Research Article GU J Sci 37(4): 1691-1705 (2024) DOI: 10.35378/gujs.1427984

Gazi University

Journal of Science

http://dergipark.gov.tr/gujs

A Scale Development and Application Study on Smartphone Security Awareness

Mevlut YILDIRIM[1,*], Veysel DEMIRER[2]

[1]*Kutahya Health Sciences University – Simav Vocational School of Health Services, Kütahya, Türkiye*
[2]*Suleyman Demirel University – Faculty of Education, Isparta, Türkiye*

Highlights

- This study was derived from corresponding author’s master’s thesis.
- There were significant relationships between SSA and digital literacy.
- Statistically significant differences between IT level and SSA.
- Statistically significant differences between experiencing security problems before and SSA.

Article Info

Received: 04 Feb 2024
Accepted: 15 June 2024

Keywords

Smartphone security
Awareness
Scale development
Digital literacy

Abstract

This study aims to assess the extent of smartphone security awareness among students pursuing an associate degree and to ascertain if there are substantial variations in smartphone security awareness based on certain demographic variables. Furthermore, its objective is to uncover the correlation between smartphone security awareness and proficiency in digital literacy. The Smartphone Security Awareness Scale was initially designed with this particular aim. The scale comprises nine items that are measured along a single dimension, accounting for 39.6% of the overall variation. The scale’s reliability coefficient was found to be 0.78. The study sample comprised 612 associate degree students pursuing further education in two vocational colleges. The data were obtained using the internet and voluntarily. The data indicate that associate degree students had a high level of awareness regarding smartphone security. There was no significant difference in smartphone security awareness based on gender, use of security software, participation in information security training, and level of care regarding the privacy and safeguarding of personal data. No significant relationship was found between smartphone security awareness and smartphone ownership duration. However, significant differences were found according to experience of security problems and competence in using information technologies. A positive, significant, and moderate correlation was discovered between smartphone security awareness and proficiency in digital literacy. The scale devised during the investigation can be utilised in other future studies. According to the results obtained in this direction, training and seminars can be organised to increase smartphone security awareness.

1. INTRODUCTION

The concept of mobile phones has evolved into smartphones over time due to their capabilities and processing capacities [1]. Although they help individuals in many areas of daily life, their functional similarities to desktop computers cause them to attract many security threats [2]. In addition to some advantages of using these digital devices, there are also many security threats [3,4]. Although the popularity of smartphones is increasing, users’ privacy and security concerns are believed to be one of the significant barriers to using their smartphones to their full potential [5]. According to a study, users are more likely to protect their desktops and laptops than their smartphones or tablets [6]. Although many people are hesitant to perform some transactions because they are concerned about smartphone security, this situation is changing with young people, and risk intensity is increasing towards smartphones [7]. Today’s phones are seen as multifunctional minicomputers due to the functions they can fulfil [8], and with more attractive prices than buying a computer, they have become widespread among low-income individuals and young

[*] Corresponding author, e-mail: mevlut.yildirim@ksbu.edu.tr

people and have started to be used in many transactions such as financial transactions and e-commerce [9]. However, it has been stated that the security solutions traditionally applied on desktop computers do not provide complete security on smartphones and cannot always be applied [10,11]. In addition, since smartphones are mini technological devices with limited technical features, it is impossible to use PC security technologies on these platforms [12].

Every day, new applications are offered to users on smartphone platforms. Currently, there are 8.93 million applications worldwide available for download, while 1.82 million applications are available for download on the Apple App Store, and 3.553 million applications are available for download on the Google Play Store [13]. As smartphones become more powerful devices and hold the pinnacle of technology, security is becoming a major issue [14], and the number of malware is increasing as they are equipped with many features [10]. Information disclosure on smartphone platforms can be realised in a brief period of time, and if malicious code is distributed, this can lead to much more significant problems [12]. A significant problem in the field of smartphone security is the insufficient understanding among end users regarding the collection and methods of data acquisition [15]. To address this problem, it is necessary to recognise the risks posed by malware, maintain regular security software updates and scans, and increase user awareness of smartphone security best practices. Taking these steps makes mitigating the potential risks associated with malware and other security threats possible.

On the other hand, today, being able to adapt to information technologies and use technological devices effectively and efficiently is of vital importance, especially in education. In this period, when information spreads rapidly, many sources with low reliability and false information bring along various risks for society and individuals. It has been emphasised that the most significant factor in the formation of risk on web platforms is the production of misleading information and the sharing of this misleading and abusive information [16]. Depending on these ever-changing and developing technologies, various concepts have come to the fore to exist in digital society. Digital literacy (DL) has an essential place among these concepts. The term "digital literacy" was initially introduced in the literature by Gilster at 1997 [17]. In order for individuals to be more effective on digital platforms, they need to have emotional, sociological and cognitive skills, as well as digital skills. The concept of DL, as defined by Inoue et al., comprises a range of skills such as computer literacy, media literacy, and information literacy [18]. It encompasses a broad range of skills that are vital and integrated. DL defined as "the ability to survive in the digital age" [19]. From another point of view, DL defined as a series of attributes, did not see DL as a skill checklist [20,21]. They stated that it has an aspect that keeps pace with developing technologies and can change. For example, while reading and sending e-mails or searching for a word in a search engine are basic skills, taking part in different educational environments, such as Udemy and Coursera, or interacting in virtual environments requires flexibility and technical skills, self-control and problem-solving. In this sense, digital literacy and smartphone security awareness are vital for end users.

