ESJ Natural/Life/Medical Sciences

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/esj.2023.v19n15p238

Submitted: 19 January 2023
Accepted: 30 May 2023
Published: 31 May 2023

Cite As:
Asker H. & Tamtam A. (2023). *Knowledge of Information Security Awareness and Practices for Home Users: Case Study in Libya*. European Scientific Journal, ESJ, 19 (15), 238. https://doi.org/10.19044/esj.2023.v19n1p238

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 at 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 users' practices and awareness at home. The investigated factors are policy, behavior, training, knowledge of IT, and education. 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 was analyzed using Bivariate/Pearson Correlation to determine the relationship between the independent variable and the dependent variable. The results of the study showed a moderate positive correlation between policy, knowledge of IT, and education with security awareness and practice, but the behavior factor had a low correlation. These results indicate that the security awareness and practice level of employees at home is mostly at a moderate level. It is hoped that the present study provides

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

an initial step in focusing on security training sessions among higher education employees to emphasize the importance of security training and increase knowledge of information security. It is hoped that the findings of this study will serve as a starting point for further research and a focus on providing security information for the public, which will help disseminate 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 a necessity for every user. The lack of security awareness and user practices is the weakest link in information security (Halim et al., 2008). Several studies have emphasized the need to increase the security awareness of users within the organization by focusing on policies and procedures related to technology. Additionally, educating employees on information security through training programs is crucial to create a security culture among users (Ishak et al., 2014; Fakeh et al., 2012).
It is essential to protect information assets from internal threats. However, the threat posed by the human element in information systems is considered a more significant issue in information security. Research reveals that unintentional security incidents from insiders often occur, which could cause great devastation to information assets compared to outsider attacks. In addition, researchers have found that the majority of threats to information systems can be attributed to the weak experience and awareness levels of users regarding how to deal with internal and external security attacks on information assets (Parsons et al., 2014; Roy, 2010; Colwill, 2009).

The success of information security depends on suitable information security practices by end users. The weakness in user security practices constitutes a larger threat to an organization's security than any weakness in information security. Therefore, the biggest challenge in information security is to transform users from the weakest link to the defense line by enhancing security practices (Rhee et al., 2009; Asker and Tamtam, 2020). According to Huang et al. (2011), users could be the biggest vulnerability in information systems security, even with several security methods in place. These methods depend on how users utilize them. Many studies focus on different approaches to encourage users to adopt information security practices.

Technology usage mainly occurs in two locations: the workplace and home. Many programs and initiatives have been proposed to improve security awareness among users. Most of these initiatives are directed toward

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

organizations, while some national programs are aimed at home users. This indicates that education about information security is more prevalent in the workplace rather than in the home environment. Few research studies have focused on staff security awareness in both the workplace and home, highlighting the strong need to investigate security awareness in these two areas (Talib et al., 2010).

The present study aims to identify the effect of policy, behavior, IT knowledge, and education on employees' security awareness and practice levels at home. This study specifically focuses on employees' security awareness and practice at home, where they use Information Communication Technologies (ICTs) for personal use (Kritzinger and Von Solms, 2010). In this study, employees are also considered as home users.

In this study, the problem is to identify the effect of policy, behavior, training, IT knowledge, and education on employees' security awareness and practice in the workplace.

1.1 Study Questions:

1. How do the factors of policy, behavior, IT knowledge, and education influence security awareness and practice for home users?
2. What is the current level of awareness and practice of information security among home users?

2. Related Works:

Information Security Awareness of computer users (ISA) is critical in determining their security-related behavior in both the workplace and at home (Jaeger, 2018). Threats to computer systems continue to be a problem, as stated by Edwards (2015). Home computer users need to be more aware of the malicious attacks that could target them. It is a well-known fact that the strength of security is only as effective as its weakest link, which is often the end user (Schneier, 2011). To counter the threats faced by end users, there has been an increasing focus on information security awareness, education, and information dissemination.

According to a survey on the security perception of beginner internet users in the UK, 43% of participants did not understand the threats, while 38% of participants did not know how to use security packages. Additionally, 35% of them were unaware of how to protect their computers. As the number of internet users increases, there has been a widespread focus on information security awareness and practices, encompassing both end users in organizations and home users. However, it is worth noting that organizations prioritize enhancing their defense by providing security awareness and practices, while home users are often left as attractive targets for hackers (Ishak et al., 2014; Furnell and Evangelatos, 2007).

