A Second Look at the Information Security Awareness among Secondary School Students

Saida Issa Al-Jerbie and Mohd Zalisham Jali
Faculty of Science & Technology (FST)
Universiti Sains Islam Malaysia (USIM)
Bandar Baru Nilai, 71800
Negeri Sembilan, Malaysia
Cat.asker@yahoo.com
zalisham@usim.edu.my

ABSTRACT

This paper focuses on identifying and evaluating the available security awareness tools, and later presents a study conducted to assess the level of security awareness among Libyan secondary school students covering social networks, passwords, and cyber-bullying. The quantitative methodology is applied via questionnaire in order to assess the students' awareness level. Moreover, qualitative methodology is used in order to observe secondary school students manner and behavior while they are participating in the training program. The targeted group of this study was Libyan secondary school students in Malaysia, and the sample is composed of ten students aged between 13-18 years old. The findings indicated that even the students show a slight level of awareness, but they still lack practicing the information security correctly. Therefore, a study on secondary school students' awareness level, as well as conducting security training program is crucial to avoid security risks.

KEYWORDS

Security awareness - security training - secondary school students - security training tools.

1 INTRODUCTION

New development in the information security raises many responsibilities, and many organizations try 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 make people aware about the challenges that they will face in every day life. Nowadays, The information security awareness become a crucial issue. Although organizations spend high cost to secure their information, the threats still as a big challenge. Peltier [1] 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. The concatenation of information security requests deep view on the principle of information security awareness among different users. Albrechtsen and Hovden [2] stated that what is crucial in the information security execution in an organization is the awareness and the behavior of all kinds of users as execution of the information security awareness will exit the real needs of any organizations in the strength of the security of their sensitive information. The role of information technology- especially the Internet- is not circumscribed to one age group, and because of this explosion on the new smart technology teens are more exposed to the role of the Internet in everyday life. Brady [3] stated that, as the Internet meets an increasingly higher role in the daily lives of our children and as a learning and communication tool, it offers a broad scope of opportunities for people of all ages.

Students (aged 18–24 year olds) are high-risk and attractive candidates for security attacks [4]. From the literature, the researchers found that secondary school students considered as a high security risk as in term of using their passwords [5], and there is a tangible need to highly concern in this age to make the responsibility of security awareness grows with the user behavior, therefore; the age of secondary school students can be the ideal period to fulfil this challenge. In a paper for Bintziou et al., [6] they reported that there is a

need to introduce IT-security awareness at this age because, when comparing the age of the secondary school students with first and second year university students; the second students are already mapped with their way of thinking and practicing without caring to the issue of security.

While computer and Internet provide fast and effective access to information for children's schoolwork, it carries some risks for them [7]. 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 over dependence on games" [8].

Secondary school students have less experience on the effects and risks that maybe caused by using the Internet. Alhejaili [9] stated that the Internet can be the ideal place for the middle school students to search for answers and information about anything in order to help them to success. Alike, secondary school students face many risks as well as a negative effect on their behavior when they change the way of using the Internet as a source of education. Wanajak [10] stated that the Internet has a negative effect on the mental as well as the health, when the students neglect the security procedures.

This study highlighted the security risks that secondary school students may encounter while using the Internet due to lack in the scientific researches that considered with the issue of information security awareness among secondary school students. The three issues discussed in this paper are:

1- Cyber-bullying
2- Social networks
3- Passwords

Three security issues that are 1,2 and 3 were chosen as researchers found them as the most risks for students or even for the organizations.

This paper is arranged as follows; related works are first given, followed by an overview of the methodology that uphold this research. An initial results are provided, followed by a discussion of the particular results. Finally the paper concludes with recommendations for future research in order to promote the security awareness among secondary school students.

2 RELATED WORKS

This section discusses the information security awareness from different perspectives, aims at identifying the clearest view in the principal of information security related to secondary school student.

2.1 Information Security Risks

The vulnerabilities associated with the use of Internet provide many risks to different users; including secondary school students as a group of internet users. They face various risks that cause information lost or any kinds of threat for their personal information. Brady [3] further stated that as the Internet exposes children to wide risks, those children might not have the skills, abilities, and knowledge to control these risks. She reported that what is popular in the Internet usage by children are for playing games, looking up information, social networks, and making new friends.