1.1. Literature

The threats and attacks on digital platforms are similar on most digital devices. A desktop computer user can be exposed to the same attack while using his/her smartphone, and the risk situation waiting for a laptop user can be faced by a smartphone user in the same way. Although the threats are exactly the same at some points and differ in terms of attack method, technique and solution at some points, it is necessary tobe aware of all these situations. Many smartphone users are not aware of what dangers awaitthem. Many are aware of these situations when they or the individuals around themexperience such an event. However, smartphone users should know all the dangers beforehand, act accordingly and be prepared for them. In this context, security situations can be listed specifically for smartphones. Some of the situations that smartphone users should be aware of can be summarised as instant messaging applications and licence agreements, use of applications outside the official store, permissions, authentication, and online shopping. In addition to Bluetooth, WiFi, and cloud computing security, there are also phishing and malware threats apart from these situations. Examples of malware attacks include Trojan horses, aggressive adverts, spyware, ransomware, botnets, worms, and backdoors. Among these threats, especially ransomware has come to the forefront with the victimisation it has caused in recent years. It is seen as one of the most dangerous malware because security software is insufficient to prevent ransomware attacks, and users exposed to this attack are asked for a certain amount of money to regain access to their data. Even excluding attacks on end-users, it is determined that in 2021 %37 of organizations, in 2022 %66 of organizations and in 2023 with the same rate %66 organisations hit by ransomware attacks [22]. These situations have also attracted the attention of the literature on smartphone security. The security literature on smartphone applications has focused on identifying malicious applications [23-25]. There are a sufficient number of studies on smartphones and smartphone security in the literature, but studies on smartphone users' security consciousness, awareness and behaviours are limited in the relevant literature [26]. Regardless of the level of centralisation and strictness of a platform's security model, there are always some choices available to the user. These choices may involve granting access to certain restricted resources or enabling the user to choose if an application can potentially jeopardise their security and privacy. It is uncertain whether typical users can reasonably handle the responsibility of making security judgements. Studies in this field have demonstrated that average users lack the ability to make such assessments and do not fully employ security measures [27-30]. The initial study conducted disclosed a significant deficiency in security awareness [31]. They claimed that this was a result of smartphone owners having a lack of understanding regarding security and a low level of willingness to accept the authentication methods provided to them. An additional aspect highlighted in this survey is that a significant majority of 86% of the participants do not employ any form of verification, such as a personal identification number (PIN), to gain access to their mobile phones. According to a study, the participants were not conscious of the potential dangers associated with constantly keeping WiFi and Bluetooth enabled [32]. The researchers stated that educational and awareness initiatives are required to rectify usage habits. They examined users' awareness of the security risks associated with user-defined configurations and discovered that only 18 out of 38 user-defined security settings were configured accurately [33]. An another study that aimed to reveal the security awareness status with the set of questions they used and to create an infrastructure for preparing similar surveys in the future since there is currently no validated survey [34]. They also found that the rate of those who store their personal data on their smartphones is higher than those who do not and that there is a relaxation in security practices in case of overconfidence, while excessive fear prevents downloading applications and adopting technology. It has been aimed to measure the security awareness of smartphone users with the questionnaire they developed [35]. As a result of their study, they stated that the participants did not consider the official application stores risky, tended to ignore the security messages sent to them, and some users also activated remote data wiping, encryption and device discovery features. On the other hand, a questionnaire was developed to assess the security practices, education levels, and awareness behaviours of smartphone users [26]. The study results showed that many participants considered the data on their smartphones to be just as private as the data on their home computers. However, the study also revealed that many participants did not use third-party security applications and were unaware of how to protect themselves when using public WiFi networks. This suggests that there is a need for increased education and awareness regarding smartphone security and the potential risks of using public WiFi networks.

Another study, discovered that participants exhibited either a lack of familiarity with some controls, such as device password lock, finding device features, or keeping these features turned off and that most of them stored personal data on their smartphones [36]. They also stated that the participants were aware of the risks and threats but did not take security measures at the desired level and recommended that the media and non-governmental organisations carry out awareness-raising activities on this issue. It has been noted that users frequently avoid installing security software on their smartphones [37]. Although these consumers generally have confidence in legitimate app stores, they are cautious about the level of access that installed applications may have to their personal data. In this sense, they tried to increase smartphone security awareness with a conference. Lastly, a study aimed to establish the correlation between smartphone and digital data security awareness [38]. As a result of the study, he found that some students downloaded pirated applications, and many students stored their personal information on their smartphones. However, he found that most students are concerned about the privacy of their personal data, pay attention to whether they provide access to personal data when downloading applications, and if access is provided, they give up downloading that application. He pointed out that the human factor is at a key point in the context of security and the importance of raising awareness.

