ESJ Natural/Life/Medical Sciences Peer-reviewed

Comparative Study of Information Security Awareness and Practice Within Home and Work Environments: Case Study in Libya

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

Doi:10.19044/esj.2024.v20n33p1

Submitted: 16 June 2024
Accepted: 21 November 2024
Published: 30 November 2024

Cite As:
Tamtam A. & Asker H. (2024). *Comparative Study of Information Security Awareness and Practice Within Home and Work Environments: Case Study in Libya*. European Scientific Journal, ESJ, 20 (33), 1. https://doi.org/10.19044/esj.2024.v20n33p1

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 data. 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 potential information security dangers is increasing in developed countries, regions like Libya in North Africa still exhibit insufficient protection levels. The purpose of this study is to compare various factors that may influence or affect users' practices and awareness in home and work environments. Specifically, the factors investigated are policy, behavior, IT knowledge, and education. To achieve the study's goals, a quantitative methodology was employed, and a survey was created to assess the correlation between these key factors and security awareness and practices in home and workplace settings. The survey attracted 220 respondents and was analyzed using statistical methods to determine the relationship between the independent variables and the dependent variables. The results of this study indicate a moderate positive correlation between policy, IT knowledge, and education with security awareness and practice in both home and workplace environments. Only the behavior factor had a low correlation for home users.

These findings indicate that the level of security awareness and practices at home and in the workplace is generally moderate. This study aims to serve as an initial step in emphasizing the importance of security training sessions for employees and highlighting the need to increase knowledge of information security. The findings are intended to inspire further research and focus on providing security information to the public, thereby disseminating new knowledge on the importance of security training and enhancing awareness of information security.

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

1. Introduction

The enhancement and integration of technology into everyday life has had many effects. The economic impact of security breaches is estimated at nearly half a trillion dollars globally (Mamonov, S., & Benbunan-Fich, R. 2018). Information security threats have experienced a significant evolution in terms of volume and nature, shifting from savvy hackers with unerring skills who meticulously organize and crack cybersecurity walls in an attempt to gain financial benefits for their work (Talib et al., 2010). The increasing threats to information systems have brought new solutions that focus on technological means, while research focused on human factors remains limited; hence, researchers have called for more examination in this area (Metalidou et al., 2014).

The human factor has a formidable influence on the success and failure of organizations' efforts to secure and protect their services and information systems. The end-user remains the weakest link with regard to information security. Information security is not solely a technological issue but also a user issue; it is arguably one of the most important requirements in the working day of employees and employers (Kemper, G. 2019; Metalidou et al., 2014).

Albrechtsen (2007) explored users' experience of information security and their personal role in information security work. The main patterns of the study were: (1) users state they are motivated for information security work but do not perform many individual security actions; (2) high information security workload creates a conflict of interest between functionality and information security; and (3) documented requirements of expected information security behavior and general awareness campaigns have little effect on user behavior and awareness. Moreover, the author claims that users consider the user-involving approach to be much more effective for influencing user awareness and behavior. Information security awareness has been used in organizations to promote information security culture by increasing employees' (who are also considered home users) knowledge of information security.

Several organizations have instituted information security awareness programs to ensure their employees are aware of security threats (Kruger & Kearney, 2006). Both academic and commercial communities have given attention to information security awareness in the past few years. Organizations are increasingly acknowledging the significance of their information assets and the development of effective strategies to enhance awareness within the company. This has been further supported by effective corporate governance regulation and legislation (Von Solms and Von Solms, 2006). Successful security practices require management support that defines strategy to implement effective security practices in their organization to protect information assets. Information security represents a considerable concern of organizational management. Security solutions depend on technical aspects as well as appropriate end-user behavior. Employees who are also home users of computing technology are susceptible to security attacks unless they comply with organizational policy, increase their knowledge and education, and undergo training via increased awareness and practice through good information security programs (Asker and Tamtam, 2023).

This paper will conduct a comparative study of employees' attitudes toward the factors that influence security awareness and practice in both workplace and home environments.

1.1 Study Questions:

There is a difference in attitude of the participants on the factors that affect information security awareness of employees in their workplace and home.

2. Related Works:

Attacks and hacks on computer systems and information assets continue to be a problem for employees and home users. Although technological means are used to provide protection for information systems from cyber breaches and threats, there is still a risk from users represented by errors, misuse, defects, misinformation, and damage or loss of information in computer systems. In other words, errors resulting from humans using information systems represent a threat to information security and protection (Khando et al., 2021; Edwards, 2015).

