Journal of Theoretical and Applied Information Technology
30th September 2020. Vol.98. No 18

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

INFORMATION SECURITY AWARENESS BEHAVIOR AMONG HIGHER EDUCATION STUDENTS: CASE STUDY

[1]NAHIL ABDALLAH, [2]ODEH ABDALLA, [3]HAMZAH ALKHAZALEH, [4]AMER IBRAHIM

[1,3,4,] School of Engineering and Technology, Aldar College University, UAE

[2]Department of Fundamentals Religion, An-Najah National University, Nablus, Palestine

[1]nahilabed@aldar.ac.ae, [2]Odeh72@najah.edu, [3]Hamzah@aldar.ac.ae, [4]amer@aldar.ac.ae

ABSTRACT

The exchange of information is a key factor in the daily use of technology. Studies in computer security education, awareness-raising, and training among college students are limited. Most of the research focuses on computer security standards and guidance in organizational contexts. Few studies have analyzed the predictors of the adoption of computer security practices by college students. The objective of this research is to explore information security awareness among higher education students and exam key variables that are influencing this behavior. A total of 180 questionnaires were collected from undergraduate students at Aldar University College and analyzed using the Structural Equation Modelling (SEM) technique. The findings revealed that perceived usefulness, subjective norms, self-efficacy, and the quality of the security system are found to have an important effect on student behavioral awareness of security. The findings of this research will help to develop a clear understanding of the factors that affect students' security awareness behavior. The findings of the study can be used to either refute or strengthen the theories or framework that has been adopted. The findings might also contribute to the literature on security behavior and awareness in general. Findings suggest that the proposed research model is a valuable model for predicting students' attitudes towards information security and that their motivation is influenced by education in security awareness and understanding the severity of such issues. Moreover, the outcome of this research will lead to more awareness programs that can be used to promote privacy and security protection behaviors of information security.

Keywords: *Security Usefulness, Self-Efficacy, Subjective Norms, Security System Quality, Security Awareness.*

1. INTRODUCTION

The prompt growth of computer technology and networking has evolved in every aspect of our life. People rely on computers for everyday tasks more than ever for their personal, educational, and business purposes. Changes in information and communication technology (ICT) and particularly their confluence have raised several concerns connected with the protection of organizational information assets [1]. The information assets of organizations today are largely electronic. This electronic information is processed using information systems, which extensively communicate via private networks and the Internet. The high level of connectivity and access to sophisticated hacking tools, the huge growth in electronic commerce, and other factors have given the dark side of technological development an unprecedented opportunity to flourish and thrive. Computer virus attacks and spyware and computer system security breaches occur almost daily. Keeping computers secured is becoming increasingly difficult [2]. Broucek and Turner [3] stated that "in the age of hacktivism, malware, and cyber-warfare, an increasing number of publications are being produced by computer security specialists and systems administrators on technical issues arising from illegal or inappropriate on-line behaviors". These events have severe consequences on society and the economy including academia.

Security of computers has become an issue of primary importance as the number and types of information security attacks gradually occur as

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

witnessed by the increasing number of security breach incidents such as the spread of computer viruses, and hackers' invasion of proprietary network sites. With over one billion people connected worldwide to the Internet, the way people learn, interact, and communicate has had a revolutionary impact. [4]. According to Solms and Niekerk, [5], information security is defined as "the tasks of guarding the information that is in a digital format typically manipulated by a microprocessor, stored on a magnetic or optical storage device, and is transmitted over a network". Information security is meant to secure information of high importance to individuals and organizations to prevent data theft. Information security involves any process, activity, or task that protects the confidentiality, integrity, and availability of information [6].

Recent developments in network resources, personal computers, and multimedia applications indicated the development and implementation of new and innovative teaching strategies. Internet is used increasingly for educational purposes [7]. Computer technologies have become major components of the campus environment and the college experience. Students regularly use the Internet at schools, computer laboratories, libraries, and community centers. Most of them access library catalogs, online databases, and other academic resources to complete a wide range of academic tasks. Many institutions are requiring students to have computers to take advantage of Web-accessible classrooms by incorporating ICT courses into their curriculum. The advantages of incorporating advanced technologies into instruction are more efficiently accomplishing new or existing tasks and, preparing students for the job market as well as enhancing productivity [8]. Along with information technology (IT) development, however, is the increasing number of unethical acts that have been observed throughout the world. It has been realized that information security is not just a technology problem [9]. The security threats can affect the behavior and perception of IT users [10]. Information security includes both people and technology, and it is becoming more and more obvious that "the human factor is the Achilles heel of information security" [11].

Literature shows that the development of information security remains uncertain and a complicated process to protect personal and vulnerable information from cyber-attacks. Numerous sophisticated methods of security have been developed but the security of information is declining [12]. Regardless of how well designed, protection measures are applied and used by individuals. Solutions in technology are important but not sufficient [13]. Security quality often depends on individuals' successful behavior [14].

