Hindawi
Mobile Information Systems
Volume 2019, Article ID 2786913, 11 pages
https://doi.org/10.1155/2019/2786913

Research Article

Security Awareness Level of Smartphone Users: An Exploratory Case Study

Murat Koyuncu [1] **and Tolga Pusatli** [2]

[1]*Information System Engineering, Atilim University, Ankara, Turkey*
[2]*Department of Mathematics, Cankaya University, Ankara, Turkey*

Correspondence should be addressed to Murat Koyuncu; mkoyuncu@atilim.edu.tr

Received 5 December 2018; Accepted 23 April 2019; Published 13 May 2019

Academic Editor: Marco Picone

As smartphone technology becomes more and more mature, its usage extends beyond and covers also applications that require security. However, since smartphones can contain valuable information, they normally become the target of attackers. A physically lost or a hacked smartphone may cause catastrophic results for its owner. To prevent such undesired events, smartphone users should be aware of existing threats and countermeasures to be taken against them. Therefore, user awareness is a critical factor for smartphone security. This study investigates the awareness level of smartphone users for different security-related parameters and compares the awareness levels of different user groups categorized according to their demographic data. It is based on a survey study conducted on a population with a different range of age, education level, and IT security expertise. According to the obtained results, in general, the awareness level of participants is fairly low, which needs considerable improvement. In terms of age, the oldest group has the lowest level followed by the youngest group. Education level, in general, has a positive effect on the awareness level. Having knowledge about IT is another factor increasing the security awareness level of smartphone users.

1. Introduction

Proliferation of smartphones clearly shows their wide adoption by the public. Today, smartphones have even reached to the point of addiction for many and have become an indispensable instrument in people's daily lives [1]. Smartphones can be used for many different purposes besides phone calls: these include not only sending/receiving e-mails but also staying online in social media using programs such as Twitter, Google+, and Facebook as well as conducting electronic financial transactions. The flexible structure of smartphones gives designers and developers the ability to imagine and develop new and innovative applications. Therefore, today smartphone users have a large application portfolio to be installed and used for different purposes. The related figures can be seen from Google Play Store and Apple App Store containing about 3.8 million and 2 million applications, respectively, as of the first quarter of 2018 [2]. The number of cumulative app downloads has reached 178.1 billion mobile apps in 2017, which is a clear indication about smartphone usage [3]. In computer history, the market share of smartphones overtook the leadership of desktops in 2016, and mobiles, desktops, and tablets had 52.52%, 43.63%, and 3.85% of the market share as of June 2018, respectively [4].

On the one hand, there are many advantages in using smartphones, but on the other hand, there are many security threats as well [5–7]. New mobile malware threat statistics show not only a dramatic increase in the number of new malwares but also an increase in sophistication and complexity. Symantec observed 18.4 million mobile malware detections in total in 2016, which is an increase of 105 percent in 2015 [8]. The total count of malware detected over 6 months by McAfee Labs in 2016 is 37 million [9]. The number of threat families in the Google Play Store increased by a whopping 30% in 2017, making even the official

Android App Store a risky proposition for users according to McAfee 2018 Q1 Mobile Threat Report [10]. These numbers show clearly the level of risk for mobile devices. According to the study done by McGill and Thompson [11], users are much more likely to be actively protecting their home computer/laptop than their smartphone/tablet. Although many people are still reluctant to use their mobile devices for important transactions such as financial activities, this use pattern is changing with youngsters who are no longer so reluctant to use mobile devices for such transactions. Therefore, mobile devices are more likely to be at risk than a home computer. Although smartphones are generally considered as private devices, they can also be used for organizational tasks in the scope of the "bring your own device" (BYOD) concept [12]. As a result, security for smartphones becomes crucial.

As indicated in some of the latest studies, user awareness is a critical factor for smartphone security. For example, European Network and Information Security Agency (ENISA) highlights "lack of user awareness" as a vulnerability for smartphone security [13]. Similarly, Jeon et al. [6] listed user unawareness as one of the vulnerabilities for smartphones. Watson and Zheng [14] investigate user awareness of mobile security recommendations and conclude that especially those without strong information technology familiarity tend to ignore or be unaware of many critical security options. Therefore, they suggest to develop methods to improve awareness and adoption of mobile security. Smartphones become a valuable target for attackers because of the information they contain. It is, therefore, critical for smartphone users to take precautionary measures, including awareness of vulnerabilities and threats as well as adoption of security controls against threats [15]. Dinev and Hu [16] define *technology awareness* as a user's raised consciousness of and interest in knowing about technological issues and strategies to deal with them and show the technology awareness as one of the stimuli for determining the attitude in their awareness-centric model. Bitton et al. [17] present a hierarchical taxonomy for security awareness specifically designed for mobile device users in which a set of measurable criteria is defined and categorized according to different technological focus areas and within the context of psychological dimensions. In this scope, this study aims to investigate the levels of awareness of smartphone users on different security-related parameters and compare these levels based upon age, education level, and cybersecurity knowledge level.

Although there are studies investigating the security awareness level of computer users, only a limited number of them have focused on smartphone security, which has a different user behavior pattern than normal computers [11, 17]. Also, most of the studies investigate smartphone awareness in a restricted environment such as a university with students and/or faculties [14, 16, 18–21]. However, this study aimed to collect data from a wide range of population in terms of demography. In addition, smartphone proliferation continues, and people become more and more familiar with this technology. Thus, there is a requirement to observe the latest awareness level of users. Based upon this, the authors believe that this study provides valuable information to the literature to understand current awareness levels of smartphone users from different demographic perspectives for the purpose of developing methods to improve it.