Information security awareness has been used in organizations to promote information security culture by increasing employees' knowledge of information security. Several organizations have instituted information security awareness programs to ensure their employees are aware of security threats (Kruger & Kearney, 2006). Both academic and commercial communities have given attention to information security awareness in recent years. Organizations are increasingly acknowledging the significance of their information assets and the development of effective strategies to enhance awareness within the company. This is supported by successful corporate governance regulation and legislation (Von Solms and Von Solms, 2006).

Unclear and unorganized methodologies in relation to current security awareness approaches and their proposed classifications provide a guide to identify the range of options available to researchers and practitioners when designing their research and practice on information security awareness. On the other hand, home users have various resources to enhance their online threat awareness, and they are provided with supporting information from anti-virus providers, operating system vendors, and government initiatives (Talib et al., 2012; Tsohou et al., 2010). Information security policies (ISPs) are considered to be a significant practice within information security to increase employees' awareness of information security issues (Jaeger, L. 2018). Evidently, the main threats to information security occur due to employees who do not comply with their organization's security policy.

Employees' awareness, beliefs, attitudes, and social norms have important and recognizable effects when it comes to complying with security policies. Information security programs should include all factors that promote employees to comply with security policy, such as beliefs which show positive attitudes towards security policy (Bulgurcu et al., 2010).

It is clear that most threats faced by information systems are due to erroneous user behavior. Several studies in information security have linked information security incidents in organizations with employee behavior, which results from a lack of security awareness in their organizations (Guo, 2013; Lim et al., 2009).

Human behavior varies among individuals, where users' behavior can be influenced by demographic groups. There is a relation between users' security behaviors and their information security awareness level. The success of security in the organization relies on the behavior of employees who administer and maintain information resources; suitable and constructive behavior of employees and system administrators can promote the efficacy of information security (Grant, 2010).

Training in information security awareness is one of the most important factors for improving information security of end users. Training frequency, training method, and training compliance monitoring are all mentioned in the literature as playing a role in security awareness training effectiveness (Quagliata, 2010).

Offering training is one of the factors that increase employees' level of satisfaction. However, employees' training on security risks and measures against attacks should be conducted carefully (Metalidou et al., 2014).

Training programs are significant for disseminating security awareness to users to do their jobs (Bada & Sasse, 2014).

With respect to home users, most training programs are provided in institutions for employees while few programs are concerned with security training for home users (Hammarstrand, J., & Fu, T. 2015).

Additionally, there is an impact of customer knowledge, as presented by Gharaibeh & Zanoon (2013), on the security of E-business, which discussed some security gaps resulting from low levels of customer knowledge in information technology. Most organizations depend on information technology in their work, such as managing records, as technology helps to facilitate daily work through organized information. Knowledge can alter human behavior, and users can behave appropriately when something occurs regarding information security systems.

Integrating awareness of information security into the educational system develops appropriate knowledge among individuals, which will increase the next generation's access to an appropriate background in information security (Hentea et al., 2006).

Security education, training, and awareness (SETA) programs are educational programs designed to develop security awareness among employees to reduce security violations that refer to deficient security awareness. The SETA program could be considered as part of risk management, which determines the security tone for employees by keeping security as a daily activity in their work (Alyami et al., 2024).

Five main factors that have an impact on security awareness and practices were presented in the study of Askar & Tamtam (2020), where the study presented the effects of behavior, policy, training, knowledge, and education on the security awareness and practices of employees in their workplace.

On the other hand, the two researchers presented the impact of these factors on the security awareness and security practices of home users (Asker & Tamtam, 2023). Figure 1 shows the conceptual framework of the factors that influence information security awareness and practices in both workplace and home environments.