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

Several initiatives and strategies have been proposed to enhance information security awareness for end users. Most of these initiatives have focused on organizational users, while a few have been directed toward home users (Talib et al., 2010; Kritzinger & Von Solms, 2010; Furnell & Evangelatos, 2007). Home users are particularly vulnerable to being targeted by cybercriminals due to various factors. For instance, they may lack awareness of the risks and threats associated with internet usage. Shockingly, 95% of home user accounts have been exposed to internet attacks, and approximately one out of every 600 downloaded files from the internet contains malicious software (PDF). These findings indicate that novice users are more likely to encounter internet security threats due to a lack of security awareness in recognizing and protecting against such threats. To address this issue, the study proposed the e-awareness model, which consists of an e-awareness portal and an enforcement component. The model aims to improve the security awareness of home users by familiarizing them with the risks they may encounter on the internet (Kritzinger & Von Solms, 2010).

In their study, Furnell & Evangelatos (2007) presented important reasons and factors that can make home users more prone to computer attacks and threats. For instance, attackers target users who lack security awareness and are more susceptible to online scams. They have realized that attacking home users is easier. Therefore, it is crucial to educate home users about information security awareness. Unlike organizations, home users lack an understanding of the significance of security awareness and often lack the financial resources required to provide security awareness programs.

One of the most significant mechanisms for securing organizational information assets is the formulation and application of an information security policy. The security policy serves as the foundation of any security system by defining the strategies of an organization's information security approach through a written document. It outlines the overall policies of the organization and aims to define employees' rights and responsibilities within the organization (Doherty et al., 2009).

The importance of the human factor in computer security has been highlighted by (Parsons et al. 2010). Their study focused on the impact of human behavior on providing secure information systems. The authors examined the influence of individual differences, cognitive abilities, risk perception, and personality traits on the behavior of employees within organizations, which in turn affects information security awareness. The study suggests that both security and flexibility are crucial factors that users require in information systems. However, the best way to enhance information security is by improving all aspects of information security, starting with technical measures, information security awareness, security behavior of employees, and establishing security policies within organizations. The

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

endeavor of security awareness is to change behavior and promote good security practices among users by instilling a sense of responsibility in employees regarding their role in protecting information assets. According to (Tsohou et al. 2010; Schultz, 2004), security training is an ongoing process and a significant factor in improving security awareness within an organization. It helps increase employees' security awareness, enhances their understanding of security issues, and ensures they are aware of threats and how to protect their information assets. Prior research has demonstrated that implementing awareness training programs improves security effectiveness.

Nowadays, access to information and proficiency with technology are becoming increasingly important. An inclusive society will require everyone to have high levels of knowledge and skills. Additionally, knowledge of technology is crucial as information is organized and communicated using technology, which can influence human behavior. With knowledge, users can respond appropriately to situations, make informed decisions, and take timely actions to prevent inappropriate events from occurring in the workplace and at home. For example, having knowledge of specific technologies related to security and privacy when using the internet can help users avoid potential harm (Fakeh et al., 2012).

The education level merges all security skills and efficiencies from different specializations into a common source of knowledge. Additionally, it provides a foundation of concepts, issues, and principles that shape IT security professionals (Wilson & Hash, 2003).

Several studies indicate the necessity of promoting information security education to enhance the information security awareness of employees, (who are also considered home users). Applying security education is significant for an organization's security management practices. Education can impact employees' knowledge, and information security education can be implemented through campaigns, briefings, discussions, speeches, and seminars to enhance information security within an organization (Fakeh et al., 2012; Takemura, 2010; Hight, 2005).

In summary, based on the existing literature, there is sufficient justification to conduct research on the proposed key factors that influence the security awareness and practice of employees in the home environment. These key factors include policy, behavior, training, knowledge of technology, and education. The conceptual framework for security awareness and practice illustrates the relationship between the identified factors and security awareness and practice. Figure 1 illustrates the conceptual framework of the factors that influence information security awareness and practices in the home environment.

