ESI Preprints **Not Peer-reviewed**

Knowledge of Information Security Awareness and Practices for Home Users: Case Study in Libya

Hamida Asker, (MSc)
Nalut University, Libya
Abdalmonem Tamtam, (PhD)
Nalut University, Libya, Dublin City University, Ireland

Doi: 10.19044/esipreprint.2.2023.p22

Approved: 04 February 2023
Posted: 8 February 2023

Cite As:
Asker H. & Tamtam A. (2023). *Knowledge of Information Security Awareness and Practices for Home Users: Case Study in Libya*. ESI Preprints.
https://doi.org/10.19044/esipreprint.2.2023.p22

Abstract

The abundance of information available through the Internet, mobile applications, and cloud computing has made it convenient for users to access a wide range of information. However, this convenience comes with a cost as this information is constantly at risk of being compromised by cybercriminals and hackers. While the recognition of the potential dangers of information security is increasing in developed countries, in regions like Libya in North Africa, the level of protection for this information is insufficient.

The purpose of this study is to examine the various factors that may influence or affect the users' practice and awareness at home. The investigated factors are policy, behavior, training, knowledge of IT and education. In order to accomplish the goals of this study, a quantitative methodology was implemented. Specifically, a survey was created to assess the correlation between key factors and security awareness and practices in the home environment. The survey attracted 220 respondents and analyzed using Bivariate/Pearson Correlation to determine the relationship between the independent variable and the dependent variable. The result of the study showed that there was a moderate positive correlation between policy, knowledge of IT and education with security awareness and practice, but behavior factor has a low correlation. These results indicated that security

awareness and practice level of employees at home are mostly at the middle level. It is hoped that the present study provides an initial step to focus on security training sessions among higher education employees to reflect new knowledge on the importance of security training to increase the knowledge of information security.
It is hoped that the findings of this study will serve as a starting point for further research and focus on providing security information for public, which will help to reflect new knowledge on the importance of security training and increase awareness of information security.

Keywords: Security awareness, Security practice, Information security, home users

1. Introduction

With the increasing dependence on information systems, it has become clear that the protection of these systems is necessity for every user. Lack of security awareness and practice of the users are the weakest link in information security (Halim et al., 2008). Several studies emphasized the need to increment the security awareness of users within the organization by focusing on policies and procedures referring to technology, as well as, educating the employees on information security by providing training programs to create a security culture among users (Ishak et al., 2014; Fakeh et al., 2012).

It becomes essential to protect information assets from internal threats. However, the threat of the human element in the information systems is considered more important issue in information security. Researches reveal that unintentional security incidents from the insiders often occur, which could cause great devastation to information assets more than outsider attacks. In addition, researchers found that the majority of threats to information system can be attributed to the weak experience and the awareness level of users of how to deal with the internal and external security attacks to information assets (Parsons et al, 2014; Roy, 2010; Colwill, 2009).

The success of information security depends on a suitable information security practice by the end users, the weakness in user security practices constitutes a larger threat to an organization's security more than any weakness in information security, therefore, the biggest challenge in information security are to transform users from the weakest line to the defense line by enhancing security practices (Rhee et al., 2009; Asker and Tamtam, 2020). According to Huang et al., (2011), the users could be the biggest vulnerability in information systems security, even with several

security methods. These methods depend on how the user using them, many studies focus on different angles that can encourage users to follow information security practices

Using of technology is mainly in two locations which are workplace and home. Many programs and initiatives were proposed to improve security awareness among users, most of these initiatives are directed towards organizations while some national programs are directed to home users, this interprets that education about information security occurred more in the workplace rather than the home environment. Few research studies focused on staff security awareness both in workplace and home so there is a strong need to investigate security awareness in these two areas (Talib et al., 2010).
In the present study, the problem is to identify the effect of policy, behavior, knowledge of IT, and education on employees' security awareness and practice level in home. This study focuses on employee's security awareness and practice at home where the employees use Information Communication Technologies ICTs for personal use (Kritzinger and Von Solms, 2010). In this study employees also considered as home user.
In this study, the problem is to identify the effect of policy, behaviour, training, knowledge of IT, and education on employees' security awareness and practice in workplace.

1.1 Study Questions

1. How the factors of policy, behavior, knowledge of technology and education might give influence to the security awareness and practice for users at home?
2. What is the current awareness and practice level of information security among users at home?