This study aims to assess the extent of smartphone security awareness (SSA) among associate degree students. Additionally, it aims to determine if there are any significant differences in SSA based on different demographic factors, as well as examine the correlation between SSA and DL. In this regard, the research questions were determined and answered as follows:

1. What is the level of SSA of associate degree students?
2. SSA scores;
   a. At what level is there a relationship between the duration of ownership of a smartphone?
   b. Does it vary according to the status of experiencing security problems before?
   c. Does it vary according to the use of security software?
   d. Does it vary according to the IT level?
   e. Does it vary according to the status of receiving information security training before?
   f. Does it vary according to the level of concern about the privacy and protectionof personal data?
   g. At what level is there a relationship between SSA and DL?

2. MATERIAL METHOD

Relational survey models are a type of statistical model used to examine the relationships between variables [39]. These models can provide insight into the connections between different variables and the strength of these relationships, but they do not allow for causal conclusions to be drawn. Instead, they are used to explore potential correlations and associations. It has been noted that one of the primary objectives of relational studies is to understand essential behaviours by explaining the relationships between variables [40]. In this study, using a relational survey model allowed the researchers to examine the relationship between smartphone security awareness and digital literacy skills, which is a crucial aspect of understanding these behaviours.

2.1. Data Collecting Tools

In this present study, the questionnaire form used for data collection consists of three parts. The first part aims to obtain the students' demographic characteristics and some variables. The second section includes the "Smartphone Security Awareness Scale", developed within the scope of the research to measure students' smartphone security awareness. The third part is the "Digital Literacy Scale", in which the relationship between security awareness on smartphones and the relationship between them is examined to ensure concurrent validity.

Personal Information Form

To determine the demographic characteristics of the study group and to obtain more detailed information about the study group, the researcher created a "Personal Information Form". During the creation of the form, first of all, variables that are thought to affect security awareness on smartphones and, at the same time, affect digital literacy were included. The personal information form used in this study included 11 questions covering socio-demographic variables (such as age, gender, and class) and questions related to smartphone use and security experiences. Specifically, the form included questions about the length of time the students used smartphones, whether they had experienced any security issues in the past, and whether they had received any information security training. These questions were designed to provide insight into the study group's smartphone use and security practices.

Smartphone Security Awareness Scale

In this study, a five-point Likert-type scale that can measure the level of smartphone security awareness at the level of associate degree students was developed considering the existing literature (Appendix A). In the development of the scale, the four-step scale development stages were followed to ensure content validity [41]. In this context, the steps of defining the problem, writing items, getting expert opinion, pre-application and finalising the scale were completed. In the item writing stage, the steps, such as the number of scale points being odd and even, the number of scale points and the naming of scale points, were considered [42]. The completed 15-item pre-application form was named the "Smartphone Security Awareness Scale" and abbreviated as "SSAS". An exploratory factor analysis (EFA) was conducted with the first study group of 311 participants, and a confirmatory factor analysis (CFA) was conducted with the other study group of 308 participants. The EFA test was conducted with 15 items to test the scale's construct validity. KMO and Barlett's test of sphericity test was also applied. If the KMO value is greater than 0.50, it means that factor analysis can be performed on the available data [43]. On the other hand, Barlett's test of sphericity should create a significant difference in performing factor analysis. The KMO coefficient was found to be 0.864, and Barlett's test of sphericity chi-square ($\chi 2$) value was 1113.48 ($p<0.001$). As a result of the analysis using the principal components method, since the factor loadings of item 2, item 7 and item 8 were found to be below 0.30, these three items were removed from the questionnaire. As a result of the reanalysis, it was decided that the scale had a single-factor structure considering the Eigen value and Scree Plot graph. While the factor loadings of the items in the scale varied between 0.53 and 0.72, it explained 34.5% of the total variance with its current structure of 12 items.

After the EFA procedure, CFA was conducted to determine the construct validity of the model obtained. Before starting the CFA, a normality test was applied to the second data set, and four data found to be outliers were discarded from the questionnaire. As a result of the analysis performed through the AMOS Graphics programme, items 1, 9 and 10, which were found to have loadings lower than 0.50, were excluded from the questionnaire. The remaining nine items with a loading of 0.50 or above constituted the final version of the scale. When the fit criteria were examined, it was found that Chi-square/sd = 1.987, NFI = 0.952, GFI = 0.968, CFI = 0.975, RMSEA = 0.056 and SRMR = 0.036. With these results, it was determined that the scale has acceptable fit and excellent fit values.

Finally, Cronbach's Alpha test was performed for the reliability analysis of the developed scale, and the reliability coefficient was found to be 0.782. This result indicates that the data obtained is 78.2% reliable. In addition, the scale explains 39.6% of the total variance in its final form, which consists of nine items. From this scale, which is scored between 1 and 5, participants can get a minimum score of 9 and a maximum score of 45.