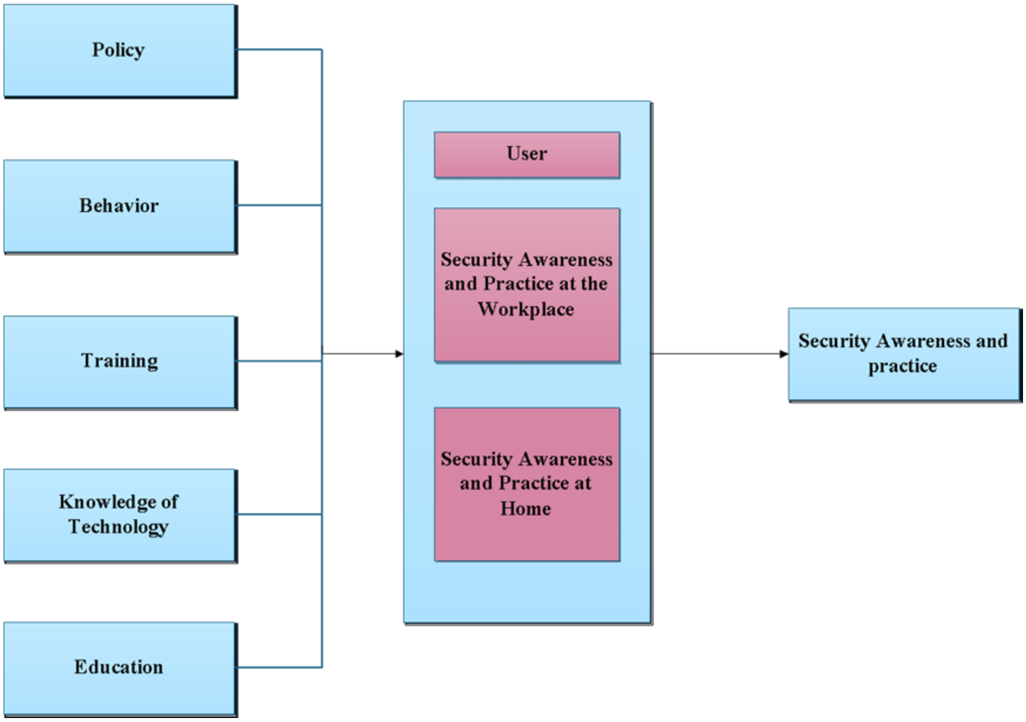
Policy
Behavior
Training
Knowledge of Technology
Education
User
Security Awareness and Practice at the Workplace
Security Awareness and Practice at Home
Security Awareness and practice

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

According to a report by Specops Software in 2020, the United States has witnessed the highest number of cyberattacks, with 156 incidents reported between May 2006 and June 2020. Notably, 2018 marked the peak year for such attacks, with a total of 30 incidents recorded. One of the most recent cyberattacks in the United States occurred in May 2020, detected by the National Security Agency (NSA). The agency uncovered those hackers exploited a vulnerability in a widely utilized email server to access sensitive information from American organizations.

Following the United States, the United Kingdom has faced the second-highest number of cyberattacks, with 47 significant incidents reported between May 2006 and June 2020. This includes large-scale attacks targeting the digital platforms of the Labour Party during the 2019 general election. India ranks third in the number of significant cyberattacks, experiencing 23 incidents. In June 2020, India encountered a high-profile attack where malware was deployed to target nine human rights activists, compromising their keystrokes, recording their audio, and stealing their personal information.