2. Related Works

Information Security Awareness of Computer Users (ISA) is critical to determining their security-related behavior in both workplace and home place (Jaeger, 2018). Threats on computer systems continue to be a problem. according to (Edwards, 2015) Home computer users need to be more aware of the malicious attacks that could targeted them. it is a well-known fact that the strength of security is only as effective as its weakest link, and the latter is, more often than not, the end user (Schneier, 2011). In an attempt to counter the threat experienced by end-users, increasing concentration has been directed towards information security awareness, education and information dissemination.

According to a survey on the security perception of beginner users of the internet at (UK), 43% of participants did not understand the threats, where, 38% of the participants did not know how to use security packages,

while, 35% of them did not know how to protect their computers. With the increase number of internet users, the attention to information security awareness and practices have become widely where it covers end users at organizations, as well as, users at home. Furthermore, organizations increase their defense by providing security awareness and practices while the home users left as attractive targets for hackers (Ishak et al., 2014; Furnell and Evangelatos, 2007).

Several initiatives and strategies were proposed to ameliorate information security awareness for end users; most of the initiatives were focused on organizations users, while, a few initiatives were directed to home users (Talib et al., 2010; Kritzinger & Von Solms, 2010; Furnell & Evangelatos, 2007). Home users are prone specifically to be targeted by cyber criminals due to many factors such as, home users are not aware of the risks and threats of using internet, 95% of home users accounts were exposed to internet attacks, one out of 600 (PDF) files that users download from internet contains of malicious software. This reveals that novice users are more likely to face internet security threats due to the lack of security awareness in recognizing the threats and understanding the required protection. The study proposed the e- awareness model that consists of e-awareness portal, and the enforcement component, to improve security awareness of home users through acquaint home users on risks that they could be facing on internet (Kritzinger & Von Solms, 2010).

In their study, Furnell & Evangelatos, (2007) presented important reasons and factors that can make home users more prone to exposure to computer attacks and threats. For instance, by targeting the users that do not have any security awareness about the security risks; they are easy exposed to online scam, as the attackers have realized that it is easier to attacking home users, therefore, we should educate home user on information security awareness. Unlike organization, home users lack the understanding of the significance of security awareness and lack the fiscal resources that are required to provide security awareness programs.

One of the most significant mechanisms that help to secure organizational information assets is through the formulation and application of information security policy.

Security policy is the basis of any security system by defining the strategies of an organization's information security approach through a written document, indicating overall policies of the organization; the policy aims to define employee’s prerogatives and responsibilities in an organization (Doherty et al., 2009).

The importance of human factor in computer security has been presented by (Parsons et al., 2010). Their study focused on the effect of human behavior on providing secure information systems. The authors

presented the impact of individual differences, cognitive abilities, appreciation of risk and personality traits on the behavior of the organizations' employees that affect the information security awareness. The study suggests that security and flexibility are two factors that users need in information systems. However, the best way to improve information security is by improving all information security aspects starting with technical means, information security awareness, security behavior of employees, and establishing security policy in organizations. Endeavor of security awareness is to change behavior, as well as, promote good security practices of users by entrenching the principle of responsibility in employees about their role in protecting information assets. According to (Tsohou et al., 2010; Schultz, 2004) security training is a continuing process and a significant factor to improve security awareness for an organization by increasing employees security awareness, as well as, to comprehend security problems and to confirm that employees are aware about the threats and how to protect their information assets. Prior researches have shown that implementing awareness training program improves security effectiveness.

Nowadays, access to information and proficiency with technology are becoming more important. An inclusive society will increasingly require everybody to have high levels of knowledge and skills. Also, Knowledge of technology is important, as information is organized and communication by using technology so knowledge can change human behavior. By having knowledge, users can act appropriately as they know how to act when something occurs, by making the right decision for a situation, and in the exact time to avoid inappropriate events in the workplace and home place, such as, knowledge of specific technologies that relate to their security and privacy when using the internet, can avoid harm from happening (Fakeh et al., 2012).

Education level merges all security skills and efficiencies from different specializations into the common source of knowledge; in addition, it also provides a foundation of concepts, issues, and principles that produce (IT) security professionals (Wilson & Hash, 2003).