The rest of the paper is organized as follows. The next section presents related studies. Section 3 explains the methodology used for the study. In Section 4, the essential statistical analysis results are presented and discussed. Section 5 includes the conclusions, theoretical and practical implications, and future research recommendations.

2. Related Studies

While ease-of-use and speed are tempting to users, there are considerable risks associated with these advantages. Studies including the one by Androulidakis [22] have drawn attention to the threats in mobile telephones due to lack of awareness in security and privacy. Mylonas et al. [23] explore the security awareness of smartphone users, who download applications from official application repositories. Their survey findings show that the majority of users trust the app repository, security controls are not enabled or not added, and users disregard security during application selection and installation. McIlwraith [24] explains security awareness as a concept having two parts: the first part is the practice of making people aware of the issues relating to information security; the second part involves encouraging them to act in a way that is appropriate to the value of the information they handle as part of their everyday work activities. Markelj and Bernik [21] state that safety in cyberspace depends on the users' knowledge of threats and their appropriate response to them. To achieve this, user awareness should be raised, and users should be informed of threats and undergo suitable education on work safety in cyberspace.

From the given studies above, it is clear that awareness about smartphone security threats and mechanisms to be used against these threats is important. In this scope, we need to reveal the parameters that users should be aware of. In other words, on the basis of smartphones, what are the important issues for users in terms of security?

Harris et al. [25] explore the factors that influence a consumer before installing a mobile application and conclude that consumers look more at security when determining risks. Perceiving less risk leads to more trust, which then leads to more intent to install apps. European Network and Information Security Agency (ENISA) highlights "lack of user awareness" as a vulnerability for smartphone security [13] and recommends not to install applications unless the source is well known and trusted. Unawareness of risks related to installing applications from untrusted sources is shown as one of the vulnerabilities by Jeon et al. [6], asserting that, at the first step, "being aware of developers of the applications and their repositories" is one of the parameters that smartphone users should consider.

In order to benefit from the installed applications, a user should accept to share private information that the installed application asks or allow the application to access different

resources [6]. Despite these concerns, a work reported by Felt et al. [26] finds that a majority of the users tested does not pay attention to warnings while installing applications. Harris et al. [19] investigate the installation of apps asking for excessive permissions with the assumption that excessive permissions can increase security risk. In the ENISA's guidance [13], users are recommended to be aware of what installed applications can access, run, and activate on mobile phones. On the other hand, developers add mostly an end-user license agreement (EULA) document to inform and get consent from users about the application activities. However, this does not guarantee that the user reads and understands the content. According to a study conducted by Chin et al. [27], "participants do not greatly consider existing security indicators like privacy policies and EULAs. Instead, they rely on user reviews and popularity to signal the quality and safety of applications." While developers cannot force users to read and understand the content, at least, they do ask the user to click the "I agree" button. However, how many users really know what they agree is open to discussion. As a consequence, "being aware of EULA and resources that an application can access" is another parameter to be investigated in user awareness.

In Benenson et al. [28], the authors try to establish a mental model of IT security for mobile devices. According to their findings, users of mobile devices can be divided into two categories: those who consider their devices as a phone are associated with a lower security awareness and see themselves not responsible for the security of their devices; on the other hand, those who consider their devices as a smartphone are more aware of mobile security risks and also consider themselves more responsible to provide security for their devices. Information security is an issue for which multiple players should take responsibilities; these include state, service provider, organization (in case the workplace is included), and the individuals themselves [29, 30]. For instance, states should make laws and establish, or encourage, supporting organizations such as CERT [31]. Technologies such as cloud computing make the responsibilities more complicated and force the parties to act together [32]. Unfortunately, a considerable finding has revealed in Zaaba et al. [33] that employees using IT at their work places claim "I do not care whether I have the antivirus or not as I believe it's not my responsibility. It's my company's asset anyway." Concerning this literature, we evaluate that "being aware of smartphone user responsibilities (not considering security as a third-party responsibility)" should be another parameter to be investigated.

An attacker may deploy a rogue network access point, and users may connect to it. Then, the attacker may intercept the user communication to carry out further attacks such as phishing [13]. Gkioulos et al. [18] investigate security awareness of the digital natives, who are university students, for mobile devices. Network access focusing on the usage of free unsecured Wi-Fi connection is one of the investigated issues for awareness in the study. Attackers can corrupt, block, or modify information on the wireless network by sniffing, spoofing, or eavesdropping [6]. Because of that untrusted networks may become a nightmare for unaware smartphone users. Furthermore, a malware in a smartphone can communicate for different purposes such as leaking out information at unexpected times. Therefore, keeping smartphone always connected to the Internet increases risks. In the scope of these resources, "being aware of risks of uncontrolled Internet connections" is taken as another parameter to be investigated in this study.

According to ENISA, the amount of personal data, sensitive documents, and credentials stored and processed by smartphones makes them an appealing target for attackers [13]. Smartphones may be infected with malware specifically designed for stealing credit card numbers and online banking credentials. However, these devices have smaller interfaces which make entering some information more difficult compared to PCs. Therefore, users prefer to store credentials on smartphones for easiness. As a consequence, management of credentials and use of protection technologies is one of the parameters investigated by researchers for awareness [18]. In the light of this literature, "being aware of risks of storing credentials on smartphones" is also selected as one of the parameters to be investigated to measure the security awareness level of smartphone users.

Li and Clark [34] focus on malware targeting mobile phones and how dangerous they can be. When a user installs an application on a mobile device, he or she can only know what the application can do from the explanations provided by the developer. Even applications installed from Google Play Store and Apple App Store may have security breaches. Hence, hackers are tempted by this advantage to spreading malware. According to Markelj and Bernik [21], the knowledge of threats that the users of mobile devices may face and the use of security measures are essential. That is, users should be aware of security threats and security solutions to be applied against these threats [15]. In this scope, "being aware of technical measures" is another parameter that should be investigated.