The Internet offers students fast access to numerous sources of information. Students always use the Internet for personnel purposes and not only for their academic purposes such as keeping in touch with their friends via e-mail, chatting, and blogs. It is not clear whether students' are security-aware. Nor is it clear what part security awareness plays in motivating students into practicing good security behavior [15]. Based on Moallem [16], college students are not aware of how to protect their data, although they believe they are being observed when using the Internet and that their data are not even secure on university systems. Students cannot secure their systems against security threats when browsing the Internet and thus lead to illegal access to their personal information or identity theft. With this explosion of use, information and computer security are becoming significant subjects [17]. People do not think that they are at risk and often fail to recognize security risks. The absence of security education can be blamed for the lack of awareness amongst students. Students have to understand security threats, the damages that these threats can cause, and also methods on how to mitigate these damages if it occurs [18]. Behavior toward the security of information is increasingly being paid attention, especially when they use security technologies that have failed to protect businesses against cyber-attacks [19]. Therefore, this study was incepted to build on what was found in past studies in achieving the objectives of the study wherever possible. By investigating critical factors in the local context, the study attempts to fill a gap in the individual country-level security awareness research. Hence, the objective of this empirical study is to examine information security awareness behavior among university students.

2. INFORMATION SECURITY AWARENESS

Information is defined as a resource, commodity, perception of pattern, and constitutive force in our lives. The information has some characteristics that make it valuable to its owner and its intended users. However, in any case, information security ensures that the information is not accessed, used, disclosed, disrupted, modified, seen, recorded, or destructed

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

by an unauthorized entity. Security awareness is an often-overlooked factor in an information security program. While organizations expand their use of advanced security technology and continuously train their security professionals, very little is used to increase the security awareness among the normal users, making them the weakest link in any organization [20].

It is vital that organizations have a security awareness program in place to ensure employees are aware of the importance of protecting sensitive information, what they should do to handle information securely, and the risks of mishandling information. Employees' understanding of the organizational and personal consequences of mishandling sensitive information is crucial to an organization's success

Information security awareness according to [17] has been used in different contexts and this diversity at times frustrates information security researchers, practitioners, and security managers. Some believe Information security awareness is only seeking and directing the attention of individuals to information security and that they should be concerned about it, while others believe that it is not just a matter of directing but it is also ensuring compliance of the individuals. Despite the understanding that awareness is important, it is not beyond doubt whether a clear message is being communicated to users in the first place. With all this emphasis on awareness, the question one has to ask is: are security measures being implemented?

3. RESEARCH DESIGN AND METHODOLOGY

Gray [21] defines research design as "a strategic plan for a research project, setting out the broad structures and features of the research". A research design is a master plan specifying the methods and procedures for collecting and analyzing data. According to Sekaran [22], a research design involves a series of decision-making choices regarding the purpose of the study, research strategy, study setting, type of investigation, the extent of researcher interference, time horizon, data collection methods, sampling design, unit of analysis, measurement and data analysis.

The research design applied in this study is quantitative design whereby instruments are developed and data are collected. The quantitative study is based on testing the theory comprises of variables measured with numbers and analyzed with statistical procedures [23]. It involves obtaining information directly from participants using a questionnaire or interview. Normally, surveys are selected for several purposes. Among the two most common purposes are, to enhance the body of theoretical and conceptual knowledge of the discipline concerned based on the empirical data obtained. Secondly, the survey research design can generalize a population based on the samples of the study. Inferences can be made on the behavior and characteristics of the population.

The first part of the survey focuses on the background information of respondents namely: gender, age, and faculty. The respondents are asked in the second part of the questionnaire to indicate how much they agree on the criteria items on a scale of '1' (strongly agree) to '5' (strongly disagree). It is significant to state that the instruments of this study do not contain any common method biases since the survey instruments are adapted from previous studies and modified to suit the context of the present study. Respondents are university students. Pilot testing was done before the actual survey to ensure item reliability and validity. Cronbach's Alpha is used to test the reliability of the questionnaire; it showed very strong reliability at 0.812. A convenience non-probability sampling method is used.

The population for this study consisted of undergraduate students from Aldar University College in Dubai. The study involved all faculties within the main campus. The sampling method that is used in this study is cluster random sampling. The population in cluster samples is distributed into groups or units, called strata that must be representative of the study population. It means that they should represent the heterogeneity of the population that is studied and they should be homogeneous among them. The sample was drawn from the clusters.

Similarly, the sampling size refers to the number of selected subjects. It is the actual number of respondents chose as a sample to represent the population characteristics, the decision to select the size of the sample will depend on certain characteristics. These characteristics are the variability in the population, precision or accuracy needed, desired confidence level, and type of sampling design [22]. Several rules of thumb for the minimum sample size of structural equation models have been proposed. A widely-accepted

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ratio of a sample size to estimate parameters is N:p = 5:1 [24].

"A ratio of five responses per the parameter is required to obtain a trustworthy estimation". With a total of 22 elements, the effective sample size required to test the trustworthiness of the model would be 110. However, Hair et al.,[25] stated that "a sample size exceeding 400 to 500 becomes too sensitive as almost any difference is detected, making all goodness-of-fit measures indicate a poor fit". The study sample is drawn from that part of the population, which is close to hand. A total of 195 students participated in the study, with 180 valid questionnaires, a high response rate of 92% is achieved. "The research model and hypotheses are to be examined through the analysis of data extracted from various questionnaires using structural equation modeling (SEM). SEM is a very powerful analytical technique, which has been used by many researchers".