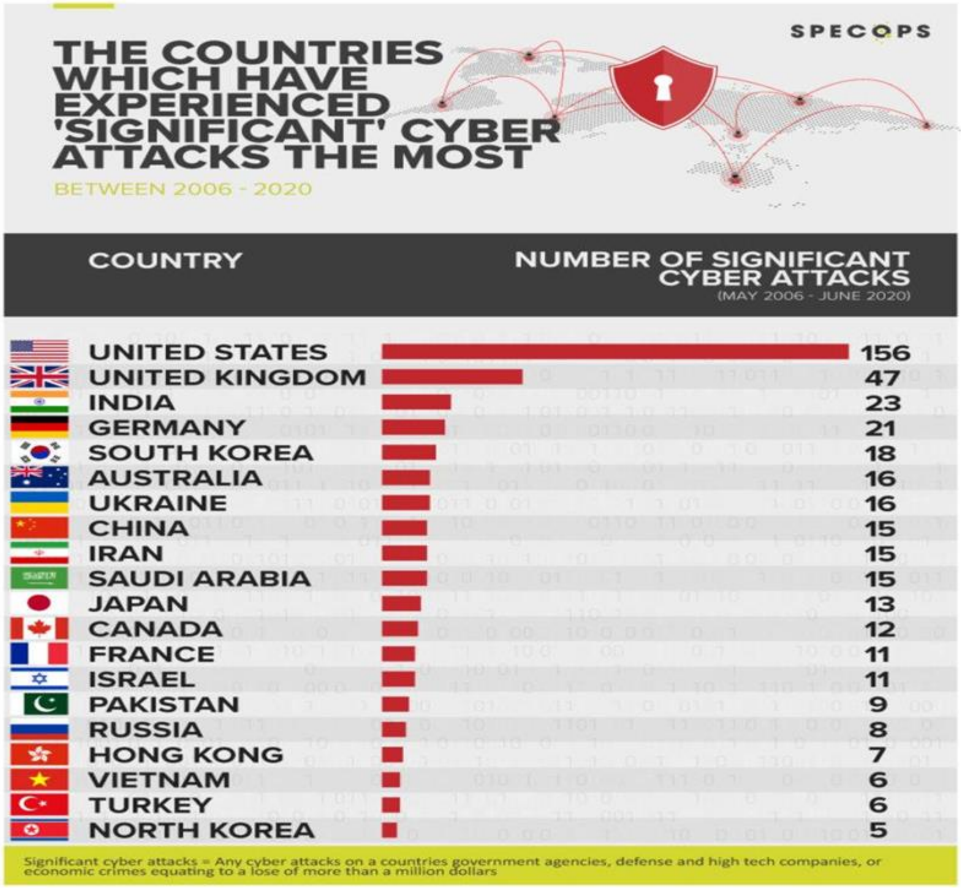

Figure 2: Significant Cyber Attacks Per Country 2006-2020

Methods:

The aim of this paper is to conduct a comparative study, identify and describe the relationship between employees' security awareness and practices at home and in the workplace.

A total of 202 questionnaires were collected from participants in Nalut city, situated at the western end of the Nafusa Mountains in Libya. The survey employed a three-point Likert scale, with responses categorized as "1 = No, 2 = Not Sure, and 3 = Yes."

The questionnaire was divided into three sections:

1. Section 1 gathered demographic information from the respondents.
2. Section 2 focused on acquiring insights into their security awareness and practices, both at home and in the workplace, with questions designed to gauge the level of information security awareness and practice.

3. Section 3 sought to gather information concerning the factors influencing information security awareness and practices in both home and workplace environments.

4. Findings:

The data were analyzed using SPSS version 29 (Bennett et al., 2022). The analysis included descriptive statistics and correlation tests to identify key factors influencing information security awareness and practices among users at home and the workplace in the Nalut area.

4.1 Demographic information:

The table below presents the distribution of demographic information including gender, age group and education.

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

The results of the descriptive statistics for each item of security awareness at home and the workplace are presented in Table 2.

Table 2: Descriptive Statistics for Security Awareness at Home and Work Environments

Items	Home		Workplace	
	Mean	Confidence Interval for Confidence level 95%	Mean	Confidence Interval for Confidence level 95%
I am aware with the vulnerabilities associated with sharing devices.	2.65	2.65 ±0.0923 (±3.5%)	2.62	2.62 ±0.0952 (±3.6%)
I am aware with the encryption that can prevent unauthorised	2.50	2.50 ±0.103 (±4.1%)	2.50	2.50 ±0.103 (±4.1%)

access to confidential information.				
I am aware that it is important to back up my files.	2.67	2.67 ±0.0894 (±3.3%)	2.64	2.64 ±0.0946 (±3.6%)
I am aware that information security is necessary to protect my information.	2.80	2.80 ±0.0678 (±2.4%)	2.75	2.75 ±0.0792 (±2.9%)
I am aware with virus protection software that requires frequent updates.	2.73	2.73 ±0.0800 (±2.9%)	2.81	2.81 ±0.0641 (±2.3%)

Participants were asked about their security awareness at home and workplace using a Likert scale with "1 = No, 2 = Not Sure, and 3 = Yes". The results revealed an overall mean of 2.67 for home and overall mean of 2.66 for workplace. The statement with the highest mean at home was "I am aware that information security is necessary to protect my information" with a mean of 2.80 and Confidence Interval for Confidence level 95% 2.80 ±0.0678 (±2.4%). while in workplace was "I am aware with virus protection software that requires frequent updates" with a mean of 2.81 and Confidence Interval for Confidence level 95% 2.81 ±0.0641 (±2.3%). On the other hand, the statement with the lowest mean was for both environments "They were aware of encryption that can prevent unauthorized access to confidential information" with a mean of 2.50 and Confidence Interval for Confidence level 95% 2.50 ±0.103 (±4.1%).