Digital Literacy Scale

The 'Digital Literacy Scale,' initially developed and then adapted to be used in Turkish, was utilised to assess the digital literacy skills of students [44, 45]. This scale consists of 10 items and employs a five-point Likert scale that ranges from "Strongly Disagree" to "Strongly Agree". The factor loadings of the items on this scale vary between 0.46 and 0.74, suggesting satisfactory item consistency. The scale is designed as a unifactorial structure, accounting for 40% of the overall variance. The scale's dependability, as measured by its Cronbach Alpha value, was determined to be 0.86, indicating strong internal consistency [45].

2.2. Sample

Data from respondents was collected using a convenience sample technique. The study focuses on a target group of 1098 associate degree students enrolled in two vocational schools at Isparta University of Applied Sciences for the 2020/2021 academic year. Out of these students, a total of 619 took part in the survey. Survey participation was voluntary, and the sample was selected by excluding surveys that were considered unreliable from the study.

Table 1. *Demographic characteristics of the sample*

Demographic Variables	Groups	Frequency	Percentage (%)
Gender	Male	295	48.20
	Female	317	51.80
Classroom	1st class	252	41.20
	2nd class	360	58.80
Smartphone Operating System	Android	412	67.30
	IOS	200	32.70
	Low	58	9.50
	Centre	400	65.40
IT level	High	154	25.10
	Total	**612**	**100**

Table 1 shows that the number of male and female participants is quite close to each other, and mostly 2nd-year students participated. The number of users with the Android operating system is more than twice the number of users with the IOS operating system. In the competence of using information technologies, the intensity of those who stated themselves as intermediate level draws attention. On the other hand, the lowest age among the participants of this study was found to be 17, and the highest age was 48 (X = 20.61, s = 2.02), and it was observed that the age distribution was between 19-22 (n = 522). In addition, the duration of owning a smartphone was found to be at least 1 year and at most 15 years, and it was observed that more than half of the participants had been using smartphones for 6 years (n = 102), 7 years (n = 103) and 8 years (n = 127).

2.3. Data Analysis

The statistical analysis of the research data was conducted using the SPSS 20 package program. Descriptive statistics were calculated to summarise the data, including percentages, arithmetic means, and frequencies. In addition, the program was used to determine the correlation between variables. The data were collected in a Google Spreadsheets service and were then transferred to a single Microsoft Excel file for further analysis. The relevant variables were then created in the SPSS program, and the data were analysed to investigate the relationships between the variables of interest.

Once it was determined that the data set exhibited a normal distribution, the correlation between smartphone security awareness and digital literacy was examined using Pearson Correlation. A thorough range of statistical studies was utilised to determine if there were any significant differences among the variables. The statistical analysis involved the utilisation of One-way ANOVA testing and Independent Samples t-tests, in addition to Pearson Correlation tests. A confidence level of 95% was consistently maintained throughout the research.

3. THE RESEARCH FINDINGS

When the descriptive statistics of smartphone security awareness were analysed, the skewness value was determined to be -0.38, and the kurtosis value was 0.23. The standard deviation value (s = 0.54) shows that there is no excessive difference between the participants according to the measured feature. Considering the mean values, it is seen that the students' (X = 4.15) smartphone security awareness levels are at a high level. The mean distribution of associate degree students' responses to the smartphone security awareness scale according to the items is presented in Table 2.

Table 2. *Findings related to the mean distribution of the responses to the smartphone security awareness scale according to the items (n = 612)*

Variable	Item No	X	SD
SSAS	1	3.99	0.94
	2	4.14	0.83
	3	4.54	0.78
	4	4.14	0.88
	5	3.69	1.07
	6	4.00	0.92
	7	4.49	0.79
	8	4.23	0.94
	9	4.10	0.92

Table 2 shows that the highest mean score is in item 3 (X_3 = 4.54), and the lowest mean score is in item 5 (X_5 = 3.69). On the other hand, when the standard deviation values were analysed, it was determined that there was no excessive difference between the answers given.

Independent Samples T-Test analysis was performed to determine whether the smartphone security awareness levels of associate degree students differed significantly according to gender, and it was observed that there was no statistically significant difference between the average smartphone security awareness score of female students (X_F = 4.16, s = 0.52) and the average smartphone security awareness score of male students (X_M = 4.12, s = 0.56) [t(612) = 0.77, $p>0.05$]. Accordingly, there is no difference between male and female students regarding smartphone security awareness levels.

Pearson correlation coefficients were used to determine whether there is a relationship between the smartphone security awareness of associate degree students and the variable of the duration of owning a smartphone. According to the findings, no significant relationship was found between the variable of the duration of owning a smartphone and smartphone security awareness (r = 0.04, $p>0.05$).

It was examined whether the smartphone security awareness levels of associate degree students differ significantly according to the status of experiencing security problems. In this context, Independent Samples T-Test analysis was performed. Smartphone security awareness varies according to the status of experiencing security problems, and the change is statistically significant (t(612) = 2.84, $p<0.001$). Accordingly, it was observed that students who had not experienced security problems before (X_N = 4.17, s = 0.53) had a higher level of smartphone security awareness than students who had experienced security problems before (X_Y = 4.01, s = 0.57).