3. RESEARCH FRAMEWORK AND RESEARCH ITEMS

To develop the theoretical framework for the study, several theories and frameworks have been reviewed. The study extends prior research on IT adoption by offering a conceptual model of constructs that synthesized multiple components theoretical perspectives such as the information systems success model and technology acceptance model. The reason for this integration of different theoretical models were the complexities of the organizational and social the context within which students with varying individual personality traits make up their decision in using e-learning systems. Thus, this study contributes to future research that will be developed, synthesizing different theoretical models. The main contribution of this study is the establishment of an empirically based which consists of various variables which include subjective norms, self-efficacy, system quality, and Perceived usefulness of computer security (Figure 1). The justification for the selection of the dimensions or factors is based on, TAM, IS success model, and the various models presented in the literature. The central focus of the model is on information security behavior.

To further discuss the model development, all the independent and dependent variables are operationalized and dimensions for each concept are to be identified. Leedy and Ormrod [26] defined a variable as any quality of characteristics in a research investigation that has two or more possible values. Creswell [27] further categorized the variables into different groups: independent, dependent, intervening, moderating, control, and compounding.

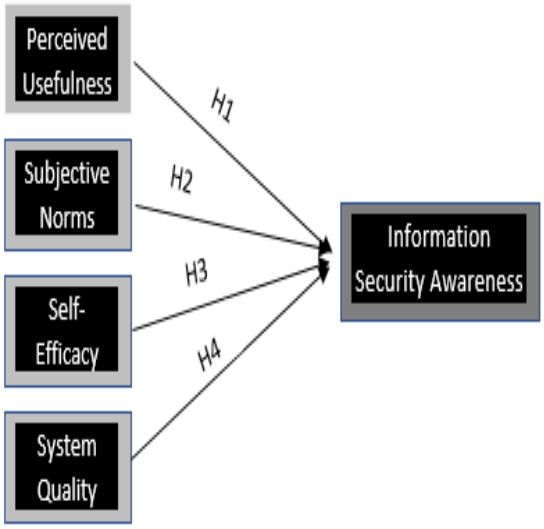

Figure1: Research Model

Extensive research over the past decades has provided evidence that perceived usefulness has a significant effect on individual behavior, either directly or indirectly because of the reinforcement value of outcomes [28]. Perceived usefulness is defined by Davis [29] as "the degree to which a person believes that using a particular system would enhance his or her job performance". There is widespread empirical literature that has demonstrated that perceived usefulness directly and positively influences individual awareness toward technology. Students who believe in a positive accept-performance relationship will lead to foster the acceptance of technology and that will influence behavioral intention to adopt security measures. An empirical study done by Abdallah and Abdallah [30] found that perceived usefulness has significantly impacted both ethical judgment and behavioral intention. Students who have an important understanding of information security are more motivated to be proactive in their data security behavior. Hence, the following hypothesis is formulated:

- H1: "Perceived Usefulness has a positive relationship with information security awareness"

On the other hand, literature also found that subjective norms had a significantly positive effect,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

on students' adoption of computer security measures. Subjective norms are defined as "one's perceptions or assumptions about others' expectations of certain behaviors that one will or will not perform"[31]. Social environment can influence the shape of person practices, judgment, opinion, and belief, whereby it occurs when an individual's opinion and action that was affected by other people [42]. It is commonly believed that the proximity peers, such as friends and friends of friends, have a social influence on the joining of a certain group of that node, the effect can also be the other way around when people get to know others by their common interests and memberships in the same groups. As argued by reasoned action theory, a person has a greater chance of being influenced by social influence. The explanation is that, even when people themselves do not accept the behavior or its effects, they will choose to conduct a behavior if they feel one or more relevant points of reference should be taken into account and driven to follow the references. Based on the aforementioned argument, the study hypothesized that:

- H2: "Subjective norms have a positive effect on behavioral intention to practice information security".

Self-efficacy is a belief in an individual's or students' capability to perform certain behaviors or it is one's personal beliefs about his or her ability to use information security products [32]. Self-efficacy is an important construct of social cognitive theory. The most powerful of self-efficacy is the interpreted result of one's previous attainments or mastery experience. People with high levels of self-efficacy exhibit stronger forms of self- conviction on their willingness to mobilize motivations, their cognitive resources, and other intended courses of actions that would be required to effectively carry out a given task. From security perspectives, computer self-efficacy refers to "the perceived ability of individuals to cope with the condition if attained" [28]. Self-efficacy or security knowledge of students would lead them to form negative attitudes toward their intention to use the technology. According to Alqarni [28], The computer efficacy of individuals should influence sensitivities, threats, and expectations, and the higher it gets the greater the readiness of a student to conduct the behavior. Students' knowledge is a robust factor in increasing the understanding and awareness of computer safety and practice. Therefore, the following hypothesis is proposed:

- H3: "Self-efficacy has a positive relationship with information security awareness"

System quality refers to the quality and functionality of security systems themselves.it signifies the accessibility, convenience, efficiency, flexibility, reliability, and responsiveness in the function of an information system [33]. Practically, high systems quality can create a convenient operating environment in which individuals can effectively classify functional system groups and navigate the materials the system provides efficiently. This means that the quality of security systems implemented and used has a positive impact on student behavior and awareness toward the use of these systems.