Several studies indicate the necessity of promoting information security education to motivate employee (who are also considered as a home users too) information security awareness, applying security education is significant for organization's security management practices. Education can affect the knowledge of employees while information security education for employees can be applied through campaigns, briefings, discussions, speeches, and seminars that increase information security in an organization (Fakeh et al., 2012; Takemura, 2010; Hight, 2005).

In brief, the above literature, to ensure that information security could be achieved in the home place, there is a sufficient review of literature to

warrant research into the proposed key factors that affect security awareness and practice of employees at home place. These key factors are: policy, behavior, training, knowledge of technology, and education. The conceptual framework for the security awareness and practice present the relation between the factors that are identified and the security awareness and practice. Figure 1 shows the conceptual framework of the factors that influence information security awareness and practices in home place.

As reported by Specops Software in (2020), the United States has seen the highest number of cyber-attacks, with 156 incidents occurring between May 2006 and June 2020. Notably, the year 2018 saw the most attacks, with a total of 30 incidents taking place throughout that year.

One of the most recent cyber-attacks in the United States occurred in May 2020 and was discovered by the National Security Agency (NSA). The agency found that Russian hackers were exploiting a vulnerability in a widely used email server to access sensitive information from American organizations.

The United Kingdom has experienced the second highest number of cyber-attacks after the United States, with 47 significant attacks between May 2006 and June 2020. This includes the large-scale cyber-attacks that targeted the Labour Party's digital platforms during the 2019 general election. India ranks third in the number of significant cyber-attacks, with 23 incidents. In June 2020, India experienced a high-profile attack where malware was used to target nine human rights activists by logging their keystrokes, recording their audio, and stealing their personal information.