In addition to the parameters given above, password/pattern usage, PIN usage, application update behaviors of users, which are also considered as security-related activities, are included in this study. Although it is possible to add other parameters, we have decided to limit this study in this scope since it will provide enough information to measure and evaluate the security awareness level of smartphone users.

3. Method

To determine the security awareness level of smartphone users, a survey is prepared and conducted as detailed in the following subsections.

3.1. Participants. The prepared survey is printed out and delivered to a pollster after pretesting by a limited number of participants. The survey is conducted in a popular shopping center in Ankara by the pollster in a week's period in summer 2018. In this way, we aimed to include a wide range of participants for demographic variables as it is possible to

find people from different ages, education level, and professions in such a location. Volunteer participants filled out the survey forms with the help of the pollster. The total number of participants is 155 ($N = 155$).

3.2. Measures. The participants are asked questions divided into three parts: the first part includes questions to determine demographic features including gender, age, level of education, and IT security knowledge, and the second part has six questions about smartphone usage by participants including duration, purpose, operating system, application update method, password, and PIN usage. As the result of the literature survey summarized earlier, the authors have decided to investigate awareness of smartphone users on six parameters and developed questions to measure their awareness levels, as shown in Table 1. For each parameter, two or three questions are developed as seen in Table 1. In connection with that, the third part of the survey includes these 13 questions prepared in 5-point Likert scale to measure user preferences, starting with 1 (strongly disagree) and gradually ending with 5 (strongly agree).

Internal consistency of the data is checked using Cronbach's alpha. All values are above 0.7 meaning that the reliability of the data is at an acceptable level.

4. Results and Discussion

4.1. Descriptive Statistics. The population's demography is summarized in Table 2. The number of female participants is higher than the males with a percentage of 58.1%. The age of the participants is divided into five categories, and the most populated category is the 21–30-year range with 36.1%. The age distribution shows that we have participants from a wide range of ages. The employment status of the participants is shown under the employment/sector section of Table 2. 19.4% and 50.3% of the participants work for public and private sectors, respectively. 25.8% are students and 4.5%, which is categorized as "others" includes the unemployed, housewives, and the retired. The education level is also determined with a question. Effort is made to include participants from different educational backgrounds, as seen in Table 2. The highest portion (41.9%) has a bachelor degree, while high school diploma is in the second order (27.1%) including also university students who are not graduates yet.

Table 3 gives some descriptive statistics about smartphone usage in the population. About half of the respondents had been using smartphones for more than 6 years. As the operating system of the smartphone, Android and IOS are dominant platforms with 60% and 36.1% usage rates, respectively. The next three items in the table are important for applying the least and basic security countermeasures. The first item is related to updating operating systems and applications. 65.8% of participants use the automatic update option, while 17.4% prefer manual updates. The rest either do not know or do not update applications in their smartphones. 76.8% and 67.7% declare that they use regularly password/pattern to access their phone and PIN to access their SIM cards, respectively.

The figures obtained in the current study for updates and password usage are rather similar to the numbers reported by Benenson et al. [28]. The rate of the participants who do not know or do not care about updates is 16.7% in this study and 15% in their study. The rate for password usage is 17.4% in this study and 23% in theirs. The ratio of updating smartphones automatically or manually is 83.3%. Gkioulos et al. [18] report 79.5%, 81.3%, and 88.6% regular update ratios for three different competence groups. In the study carried out by McGill and Thompson [11], the ratio of smartphone users using the automatic update option is calculated as 54.4%, while it is 65.8% in the present study. Interestingly, the ratios are rather similar.

Figure 1 shows the application types used by the participants in percentage. Accordingly, social media, image/video, and mapping applications occupy the first three mostly used types in the list. From the security point of view, a critical issue is that smartphones are used for online shopping and banking activities and their usage rates are 37.4 and 47.1% among the participants of the present study. This type of application usage is a clear indication why smartphone security awareness is important for users.

4.2. Security Awareness Level. The security awareness levels of all participants for the six parameters are given in Table 4. The mean values between 1 and 5 are seen in the table. Higher values are better, implying 5 represents the maximum awareness level and 1 represents the minimum. A value greater than 3 is considered as a "positive indication," while a value less than 3 is considered as a "negative indication" in terms of smartphone security awareness. Our findings confirm several prior research results, as well as add some new insights as follows.

4.2.1. Being Aware of Developers of the Applications and Their Repositories. The obtained results show that, although users generally install applications from well-known repositories such as Google Play and App Store, there are users downloading and installing applications from other sources. However, a vast majority prefers to download applications from official platforms with a mean value of 3.97. The percentage of downloading applications only from official repositories is 74.84% (marked "agree" and "strongly agree" in the questionnaire), while Parker et al. [15] report 96.9% and Chin et al. [27] report 85% for the same parameter. Although the given numbers are different, they clearly show that, in general, users prefer official repositories for application downloading. We understand that 17.42% of participants also install applications from other sources, while 29.6% and 19.8% are reported by Parker et al. [15] and Watson and Zheng [14], respectively. According to the findings of Mylonas et al. [23], users believe that downloading apps from such repositories is secure. Although there is no full guarantee to have secure apps, we know that applications shared by such repositories are passed through serious controls. For example, Google declares that it vets every app and developer in Google Play and suspends those who violate

Table 1: Issues to be investigated and survey questions.