To provide their students with news, events, e-mails, classes, academic year schedules, student trademarks, and other personal information stored in their database system, education institutions rely on computer networks and technology. Thus, these systems have to be protected from multiple dangers, including malware, spyware, cross-site (XSS), viruses, worms, trojan horse, phishing, Denial-of-Service (DoS) and DDoS [2]. Therefore, a student will not be satisfied with a security system if the quality of such a system is unreliable [9]. This means that system quality has positive impacts on information security behavior among students. Hence, the study hypotheses that:

- H4: "Information security system quality has a positive relationship with information security awareness"

4. FINDINGS OF THE STUDY

Upon completion of the data collection, the researcher embarks on the data analysis. However, before conducting the actual data analysis, preparatory procedures are to be undertaken as suggested by Fowler [34]. The procedure involves five phases of activities as follows:

- Deciding on a format, i.e., the way the data will be organized in a file
- Designing the code, i.e., assigning appropriate values to responses
- Coding, i.e., forming categories for responses where applicable
- Data entry, i.e., keying in data inappropriate storage medium
- Data cleaning or editing i.e., final checking on the data file to ensure accuracy, completeness, and consistency.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

After establishing the research design and data collection procedures, this section presents the data analysis tools and techniques adopted in this research study. To achieve research objectives; the data analysis was divided into two stages. In the first stage, preliminary data analysis was performed with the help of SPSS version, 23. Findings generated at this stage of analysis provided the general picture of the respondent's demographic statistics and their response to the survey instrument. In the second stage, the evolution of a structured model using the SEM technique was employed with the help of AMOS version 23.0. At this stage, interrelationships between multiple independent and dependent variables were examined to test the proposed hypothetical framework developed. In addition to this, both the measurement model and structural model analysis techniques were employed to identify the level of significance of various factors affecting security awareness behavior.

Preliminary data analysis for the present study was performed with the help of SPSS version, 23. SPSS has been accredited by many researchers and widely accepted in various research areas including but not limited to, business studies, IS, social sciences, and marketing research. Therefore, the researcher decided to use this tool for data coding, identification of missing values and outliers, and the assumption of normality (i.e. using mean, Kurtosis, and skewness statistics). Additionally, descriptive statistical tests were also performed with SPSS. Likewise, EFA was also conducted for factor/dimension reduction by summarizing information from many variables used in the proposed framework into a smaller number of factors [25].

Data examination is sometimes also referred to as data screening is conducted next. It is the process of ensuring that the collected data is completed and suitable for analysis. This step also tests the data to ensure if it is useful, reliable, and valid for further testing [35]. In most self-administrated survey research, there are some chances for the existence of incomplete data or improper data entry. Tabachnick and Fidell [36] contend that missing data problems occur in survey-based research when respondents fail to respond to one or more questions in the instrument, which can cause potential issues in the data analysis process. Some researchers argued that the possibility of missing data patterns can be categorized into three types i.e. missing at random also known ignorable (MAR), missing completely at random (MCAR), and missing not at random or not-ignorable (MNAR). They further postulated that MCAR can be treated with any mechanism and results would be acceptable to generalize, whereas, treating MNAR could yield biased results. There are no clear guidelines regarding the extent of missing data treatment. [25] suggested that in the case of the random missing data pattern, data missing fewer than 10% can be ignored but it required remedial adjustment if it is higher than 20% to 30%. Similarly, Cohen et al., (2013) suggested that missing data up to 5% or even 10% on a particular variable may not be considered as large. Most simple analysis should yield reliable results even in case if the percentage of cases with missing observations is approximately less than 5%.

Therefore, to treat the missing (incomplete) data, the researcher followed four simple steps as recommended by Hair et al., [25]. 1) examined the extent of missing data, 2) investigate the pattern of missing data, 3) examined the randomness of missing data, 4) applied appropriate techniques e.g. imputation method to fix the issue. [25] identified several imputation methods such as regression imputation, mean substitution, case substitution, and hot or cold deck imputation methods. Researchers in this study employed the mean substation method. The reason is plausible in that the mean substitution approach is the most commonly adopted/accepted under MAR, MCAR, issues as well as the mean calculated with this approach is treated as the best single replacement for any missing value.