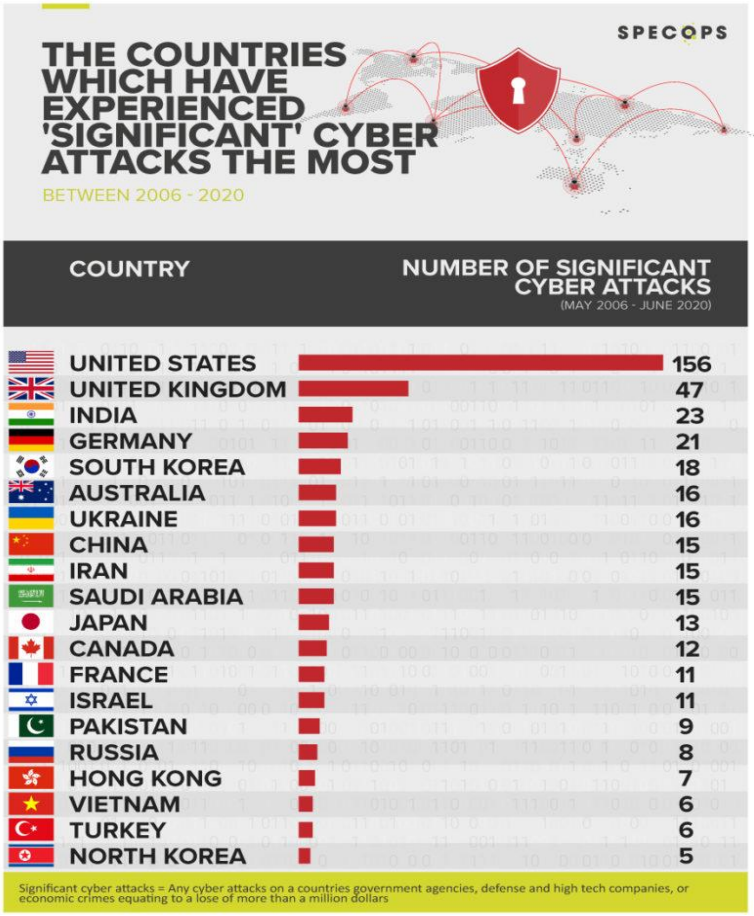

Figure 2. Significant Cyber Attacks Per Country 2006-2020

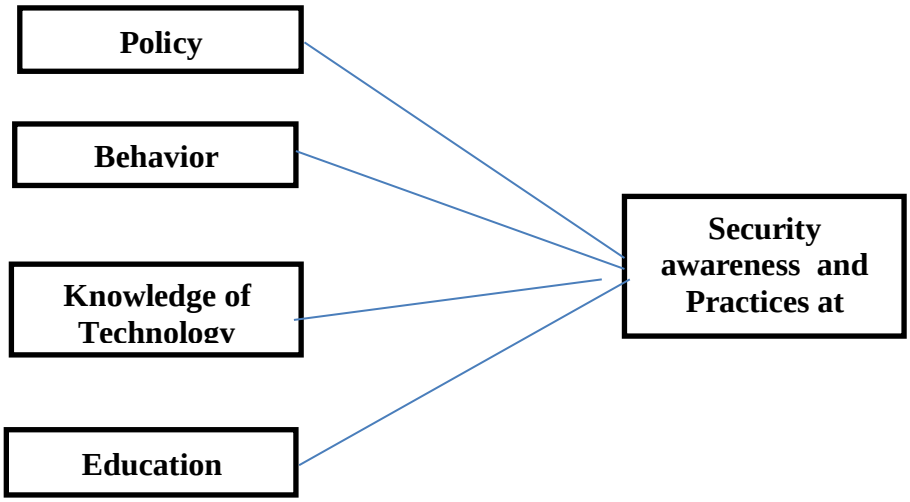

Figure 1. A conceptual framework for the security awareness and practice

3. Methods

The purpose of this study is to identify and describe the relationship between employee's security awareness and practice, dependent variable and to find out the relation between the factors that are defined in the conceptual framework of information security awareness and users' security awareness and practice at the home.

Almost 202 questionnaires collected from the participants from Nalut city, which located at the western end of the Nafusa Mountains in Libya. The survey used a three-point Likert scale with "1 = No, 2 = Not Sure and 3 = Yes". Section 1 obtained information related to the respondents. Section 2 is obtaining information related to security awareness and practices at home. These questions show the level of information security awareness and practice. Section 3 obtained information related to factors that affect information security awareness and practices at home.

4. Findings

The data analyzed using SPSS version 28, the analysis included descriptive and correlations to identify the major factors for evaluating information security awareness and practice for users at home in Nalut area.

4.1 Demographic information

The table below shows the distribution of demographic information, gender, age group, education and job role.

Table 1. Frequencies of demographic information

Demographic factor		Frequency	Percent
Gender	Male	89	44.1%
	Female	113	55.9%
Age Group	Below20	3	1.5%
	20-24	18	24.3%
	25-29	49	34.7%
	30-34	70	33%
	35-39	29	14.4%
	40 and above	33	16.3%
Education Level	Certificate	24	11.9%
	Diploma	70	34.7%
	Bachelor	60	29.7%
	Master	43	21.3%
	PhD	5	2.5%

4.2 Descriptive Analysis

4.2.1 Security Awareness at home

The results of the descriptive statistics to each item of the security awareness at home are presented in table 2.

Table 2. Descriptive Statistics for Security Awareness

Items	Home	
	Mean	±Std. Deviation
I am aware with the vulnerabilities associated with sharing devices.	2.65	.669
I am aware with the encryption that can prevent unauthorized access to confidential information.	2.50	.748
I am aware that it is important to back up my files.	2.67	.648
I am aware that information security is necessary to protect my information.	2.80	.492
I am aware with virus protection software that requires frequent updates.	2.73	.580

Respondents were asked about their security awareness at home by using a Likert scale with "1 = No, 2 = Not Sure and 3 = Yes". Results revealed that the overall mean = 2.67 and standard deviation = 0.62 for home users. The highest mean refers to the statement that I am aware that information security is necessary to protect my information with (2.80) and the lowest mean refers to the statement they were aware with the encryption that can prevent unauthorized access to confidential information with (2.50) this might be due to encryption is the advanced level of security protection procedures.

4.2.2 Security Practice at the home

The results of descriptive statistics to each item of security practice at home are presented in table 3.

Table 3. Descriptive Statistics for Security Practice

Items	Home	
	Mean	±Std. Deviation
I log off my computer whenever I leave it.	2.72	.656
I regularly backup my data.	2.51	.761
I do not download or install unauthorized copies of software.	2.63	.642
I make sure the antivirus software is enabled and updated.	2.64	.663
I use firewall protection	2.67	.640

Respondents were asked about their security practice at home by using a Likert scales of "1 = No, 2 = Not Sure and 3 = Yes". Results revealed that the overall mean = 2.63 and standard deviation = 0.67 for home users. The highest mean score refers to respondents who log off their computer whenever they leave it with (2.72), comes second with use of firewall protection with mean score (2.67) at home. The lowest mean score goes to respondents regularly backup their data with (2.51) for home, this might be due to that in the home backup data is one of the policy and procedures to recover from disaster that could damage information system.