Independent Samples T-Test analysis was conducted to determine whether there was a significant difference according to the use of smartphone security software by associate degree students, and it was found that there was no statistically significant difference between the average smartphone security awareness score of students using security software (X_Y = 4.15, s = 0.53) and the average smartphone security awareness score of students not using security software (X_N = 4.14, s = 0.55) [t(612) = -0.23, $p>0.05$].

One-way ANOVA tests were carried out to determine whether the smartphone security awareness levels of associate degree students showed significant differences according to their perceptions of competence in using information technologies, and the results obtained are presented in Table 3.

Table 3. *Findings related to smartphone security awareness according to perceptions of competence in using information technologies*

Variable	**IT level**	n	**X**	**SD**	**F**	**Difference**
SSA	Low (A)	58	3.89	0.52	12.98**	A-B**
	Medium (B)	400	4.13	0.53		A-C**
	High (C)	154	4.30	0.55		B-C**

***p*<0.001

From Table 3, it is seen that smartphone security awareness varies according to the perceptions of competence in using information technologies, and this change is statistically significant (F(2, 299.80) = 12.98, p<0.001). Tukey HSD test, one of the post-hoc tests, was applied to determine from which groups the differences originated (α =0.017). Accordingly, it was determined that students with a high level of perceived competence in using information technologies (X_C = 4.30, s = 0.55) had more smartphone security awareness than the others and students with a medium level of perceived competence in using information technologies (X_B = 4.13, s = 0.53) had more smartphone security awareness than students with a low level (X_A = 3.89, s = 0.52).

Independent Samples T-Test analysis was performed to determine whether the smartphone security awareness levels of associate degree students differ significantly according to the status of receiving information security training, and it is seen that there is no significant difference between the students who received information security training (X_Y = 4.19, s = 0.56) and the students who did not receive information security training (X_N = 4.13, s = 0.54) according to the level of smartphone security awareness (t(612) = -1.06, p>0.05).

Independent Samples T-Test analysis was performed to determine whether the smartphone security awareness levels of associate degree students differed significantly according to whether they were concerned about the privacy and protection of their personal data, and there was no significant difference between students who were concerned about the privacy and protection of their personal data (X_Y = 4.13, s = 0.53) and students who are not concerned about the privacy and protection of their personal data (X_N = 4.16, s = 0.57) according to the level of smartphone security awareness (t(612) = 0.51, p>0.05).

Pearson correlation coefficients were used to determine whether there is a relationship between smartphone security awareness and the digital literacy level of associate degree students. According to the findings, it was determined that there is a positive and moderately significant relationship between smartphone security awareness and digital literacy (r = 0.53, p<0.001, r^2 = 0.28). Accordingly, it was determined that as the level of digital literacy increases, the level of smartphone security awareness increases. In addition, it can be said that digital literacy explains 28% of the change in smartphone security awareness, and convergent validity is confirmed.

4. DISCUSSION AND RESULTS

In this study, it was found that students have a high level of smartphone security awareness. In addition, it was found that the level of smartphone security awareness did not vary according to gender. Although previously, the percentage of women owning and using a smartphone was very low, today, both genders use smartphones, and there is much less difference between genders in terms of the percentage of users [46]. In contrast, it has been reported that gender showed unexpected relationships with security behaviours [47]. It was reported that women are more security conscious and have a view towards improving existing authentication methods [48]. With this, it was found that men are generally more knowledgeable about security threats than women and trust official app stores more than women [49]. In addition, they found that men are more knowledgeable about malware attacks that may be caused by smartphone applications and give high priority to security when downloading applications. It was observed that women were more knowledgeable about malware attacks caused by SMSs than men. It was stated that women are more likely to save personal data on their smartphones [34]. However, in the current study, it is seen that there is no difference between female students and male students.

It is seen that there is no change in smartphone security awareness according to the duration of owning a smartphone. No difference was observed between new and more experienced users in terms of smartphone security awareness level. Smartphones are used both by experienced users who are knowledgeable about security and by people who ignore security issues [34]. This study found that students who had not experienced a security problem before had a higher level of awareness than students who had experienced a security problem. This is thought to be due to the fact that conscious users do not experience security problems. It was stated in their study that when it comes to choosing an application from the official application store, smartphone users ignore security issues and that users who do not consider security software necessary are more likely not to consider security issues in application selection [35].

On the other hand, in this study, no difference was observed in terms of smartphone security awareness between participants who use security software and those who do not. A study found that only 14.7% of the participants used software to secure their smartphones [37]. Similarly, it is reported that there was a lack of awareness when it came to additional security software such as virus scanners [26]. It was stated in their survey that the majority of users trust official app stores and tend to disable security software [35]. In this study, the number of those who do not use security software is higher than the number of users (Table 8). All these findings regarding the use of security software on smartphones are in line with a study's findings that 100% of respondents use security software on their PC/laptop devices, but only 31% use security software on their smartphones [50].

It was determined that the participants' awareness of security on smartphones varied according to their perceptions of competence in using information technologies. It was determined that the participants who stated themselves as high in the competence of using information technologies had higher smartphone security awareness than the others, and the participants who stated themselves as medium level had higher smartphone security awareness than those with low-level competence. It was noted that there was no significant difference across the level of using information technologies and whether a mobile application accessed personal data during installation and being aware of security software [37]. It was stated that participants who expressed themselves as experienced in using information technologies did not see any risk in downloading applications from official application stores [36].