This section further discusses three risks namely; cyber-bullying, social networks and passwords. A report cited by Smith et al., [11] cyber-bullying can be "Forms of bullying using electronic devices such as mobile phones, emails, or text messages". Cyber bullying is becoming more prevalent with the increased conserving of technology. This report took place in 14 different schools in London, focusing on users aged from 11 to 16 years old. The report employed a quantitative methodology via questionnaire, with some qualitative sections. The authors classify seven types of cyber-bullying as follow:

1- Text message bullying
2- Picture /Video clip bullying (via mobile phone camera)
3- Phone call bullying
4- Email bullying
5- Chat room bullying
6- Bullying through instant messaging
7- Bullying via websites

Alhejaili [9] stated that cyber-bullying is becoming a serious threat which may affect secondary school students negatively. The author also listed different kinds of risks that children may suffer from online services.

Moreover, Alhejaili [9] and Brady [3] added a security risk to the list of content, contact, and conduct risks. As Brady stated that security risks could be applied to children from the nature of the Internet as viruses, spyware, spam, identity theft, disclosure of personal information and phishing. In the same study, the NCTE [12] "National Center for Technology in Education" based in Ireland, conducted a survey on children's use of the Internet. The findings indicated that children have a significant increase in the use of instant messaging, number of children providing personal information, and the use of social networks as daily activities.

Padric [5] showed the risky behavior by the habits of the secondary school students who are concerned with the way of using and sharing their passwords. through online questionnaire sent to students, the results indicated that secondary school students have a high level of risk in term of passwords (both in term of behavior and construction), and the security and /or privacy was high. However, gender did not show any differences.

According to the Internet world state, the rank of young people who use the Facebook in Libya recorded 781,700 Facebook users on December 2012 which form a percentage of 13.9% of the population. Libya registered 954,275 Internet users as on June 2012 that form a percentage of 17.0% of the population (5,613,380 populations, 2012) [13]. In the same term and based on the focusing area of this study, Libyan secondary students expos to the usages of the Internet and the risks that are associated with it.

2.2 Information Security Awareness Training Program

There are many different security awareness training programs that could be categorized based on the need of the respondents and field of the study. The important of conducting the security awareness and training program could be best understood from the next statement, "An awareness and training program is crucial in that it is the vehicle for disseminating information that users, including managers, need in order to do their jobs. In the case of an IT security program, it is the vehicle to be used to communicate security requirements across the enterprise" [14].

Veseli [15] measured the effectiveness of a security awareness program before and after conducting the training. The participants were 327 employees of GUC (Gjovik University College) in Norway. The training was based on different kinds, such as: a classroom-based style, discussion-based group style, and web-based training style. All previous styles were to identify the effective security awareness program. The research found that classroom training based style is the most effective training in improving the knowledge, attitude, and behavior of the responding. Rahman and Hidayah [16] developed a prototype to evaluate information security awareness level for teacher and student in Malaysian secondary school. The purpose of the Prototype is to identify the level of information security awareness based on assessment model. As a result of this research, the prototype is considered effective in evaluating the students' awareness level.

2.3 Evaluation of Information Security Awareness

Padric [5] conducted a research on online threat awareness. The targeted group of this research is secondary school students in Grahamstown. The students were in the grades 8 to 12. The objectives of this research are to determine the actual levels of awareness, and the difference between these levels and self-perceived levels of the participants. The quantitative results showed that secondary school students registered a high level of risks, as they unaware of the online safety and security. These risks could be clearly shown in the information security, online privacy, and indeed online safety. The author proposed that the awareness and education program should not only focus on the concepts, but on the awareness and behavior precisely.

Wanajak [10] discussed the Internet Addiction (IA) as a new academic field. This research takes place in Thai secondary school students in Chiang Mai, Thailand. The sample size was 952 secondary school students. This study focused on finding a definition to (IA) as well as to investigate the spread of the Internet and its

impact on secondary school students. The finding of this study indicated that the IA definition as it is accepted from the Delphi panel "Repetitive Internet use leading to abnormal behavior which causes negative consequences to its users or others in the community in any way, such as psychological, physiological, behavioral, sociological or other important functional impairments". The survey resulted to only 3.7% of Thai secondary school students who are ordered as Internet addiction and they recorded some difficulties with school work, physical, mental health problems and relationship problems. The author proposed that society, governments, schools and parents have to work together to spread the awareness toward changing the behavior of Thai secondary school students. Bayer [17] found that the only way to establish security awareness is by starting education programs as soon as the youth started communicating with computers in early ages. In addition, the study explained the importance of school to improve security awareness among students through focused educational materials to understand the risks of daily practices on the Internet.