4.2.3 Policy

The results of descriptive statistics to each item for policy at home and are presented in Table 4.

Table 4. Descriptive Statistics for Policy

Items	home	
	Mean	±Std. Deviation
Team related to security is needed.	2.55	.691
I know who to contact if my computer is hacked or infected.	2.61	.698
My computer is configured to automatically update.	2.60	.663
I have policies on which websites I am allowed to visit.	2.26	.854
There are guidelines regarding information security that I can refer to.	2.27	.852

Respondents were asked about the policy at their home by using a three- Likert scales "1 = No, 2 = Not Sure and 3 = Yes". The results revealed that the overall mean = 2.45 and standard deviation = 0.75 for home users, the highest mean refers to who to contact if my computer is hacked or infected (2.61), then computer is configured to automatically update (2.60). The lowest mean refers to policies of the allowed websites to be visited with a mean of (2.26).

4.2.4 Behavior factor

The results of the descriptive statistics to each item of the behavior factor at home presented in table 5.

Table 5. Descriptive Statistics for Behavior

Items	Home	
	Mean	±Std. Deviation
I'll make sure that when I delete a file from the computer or USB stick, that the information is totally removed.	2.65	.645
I feel that my PC is safe.	2.50	.700
I often take information from the office and use a computer at home to work on it.	2.52	.748
I do not share my password.	2.56	.704
I use the same password both for work and home accounts.	2.48	.774

Respondents were asked about their behavior practices in using computers at home by using a three- Likert scales "1 = No, 2 = Not Sure and 3 = Yes". The results revealed that the overall mean = 2.54 and standard deviation = 0.71 for home users. The highest mean refers to that the users will make sure that the information is totally removed when they delete a file from the computer or USB stick with a percentage of (2.65) at home while if they do not share their password at home with (2.56). The lowest mean refers to two statements the users use the same password both for work and home accounts with mean (2.48).

4.2.5 Knowledge of IT

The results of descriptive statistics to each item of knowledge of IT at home presented in Table 6.

Table 6. Descriptive statistics for knowledge of IT factor

Items	Home	
	Mean	±Std. Deviation
I have installed, updated, and enabled, antivirus software on my computer.	2.63	.695
I know what the risk is when opening e-mails from unknown senders; especially if there is an attachment.	2.61	.684
I know what an email scam is and how to identify it.	2.45	.726
I know how to use antivirus software and how to scan for viruses.	2.57	.731

Respondents were asked about their knowledge of IT at home by using a three- Likert scales "1 = No, 2 = Not Sure and 3 = Yes". The results revealed that the overall mean = 2.54 and standard deviation = 0.72 for home users. The highest mean (2.63) for home refers to two statements the users have installed, updated, or enabled, antivirus software on their computers.

The lowest mean score refers to the users' knowledge about what an email scam is and how to identify it with (2.45), this might due to the fact that the users are not familiar with the threats of an email application.

4.2.6 Education

The results of descriptive statistics to each item of education at home presented in table 7.

Table 7. Descriptive statistics for Education

Items	Home	
	Mean	±Std. Deviation
I know what social engineering (phishing) attack is.	2.50	.781
I know what to do if my computer is infected with a virus.	2.56	.697
I never found a virus or a Trojan on my computer.	2.49	.755
My computer has no value to hackers, they do not target me.	2.47	.761
I always download and install software on my computer.	2.64	.641

Respondents were asked about their education at home by using a three- Likert scales "1 = No, 2 = Not Sure and 3 = Yes". The results revealed that the overall mean = 2.53 and standard deviation = 0.72 for home users. The highest mean goes to the users are always download and install software on their computers with (2.64). The second mean goes to two statements if they know what social engineering (phishing) attack is, and if they know what to do if their computer is infected with a virus with (2.56). The lowest mean refers to if the users never found a virus or a Trojan on their computer with (2.50), this may be due to the fact that virus threats are common through using the internet.