4.2.2 Security Practice

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

Table 3: Descriptive Statistics for Security Practice at Home and Work Environments

Items	Home		Workplace	
	Mean	Confidence Interval for Confidence level 95%	Mean	Confidence Interval for Confidence level 95%
I log off my computer whenever I leave it.	2.72	2.72 ±0.0905 (±3.3%)	2.67	. 2.67 ±0.0895 (±3.4%)
I regularly backup my data.	2.51	2.51 ±0.105 (±4.2%)	2.51	2.51 ±0.106 (±4.2%)
I do not download or install unauthorized copies of software.	2.63	2.63 ±0.0885 (±3.4%)	2.59	2.59 ±0.0946 (±3.7%)
I make sure the antivirus software is enabled and updated.	2.64	2.64 ±0.0914 (±3.5%)	2.58	2.58 ±0.0960 (±3.7%)
I use firewall protection	2.67	. 2.67 ±0.0883 (±3.3%)	2.62	2.62 ±0.0942 (±3.6%)

Participants were asked about their security practices at home and in the workplace using a Likert scale of "1 = No, 2 = Not Sure, and 3 = Yes." The results revealed an overall mean score of 2.63 for home users and 2.59 for workplace users.

The highest mean score for both environments was observed for the statement: "Participants log off their computer whenever they leave it," with a mean score of 2.72 and a 95% Confidence Interval of 2.72 ± 0.0905 (±3.3%). Conversely, the lowest mean score for both environments was recorded for the statement: "Participants regularly back up their data," with a mean of 2.51 for home users and a 95% Confidence Interval of 2.51 ± 0.105 (±4.2%).

This difference may stem from the perception that data backup is not a critical issue, despite its importance as a policy and procedure for disaster recovery and protecting information systems.

4.2.3 Policy

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

Table 4: Descriptive Statistics for Policy at Home and Work Environments

Items	Home		Workplace	
	Mean	Confidence Interval for Confidence level 95%	Mean	Confidence Interval for Confidence level 95%
Team related to security is needed.	2.55	2.55 ±0.0953 (±3.7%)	2.69	2.69 ±0.0832 (±3.1%)
I know who to contact if my computer is hacked or infected.	2.61	2.61 ±0.0963 (±3.7%)	2.49	2.49 ±0.105 (±4.2%)
My computer is configured to automatically update.	2.60	2.60 ±0.0914 (±3.5%)	2.54	2.54 ±0.0964 (±3.8%)
I have policies on which websites I am allowed to visit.	2.26	2.26 ±0.118 (±5.2%)	2.59	2.59 ±0.0996 (±3.8%)
There are guidelines regarding information security that I can refer to.	2.27	2.27 ±0.117 (±5.2%)	2.56	2.56 ±0.0961 (±3.8%)

Participants were asked about the policy at home and workplace using a Likert scale of "1 = No, 2 = Not Sure, and 3 = Yes" The results revealed an overall mean of 2.45 for home users and mean of 2.57 for workplace. The highest mean score was obtained for the statement "Knowing who to contact if my computer is hacked or infected" for home users with a mean score of 2.61 and Confidence Interval for Confidence level 95% 2.61 ±0.0963 (±3.7%), while the highest mean score was obtained for the statement " Team related to security is needed " for workplace with a mean score of 2.69 and Confidence Interval for Confidence level 95% 2.69 ±0.0832 (±3.1%). 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 and Confidence Interval for Confidence level 95% 2.26 ±0.118 (±5.2%) for home users and “I know who to contact if my computer is hacked or infected” with a mean score of 2.49 and Confidence Interval for Confidence level 95% 2.49 ±0.105 (±4.2%) for workplace.