Crossler [18] focused on future challenges upon researchers and how to provide the exact way to users ' behavior, understand the hacker policies, and to deal with information security. All of this was tested on four groups' members. As a result of this study, found that culture, fear, improving information security compliance, and unmasking the mystery of the hacker world, all of this will fulfil the future behavioral information security research. From elementary to high school students 2447 investigated by their level of awareness in Turkey. The result was that the rank of awareness was high in ethical issues such as the use of file-sharing sites. On the other hand, they have a low level of knowledge about the role. In this case the authors suggest to have education subjects related to security awareness, education, and related activities to improve student's positive knowledge of how they must use the Internet [8].

2.4 Success of Information Security Awareness

Alhejaili [9] discussed the usefulness of teaching security awareness for secondary school students, his idea, passed on providing an online interactive program to reduce the risks that could affect the middle students. He also stated that there is a need to examine the current state of security awareness among students and their families, and to ensure whether the schools provide an online safety for these students. The finding of this research showed that 94.5% of secondary school students use the Internet and Smartphone and most likely were used to surf the Internet and social media websites. Also, this study showed that 74.5% of middle students use the Internet in term of online gaming or online video gaming. This study found that 58.2% of parents did not use the parents filter. The author suggests that "Netsmartz" and "OnGuardOnline" are a good educational resource as they provide some information and technical tips on how to deal with some kinds of attack. Olusegun and Ithnin [19] applied training in UTM (Malaysia) on 900 students faculty and staff members to assess their awareness after having information security awareness training (ISAF) program. The finding of this study reveals that ISAF program does not address all the needs required by the users which means there is a need to adjust the program to meet their needs.

Pltier [1] discussed the successful element of information security awareness program. Moreover, he addressed the importance of employees in information security in an organization, and how to make security programs related to the variety of audiences. Pliers' results found that security awareness is a process that needs a perfect change in employees' behavior. This has to start from the time of employing any employee, and that has to continue with them every year. In addition, security awareness has to start from childhood, and everywhere in different media.

From the statement above it is clear that there must be a further researching to identify the best tools to apply information security awareness among secondary school students.

The expected tools have to be suitable to the age of these students as well as their needs to straighten security awareness. Measuring the level of security awareness is another issue to be focused in this research as the employees still did not have enough awareness on how to secure their sensitive information. At this point of view, the security awareness has to be started earlier to measure its effectiveness.

2.5 Summary

From literatures, researchers found that there is a tangible need to educate students about security risks associated with Internet usages. The end users "in the case of our study: secondary school students" are the weakest link in the security awareness. As observed from the previous studies, the quantitative methodology is the best tool to assess the level of security awareness [6], [10], [3], [18]. In order to fulfill the expected security awareness, an information security program is essential [1], [15]. Based on these findings, this study uses a questionnaire in order to assess the level of awareness. Moreover, an actual security training program conducted to have a real impact on students' performance.

3 STUDY ON THE INFORMATION SECURITY TRAINING TOOLS

This study aims at identifying and evaluating available security awareness training tools that potentially can be used for secondary school students. In order to achieve this; searching for South East Asia cyber portals and CERTs was conducted. From table 1, it is clear that Malaysia, Singapore, and Brunei already setup a security cyber portal and the majority of South East Asia countries have CERTs as showed in table 2.

Table 1 Available -Non Available Cyber Security Portal

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

Table 2 Available CERT and Security Cyber Portal

Country	Available CERT	No-Security training tools for puplic
Philippine (PH-CERT)	√	√
Thailand (TH-CERT)	√	√
Indonesia (ID-CERT)	√	√
Cambodia (COM-CERT)	√	√
Vietnam (VN-CERT)	√	√
Laos (LAO-CERT)	√	√
Myanmar (MM-CERT)	√	√
Malaysia (My-CERT)	√	√
Singapore (SING-CERT)	√	-
East- Timor	-	√
Brunei (BRU-CERT)	√	-

From the table 1 and 2, it could be concluded that countries with a cyber security portal provide some awareness tools, tips for cyber security, news, as well as contact information for any future emergency case. The available security awareness training tools are shown in table 3.