4.3 Correlation Analysis

In this study, a Pearson Correlation analysis was conducted to investigate the correlation between the independent variables. (policy, behavior, knowledge of technology and education) and the dependent variables (security awareness and security practice) in home. Correlation analysis used with a statistical method to describe the strength and direction of the linear relationship between two variables (Pallant, 2013). The degree of correlation measures the strength and significance of the relationship between variables. This was done by performing bivariate association and calculating the Pearson Correlation coefficient with significant levels. The Pearson Correlation coefficient can only take on a value within a range of -1 to 1, with -1 indicating a strong negative correlation, 0 indicating no

correlation, and 1 indicating a strong positive correlation. Burn (2000) provides a guide to explain the strength of the relationship between two variables (r) as shown in table 8.

Table 8. Burn Guideline of Correlation Strength

Absolute Value of Correlation Coefficient	Remarks on Correlation (rho)	Nature of Relationship
0.90 - 1.00	Very high correlation	Very strong relationship
0.70 - 0.90	High correlation	Marked relationship
0.40 - 0.70	Moderate correlation	Substantial relationship
0.20 - 0.40	Low correlation	Weak relationship
Less than 0.20	Slight correlation	Relationship so small as to be negligible

Source: Burn (2000)

4.3.1 Independent Variables and Security Awareness at Home

Table 9 represents an outline of the relationships between the independent variables (policy, behavior, education and knowledge of technology) and the dependent variable (security awareness) in home. In general, the results revealed that there are a moderate positive relationship between policy, education, knowledge of IT except behavior has a low positive relationship and the correlation value were (R = .393**)

Table 9. Summary of correlations of variables Policy, Behavior, Education, Knowledge of IT and Security Awareness at Home(Dependent variable) of the study model

Independent variables	Correlation coefficient	Strength of relationship
Policy	.403**	Moderate
Behavior	.393**	low
Education	.526**	Moderate
Knowledge of IT	.518**	Moderate

* Correlation is significant at 0.01 level (2-tailed).

4.3.2 Independent variables and Security Practice at Home

Table 10 represents an outline of the relationships between the independent variables (policy, behavior, education and knowledge of technology) and the dependent variable (security practice) at home. The results showed that there are significant moderate relationships between policy, behavior, education and knowledge of IT with security practice at home.

Table 10. Summary of Correlations of Variables Policy, Behavior, Education, Knowledge of IT and Security Practice at Home (Dependent variable) of the study model

Independent variables	Correlation coefficient ®	Strength of relationship
Policy	.430**	Moderate
Behavior	.472**	Moderate
Knowledge of IT	.541**	Moderate
Education	.602**	Moderate

* Correlation is significant at the 0.01 level (2-tailed)

Information security awareness for home users must be continuously developed through security awareness campaigns and training programs, in order to increase the level of awareness and practices among home users. This will not only help employees to practice proper security behavior in their homes but also increase their IT knowledge.

Conclusion

Technology users have to improve their information security awareness and practice, in order to be more conscious of the need to adopt good security habits in their daily activities. This study reviewed existing knowledge on security awareness and practice and focused on five key factors: policy, behavior, knowledge of IT, and education. A survey instrument was created to gauge the perception of these independent variables and their relationship with the dependent variable. The results of the study indicated that all factors (policy, behavior, education, and knowledge of IT) have moderate positive relationships with security awareness and practice in the home. However, only behavior had a low positive relationship with security awareness at home. Overall, the respondents had a moderate level of security awareness and practice in the home. It is recommended that users should enhance their knowledge of security awareness at home.

References:

1. Asker, H., and Tamtam, A. 2020. "An investigate of the information security awareness and practice level among third level education staff, case study in Nalut Libya" *European Scientific Journal*. Vol. 16. No. 15. pp. 20- 33
2. Colwill, C. 2009. "Human factors in information security: The insider threat–Who can you trust these days?" *Information security technical report*. Vol. 14. pp. 186- 196
3. Doherty, N. F., Anastasakis, L., and Fulford, H. 2009. "The information security policy unpacked: A critical study of the content of university policies". *International Journal of Information Management*, 29(6), pp. 449-457.
4. Edwards, k. 2015. Examining the Security Awareness, Information Privacy, and the Security Behaviors of Home Computer Users. *Thesis Degree of Doctor of Philosophy*, College of Engineering and Computing Nova Southeastern University.
5. Fakeh, S. K. W., Zulhemay, M. N., Shahibi, M. S., Ali, J., and Zaini, M. K. 2012. "Information Security Awareness Amongst Academic Librarians". *Journal of Applied Sciences Research*, 8(3), pp. 1723-1735.