The demographic findings of the study are discussed in this section. The first section of the survey instrument requested respondents to provide demographic and background information (gender, age, faculty, and department). Table 1 shows that the gender distribution is skewed in favor of males with 60.5%, while females with 39.5%. Across the universities, the male population was found to outnumbered the female population.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: Demography Statistics of Respondents

Variable	Item	Frequency (N= 180)	Percentage (%)
Gender	Male	109	60.5
	Female	71	39.5
Age Group	< 20	70	38.8
	> 20	110	61.2
Faculty	Social Science	43	23.8
	It & Engineering	87	48.3
	Business	50	27.7

In this research, Cronbach's coefficient alpha (α) reliability method was employed to evaluate the internal consistency of every construct. The consistency of the respondents' responses was examined to evaluate the reliability of the measurement. The reason for selecting Cronbach's an (inter-item consistency reliability) is plausible because it is an easier option to calculate and it is also the most commonly used approach in academic research. As reported by Sekaran [22], the values of Cronbach's a coefficient less than 0.6 should be considered weak, between 0.6 and 0.7 as satisfactory, and more than 0.8 as good. Similarly, Gliem and Gliem [37] suggested that Cronbach's coefficient value equal to or greater than 0.7 indicate adequate reliability. Consequently, this research study assumed that the minimum cut-off value for Cronbach's coefficient should be 0.7 or greater to examine the overall reliability of latent constructs used in the proposed model. Table 2 depicts Cronbach's alpha for measures used in the instrument. All measures recorded α value greater than 0.80, suggesting that the measures are highly reliable. Therefore, there was no need to change and refine the questionnaire for increasing the alpha coefficients.

Table 2: Reliability Tests

Variable	No Items	Cronbach's alpha
Perceived Usefulness	6	0.82
Subjective norms	5	0.81
Self-efficacy	6	0.84
Information security system quality	5	0.86

In SEM analysis, first confirmatory factor analysis CFA is performed to assess the model fit and then hypothesized relationships between latent constructs are assessed to calculate the path coefficient. Finally, the proposed model is revised to reach a model that fits the data well.

Confirmatory factor analysis is required to check the validity of the measurement model via goodness of fit (GOF) and (2) composite reliability and validity using AMOS version 23.0. GOF indices, as shown in Table 3, are divided into three categories: i.e. absolute fit, incremental fit, and parsimonious fit indices [38]. Results of initial CFA model lit indices (X2/df = 1.587, RMSEA = 0.047, NFI = 0.933, TLI = 0.947, CFI = 0.953, and AGFI = 0.842) found to be in acceptable limits. In addition to these GOF measures, the values of standard regression weights (factor loading) for all items found to be > 0.7, standard residual values found within the acceptable limit (above 2.58 or below -2.58) and values of the critical ratio found > 1.96. Accordingly, based on all these acceptable findings, it is found that the data were properly adapted to the research model and no further re-specification and refinement were required.

After CFA, construct validity is to be tested using discriminant and convergent validity. Convergent validity assesses the extent to which two measures of the same concept are correlated. All of the items in factor analysis should load highly on their latent variables to show good convergent validity. Based on the recommendation of, the best results of convergent validity can be obtained if standardized loading estimates are 0.7 or higher, estimation of AVE is greater than 0.5, and the estimation of reliability is above 0.7. Following the above-mentioned recommendation, this research study assumed the minimum cut off criteria for factor loadings, AVE, and composite reliability as 0.7 > 0.5 > 0.7 respectively, in assessing the convergent validity. The results show that convergent validity and discriminant validity criteria are satisfactorily met.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 3: Structural Model and measurement model fit indices

Measure indices	Fit indices	Structural Mode	Measurement Model	Limit
Absolute fit measure	X2	3618.809	3555.51	
	X2/Df	1.589	1.547	$1< \chi2/df<3$
	RMSEA	0.037	0.039	*<0.05*
Incremental fit measure	NFI	0.903	0.937	*≥ 0.90*
	TLI	0.927	0.927	*≥ 0.90*
	CFI	0.933	0.903	*≥ 0.90*
Parsimony fit measure	AGFI	0.802	0.882	*≥ 0.80*
*"Notes: **χ2** = chi-square; **df**= degree of freedom; **RMSEA** = root mean square error of approximation; **NFI** = normated fit index; **CFI** = comparative fit index; **TLI** = Tucker-Lewis index, **AGFI** = adjusted GOF index".*				

After the CFA validation, the next step of the analysis is to test the causal hypotheses presented in the proposed research model and the strengths of the relationships among the constructs with the help of a structural model. The researcher used GOF indices and examined other parameter estimates to evaluate the hypothesized structural model. Table 3 present the findings of the fit indices of the structural model. The likelihood ratio chi-square ($\chi2$ = 3555.519; p = .000) was significant (p < .001); x2/df achieved an acceptable fit of 1.547 and found well within limits i.e. 1.0 < x2 / df < 3.0). Furthermore, the findings for TLI and CFI were 0.927 and 0.903 respectively, and were above the recommended value of ≥ 0.90. Similarly, the results of AGFI (0.882) met the recommended criteria of ≥ 0.80. Lastly, the value of RMSEA found within the recommended criteria of < 0.5 and reached an acceptable figure of 0.039.

"To inspect the hypotheses of this research, critical ratios, standardized estimates, and p-value were used. It was assumed that a relationship is statistically significant at the 0.05 levels when the critical ratio (CR or t-value) found higher than ± 1.96" [25]. All the casual paths in the model were examined based on the path estimates and CR (t-value). Results demonstrated that t-values for twenty-two causal paths estimate found above the 1.96 (critical value) and significant at p ≤ .05. However, t-values for thirteen casual paths were found not statistically significant. The parameter estimates are presented in table 4 and the overall structural model is depicted in figure 2. Results presented in Table 4 shows that all four hypothesized paths between the variables found to be significant. For example, the hypothesized path between perceived usefulness and information security awareness with a CR value of 7.721 (>± 1.96) was statistically significant (p = 0.001). Similarly, facilitating conditions and AU; information quality. Similarly, hypotheses H2, H3, and H4, are all supported based on the results presented in Table 4. Figure 2 depicts the final structural model.