Parameters	Questions
(1) Being aware of developers of the applications and their repositories	I check the developers of the applications I install I install applications only from official repositories such as App Store and Play Store
(2) Being aware of EULA and resources that an application can access	I read the end-user license agreement (EULA) of my applications I pay attention to what my applications can access, run, and activate on my mobile
(3) Being aware of smartphone user responsibilities	In case of an unpermitted use, it is enough to say "someone else has done it" The government protects me, I do not have to take any additional precautions The service provider is responsible for cybersecurity
(4) Being aware of risks of uncontrolled internet connections	My GSM data connection is not always on I do not use open Wi-Fi connections in public places
(5) Being aware of risks of storing credentials on smartphones	I do not store my credentials on the smartphone for financial applications (I have to enter my credentials each time I use the application) My social media accounts are not always on (I have to enter my PW each time I get connected)
(6) Being aware of technical measures	I encrypt my files stored on smartphones I use antivirus programs

Table 2: Demographic structure of the population.

	Frequency	Percentage
Gender		
Male	65	41.9
Female	90	58.1
Total	155	100.0
Age		
<21	36	23.2
21–30	56	36.1
31–40	32	20.6
41–50	24	15.5
>50	7	4.5
Total	155	100.0
Employment/sector		
Public	30	19.4
Private	78	50.3
Student	40	25.8
Others	7	4.5
Total	155	100.0
Education		
<High school	8	5.2
High school	42	27.1
Bachelor	65	41.9
Master	19	12.3
PhD	21	13.5
Total	155	100.0

Table 3: Statistics for smartphone usages.

	Frequency	Percentage
History (in years)		
<6	75	48.4
6–10	49	31.6
>10	31	20.0
Operating system		
Android	93	60.0
IOS	56	36.1
Others	6	3.9
Updates		
Automatic	102	65.8
Manual	27	17.4
Not known	19	12.3
No update	7	4.5
Password/pattern		
Yes	119	76.8
Sometimes	9	5.8
No	27	17.4
PIN		
Yes	105	67.7
Sometimes	3	1.9
No	46	29.7

their policies. Therefore, we evaluate that downloading and installing apps from official repositories is more secure than downloading and installing from unknown sources (for example, there are sites providing pirated software). Furthermore, the developer of an application can be a good indication in terms of security; therefore, reviewing available information about developers is considered a good precaution [19]. According to our results, a minority of users check the developers of applications only to a certain extent, and the obtained result is not very high with a mean value of 3.23. Harris et al. [19] reports that only 26% of users investigate the developers when they install applications. Although our finding is much better with 48%, it is still not at a satisfactory level. Overall, "being aware of developers of the applications and their repositories" gives the highest level among the measured parameters with a value of 3.60, which is the average of the measured two questions. However, this value is not as high as expected for a satisfactory awareness level, which is supposed to be greater than 4.00.

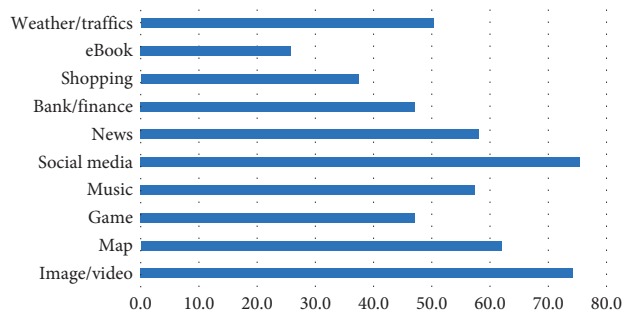

Figure 1: Used application types.

Table 4: Awareness levels.

	Mean	SD
Being aware of developers of the applications and their repositories	*3.60*	*1.30*
I check the developers of the applications I install	3.23	1.37
I install applications only from official repositories such as App Store and Play Store	3.97	1.22
Being aware of EULA and resources that an application can access	*3.16*	*1.36*
I read the end-user license agreement (EULA) of my applications	2.65	1.42
I pay attention to what my applications can access, run, and activate on my mobile	3.66	1.31
Being aware of smartphone user responsibilities	*3.29*	*1.28*
In case of an unpermitted use, it is enough to say "someone else has done it"	2.67	1.26
The government protects me, I do not have to take any additional precaution	2.58	1.21
The service provider is responsible for cybersecurity	2.88	1.37
Being aware of risks of uncontrolled Internet connections	*2.82*	*1.48*
My GSM data connection is not always on	2.66	1.45
I do not use open Wi-Fi connections in public places	2.97	1.51
Being aware of risks of storing credentials on smartphones	*3.08*	*1.49*
I do not store my credentials on the smartphone for financial applications (I have to enter my credentials each time I use the application)	3.55	1.47
My social media accounts are not always on (I have to enter my PW each time I get connected)	2.61	1.51
Being aware of technical measures	*3.07*	*1.42*
I encrypt my files stored on smartphones	2.88	1.34
I use antivirus programs	3.27	1.49

4.2.2. Being Aware of EULA and Resources that an Application Can Access. It is measured with two questions: the first for EULA and the second for access permissions, and their means are 2.65 and 3.66, respectively. According to the results, only 29.03% of the participants read EULA. In another study, Parker et al. [15] found that 82 percent of respondents do not read the license agreement. Chin et al. [27] found that participants do not greatly consider existing security indicators, such as privacy policies and EULAs. These results clearly show that smartphone users are not aware of the importance of EULA for security. An installed application can do an activity which is risky for the user. The interesting point is that, in general, such activities are written in the EULA, and the application requires user consent to this EULA during installation. As a consequence, approving EULA without reading it may cause serious security problems later. On the other hand, most of the participants pay attention to what the installed applications can access, run, and activate on their mobiles. 63.87% of the participants declare that they read the permission requests upon initial installation of an application, which is a very close number (58.8) to that of reported by Parker et al. [15]. According to the results obtained by Mylonas et al. [23], the percentage of users who always view security messages is 38.6%, while 48.3% examine them only sometimes. Especially, when an application requests more than the minimum required permissions, it may lead to risk of information theft and remote attacks [19]. Although the majority of users declare that they control permission requests of applications, still there is a significant number of those who do not control it. That means an important number of users are often unaware of the implications when granting permissions to applications. On average, the "being aware of EULA and resources that an application can access" parameter is slightly higher than 3, which means users are not very cautious in this regard.