Table 3 Security Awareness Tools

Cyber portal	Video	Poster	Quiz (Game type)	Newsletter	Screen server
Malaysia (Cyber-safe)	√	√	√	√	√
Singapore (Go safe online)	√	√	√	√	-
Singapore (Cyber-wellness)	-	-	√	√	-
Brunei (Secure verify connection)	√	-	√	-	-

4- STUDY ON THE INFORMATION SECURITY AWARENESS

The study proceeded with evaluating the information security awareness for secondary school students. The quantitative research methodology was used to assess students' awareness, security practices, their personal opinion on security issues, and evaluating security awareness training tools. Data were collected from Libyan secondary school students in Malaysian area by using a survey questionnaire. The scaled data collected from the participants were statistically and descriptively analyzed using SPSS version 20.

Initially, 10 students with mixed gender were selected. To assess the level of awareness, a pre and post questionnaire was applied. Both pre and post questionnaire are the same, the only difference between them is based on the fifth section in the post-questionnaire, this section was designed especially for evaluating the security awareness training tools that occurred from the cyber security portal of South-East Asia. Students are first invited to answer the pre-questionnaire in order to evaluate their current knowledge. Upon completion, they will be invited to listen and participate in training program based on the provided tools of South East Asia cyber portals. After completion of this training, a post-questionnaire was given to them to be answered. Both pre and post questionnaires will be collected, analyzed and compared to assess their awareness level. While participating in the training, the secondary school students were observed regarding their attitudes and manners.

4.1 Training Material

All the training materials are organized in their original source based on four cyber portals "Malaysia (Cyber safe)", "Singapore (Go safe online)", "Singapore (Cyber Wellness)", and "Brunei (Bru-secure verify connection)".

The tools which are used in the training:

- Games
- Videos
- Posters

The objective of these tools is to touch the needs and risks caused by the students, in case if they skip security procedures. A brief about the topics of "Social networks, passwords, and cyber-bullying" was articulated on the secondary school students in order to provide a deeper understanding of the risks associated with them. Within this training, secondary school students are invited to practice each tools from each cyber portal separately. After the students completed the first test, they are requested to answer the post questionnaire as in this version the fifth section focused on evaluating the security awareness material is provided from cyber portals from secondary school students' perspective.

4.2 Data Analysis and Results

The initial results of the study will focus on the main sections of the questionnaire which are:

1- Demographic and general security information.
2- Security practices.

3- Participants' evaluation of the information security awareness training material that was conducted as part of this research.

4.2.1 Demographic and General Security Information

Based on the results observed from the analyses of the initial data, it was found that 20% of the participants were male and 80% were female. The targeted age of the participants was about thirteen years old to eighteen years old (40% fourteen years old, 20% sixteen years old, and 40 % on seventeen years old). In term of grade, 10% were in the eight grade, 30% were in ninth grade, 50% in eleventh grade, and finally 10% were in twelfth grade. The nationality of the participants was 100% Libyan students. The demographical data were the same in both questionnaires.

In part of general security information we asked students about when they starting using social networks. The findings indicated that 30% since one year, 30% since five months, 20% since two months, 10% since two years, and 10% others. For further information, we asked students about how many social networks they have. The findings indicated that 60% of the students have four social networks, 30% have only one, and 10% have three social networks. When asking the students about the kind of social networks they use, it found that- (Facebook, YouTube, What's-App) are the most popular ones.

The negative effects that caused by the wrong usage of technology appears in the form of Cyber-bullying. Based on this study majority 70% of the students are being bullied by text messages while 20% by email.

In the state of asking secondary school students about the kinds of passwords they are using, they indicated that 70% of them use their date of birth as a password, while 30% use only three letters. This finding can be described as they do not care to real dangers of using passwords.

Table 5 Passwords Related Questions "Pre-questionnaire"

How many times did you change your passwords			
Do not change passwords	Once a Month	Once a Year	Twice A year
40%	30%	20%	10%

Secondary school students appear to show a high level of awareness after participated in the training program. The results of the post – questionnaire in the first section showed some of the critical issues. Table 6 lists some students' answers that are obtained from what they have learned from the training program.