Table 4: The estimate of the Hypothesized Model

	Stand. Regression Weights (β)	SE	C.R.	P	Valid
H1	0.334	0.074	3.3981	***	YES
H2	0.1687	0.056	1.826	0.213	YES
H3	0.179	0.009	3.316	***	YES
H4	0.278	0.195	2.648	0.015	YES
Notes: "Std. Reg. Weight = Standardized regression weight" SE = "Standard error of regression weight" CR = "Critical ratio of regression weight" *p* =" Level of significance of regression weight" (*** *p* < 0.001)					

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

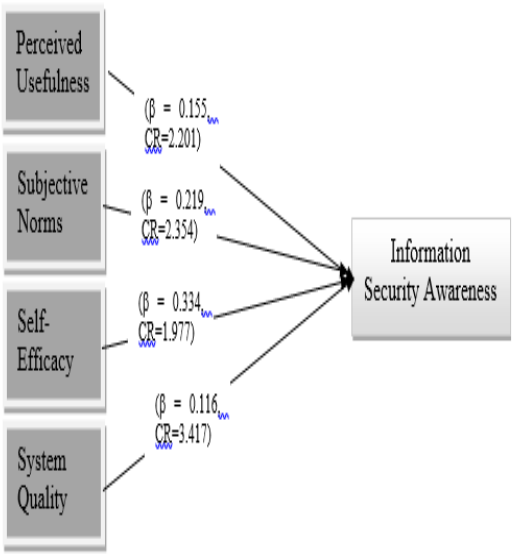

Figure 2: Structural Model

4. DISCUSSION

The technology acceptance model and information system success model was integrated into the research to examine the key variables of information security awareness among higher education students at Aldar University College in Dubai. In addition to perceived usefulness, subjective norms, and self-efficacy abducted from the technology acceptance model added element like information security quality is new to the framework to strengthen model predictive power. It is very significant to mention that the findings of this research validate previous studies employing TAM theory in the context of security behavior and awareness.

Originally, six items were used to measure the perceived usefulness of information security construct. The mean scores of items found between 3.55 (0.983) and 4.12 (0.694), and greater than the neutral scale point. Based on the high ratings of the construct items, it can be predicted that respondents' interest was found to be very much inclined towards the benefit of security systems. Five measures are used to test the subjective norms factor and the items mean rating found to be between 3.29 (0.952) and 3.53(0.907). This indicated that respondents are very much concerned with colleagues' and friends' opinions. The self-efficacy construct was measured by six items and the mean score of all items was found between 3.89 (0.728) and 4.01 (0.656). The mean rating values of measurement items indicated that respondents had some confidence toward computers and information systems. Finally, six items were used to measure the security system quality construct. The mean scores of items found to be between 2.95 (1.051) and 3.34 (1.097). Based on the high ratings of the system quality construct items it can be predicted that students are very much concerned about system flexibility, user-interface design, system functionality. The hypothesized relationship between perceived usefulness and security awareness tested through hypothesis H1 (i.e. Perceived Usefulness → Security Awareness) was found to be significant. Therefore, based on the parameter estimate results (β = 0.165, t-value = 1.954, p = 0.001), the proposed hypothesis was supported. These empirical findings suggest that students are driven based on their beliefs established through the perception of its relative advantage after considering its usefulness. These results are in accordance with the findings of other research studies [39-41].

As a social aspect, subjective norms is as a person's perception that most people who are important to him think he should or should not perform the behavior in question. Students will generally intend to perform the behavior when they have a positive attitude toward it and when they believe that important individuals think they should do so. Subjective norms were hypothesized to have a direct effect on students' information security behavior and awareness. The results of parameter estimates (β = 0.219, t-value = 3.135) were statistically significant at p = 0.001 level and indicated that social influences (subjective norms) are strong factors that affect students' awareness.

Moreover, the self-efficacy of computers and technology and information systems was hypothesized to have a direct positive effect on security awareness among students. The results of parameter estimates (β = 0.334, t-value = 3.591) for hypothesis H3 (Self-efficacy → security awareness) found to be statistically significant at p = 0.001 level and indicated that the self-knowledge of students is a strong predictor to increase security awareness. These results are in accordance with the findings of other research studies [30, 39]. The study results propose that students with high confidence in self-efficacy towards information security are more likely to practice information security such as updating antivirus software and protecting personal information from security breaches. According to Abdallah and Abdullah [30], students with strong motivation to implement

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

information security behavior value more information security as they have more knowledge of information security. Most of the students believed fairly in their abilities in keeping their computers and information safe and secure. Students, however, decided that they could download antivirus applications even when nobody around to help them. Besides, the usefulness of security systems, subjective norms, and self-efficacy. The results indicate that the quality of the security measures and systems implemented affects students' behavioral awareness. Based on DeLone and McLean [33], System quality refers to "the performance of the system itself in terms of accessibility, flexibility, integration, language, functionality, complexity, responsiveness, and interface design" to help instructors conduct teaching activities and facilitate learning. In the proposed hypothetical model, three hypotheses were proposed to investigate the effect of system quality on PU, PEOU, and AU. Results of parameter estimates for Hypothesis H4 (System Quality → Security Awareness) ($\beta = 0.116$, t-value = 2.813) at 0.001 ($p < 0.05$) level indicated that this hypothesis found to be statistically significant and hence, the hypothesis was supported.