4.2.3. Being Aware of Smartphone User Responsibilities. This parameter aims to measure whether users are aware of their responsibilities or consider smartphone security as a third-party responsibility. The average of the three questions is 3.29, which shows a positive but low awareness level. Notice that the questions of this parameter are reverse scored since the questions imply negativity in terms of security. Benenson et al. [28] report that 36% of smartphone users see themselves responsible for the security of their devices and the rest consider it as the responsibility of producers. Interestingly, we have obtained the same number (36%) representing the ratio of users who do not accept the security as the responsibility of only service providers. That is, they consider that they are also responsible for it. There are many smartphone users having the tendency to consider smartphone security as the responsibility of third-parties, such as the service provider and the government. Such users are not likely to take enough measures to protect their smartphones against threats. According to Lie et al. [29], end users are in a key position as they install technical safeguards for IT security at the most basic level. Therefore, their basic cybersecurity awareness should be improved with the support of the government and the private sector.

4.2.4. Being Aware of Risks of Uncontrolled Internet Connections. For this parameter, we checked whether the participants are always connected to the Internet via GSM data connection and also whether they connect to free Wi-Fi in public places such as coffee shops, malls, and restaurants, and the obtained mean values are 2.66 and 2.97, respectively. From these numbers, we first understand that most of the participants prefer to be always online and connect to Wi-Fi access points in public places. Only 34.84% marked "agree" and "strongly agree" options, which shows a controlled connection to the Internet. That is, they connect to the

Internet when they need it. 54.84% of them prefer to be always online with their GSM connections on. Another interesting point is that a major portion of the participants (44.52%) declare that they connect to free Wi-Fi in public places. This number is very similar to that given by Gkioulos et al. [18], which is 43.6%, for the non-IT-related group. Many studies show free Wi-Fi connections as a threat for smartphones because of different security risks [6, 13]. For example, a smartphone user having the intention to use free Wi-Fi can accidentally connect to a rogue access point which may create unexpected security problems [35]. Such a device may be exposed to several risks including, but not limited to, man-in-the-middle attack, flooding the network with useless data (DoS attack), and theft of valuable information. McAfee reports that network spoofing has increased dramatically during the 18 months leading to the first quarter of 2018, with hackers setting up their networks in public places, waiting for users to connect, and watching the traffic for sensitive information such as banking logins and credit card numbers [10]. Therefore, smartphone users are expected to be aware of such risks and, accordingly, be alert when they connect to a network. However, the obtained results do not show a satisfactory level of awareness and indicate the need to increase such awareness among smartphone users.

4.2.5. Being Aware of Risks of Storing Credentials on Smartphone. The obtained mean values are 3.55 and 2.61 for the questions "I do not store my credentials on the smartphone for financial applications" and "My social media accounts are not always on," respectively. These numbers show that participants are more cautious toward financial applications such as online banking. However, for social media accounts they prefer to store them on the smartphone for quick access. It is likely that they do not consider storing social media credentials as dangerous as storing financial applications' credentials. In the study of Gkioulos et al. [18], the ratios of users saving their credentials to stay logged in are 40.3%, 30.8%, and 48.6% for general, medium, and high smartphone competency levels, respectively. Jones and Chin [20] report that 29% of participants store their credentials such as PIN and password in their smartphones (data from 2014). In the current study, it is 29% which is exactly the same ratio given by Jones and Chin [20] and a very close figure to that obtained for medium competency by Gkioulos et al. [18]. McAfee [10] reports that there is an increase in malicious banking trojans that take advantage of vulnerabilities in the Android platform and which add crypto ransomware capabilities to smartphones among other malicious activities. Therefore, we evaluate that there is a clear requirement to increase the awareness level on this issue.

4.2.6. Being Aware of Technical Measures. It is measured by two questions asking about file encryption and antivirus usage by the participants. As seen in Table 4, on average, the result is 3.07 which indicates that this awareness level is not at a satisfactory level for "being aware of technical measures." According to the results, the usage rate of antivirus programs is higher than file encryption. Jones and Chin [20] analyze smartphone security practices of undergraduate students and compare the results of 2011 and 2014. According to their 2014 results, 57% and 52% of the participants use antivirus and encryption, respectively. Our results show 54.19% antivirus and 37.42% encryption usage rates. Although these antivirus usage rates are close, the encryption usage rates are rather different. The reason may be related to the difference in the population. While they include only undergraduate students, our study covers a wide range of people. In another study, McGill and Thompson [11] report the usage of security software as 44.6%. In a study done with university students, Markelj and Bernik [21] determined 29.5% and 5.8% usage ratios for antivirus and encryption usage, respectively. All these figures obtained from different studies do not show high usage rates for technical measures, such as antivirus and file encryption, which is an indication of low awareness.

4.3. Security Awareness Levels of Age Groups. First, we evaluated age groups in terms of different parameters given in Table 3. For operating systems, age is not a distinguishing feature. There are no significant differences among different groups for smartphone operating system preferences. For PIN usage, the age again does not give any significant differences. However, for password/pattern usage and system update, we observe major differences among groups (password/pattern: $X^2 = 22.95$, $\mathrm{df} = 8$, $p < 0.05$, update: $X^2 = 22.32$, $\mathrm{df} = 12$, $p < 0.05$). The 21–30 age group is the most sensitive one with 87.5%, while the oldest group is the one with the lowest ratio 28.5%. On the contrary, the 31–40 age group prefers to use the automatic update option with 84.4%, which is the highest value. The oldest group has again the lowest value with 42.9%, which indicates that their awareness level is lower than the others. Jones and Chin [20] analyzed the update behavior of users based on the age feature, observing no significant difference. The participants of their study were all students. However, in the current study, the age range of the participants is rather large and, therefore, significant differences are observed among the age groups.