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

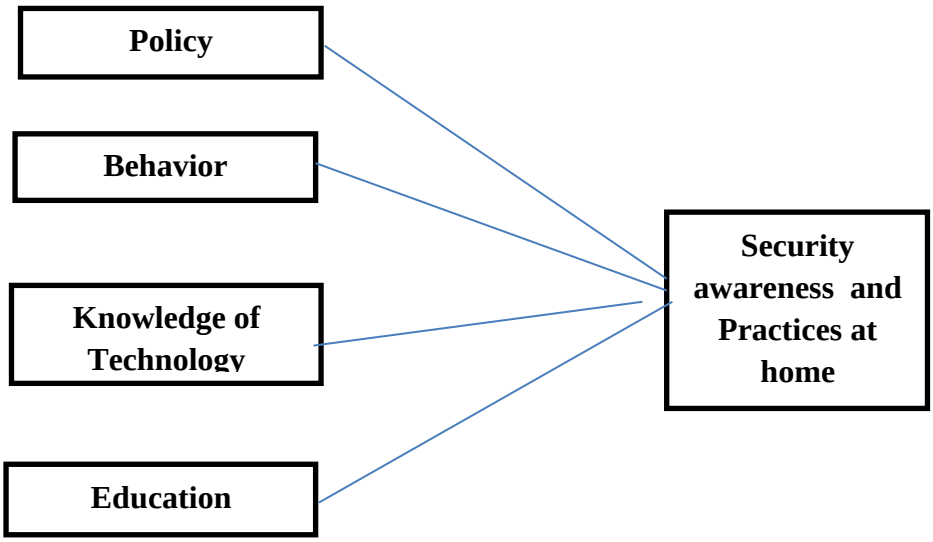

Figure 1. A conceptual framework for security awareness and practice

According to Specops Software's report in (2020), the United States has recorded the highest number of cyber-attacks, with 156 incidents occurring between May 2006 and June 2020. Notably, the year 2018 witnessed 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 happened 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 gain access to 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 digital platforms of the Labour Party during the 2019 general election. India ranks third in the number of significant cyber-attacks, with 23 incidents. In June 2020, India faced 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.

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

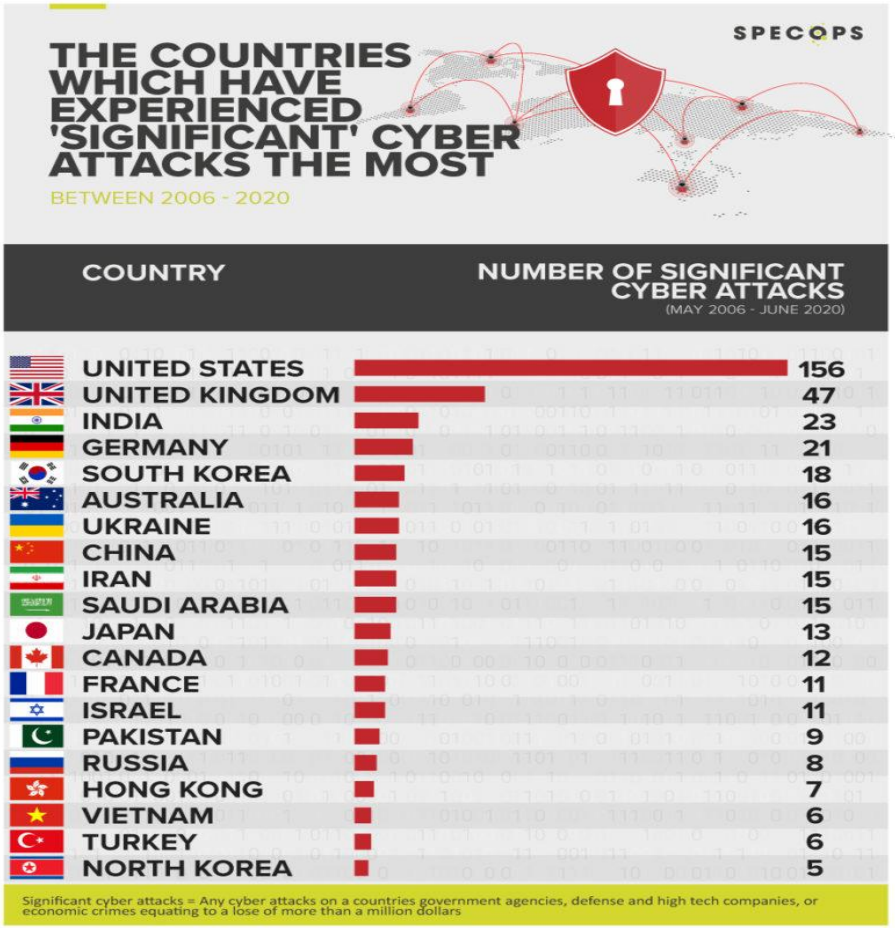

Figure 2. Significant Cyber Attacks Per Country 2006-2020

Methods:

The purpose of this study is to identify and describe the relationship between employees' security awareness and practice, the dependent variable, and to investigate the relationship between the factors defined in the conceptual framework of information security awareness and users' security awareness and practice at home.

Approximately 202 questionnaires were collected from participants in Nalut city, which is located at the western end of the Nafusa Mountains in Libya. The survey utilized a three-point Likert scale, with "1 = No, 2 = Not Sure, and 3 = Yes." Section 1 gathered information related to the respondents, while Section 2 focused on obtaining information about security awareness and practices at home. These questions aimed to assess the level of information security awareness and practice. Section 3 collected information regarding the factors that influence information security awareness and practices at home.

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

4. Findings:

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

4.1 Demographic information:

The table below presents the distribution of demographic information including 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 for each item of security awareness at home are presented in Table 2.