6. Furnell, S., and Evangelatos, K. 2007. "Public Awareness and Perceptions of Biometrics". *Computer Fraud & Security,* 2007. 1, pp. 8-13.
7. Halim, A. Abu Bakar, A. Hamid, H. and Alwi, N. 2008. "A Study of Information Security Awareness Among USIM Staff". Technical Report. USIM.
8. Huang, D. L., Patrick Rau, P. L., Salvendy, G., Gao, F., and Zhou, J. 2011. "Factors affecting perception of information security and their impacts on IT adoption and security practices". *International Journal of Human-Computer Studies*, 69(12), pp. 870-883.
9. Hight, S. D. 2005. "The importance of a security, education, training and awareness program", November 2005. Retrieved on 10 March 2022 from: http://www.infosecwriters.com/text resources/pdf/SETA SHight.pdf.
10. Ishak, I.S., Ishak, I.S., Abu Hassan, R., Suradi, Z., and Mansor, Z. 2014. "Information Security Awareness and Practices In Malaysian IHLs: A Study at UNISEL". *DOI: 10.15224/978-1-63248-034-7-29 Conference: Second Intl. Conf. on Advances in Computing, Electronics and Electrical Technology - CEET 2014, At Kuala Lumpur.*
11. Jaeger, L. (2018, January). Information security awareness: literature review and integrative framework. In *Proceedings of the 51st Hawaii International Conference on System Sciences*
12. Kritzinger, E., and von Solms, S. H. 2010. "Cyber security for home users: A new way of protection through awareness enforcement". *Computers & Security*, 29(8), pp. 840-847
13. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., and Jerram, C. 2014. "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)". *Computers & Security*, 42, pp.165-176.
14. Parsons, K., McCormac, A., Butavicius, M., and Ferguson, L. 2010. " Human factors and information security: individual, culture and security environment". (No. DSTO-TR-2484). *Defence Science and Technology Organization Edinburgh (AUSTRALIA) Command Control Communications and Intelligence Div. Technical Report*
15. Roy Sarkar, K. 2010. "Assessing Insider Threats to Information Security Using Technical, Behavioral and Organisational Measures". *Information Security Technical Report*. Vol. 15. pp. 112-133.
16. Rhee, H. S., Kim, C., and Ryu, Y. U. 2009. "Self-efficacy in information security: Its influence on end users' information security practice behavior". *Computers & Security*, 28 (8), pp. 816-826.

17. Schneier, B. 2011. "Secrets and lies: digital security in a networked world". *John Wiley & Sons.* ISBN. 0-471-25311-1.
18. Specops company 2020. “Which Country Has the Highest Number of Significant Cyber-Attacks”. Retrieved on 10 March 2022 from: https://specopssoft.com/blog/countries-experiencing-significant-cyber-attacks/
19. Schultz, E. 2004."Security Training and Awareness Fitting a Square peg in a Round Hole". *Computers & Security*, 23 (1), pp. 1-2.
20. Talib, S., Clarke, N. L., & Furnell, S. M. 2012. "Establishing A Personalized Information Security Culture". *International Journal of Mobile Computing and Multimedia Communications (IJMCMC), 3*(1), pp. 63-79.
21. Talib, S., Clarke, N. L., and Furnell, S. M. 2010. "An analysis of information security awareness within home and work environments". In Availability, Reliability, and Security, 2010. *ARES'10 International Conference* on (pp. 196-203). IEEE
22. Tsohou, A., Karyda, M., Kokolakis, S., and Kiountouzis, E. 2010. "Analyzing information security awareness through networks of association". In Trust, Privacy and Security in Digital Business (pp. 227-237). Springer Berlin Heidelberg.
23. Takemura, T. 2010."A quantitative study on Japanese workers' awareness to information security using the data collected by web-based survey. *American Journal of Economics and Business Administration*, 2(1), pp. 20- 26.
24. Wilson, M., and Hash, J. 2003."Building an information technology security awareness and training program". NIST Special publication, 800, 50.