The awareness levels of different age groups for the measurements given in Table 1 are presented in Table 5. An overall evaluation can be done considering the averages given in the last row. According to the results, the groups younger than 21 and older than 50 having very close numbers are distinguishably different than the other three groups. The oldest group has the lowest awareness level, followed by the youngest group. The 41–50 age group has the highest level. Another point is that the awareness level increases according to age, except in the last group.

4.4. Degree of Security Awareness according to Education Level. Another analysis is done according to the education levels of participants including five categories as having PhD, MS, BS, high school, and lower than high school degrees(<HS). The obtained results do not show any significant differences for operating system preferences and

Table 5: Awareness levels according to age.

Ages	<21	21–30	31–40	41–50	>50
Being aware of developers of the applications and their repositories	3.50	3.69	3.67	3.65	3.15
Being aware of EULA and resources that an application can access	2.99	3.34	3.38	3.00	2.02
Being aware of smartphone user responsibilities	3.16	3.17	3.29	3.59	3.28
Being aware of risks of uncontrolled Internet connections	2.67	2.76	2.74	3.04	3.58
Being aware of risks of storing credentials on smartphones	2.87	2.80	3.21	3.83	3.22
Being aware of technical measures	2.92	3.19	3.08	3.07	2.72
Averages	3.02	3.16	3.22	3.36	2.99

password/pattern usages. However, we observe significant differences for PIN usage and system updates (PIN: $X^2 = 15.78$, $df = 8$, $p < 0.05$, update: $X^2 = 29.78$, $df = 12$, $p < 0.05$). The group having a PhD-level education has the highest ratios for PIN usage and system updates with 90% and 95.2%, respectively. On the contrary, the group having lower than high school education has the lowest values, which are 50% for PIN usage and 37.5% for system updates.

We observe two trends in the results, as seen in Table 6, for the third part of the questionnaire. Most of the parameters have increasing trends such that awareness level increases with the education level. That is, the group having PhD degrees has the highest value. However, for the second and sixth parameters, level values increase up to the BS degree and then decline. One reason for that may be the age factor. If we consider the levels given for ages, the oldest group has the lowest level. The participants having PhD degrees probably are older than the others. Therefore, for some parameters, even though the education level is high, the awareness levels are lower compared to other groups. When we look at the overall picture, the group having PhD degrees has the highest awareness level, followed by BS and MS groups. As a whole, the awareness level of the participants having BS or higher education degrees is better than the other groups. Our finding related to the education level confirms the result of Öğütçü et al. [36] who state that the higher the education level, the more their information security awareness is. Based on these results, we can state that the education level has a positive effect on the degree of security awareness among smartphone users.

4.5. Security Awareness Level according to Cybersecurity Knowledge. Another comparison is made considering the cybersecurity knowledge level of participants. The first group includes those who have taken at least one course about IT security at their university education or special training programs. The second group represents the ones having some knowledge about IT security although they do not have a formal training about it. The last group consists of those who have no idea about IT security.

There are no significant differences among different groups for operating system preferences, password/pattern usage, PIN usage, and system update options. The obtained results are given in Table 7 for the third part of the questionnaire. Except the last parameter, the awareness levels of the first group—having IT security training—are the highest. On average, the first group again has the highest value followed by the second group. Mylonas et al. [23] report that users with excellent IT skills tend to be aware of smartphone malware, as well as smartphone security software. Watson and Zheng [14] state that, especially those without strong information technology familiarity tend to ignore or be unaware of many critical security options. Benenson et al. [28] conclude that users with good security knowledge often use additional technical protection means. These results are considered as a clear indication for the importance of training on IT (including IT security) to improve the awareness level of users.

On the contrary, for "being aware of technical measures," although the difference is not substantial, the first group has a low value. The reason for this may be related to users trusting themselves as regards IT security knowledge. That is, since they know how to use smartphones securely in general, they do not encrypt the files on their smartphones or install antivirus programs. Gkioulos et al. [18] state that specific areas are not significantly affected by their security awareness or background. That is, although the high-security competence group is expected to have higher awareness due to their specialized education, they could not see any difference compared to other groups for some security measures. In addition, according to Kang et al. [37], technically oriented individuals who had their education in the IT domain did not in general take additional steps to protect their information, in comparison with the other group consisting of people from different domains in their study. Although they know more and express higher awareness for other issues, the usage behavior of technical measures such as encryption and antivirus programs is not very different. Mylonas et al. [23] conclude that users having high IT skills tend not to encrypt their data. Interestingly, different studies, including the present one, report similar behavior for users having higher IT skills, requiring further investigation to understand the reasons behind it.

5. Conclusions and Implications

5.1. Conclusions. This study aimed to investigate the awareness level of smartphone users from different perspectives including age, education level, and cybersecurity

Table 6: Awareness levels according to education.

Education degree	<HS	High school	BS	MS	PhD
Being aware of developers of the applications and their repositories	3.50	3.58	3.59	3.69	3.72
Being aware of EULA and resources that an application can access	2.63	3.03	3.40	3.12	2.91
Being aware of smartphone user responsibilities	3.11	3.13	3.20	3.28	3.99
Being aware of risks of uncontrolled Internet connections	2.75	2.67	2.88	2.71	3.02
Being aware of risks of storing credentials on smartphones	2.88	2.90	2.93	3.37	3.72
Being aware of technical measures	3.00	3.12	3.19	2.94	2.89
Averages	2.98	3.07	3.19	3.18	3.37

Table 7: Awareness levels according to cybersecurity knowledge.