Table 6 General Security Information "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
30%	30%	10%	30%
How many passwords do you plan to use for all your accounts?			
One only	Three	One for each	Five
10%	20%	70%	0%
How many times do you plan to change your passwords?			
Once a month	Once a year	Twice a year	I didn't change my password
80%	10%	10%	0%

4.2.2 Personal Opinion

The last section in the pre-questionnaire is asking secondary school students their personal opinion based on some aspects related to the previous mentioned issues. From the results based on the students' personal opinion, it is found that 70% of the students did not care to change their passwords after sharing it with others. 60 % of the students agreed to make new friends via social networks; even they did not know them well. Finally, 50% of the students agree

that cyber- bullying is more dangerous than normal bullying. Moreover, the personal opinion of secondary school students in post questionnaire shows a real attention as 80 % of the students will not bully the bullier and 100% of them will not use the same passwords for all their accounts.

4.2.3 Training Program Tools Evaluation "Post-Questionnaire"

Based on secondary school students' practices on the training program, they required to evaluate the materials based on what they exercised and as these chosen tools were almost for this age especially. From the results, we obtained that games were the most what students like as there was no negative evaluation recorded in every case of the provided countries.

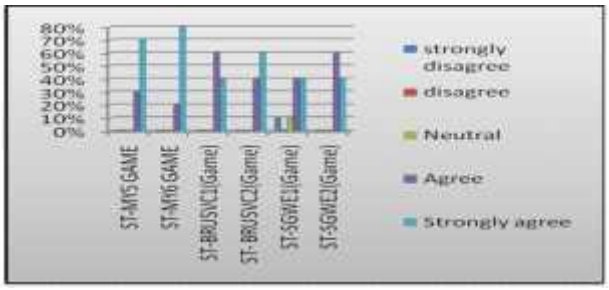

Figure (4. 1) The Evaluation of Training Games

4.3 Discussion

The researchers noticed that the students feel excited when they are asked to participate in this study as they start asking which kind of researches they have to take part in. After giving instructions to them regarding their role as participants, some of them ask "Why we need to answer these questions?". When the students finished answering the pre questionnaire, they sit for a training program.

The security practice is a critical part of how the secondary school students are really aware about security risks, and how they apply their knowledge in their daily life. Based on the students' performance in this section, it is noticed that students did not apply the security rules to avoid any possible risks. Otherwise, secondary school students showed a real positive interaction during the training program as the results from the post questionnaire indicated that there were an enhancement in the level of security awareness and practices. This could be considered as an important outcome of the training program.

In the pre_questionnaire, secondary school students showed a slight level of awareness and that was based on some issues that were discussed in the training program as creating new accounts. In the training program, students were asked to use passwords composed of more than 8 digits long, as well as conforming them by mixing with letters and characters. Furthermore, the post questionnaire showed a high level of awareness as a percentage of 90% of students agreed that posting personal information via social networks is unsafe.

The students interaction was very positive when they start playing the games compared to their case when they watching the videos. Most of the students showed real attention to the subject of the games, and they perform some kind of competition for the games that demanded answering questions. Finally, the post questionnaire given to students. Some of them suffered boredom as they ask "Why we need to answer the same questionnaire for the second time". All students' inquiries were answered by the researchers.

After searching the security awareness tools on South-East Asia, an actual employing to these materials occurred. The posters, videos, games, were conducted in a real security training program for secondary school students.

5 CONCLUSION

Information security requires real works and attention to spread the awareness among different end users. The purpose of a security awareness program can be defined as to have a better understanding of security risks that cause harm and data lost from the end users. This study is designed for secondary school students to offer early awareness on what's required in reducing security risks. Quantitative and qualitative methodology are used in order to fulfil this research objective. Secondary school students were the targeted group of this research aged from 13 to 18

years old. An actual training program took place in order to achieve applicable objectives in enhancing the awareness level between secondary students.

The findings of this study indicated that secondary school students have an acceptable awareness level in ethical issue, such as "the password" have to be more than 8 letters in length, but in the real security practices they use their date of birth as a password. Also, students appeared less awareness on the risks associated with accepting an invitation "Friends request" from people they did not know. Students showed a risky behavior when they answered to "bully the bullier" in case they have been Cyber-bullied. Moreover, some students indicated that they are meeting strangers they had only chatted with them online. The training materials were very useful as the results of the post questionnaire showed an enhancement in the awareness level. From the above statements, we summarized that the level of awareness among secondary school students needs to meet the security practices to avoid security risks. This study is going to cover all the security risks that secondary school students may encounter in the future and this is as a part of future work for this study.