In contrast to previous works and existing models in the area of security behavior awareness, the current study extended the research scope by combining the most critical factors identified in the relevant literature. All these factors are attempted to apply them in the local context. It is recognized that the majority of studies focus on access to technology and context whereas in developing countries majority are concern about individuals, with few studies exhibit a comprehensive view. Therefore, the proposed model contained variables that have not been integrated into one framework subject previously, which allows simultaneously examining for validation and relationship. Most of the studies have examined users' behavior awareness by using the original technology acceptance model (TAM). They did not utilize a framework for developing their research models. This situation is a limitation because there is no a clear pattern in selecting the external variables of the research models. Researchers are advised to avoid using a single linear methodology when evaluating individual behavioral awareness. Therefore, in this study, a multidimensional approach is considered to evaluate the behavioral intention of higher education students towards security, and the variables of the research model are selected under the control of related dimensions.

Previous research has focused heavily on technological solutions for computer security risks. Recent behavioral research has noted the importance of the human element and its role in shielding computers, the information stored on them, and users' privacy from dangerous and unauthorized penetrations. One of the most important implications of this research is the heightened focus on the usability and training of computer security practices. College administrators, professors, and stakeholders should design courses, workshops, and special sessions on the usefulness and ease of use of computer security practices. Another important implication of this study is the significance of perceived vulnerability concerning adopting computer security practices. Students are found to more likely to adopt computer security practices if they feel vulnerable to security threats. Colleges may start a lean, cost-effective, campaign where professor, lecturer, and staff member sends out regular emails to their students and clients which raise awareness about the risks involved with computer security practices

The findings of the study can be used to either refute or strengthen the theories or framework that has been adopted. The findings might also contribute to the literature on security behavior and awareness in general. Besides, The schools seem to be actively working towards enhancing students ' awareness of these problems and how to protect themselves against potential cyber-attacks such as ID theft or ransomware. The majority of students are also aware of the potential consequences of providing an entire university population with personally identifiable information like identity theft and stalking but feel comfortable providing this information.

5. CONCLUSION

Information security includes a thorough comprehension of both human and technical aspects. Threats to the security of information could be diminished if individuals perform information behavior effectively. The information security success relies on the actual behavior of the people

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

involved. The objective of this article was to examine the security awareness factors among students at Aldar College University. This study investigates the possibility of the incorporation of individual, institutional, and environmental as a reflective construct that connects to information security awareness. The study was conducted based on a questionnaire using a descriptive case study approach. 180 valid responses were covering all the faculties. The target was to get a general understanding of information security awareness behavior and to further understand how different factors may impact on it. The results of this research exposed that perceived usefulness; subjective norms, self-efficacy, and security system quality are the main variables influencing security awareness. The self-efficacy of computers and technology and information systems was hypothesized to have the most effect on security awareness among students

The study makes important contributions to the emerging body of knowledge on the behavioral and educational settings about the information security issue. Initially, the study offers a theoretical explanation of the student's awareness of security. Furthermore, the research has shown that the important factors influenced by the individual can help to motivate precaution-taking behavior in information security issues. However, there are limitations to this research some of which include the study merely focuses on one educational institution. Thus, a future study may increase the population size and include different institutions. Besides, future studies should focus on individual practices in detail, as well as other recommended security practices.

REFERENCES

[1] L. Muniandy, B. Muniandy, and Z. Samsudin, "Cyber Security Behaviour among Higher Education Students in Malaysia," *J. Inf. Assur. Cyber Secur,* vol. 2017, pp. 1-13, 2017.

[2] S. Al-Janabi and I. Al-Shourbaji, "A study of cyber security awareness in educational environment in the middle east," *Journal of Information & Knowledge Management,* vol. 15, p. 1650007, 2016.

[3] V. Broucek and P. Turner, "A Forensic Computing Perspective on the Need to Improve User Education for Information Security Management," ed: Current Security Management & Ethical Issues of Information Technology …, 2003.

[4] Y. K. Peker, L. Ray, S. Da Silva, N. Gibson, and C. Lamberson, "Raising Cybersecurity Awareness among College Students," in *Journal of The Colloquium for Information System Security Education*, 2016, pp. 17-17.

[5] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *computers & security,* vol. 38, pp. 97-102, 2013.

[6] T. R. Peltier, *Information security risk analysis*: Auerbach publications, 2010.

[7] S. I. Al-Jerbie, M. Z. Jali, and N. Sembilan, "A second look at the information security awareness among secondary school students," in *The International Conference on Information Security and Cyber Forensics (InfoSec2014)(pg. 88-97)*, 2014.