IT security knowledge level	Have training	Have some knowledge	Have no knowledge
Being aware of developers of the applications and their repositories	3.72	3.67	3.54
Being aware of EULA and resources that an application can access	3.49	3.14	2.95
Being aware of smartphone user responsibilities	3.40	3.35	3.24
Being aware of risks of uncontrolled Internet connections	3.38	2.65	2.60
Being aware of risks of storing credentials on smartphones	3.21	3.09	2.89
Being aware of technical measures	3.04	3.24	3.02
Averages	3.37	3.19	3.04

training. The awareness levels of users are measured for different parameters, which are considered important for IT security. The reached conclusions of the study can be summarized as follows:

(i) The overall awareness level of the participants is not at a satisfactory level and needs improvement.

(ii) In terms of age, the oldest group (>50) has the lowest awareness level followed by the youngest group (<21).

(iii) The group having BS or higher education degrees has a better awareness level, which can be considered as an indication of the importance of education for cybersecurity.

(iv) The group having IT security training has the highest awareness level, which is another indication for the importance of training for cybersecurity.

(v) Studies done in previous years pointed out low security awareness levels among smartphone users [20, 21, 23]. The results of the current study indicate that risky behavior among users continues, and there is no clear improvement on their security awareness level.

5.2. Theoretical Implications. The current study makes several contributions to the literature. First, this study examines the security awareness level of smartphone users from different perspectives including age, education level, and security training. The existing studies prove that smartphone users have a different behavior than normal computer users [11, 17]. Therefore, those investigating computer users cannot necessarily be regarded as a direct indicator for smartphone use. On the contrary, there is very limited research focusing on the measurement of the smartphone security awareness level. As such, this study can contribute to the domain.

Second, the present study addresses the security awareness level of users from a wide range of demography. Although there are several studies investigating the security awareness level of smartphone users, most of them were conducted in universities with the participation of students and faculties [14, 16, 18–21]. There is a clear requirement to conduct studies to include different segments of the general public to generalize the derived conclusions. In line with this, the present work has been realized with the participation of people from a wide range of age, education level, and cybersecurity training.

Third, it provides valuable information to the literature to understand current awareness levels of smartphone users. Current statistics show that smartphone usage increases while security risks increase as well drastically. Such risks may cause severe loss for those involved. Thus, there is a requirement to observe the latest awareness level of users and share this information.

Fourth, it is also useful to see and understand similarities and differences between countries in terms of security behavior as different nationalities may have different awareness levels and behavior depending on various factors, thus necessitating further studies in this regard.

5.3. Practical Implications. With the increasing importance of IT security, the present study has three important practical implications. First, based on our findings, it is clear that the security awareness level of smartphone users needs to be improved. This can be achieved by a collective effort supported by governments, nongovernmental organizations, and others. This study can provide helpful information for them.

Second, our results can also be beneficial for hardware and software developers, for example, by showing that the awareness levels of young and old users are comparatively lower than others. Therefore, the design and implementation of security within smartphone platforms can be made simple and nontechnical to support old and very young users and also those from non-IT domains.

Third, our findings show clear evidence for the positive effect of education at the BS, MS, and PhD level for security awareness. Training on IT security also has a positive effect. Therefore, governments, institutions, and the private sector responsible for education can benefit from this study to add courses or modify the contents of existing courses to improve security awareness among individuals as a whole.

5.4. Future Work. This study has been conducted with the help of 155 volunteer participants from different segments of population. The same study can be repeated with more participants to generalize the obtained results. In addition, the study can be extended with additional questions to investigate other issues related to smartphone security. Here, we investigate the awareness level of smartphone users based on their usage behaviors. The research can be extended to understand the reasons behind such users' behaviors. Also, the present study was conducted based on individuals' perspectives and, hence, can be extended to include organizations for the purpose of understanding the security awareness level of users when they use their smartphones for business or any other initiatives that require teamworking.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] C. Chen, K. Z. K. Zhang, X. Gong, S. J. Zhao, M. K. O. Lee, and L. Liang, "Understanding compulsive smartphone use: an empirical test of a flow-based model," *International Journal of Information Management*, vol. 37, no. 5, pp. 438–454, 2017.

[2] Statista, "Number of apps available in leading app stores as of 1st quarter 2018," July 2018, https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores.

[3] Statista, "Number of mobile app downloads worldwide in 2017, 2018 and 2022," July 2018, https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads.

[4] StatCounter, "Desktop vs. mobile vs. tablet market share worldwide," July 2018, http://gs.statcounter.com/platform-market-share/desktop-mobile-tablet/worldwide.

[5] W. He, "A survey of security risks of mobile social media through blog mining and an extensive literature search," *Information Management and Computer Security*, vol. 21, no. 5, pp. 381–400, 2013.

[6] W. Jeon, J. Kim, Y. Lee, and D. Won, "A practical analysis of smartphone security," in *Human Interface, Part I, HCII 2011, LNCS 6771*, M. J. Smith and G. Salvendy, Eds., pp. 311–320, 2011.

[7] M. Theoharidou, A. Mylonas, and D. Gritzalis, "A risk assessment method for smartphones," in *Proceedings of the Information Security and Privacy Research (SEC), IFIP AICT*, Heraklion, Greece, June 2012.

[8] Symantec Corporation, *Internet Security Threat Report (ISTR)*, Vol. 22, Symantec Corporation, Mountain View, CA, USA, 2017.

[9] B. Snell, *Mobile Threat Report: What's on the Horizon for 2016*, Intel, Santa Clara, CA, USA, 2016.