6 REFERENCES

[1] T, R. Pltier. "Implementing an Information Security Awareness Program", CISSP,CISM Information system security, security management practices. Vol - 14, issue 2, page 37-49.May /June 2005.

[2] E. Albrechtsen. & J. Hovden. "Improving information security awareness and b Behavior through dialogue, participation and collective reflection. An Intervention study". Computer & Security. 2010. Vol. 29. pp. 432-445.

[3] C. Brady. 2010. "Security Awareness for Children".

[4] A. Marks. "Exploring universities' information systems security awareness in a changing higher education environment: a comparative case study research". PhD thesis, University of Salford; 2007.

[5] M. Padric. "An investigation of online threat awareness and behaviour patterns amongst secondary school learners". Master thesis. Rhodes university. Dec 2012.

[6] A. Bintziou, N. Alexandris and V. Chrissikopoulos. "Introducing IT- security aw Awareness in schools: the Greek Case". IFIP WG 11.8 st World Conference on Information Security Education WISE1. Citeseer. 1999.

[7] K. Subrahmanyam, R. E. Kraut, P. M. Greenfield and E. F. Gross. "The impact of home computer use on children's activities and development". The future of children.2000. pp. 123-144.

[8] Tekerek, M. and A. Tekerek. "A Research on Students' Information Security Awareness". Turkish Journal of.2013. Vol. 2.

[9] H. Alhejaili. "Usefulness of Teaching Security Awareness for Middle School Students". Rochester Institute of Technology. 2013.

[10] K. Wanajak. "Internet use and its impact on secondary school students in Chiang Mai, Thailand" Edith Cowan University. 2011. Phd thesis.

[11] P. Smith, J. Mahdavi, M. Carvalho and N. Tippett. "An investigation into cyber-bullying, its forms, awareness and impact, and the relationship between age and gender in cyber-bullying". Research Brief No. RBX03-06. London: DfES. 2006.

[12] NCTE. " Watch Your Space Survey: Survey of Irish Teenagers Use of Social Networking Websites". 2008.

[13] Miniwatts Marketing Group. "Internet World Stats". 2012. Available at: http://www.internetworldstats.com/stats.htm http://www.internetworldstats.com/stats5.htm#top. (Date of access, 15/12/2013).

[14] M. Wilson and J. Hash. "Building an Information Technology SecuritAwareness and Training Program". NIST Special publication. 2003. Vol. 800. pp. 50.

[15] I. Veseli. "Measuring the Effectiveness of Information Security Awareness Program". Master thesis. Department of Computer Science and Media Technology Gjøvik University College. 2011.

[16] A. Rahman, & N. Hidayah. "A prototype to Evaluate Information Security Awareness Level for Teacher and Student in Secondary School" Universiti Teknologi Malaysia, Faculty of Computer Science and Information Systems. 2009.

[17] A. Beyer, and C. Westendorf. "How to Establish Security Awareness in Schools". ISSE 2009 Security Electronic Business Processes, Springer: 177-186. 2010.

[18] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin and R. Baskerville. "Future Directions for Behavioral Information Security Research". Computer & Security. 2013. Vol. 32. pp. 90-101.

[19]O. J. Olusegun, & N. B. Ithnin. "People are the answer to security: establishing a sustainable Information Security Awareness Training (ISAT) program in organization". 2013. ArXiv preprint arXiv: 1309.0188.

[20] List of CERTs: (last date of access : 08/09/2014)
" Brunei" http://www.brucert.org.bn/
" Malaysia" http://www.mycert.org.my/en/
" Indonesia" http://www.cert.or.id/beranda/en/
" Philippine" http://www.phcert.org/
" Singapore" https://www.singcert.org.sg/

"Thailand" https://www.thaicert.or.th/about-en.html
"Cambodia" http://www.camcert.gov.kh/
"Vietnam " http://vncert.gov.vn/en/
"Laos" https://www.laocert.gov.la/en/Page-1-
"Myanmar" http://www.mmcert.org.mm/
[21] List of cyber portals:
"Singapore" www.cyberwellness.org.sg
" Singapore" www.gosafeonline.sg
"Malaysia" www.cybersafe.my
"Brunei" http://www.secureverifyconnect.info/svcdev/
"Cambodia" http://secudemy.com/