the degree or extent to which every member of staff understands the importance of information security, the level of information security appropriate to the organization and their individual security responsibilities, and acts accordingly" (ISF, 2007).

The training has its advantages that cover a wide range of ages and different jobs and attitudes. Herely (2009) in a report of SANS institute fined that the training with different kinds has its effectiveness, when this training is used in a correct way. ISF (2007) defined a security awareness program as "a continuous undertaking aimed at building and sustaining a security- positive environment".

To reduce all the risks that are associated with anticipation of the Internet, there must be a security awareness program that can affect positively on user's behavior generally and secondary school students especially. (NIST 800-16, 1998) defined "the important security awareness program as robust to ensure that people understand their IT security responsibilities, organizational policies, and how to properly use and protect the IT sources entrusted to them" (Wilson et al., 1998).

Veseli (2011) found that security awareness-training program with all different kinds (classroom, discussion based, and web based training style) was an evidence of their effectiveness in increasing the awareness between the participant.

Thus, this study will try to investigate the security awareness among Libyan secondary school students, starting from the necessity of early knowledge about information security, and safety use of new technology. Bintziou et al., (1999) in their paper reported that there is a need to introduce IT-security awareness in secondary school as this age is the ideal age to teach and accept this kind of education. Also, when we compare the age of secondary school students to the first and second year university students, the latter were found already mapped their way of thinking and practicing without caring to the issue of security. Furthermore, the teaching of IT-security to the final year university student is useless. In order to provide the expected results, an information security awareness training program took place in this study.

1.2: Problem Statement

The new source of knowledge that is provided by technology is the Internet. The Internet is a great deal where students can get an open gate toward the world (Wanajak, 2011). When secondary school students start using the Internet in term of education or entertainment, there are problems related to the issue of security that starts to appear regarding their usage habits.

While computer and the Internet provide fast and effective access to information for children' schoolwork, it carries some risks to them (Subrahmanyam et al., 2000). In order to reduce these risks, information security awareness as a phenomenon has raised. It means that one should be aware of the risks of the Internet. Some of these risks can be listed as easy access to illegal sites, sites with violence and sex contents, communication with unreliable people, child abuse and overdependence on games are some of these risks. People who seek support for

illegal things such as drugs or terrorism, use the Internet as a means of propaganda (Tekerek and Tekerek, 2013).

Acquisti and Gross (2006) found that undergraduate students do not have any awareness about the security policy provided by Facebook policy. Furthermore, they do not have any knowledge about security procedures on Facebook as they share their personal information with friends and friends of friends.

Secondary school students have less experience on the effect and the risks that caused by using the Internet. Alhejaili (2013) stated that the Internet can be the ideal place when the secondary school students search for answers and information about anything to help them success. Similarly, the secondary school students face many risks as well as a negative effect on their behaviour when secondary school students change the way of using the Internet as a source of education. Wanajak (2011) the Internet has a negative effect on the mental as well as the health when the students neglect the security procedure.

Through the Internet, children can gain unlimited knowledge and new experience. According to the National Centre for Missing and Exploited Children (NCMEC), one in three teens has experienced online harassment, and one in 25 youths have received an online sexual solicitation. According to bullyingstatistics.org, more than half of adolescents and teens have been bullied online, and about the same number have engaged in cyber bullying; more than 1 in 3 young people have experienced cyber threats online. In this term the author suggests that kids should be encouraged to think carefully about photos uploaded to the Internet (Savage, 2013).

Clara and Calif (2012) reported that teens continue to take risks by posting personal information and risky photos online, without the knowledge of their parents.

Brady (2010) and based on the report of EU Kids online network classifies online risks for children into three categories- content, contact, and conduct. In the same term children are also vulnerable to the security risks that all Internet users encounter.

- Content risks: are referring to those risks that may occur when children are exposed to mass distributed content, such as age inappropriate content, incorrect content, and commercial content.
- Contact risks: that risk which may occur when children are engaged in an online communication, such as undesirable contact and cyber bullying.
- Conduct risks: are referring to risks in which the children are the initiator of content or contact risks. For example, bullying and harassing other children, creating/uploading incorrect or harmful material, and illegal downloads.

There are some difficulties in measuring information security awareness training tools related to secondary school students as well as making a change in their behaviour. Veseli (2011) stated that what crucial not is only educating the users and fulfilment of ISAP (Information Security Awareness Program), but how to measure the effectiveness of the awareness program and make a change in the behaviour.

Having understood the issues, statistics, articles, and studies listed in the above statements, we summarize that there is a tangible need to assess secondary school

students awareness level related to social networking, passwords, and cyberbullying. Moreover, to measure the effectiveness of security awareness training program provided to those students.

1.3: Research Questions

1- What is the best tool available that can be used by secondary school students to educate them about information security issues?

2- How can secondary school students perceive their level of awareness related to social networks, passwords, and cyber-bullying?

1.4: Research Objectives

1- To identify and evaluate available security awareness training tools used for secondary school students.

2- To assess the level of security awareness among secondary school students related to social networks, passwords, and cyber-bullying.

1.5: Scope of the Research

The target group of this research is secondary school students, between the age of 13-18 years old, and have access to the Internet. The secondary school students utilized for this study are Libyan secondary schools that are in Malaysia. The scope of this study includes identifying and evaluating the security awareness training tools provided by the cyber portal of South –East Asia, and assessing secondary school students' awareness level based on social networks, passwords, and cyber-

bullying. A survey questionnaire was employed, and it was divided into two versions "pre-questionnaire and post- questionnaire".

The aim of using pre and post questionnaire is to conduct a training program based on the results of the first objective of this study that was " identify and evaluate the available security awareness training tools" based on the South-East Asia cyber portals. Therefore, the training materials were evaluated by secondary school students via post-questionnaire, and this will give further view in fulfilling the second objective of this research. This study did not develop a model, but an actual security awareness training program took place. The information collected from this study provides a fundamental for future researches related to secondary school students.

1.6: Research Outcome

This work has been presented in "the International Conference on Information Security and Cyber Forensics (InfoSec2014)". The paper titled under "A Second Look at the Information Security Awareness among Secondary School Students". The conference was held at Universiti Sultan Zainal Abidin (UniSZA), Kuala Terengganu, Malaysia during the period of October 8-10, 2014.

1.7: Thesis Structure

The thesis is encompassed of five chapters. Chapter one begins with an overview on the research topic, problem statement, research questions, research objectives, brief about the methodology, and scope of the research. Chapter two, then explores related works of information security awareness. Also, security risks, evaluation, challenges, and successfulness that face security awareness are presented.

Definition of security awareness is also part is this chapter as well as the security awareness training program. Chapter three presents methodology used and the questionnaire that employed in this study. Chapter four presents the results of this study. Finally, chapter five concludes the overall work.