[10] McAfee, *McAfee Mobile Threat Report Q1, 2018*, McAfee, Santa Clara, CA, USA, 2018.

[11] T. McGill and N. Thompson, "Old risks, new challenges: exploring differences in security between home computer and mobile device use," *Behaviour and Information Technology*, vol. 36, no. 11, pp. 1111–1124, 2017.

[12] P. Baillette, Y. Barlette, and A. Leclercq-Vandelannoitte, "Bring your own device in organizations: extending the reversed IT adoption logic to security paradoxes for CEOs and end users," *International Journal of Information Management*, vol. 43, pp. 76–84, 2018.

[13] G. Hogben and M. Dekker, *Smartphones: Information security risks, opportunities and recommendations for users*, ENISA, Heraklion, Greece, 2010.

[14] B. Watson and J. Zheng, "On the user awareness of mobile security recommendations," in *Proceedings of ACM SE '17*, Kennesaw, GA, USA, April 2017.

[15] F. Parker, J. Ophoff, J. P. Van Belle, and R. Karia, "Security awareness and adoption of security controls by smartphone users," in *Proceedings of Second International Conference on Information Security and Cyber Forensics (InfoSec)*, pp. 99–104, Cape Town, South Africa, November 2015.

[16] T. Dinev and Q. Hu, "The centrality of awareness in the formation of user behavioral intention toward protective information technologies," *Journal of the Association for Information Systems*, vol. 8, no. 7, pp. 386–408, 2007.

[17] R. Bitton, A. Finkelshtein, L. Sidi, R. Puzis, L. Rokach, and A. Shabtai, "Taxonomy of mobile users' security awareness," *Computers and Security*, vol. 73, pp. 266–293, 2018.

[18] V. Gkioulos, G. Wangen, S. Katsikas, G. Kavallieratos, and P. Kotzanikolaou, "Security awareness of the digital natives," *Information*, vol. 8, no. 2, p. 42, 2017.

[19] M. A. Harris, A. G. Chin, and R. Brookshire, "Mobile app installation: the role of precautions and desensitization," *Journal of International Technology and Information Management*, vol. 24, no. 4, pp. 47–62, 2015.

[20] B. H. Jones and A. G. Chin, "On the efficacy of smartphone security: a critical analysis of modifications in business students' practices over time," *International Journal of Information Management*, vol. 35, no. 5, pp. 561–571, 2015.

[21] B. Markelj and I. Bernik, "Safe use of mobile devices arises from knowing the threats," *Journal of Information Security and Applications*, vol. 20, pp. 84–89, 2015.
[22] I. I. Androulidakis, *Mobile Phone Security and Forensics: A Practical Approach*, Springer, Berlin, Germay, 2012.
[23] A. Mylonas, A. Kastania, and D. Gritzalis, "Delegate the smartphone user? Security awareness in smartphone platforms," *Computers & Security*, vol. 34, pp. 47–66, 2013.
[24] A. McIlwraith, *Information Security and Employee Behaviour: How to Reduce Risk through Employee Education, Training and Awareness*, Routledge, New York, NY, USA, 2016.
[25] M. A. Harris, R. Brookshire, and A. G. Chin, "Identifying factors influencing consumers' intent to install mobile applications," *International Journal of Information Management*, vol. 36, no. 3, pp. 441–450, 2016.
[26] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: user attention, comprehension, and behavior," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, Washington, DC, USA, July 2012.
[27] E. Chin, A. P. Felt, V. Sekary, and D. Wagner, "Measuring user confidence in smartphone security and privacy," in *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, Washington, DC, USA, July 2012.
[28] Z. Benenson, O. Kroll-Peters, and M. Krupp, "Attitudes to IT security when using a smartphone," in *Proceedings of the Federated Conference on Computer Science and Information Systems (FedCSIS)*, Wrocław, Poland, September 2012.
[29] E. Lie, R. Macmillan, and R. Keck, "Cybersecurity: the role and responsibilities of an effective regulator," in *Proceedings of the 9th ITU Global Symposium for Regulators (GSR)*, Beirut, Lebanon, November 2009.
[30] A. Palmer, "Cyber security: the road to security begins with personal responsibility," Symantec Official Blog, 2010.
[31] M. Bada, S. Creese, M. Goldsmi, C. Mitchell, and E. Phillips, *Computer Security Incident Response Teams (CSIRTs): An Overview*, Oxford Martin School, University of Oxford: Global Cyber Security Capacity Centre, Oxford, UK, 2014.
[32] S. K. Sood, "A combined approach to ensure data security in cloud computing," *Journal of Network and Computer Applications*, vol. 35, no. 6, pp. 1831–1838, 2012.
[33] Z. F. Zaaba, S. M. Furnell, and P. S. Dowland, "End-user perception and usability of information security," in *Proceedings of the Fifth International Symposium on Human Aspects of Information Security and Assurance (HAISA 2011)*, London, UK, July 2011.
[34] Q. Li and G. Clark, "Mobile security: a look ahead," *IEEE Security and Privacy*, vol. 11, no. 1, pp. 78–81, 2013.
[35] C. Wang, X. Zheng, Y. J. Chen, and J. Yang, "Locating rogue access point using fine-grained channel information," *IEEE Transactions on Mobile Computing*, vol. 16, no. 9, pp. 2560–2573, 2017.
[36] G. Öğütçü, Ö. M. Testik, and O. Chouseinoglou, "Analysis of personal information security behavior and awareness," *Computers and Security*, vol. 56, pp. 83–93, 2016.
[37] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler, "My data just goes everywhere: user mental models of the Internet and implications for privacy and security," in *Proceedings of the Eleventh Symposium on Usable Privacy and Security*, pp. 39–52, Ottawa, Canada, July 2015.