Table 2. Descriptive Statistics for Security Awareness

Items	Home	
	Mean	±Std. Deviation
I am aware of the vulnerabilities associated with sharing devices.	2.65	.669
I am aware of 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 of virus protection software that requires frequent updates.	2.73	.580

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

Respondents were asked about their security awareness at home using a Likert scale with "1 = No, 2 = Not Sure, and 3 = Yes". The results revealed an overall mean of 2.67 and a standard deviation of 0.62 for home users. The statement with the highest mean was "I am aware that information security is necessary to protect my information" with a mean of 2.80. On the other hand, the statement with the lowest mean was "They were aware of encryption that can prevent unauthorized access to confidential information" with a mean of 2.50. This difference may be attributed to the fact that encryption is considered an advanced level of security protection procedures.

4.2.2 Security Practice at the home

The results of descriptive statistics for 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 back up 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 using a Likert scale of "1 = No, 2 = Not Sure, and 3 = Yes". The results revealed an overall mean of 2.63 and a standard deviation of 0.67 for home users. The highest mean score was obtained for the statement "Respondents log off their computer whenever they leave it" with a mean score of 2.72. The second highest mean score was for the statement "Respondents use firewall protection" with a mean score of 2.67. On the other hand, the lowest mean score was obtained for the statement "Respondents regularly backup their data" with a mean score of 2.51 at home. This difference may be due to the fact that in a home setting, backing up data is not considered as crucial as in an organizational context, where it is an important policy and procedure for disaster recovery and protecting information systems.

4.2.3 Policy

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

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

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 policies at their homes using a three-point Likert scale of "1 = No, 2 = Not Sure, and 3 = Yes". The results revealed an overall mean of 2.45 and a standard deviation of 0.75 for home users. The highest mean score was obtained for the statement "Knowing who to contact if my computer is hacked or infected" with a mean score of 2.61. This was followed by the statement "Having my computer configured to automatically update" with a mean score of 2.60. On the other hand, the lowest mean score was obtained for the statement "Having policies regarding the allowed websites to be visited" with a mean score of 2.26.

4.2.4 Behavior factor

The results of the descriptive statistics for each item of the behavior factor at home are 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, 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 behavioral practices in using computers at home using a three-point Likert scale of "1 = No, 2 = Not Sure, and 3 = Yes". The results revealed an overall mean of 2.54 and a standard deviation of 0.71 for home users. The highest mean score was obtained for the statement "Ensuring that the information is completely removed when deleting a file from the computer or USB stick" with a mean score of 2.65. This was followed by the statement "Not sharing their password at home" with a mean

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

score of 2.56. On the other hand, the lowest mean score was obtained for the statement "Using the same password for both work and home accounts" with a mean score of 2.48.

4.2.5 Knowledge of IT

The results of descriptive statistics for each item of knowledge of IT at home are 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 using a three-point Likert scale of "1 = No, 2 = Not Sure, and 3 = Yes". The results revealed an overall mean of 2.54 and a standard deviation of 0.72 for home users. The highest mean score of 2.63 for home users was obtained for two statements: "Having installed, updated, or enabled antivirus software on their computers." On the other hand, the lowest mean score was obtained for the statement "Knowledge about what an email scam is and how to identify it" with a mean score of 2.45. This may be attributed to the fact that users are not familiar with the threats posed by email scams.

4.2.6 Education

The results of descriptive statistics for each item of education at home are 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

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

Respondents were asked about their education at home using a three-point Likert scale of "1 = No, 2 = Not Sure, and 3 = Yes". The results revealed an overall mean of 2.53 and a standard deviation of 0.72 for home users. The highest mean was obtained for the statement "Users always download and install software on their computers" with a mean score of 2.64. The second highest mean was obtained for two statements: "Knowledge about what a social engineering (phishing) attack is" and "Knowledge about what to do if their computer is infected with a virus" both with a mean score of 2.56. The lowest mean was obtained for the statement "Users never found a virus or a Trojan on their computer" with a mean score of 2.50. This may be attributed to the fact that virus threats are common when 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) at home. Correlation analysis is a statistical method used 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 a bivariate association and calculating the Pearson correlation coefficient with significant levels. The Pearson correlation coefficient can range from -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 the home. In general, the results revealed that there is a moderate positive relationship

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

between policy, education, and 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 need to enhance their information security awareness and practice to develop a greater awareness of the importance of adopting good security habits in their daily activities. This study reviewed the existing knowledge on security awareness and practice, focusing on five key factors: policy, behavior, knowledge of IT, and education. A survey instrument was designed to assess the perception of these independent variables and their relationship with the dependent variable. The study findings revealed that all factors (policy, behavior, education, and knowledge of IT) demonstrated moderate positive associations with security awareness

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

and practice in the home. However, only behavior showed a low positive correlation with security awareness at home. Overall, the respondents exhibited a moderate level of security awareness and practice in the home. It is recommended that users 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

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

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

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

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.