[8] N. A. Zakaria and F. Khalid, "The benefits and constraints of the use of information and communication technology (ICT) in teaching mathematics," *Creative Education,* vol. 7, pp. 1537-1544, 2016.

[9] F. Khalid, M. Y. Daud, M. J. A. Rahman, and M. K. M. Nasir, "An Investigation of University Students' Awareness on Cyber Security," *International Journal of Engineering & Technology,* vol. 7, pp. 11-14, 2018.

[10] L. Muniandy and B. Muniandy, "State of cyber security and the factors governing its protection in Malaysia," *International Journal of Applied Science and Technology,* vol. 2, pp. 106-112, 2012.

[11] D.-L. Huang, P.-L. P. Rau, and G. Salvendy, "A survey of factors influencing people's perception of information security," in *International Conference on Human-Computer Interaction*, 2007, pp. 906-915.

[12] L. Hadlington, "Employees Attitudes towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom," 2018.

[13] M. Anwar, W. He, I. Ash, X. Yuan, L. Li, and L. Xu, "Gender difference and employees' cybersecurity behaviors," *Computers in Human Behavior,* vol. 69, pp. 437-443, 2017.

[14] J. R. Ndiege and G. Okello, "Information security awareness amongst students joining higher academic institutions in developing countries: Evidence from Kenya," 2018.

[15] K. Edwards, "Examining the security awareness, information privacy, and the security behaviors of home computer users," 2015.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[16] A. Moallem, "Cyber Security Awareness Among College Students," in *International Conference on Applied Human Factors and Ergonomics*, 2018, pp. 79-87.
[17] A. Farooq, J. Isoaho, S. Virtanen, and J. Isoaho, "Information security awareness in educational institution: An analysis of students' individual factors," in *2015 IEEE Trustcom/BigDataSE/ISPA*, 2015, pp. 352-359.
[18] P. Potgieter, "The Awareness Behaviour of Students On Cyber Security Awareness by Using Social Media Platforms: A Case Study at Central University of Technology," in *Proceedings of 4th International Conference on the*, 2019, pp. 272-280.
[19] L. Hadlington, "Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours," *Heliyon,* vol. 3, p. e00346, 2017.
[20] F. A. Aloul, "The need for effective information security awareness," *Journal of Advances in Information Technology,* vol. 3, pp. 176-183, 2012.
[21] D. E. Gray, *Doing research in the business world*: Sage Publications Limited, 2019.
[22] U. Sekaran and R. Bougie, *Research methods for business: A skill building approach*: John Wiley & Sons, 2016.
[23] J. W. Creswell and V. L. P. Clark, *Designing and conducting mixed methods research*: Sage publications, 2017.
[24] R. B. Kline, *Principles and practice of structural equation modeling*: Guilford publications, 2015.
[25] J. F. Hair, M. Sarstedt, C. M. Ringle, and J. A. Mena, "An assessment of the use of partial least squares structural equation modeling in marketing research," *Journal of the academy of marketing science,* vol. 40, pp. 414-433, 2012.
[26] P. D. Leedy and J. E. Ormrod, *Practical research: Planning and design*: Pearson Education, 2014.
[27] J. W. Creswell and J. D. Creswell, *Research design: Qualitative, quantitative, and mixed methods approaches*: Sage publications, 2017.
[28] A. Alqarni, "Exploring factors that affect adoption of computer security practices among college students," 2017.
[29] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS quarterly,* pp. 319-340, 1989.
[30] N. Abdallah and O. Abdullah, "Computer Security Behavior and Awareness: An Empirical Case Study," *International Journal on Perceptive and Cognitive Computing,* vol. 5, pp. 8-14, 2019.
[31] N. Huda, N. Rini, Y. Mardoni, and P. Putra, "The analysis of attitudes, subjective norms, and behavioral control on muzakki's intention to pay zakah," *International Journal of Business and Social Science,* vol. 3, 2012.
[32] D. R. Compeau and C. A. Higgins, "Computer self-efficacy: Development of a measure and initial test," *MIS quarterly,* pp. 189-211, 1995.
[33] W. H. DeLone and E. R. McLean, "Information systems success revisited," in *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, 2002, pp. 2966-2976.
[34] F. J. Fowler Jr, *Survey research methods*: Sage publications, 2013.
[35] J. Gaskin, "Group differences. Retrieved from stats tools package," ed, 2014.
[36] B. G. Tabachnick and L. S. Fidell, *Experimental designs using ANOVA*: Thomson/Brooks/Cole Belmont, CA, 2007.
[37] J. A. Gliem and R. R. Gliem, "Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales," 2003.
[38] Hair, W. C. Black, B. J. Babin, and R. E. Anderson, "Multivariate data analysis: Global edition," ed: Pearson Higher Education Upper Saddle River, NJ, 2010.
[39] R. Hussein, F. Lambensa, and R. B. Anom, "Information security behaviour: a descriptive analysis on a Malaysian public university," 2011.
[40] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study," *Journal of Computer Information Systems,* pp. 1-16, 2020.
[41] M.-H. Chang and D.-Y. Kang, "Factors affecting the information security awareness and perceived information security risk of employees of port companies," *Journal of Navigation and Port Research,* vol. 36, pp. 261-271, 2012.