4.2.4 Behavior factor

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

Table 5: Descriptive Statistics for Behavior at Home and Work Environments

Items	Home		Workplace	
	Mean	Confidence Interval for Confidence level 95%	Mean	Confidence Interval for Confidence level 95%
I’ll make sure that when I delete a file from the computer or USB stick, that the information is totally removed.	2.65	2.65 ±0.0889 (±3.4%)	2.70	2.70 ±0.0851 (±3.2%)
I feel that my PC is safe.	2.50	2.50 ±0.0965 (±3.9%)	2.50	2.50 ±0.0975 (±3.9%)
I often take information from the office and use a computer at home to work on it.	2.52	2.52 ±0.103 (±4.1%)	2.50	2.50 ±0.104 (±4.2%)
I do not share my password.	2.56	2.56 ±0.0971 (±3.8%)	2.59	2.59 ±0.0936 (±3.6%)
I use the same password both for work and home accounts.	2.48	2.48 ±0.107 (±4.3%)	2.51	2.51 ±0.103 (±4.1%)

Participants were asked about behavior factors at home and in the workplace using a Likert scale of "1 = No, 2 = Not Sure, and 3 = Yes." The results revealed an overall mean score of 2.54 for home users and 2.56 for workplace users.

The highest mean score was recorded for the statement: "I’ll make sure that when I delete a file from the computer or USB stick, the information is totally removed." Home users had a mean score of 2.65, with a 95% Confidence Interval of 2.65 ± 0.0889 (±3.4%), while workplace users scored slightly higher with a mean of 2.70 and a 95% Confidence Interval of 2.70 ± 0.0851 (±3.2%).

Conversely, the lowest mean score for home users was observed for the statement: "I use the same password both for work and home accounts," with a mean of 2.48 and a 95% Confidence Interval of 2.48 ± 0.107 (±4.3%). For workplace users, the lowest mean scores were tied between the statements: "I feel that my PC is safe" and "I often take information from the office and use a computer at home to work on it," both with a mean of 2.50 and a 95% Confidence Interval of 2.50 ± 0.0975 (±3.9%).

4.2.5 Knowledge of IT

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

Table 6: Descriptive Statistics for Knowledge of IT Factor at Home and Work Environments

Items	Home		Workplace	
	Mean	Confidence Interval for Confidence level 95%	Mean	Confidence Interval for Confidence level 95%
I have installed, updated, and enabled, antivirus software on my computer.	2.63	2.63 ±0.0958 (±3.6%)	2.62	2.62 ±0.0969 (±3.7%)
I know what the risk is when opening e-mails from unknown senders; especially if there is an attachment.	2.61	2.61 ±0.0943 (±3.6%)	2.56	2.56 ±0.0952 (±3.7%)
I know what an email scam is and how to identify it.	2.45	2.54 ±0.100 (±3.9%)	2.46	2.46 ±0.107 (±4.4%)
I know how to use antivirus software and how to scan for viruses.	2.57	2.57 ±0.101 (±3.9%)	2.62	2.62 ±0.0979 (±3.7%)

Participants were asked about their knowledge of IT at home and workplace using a three-point Likert scale of "1 = No, 2 = Not Sure, and 3 = Yes". The results revealed an overall mean of 2.56 for home users and overall mean of 2.56 for workplace. The highest mean score of 2.63 and Confidence Interval for Confidence level 95% 2.63 ±0.0958 (±3.6%) for home users was obtained for statements: "Having installed, updated, or enabled antivirus software on their computers" and the highest mean score of 2.62 and Confidence Interval for Confidence level 95% 2.62 ±0.0979 (±3.7%) two statements for workplace “I have installed, updated, and enabled, antivirus software on my computer” and “I know how to use antivirus software and how to scan for viruses” On the other hand, the lowest mean score was obtained from the statement for both "Knowledge about what an email scam is and how to identify it" with a mean score of 2.45 with Confidence Interval for Confidence level 95% 2.54 ±0.100 (±3.9%) and 2.46 with Confidence Interval for Confidence level 95% 2.46 ±0.107 (±4.4%). This may be attributed to the fact that participants are not familiar with the threats posed by email scams.