In this study, no difference was found in terms of smartphone security awareness between students who had and had not received any previous information security training. These results alone are not sufficient to make a prediction about the importance of security training. In their study, they found that the awareness level of participants who received previous training was at the highest level [7]. In addition, it was found that individuals with good security knowledge use additional technical protection tools, and found by another study that individuals with poor familiarity with information technologies are inclined to ignore or be unaware of many critical security choices [51,52].

While most participants expressed concern about the privacy and protection of their personal data, there was no discernible difference in smartphone security awareness between students who were concerned about their data privacy and those who had no such concerns. This is thought to be due to the fact that individuals who are concerned do not feel the need to take any additional security measures. Although researchers, 63.8%, 67.9%, and 95.2% stated that participants were concerned about the protection and privacy of personal data, 72.2%, 71.6% and 75.8% of the participants, respectively, stated that they stored their personal data on their smartphones, which supports this argument [35,36,38].

Last but not least, it was determined that a relatively substantial and positive correlation exists between the level of knowledge regarding smartphone security and the level of proficiency in digital literacy. Accordingly, as the level of digital literacy increases, the level of smartphone security awareness also increases. When conceptual models related to digital literacy are examined, it is seen that many researchers include information and security in the sub-dimensions of the models they have developed. They emphasised on skills and components such as being able to evaluate information, being able to check that resources are safe and e-security, and being able to avoid harmful situations in digital environment [53-55]. In this context, it is possible to say that individuals' digital interests, competence and skills contribute positively to both variables.

Risks and threats are not far away if data is used in the transaction. Smartphone users are in constant and unnoticed data traffic through cellular, such as WiFi, Bluetooth, and networks, even if their screens are not actively switched on. However, solutions to prevent the infection and spread of malicious code on these platforms are different from PCs or other computer devices because these devices have insufficient resources, including power (battery) and processing units [56]. Official app stores, app developers, and smartphone manufacturers are working hard to create a more and more stable security environment for end users. However, the human factor is the weakest link in information security [57].

4.1. Limitations and Implications

The first limitation of this study is that the generalizability of the research is limited to two vocational schools of higher education in Isparta University of Applied Sciences since the research data were collected from associate degree students. Secondly, the data collected in this study is limited to students for whom the questionnaires were available online.

The level of readiness and awareness of the users is of great importance to minimise victimisation in cases such as data leakage, malware attacks, theft, loss, and fraud in technological devices that individuals actively use. In this context, it is necessary to provide necessary training in groups lower than the university education level and to include security awareness more effectively in the curriculum. In addition, this study determined that students with high competence in using information technologies had high levels of smartphone security awareness. In this context, basic information technologies courses should be given at every educational level.

Future research may involve using the “Smartphone Security Awareness Scale” developed in this study with different undergraduate and associate degree samples. However, it may be necessary to re-test the validity and reliability of the scale if it is used with lower educational levels (e.g., secondary education). Also, researchers could modify and update the scale in light of changing technology and emerging trends. Moreover, the impact of other variables on smartphone security awareness could be explored to further contribute to the existing literature in this area.

In line with the findings obtained as a result of future studies, relevant training programmes can be recommended by determining which sub-areas have deficiencies. In this direction, it is suggested that the curriculum programmes for the relevant educational level should be expanded, and the textbooks should be redesigned in the context of smartphone security awareness and digital literacy. In addition, it is thought that activities, such as training seminars and conferences, will be helpful for higher education institutions.

CONFLICTS OF INTEREST

No conflict of interest was declared by the authors.

REFERENCES

[1] Jeon, W., Kim, J., Lee, Y., Won, D., “A practical analysis of smartphone security”, Symposium on Human Interface, Springer, Berlin, Heidelberg, 311-320, (2011).

[2] Parker, F., Ophoff, J., Van Belle, J. P., Karia, R., “Security awareness and adoption of security controls by smartphone users”, 2nd International Conference on Information Security and Cyber Forensics (InfoSec) IEEE, 99-104, (2015).

[3] He, W., “A survey of security risks of mobile social media through blog mining and anextensive literature search”, Information Management & Computer Security, 21(5): 381-400, (2013).

[4] Theoharidou, M., Mylonas, A., Gritzalis, D., “A risk assessment method for smartphones”, IFIP International Information Security Conference, Springer, Berlin, Heidelberg, 443-456, (2012).

[5] Chin, E., Felt, A. P., Sekar, V., Wagner, D., “Measuring user confidence in smartphone security and privacy”, Proceedings of the 8th Symposium on Usable Privacy and Security, 1-16, (2012).

[6] McGill, T., Thompson, N., “Old risks, new challenges: exploring differences in security between home computer and mobile device use”, Behaviour & Information Technology, 36(11): 1111-1124, (2017).

[7] Koyuncu, M., Pusatli, T., “Security awareness level of smartphone users: an exploratory case study”, Mobile Information Systems, 2019(1): 1-11, (2019).