4.2.6 Education

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

Table 7: Descriptive Statistics for Education at Home and Work Environments

Items	Home		Workplace	
	Mean	Confidence Interval for Confidence level 95%	Mean	Confidence Interval for Confidence level 95%
I know what social engineering (phishing) attack is.	2.50	2.50 ±0.108 (±4.3%)	2.52	2.52 ±0.109 (±4.3%)
I know what to do if my computer is infected with a virus.	2.56	2.56 ±0.0961 (±3.8%)	2.52	2.52 ±0.0994 (±3.9%)
I never found a virus or a Trojan on my computer.	2.49	2.49 ±0.104 (±4.2%)	2.51	2.51 ±0.100 (±4.0%)
My computer has no value to hackers, they do not target me.	2.47	2.47 ±0.105 (±4.2%)	2.44	2.44 ±0.106 (±4.3%)
I always download and install software on my computer.	2.64	2.64 ±0.0884 (±3.3%)	2.63	2.63 ±0.0906 (±3.4%)

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 2.49 for home users and a mean of 2.63 for workplace. The highest mean was obtained for the statement "Users always download and install software on their computers" with a mean score of 2.64 with Confidence Interval for Confidence level 95% 2.64 ±0.0884 (±3.3%). The lowest mean for both was obtained for the statement "My computer has no value to hackers; they do not target me " with a mean score of 2.47 for home with Confidence Interval for Confidence level 95% 2.47 ±0.105 (±4.2%) and mean 2.44 with Confidence Interval for Confidence level 95% 2.44 ±0.106 (±4.3%) for workplace. This may be attributed to the fact that users think that only computers with high values are hacked and targeted.

4.3 Correlation Analysis

Pearson correlation analysis was used to explore the relationships between the independent variables (policy, behavior, knowledge of technology, and education) and the dependent variables (security awareness and security practice) in both home and workplace settings. Correlation analysis is a statistical method used to describe the strength and direction of the linear relationship between two variables (Mukaka, 2012). The degree of correlation measures the strength and significance of the relationship between the variables.

This analysis was conducted by performing a bivariate association and calculating the Pearson correlation coefficient, including significance levels. The Pearson correlation coefficient ranges from -1 to 1, where -1 indicates a strong negative correlation, 0 indicates no correlation, and 1 indicates a strong positive correlation. Burn (2000) provides guidelines for interpreting the strength of these relationships (r), as summarized 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 and the Workplace

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 and workplace. In general, the results revealed that there is 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 and the Workplace (Dependent variable) of the study model

	Home		Workplace	
Independent variables	Correlation coefficient	Strength of relationship	Correlation coefficient	Strength of relationship
Policy	.403**	Moderate	.650**	Moderate
Behavior	.393**	low	.639**	Moderate
Education	.526**	Moderate	.605**	Moderate
Knowledge of IT	.518**	Moderate	.566**	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 and workplace. 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 and Workplace (Dependent variable) of the study model

	Home		Workplace	
Independent variables	Correlation coefficient	Strength of relationship	Correlation coefficient	Strength of relationship
Policy	.430**	Moderate	.616**	Moderate
Behavior	.472**	Moderate	.601**	Moderate
Education	.602**	Moderate	.569**	Moderate
Knowledge of IT	.541**	Moderate	.532**	Moderate

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

To enhance information security awareness in both home and workplace environments, users must be continuously developed through security awareness campaigns and training programs. These initiatives aim to elevate the level of awareness and improve security practices. As a result, employees will not only adopt proper security behaviors at home but also expand their IT knowledge.

Conclusion

Technology users need to enhance their information security awareness and practices to recognize the importance of adopting good security habits in their daily activities. This study reviewed existing knowledge on security awareness and practices at home and in the workplace, focusing on four key factors: policy, behavior, IT knowledge, and education. A survey instrument was designed to assess perceptions of these independent variables and their relationship with the dependent variable.

The findings revealed that all factors—policy, behavior, education, and IT knowledge—showed moderate positive associations with security awareness and practices in both home and workplace settings. However, behavior demonstrated only a low positive correlation with security awareness at home. Overall, participants exhibited a moderate level of security awareness and practices in both environments.

It is recommended that users further enhance their knowledge and adoption of security practices, both at home and in the workplace.

Conflict of Interest: The authors reported no conflict of interest.

Data Availability: All data are included in the content of the paper.

Funding Statement: The authors did not obtain any funding for this research.

Declaration for Human Participants: This study followed the Ministry of Higher Education in Libya and its Guidelines for Research Ethics Involving Human Subjects. The study was approved by the Faculty of Education at Nalut University, Libya.

References:

1. Albrechtsen, E. 2007. A qualitative study of users' view on information security, Computers & Security, Volume 26, Issue 4, Pages 276-289.
2. Alyami, A., Sammon, D., Neville, K. and Mahony, C., 2024. Critical success factors for Security Education, Training and Awareness (SETA) programme effectiveness: an empirical comparison of practitioner perspectives. *Information & Computer Security*, *32*(1), pp.53-73.
3. 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
4. Asker, H., and Tamtam, A. 2023. Knowledge of Information Security Awareness and Practices for Home Users: Case Study in Libya. *European Scientific Journal*. Vol. 19. No. 15. P. 238
5. Bada, M., and Sasse, A. 2014. Cyber security awareness campaigns: Why do they fail to change behaviour? Global Cyber Security Capacity Centre, University of Oxford: Oxford, UK
6. Bennett, K., Heritage, B. and Allen, P., 2022. *SPSS Statistics: A Practical Guide 5e*. Cengage AU.
7. Bulgurcu, B., Cavusoglu, H. and Benbasat, I., 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness". *MIS quarterly*, pp.523-548.
8. Burn, R.B., 2000. Introduction to research method. Australia: Longman
9. Edwards, k. 2015. Examining 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.
10. Gharaibeh, N. and Zanoon, N. 2013. The impact of customer knowledge on the security of e-banking. *International Journal of Computer Science and Security (IJCSS)*, *7*(2), p.81.

11. Grant, G. J. 2010. Ascertaining the relationship between security awareness and the security behavior of individuals. Nova Southeastern University. Retrieved from ProQuest Dissertations and Theses, UMI Number: 3423144
12. Guo, K.H. 2013. Security-related behavior in using information systems in the workplace: A review and synthesis. Computers & Security, Vol. 32, pp 242-251.
13. Hammarstrand, J. and Fu, T., 2015. Information security awareness and behaviour: of trained and untrained home users in Sweden.
14. Hentea, M., Dhillon, H.S. and Dhillon, M., 2006. Towards changes in information security education. *Journal of Information Technology Education: Research*, *5*(1), pp.221-233.
15. Hight, S. D. 2005. The importance of security, education, training and awareness program. November 2005. Retrieved on 10 March 2022 from: http://www.infosecwriters.com/text resources/pdf/SETA SHight.pdf.
16. Jaeger, L. 2018. Information security awareness: literature review and integrative framework. In *Proceedings of the 51st Hawaii International Conference on System Sciences*
17. Quagliata, K. 2010. Impact of Security Awareness Training Components on Security Effectiveness". Research Findings Federal Information Systems Security Educators' Association (FISSEA) Annual Conference National Institute of Standards and Technology.
18. Kemper, G. 2019 Improving employees' cyber security awareness, Computer Fraud & Security. Volume 2019, Issue 8, Pages 11-14.
19. Khando, K. Shang, G. Sirajul, M. I., and Ali, S., 2021. Enhancing employees information security awareness in private and public organisations: A systematic literature review. Computers & Security, Volume 106, 102267, ISSN 0167-404
20. Kruger, H.A., Kearney, W.D., 2007. A prototype for assessing information security awareness. Computers & Security, Volume 25, Issue 4, Pages 289-296.
21. Lim, J.S., Chang, S., Maynard, S. and Ahmad, A. 2009. Exploring the relationships between organizational culture and information security culture". In – 7th Australian Information Security Management Conference. Australia.
22. Mamonov, S. and Benbunan-Fich, R. 2018. The Impact of Information Security Threat Awareness on Privacy-Protective Behaviors. Computers in Human Behavior. 83, 32-44. https://doi.org/10.1016/j.chb.2018.01.02
23. Metalidou, Efthymia & Marinagi, Catherine & Trivellas, Panagiotis & Eberhagen, Niclas & Skourlas, Christos & Giannakopoulos, Georgios.

2014. The Human Factor of Information Security: Unintentional Damage Perspective. Procedia - Social and Behavioral Sciences. 147. 10.1016/j.sbspro.2014.07.133.

24. Mukaka M. M. 2012. Statistics corner: A guide to appropriate use of correlation coefficient in medical research. *Malawi medical journal : the journal of Medical Association of Malawi*, *24*(3), 69–71
25. 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/
26. Schultz, E. 2004. Security Training and Awareness Fitting a Square peg in a Round Hole. *Computers & Security*, 23 (1), pp. 1-2.
27. 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.
28. 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
29. 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.
30. Von Solms, R, and Von Solms S.H. (Basie), 2006. Information security governance: Due care. Computers & Security, Volume 25, Issue 7, Pages 494-497.