[8] Ben-Asher, N., Kirschnick, N., Sieger, H., Meyer, J., Ben-Oved, A., Möller, S., “On the need for different security methods on mobile phones”, Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services, 465-473, (2011).

[9] Pramod, D., Raman, R., “A study on the user perception and awareness of smartphone security”, International Journal of Applied Engineering Research, 9(23): 19133-19144, (2014).

[10] La Polla, M., Martinelli, F., Sgandurra, D., ”A survey on security for mobile devices”, IEEE Communications Services & Tutorials, 15(1): 446-471, (2013).

[11] Portokalidis, G., Homburg, P., Anagnostakis, K., and Bos, H., “Paranoid Android: versatile protection for smartphones”, In Proceedings of the 26th annual computer security applications conference (ss. 347-356), (2010).

[12] Park, J. H., Yi, K. J., Jeong, Y. S., ”An enhanced smartphone security model based on information security management system (ISMS)”, Electronic Commerce Research, 14(3): 321-348, (2014).

[13] Turner, A., “Mobile app statistics”, https://www.bankmycell.com/blog/number-of-mobile-apps-worldwide#:~:text=Today%2C%20there%20are%208.93%20million,installed%20on%20their%20, (2024).

[14] Sheila, M., Abdollah, M. F., Sahib, S., “Dimension of mobile security model: mobile user security threats and awareness”, International Journal of Mobile Learning and Organisation, 9(1): 66-85, (2015).

[15] Joshi, J., Parekh, C., ”Android smartphone vulnerabilities: a survey”, International Conference on Advances in Computing, Communication, & Automation (ICACCA), IEEE, 1-5, (2016).

[16] Çubukçu, A., Bayzan, Ş., “Digital citizenship perception in Turkey and methods of increasing this perception through conscious, safe and effective use of the internet”, Middle Eastern & African Journal of Educational Research, 5: 148-173, (2013).

[17] Spante, M., Hashemi, S. S., Lundin, M., Alger, A., “Digital competence and digital literacy in higher education research: systematic review of concept use”, Cogent Education, 5(1): 1-21, (2018).

[18] Inoue, H., Naito, E., Koshizuka, M., “Mediacy: what it is? Where to go?”, The International Information & Library Review, 29(3-4): 403-413, (1997).

[19] Eshet-Alkalai, Y., “Digital literacy: a conceptual framework for survival skills in the digital era”, Journal of Educational Multimedia and Hypermedia, 13(1): 93-106, (2004).

[20] Hockly, N., “Technology for the language teacher: digital literacies”, English Language Teaching Journal, 66(1): 108-112, (2012).

[21] Pegrum, M., “Modified, multiplied, and (re-)mixed: social media and digital literacies”, In M. Thomas, Digital Education, New York, NY: Palgrave Macmillan, 9-36, (2011).

[22] Sophos. “The state of ransomware 2024”, https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2024-wp.pdf , (2024).

[23] Nauman, M., Khan, S., Zhang, X., “Apex: extending android permission model and enforcement with user-defined runtime constraints”, Proceedings of the 5th ACM symposium on information, computer and communications security, 328-332, (2010).

[24] Zhou, Y., Jiang, X., “Dissecting android malware: characterisation and evolution”, IEEE Symposium on Security and Privacy, 95-109, (2012).

[25] Zhou, Y., Wang, Z., Zhou, W., Jiang, X., “Hey, you, get off of my market: detecting malicious apps in official and alternative android markets”, In NDSS, USA, 25(4): 50-52, (2012).

[26] Breitinger, F., Tully-Doyle, R., Hassenfeldt, C., “A survey on smartphone user’s security choices, awareness and education”, Computers & Security, 88, (2020).

[27] Furnell, S., “Why users cannot use security?”, Computers & Security, 24(4): 274-279, (2005).

[28] Furnell, S., Jusoh, A., Katsabas, D., „The challenges of understanding and using security: a survey of end-users”, Computers & Security, 25(1): 27-35, (2006).

[29] Furnell S., “Making security usable: are things improving?”, Computers & Security, 26(6), (2007).

[30] Whitten, A., Tygar, J. D., “Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0.”, USENIX Security Symposium, 348: 169-184, (1999).

[31] Breitinger, F., Nickel, C., “User survey on phone security and usage”, BIOSIG 2010: Biometrics and Electronic Signatures, Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, 139- 144, (2010).

[32] Imgraben, J., Engelbrecht, A., Choo, K.-K.R., “Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users”, Behaviour & Information Technology, 33(12): 1347-1360, (2014).

[33] Vecchiato, D., Martins, E., ”Experience report: A field analysis of user-defined security configurations of android devices”, IEEE 26th International Symposium on Software Reliability Engineering (ISSRE), 314-323, (2015).

[34] Androulidakis, I., Kandus, G., “A survey on saving personal data in the mobile phone”, Proceedings of the 6th International Conference on Availability, Reliability and Security, IEEE, 633-638, (2011).

[35] Mylonas, A., Kastania, A. Gritzalis, D., “Delegate the smartphone user? Security awareness in smartphone platforms”, Computers & Security, 34: 47-66, (2013).

[36] Talan, T., Aktürk, C., Korkmaz, A., Gülseçen, S., “Security awareness of university students in smartphone use”, Istanbul Journal of Open and Distance Education, 1(2): 61- 75, (2015).

[37] Büyükgöze, S., Bıkmaz, Z., Dereli, E., Korkmaz, A., “Mobile security awareness of computer programming students”, 2nd International Congress of Contemporary Education Research, September-October, Muğla, Turkey, 15-19, (2017).

[38] Bıkmaz, Z., ”Determination of mobile security awareness and digital data security awareness of health management students”, International Journal of Management Information Systems and Computer Science, 1(1): 22-30, (2017).

[39] Karasar, N., “Scientific research method”, Ankara: Nobel Publication Distribution, (2005).

[40] Frankel, J. R., Wallen, N. E., Hyun, H. H., “How to design and evaluate research in education (8th ed.)”, New York: McGraw-Hill International Edition, (2012).

[41] Büyüköztürk, Ş., “Questionnaire development”, Turkish Journal of Educational Sciences, 3(2): 133-151, (2005).

[42] Wilson, N., McClean, S., “Questionnaire design: a practical introduction”, Coleraine: University of Ulster, (1994).

[43] Field, A. P., “Discovering statistics using Ibm Spss Statistics: and sex and drugs and Rock’ N’ Roll (4th Ed.)”, Sage, London, (2013).

[44] Ng, W., “Can we teach digital natives digital literacy?”, Computers & Education, 59(3): 1065-1078, (2012).

[45] Üstündağ, M.T., Güneş, E., Bahçivan, E., “Turkish adaptation of digital literacy scale and investigating pre-service science teachers’ digital literacy”, Journal of Education and Future, 12: 19-29, (2017).

[46] Madden, M., Lenhart, A., Duggan, M., Cortesi, S., Gasser, U., “Teen and technology 2013”, https://www.pewresearch.org/internet/2013/03/13/teens-and-technology- 2013/, (2013).

[47] Ophoff, J., Robinson, M., “Exploring end-user smartphone security awareness within a South African context”, Information Security for South Africa, IEEE, 1-7, (2014).

[48] Sieger, H., Möller, S., “Gender differences in the perception of security of mobile phones”, Proceedings of the 14th International Conference on Human-computer Interaction with Mobile Devices and Services Companion (MobileHCI’ 12), Association for Computing Machinery, New York, NY, USA, 107-112, (2012).

[49] Pramod, D., Raman, R., “A study on the user perception and awareness of smartphone security”, International Journal of Applied Engineering Research, 9(23): 19133-19144, (2014).

[50] Murray, C., “Smartphone security risks: the extent of user security awareness”, Trinity College Dublin Master’s thesis, (2014).

[51] Benenson, Z., Kroll-Peters, O., Krupp, M., “Attitudes to it security when using a smartphone”, Proceedings of the Federated Conference on Computer Science and Information Systems (FedCSIS). September, Wrocław, Poland, (2012).

[52] Watson, B., Zheng, J., ”On the user awareness of mobile security recommendations” Proceedings of ACM SE ’17. April, Kennesaw, GA, USA, 120-127, (2017).

[53] Eshet-Alkalai, Y., Amichai-Hamburger, Y., “Experiments in digital literacy”, CyberPsychology & Behaviour, 7(4): 421-429, (2004).

[54] Hague, C., Payton, S., “Digital literacy across the curriculum”, London: Futurelab, (2010).

[55] Ng, W., “Empowering scientific literacy through digital literacy and multiliteracies”, New York: Nova Science Publishers, (2013).

[56] Zaidi, S., Shah, M., Kamran, M., Javaid, Q., Zhang, S., “A survey on security for smartphone device”, Internaitonal Journal of Advanced Computer Science and Applications, 7(4): 206-219, (2016).

[57] Åhlfeldt, R. M., Spagnoletti, P., Sindre, G., “Improving the information security model by using TFI”, IFIP International Information Security Conference, Springer, Boston, MA, 73-84, (2007).

APPENDIX A

Smartphone Security Awareness Scale (SSAS)	Strongly Disagree (1)	Disagree (2)	Undecided (3)	Agree (4)	Strongly Agree (5)
1. I know that I have to keep the location feature switched off so that my smartphone and apps do not constantly track my location.					
2. I know that I need to check whether unwanted apps are running in the background on my smartphone.					
3. I know that if I want to sell/replace my smartphone, I have to completely reset my phone.					
4. I make sure that the apps I use on my smartphone are up to date.					
5. I am aware of the symptoms that can occur if my smartphone is infected with malware (viruses, worms, trojans, etc.).					
6. I prefer to use instant messaging apps with encryption support (end-to-end, etc.) on mysmartphone.					
7. I use password methods (password, PIN, fingerprint, facial recognition, etc.) on my smartphone.					
8. I do not share the password for my smartphone with others.					
9. When I download an app on my smartphone, I look at user ratings and reviews to see if the app is secure.					