Indian Journal of Science and Technology, *Vol 11(16), DOI: 10.17485/ijst/2018/v11i16/119070,* April *2018*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Evaluation of the Attitudes towards Smartphone Applications when using Smartphone within Jordanian Community

Ahmad Mashhour[1], Zakaria I. Saleh[1] and Yaser Al-khateeb[2]

[1]Department of Information Systems, University of Bahrain, Zallaq, Bahrain; amashhour@uob.edu.bh, zsaleh@uob.edu.bh,
[2]Department of Computer Science, University of Bahrain, Zallaq, Bahrain; yalkhateeb@uob.edu.bh

Abstract

Objectives: This study investigates the attitudes towards using smartphone apps. in Jordan, while there exists some threats to mobile phone users' privacy. We also investigated user's awareness of the privacy and security threats when using smartphone applications. **Methods/Analysis:** A questioner was developed and distributed among random sample of Jordanian mobile users, Inferential Statistics (Regression and Correlation) techniques are used in the study, where Pearson correlation co-efficient is calculated to model the relationships between dependent and explanatory variables. The regression was used because it can designate whether those relationships are strong or weak. **Findings:** The study revealed more than 90% of users have installed apps on their smartphones and about 83% of them did not read the apps privacy policy before the installation. The study found that Perceived Security and IT Expertise have a positive effect on Perceived Privacy, and that Attitude towards smartphone app and Perceived Usefulness shows significant effect on apps installation. In addition, the study found that Perceived Usefulness and Perceived Privacy both have significant positive relation with Attitude towards smartphone apps. **Application:** This research covers smartphone user's privacy related issue when using the phone to run Vice over Internet Protocol (VoIP) applications, and provides several recommendations to protect users' privacy.

Keywords: Attitudes Towards, Jordan, Mobile Apps, Privacy, Security, Smartphone Apps, Threats

1. Introduction

In the era of widespread use of mobile devices, smartphone has become an essential device for communication, information exchange, and storage. Nowadays, so many people rely on their smartphones in their personal lives as well as their businesses. Most smartphone users exchange sensitive and private information using their smartphones assuming that the smartphone network is reliable and secure. While using his smartphone, a user may not suspect that his device is transmitting information to a third party who will subsequently use this information illegally. The question arises as to how much a person is protected from the illegal actions of collecting personal information while using such devices.

The advancement of wireless and mobile devices has brought the issue of security threats back into focus. The privacy issues breaches raised by digital technology are well documented by many authors including[1-3]. However, despite high percentage of concern about invasion of people privacy through new technology, they continue to deliver their sensitive data such as credit card details to smartphone. Mobile technology presents unique privacy challenges to users more than other types of technology[4-5]. Mobile devices are typically personal and carried with the user most of the times. This may facilitate unprecedented

*Author for correspondence

amounts of illegal data collection which can reveal sensitive information through communications with the associates. Mobile data also may be shared with third parties for many reasons such as to send consumers behaviorally targeted advertisements. So, it seems that many of us are willing to risk their privacy for the sake of convenience, since smartphone apps collecting our personal details, and gathering location-data to trace where we are.

Smartphones applications have the functionality of a desktop/laptop running on a general purpose operating system. In this respect many of the risks are similar to those of traditional spyware, Trojan software, and insecurely designed apps. While there is much overlap with common operating system models, the mobile device code of security model has some distinct points of differentiation.

According to the United States Federal Trade Commission Report (FTC, 2013), App developers should have a privacy policy and make sure it is easily accessible through the app stores. The FTC provides various relevant resources regarding, mobile privacy policies which includes: Mobile Privacy Disclosures, and children's Online Privacy Protection Act (CORPA).

The main threat to user privacy of smartphone is its applications (i.e. Apps) that are installed without awareness or discarding of their sequences. Many researchers reports that a high percentage of smartphone apps may threaten the user privacy[6], other surveys indicates that most of people install applications by themselves without reading "Privacy Policy" and "Terms and Conditions" of the end user's agreement and without checking it against viruses or[7]. Figure 1 forecasts the number of application download worldwide.

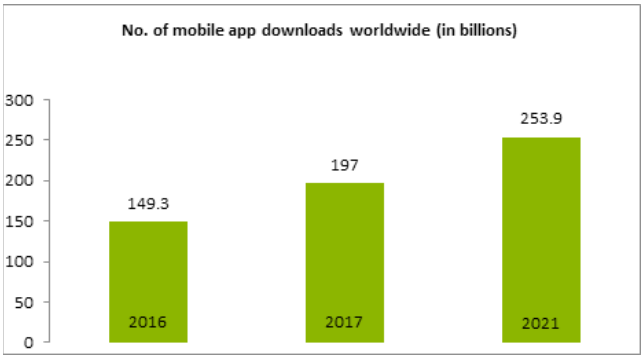

Figure 1. Mobile application download (Source: Statista, 2018)[27].

According to The Jordan Times survey[8], at least 95% of citizens in Jordan own a smartphone. Smartphone users in Jordan (as many other parts of the world) always assume that there is no reason to worry about the privacy of their phone calls and text messages sent over their mobile phones. In fact, privacy and security of the user's information and messages sent/received over their mobile phones can be legally or illegally breached by operators, law enforcements people, and individuals who has the technical expertise. Figure 2 depicts smartphone category uses by Jordanians.

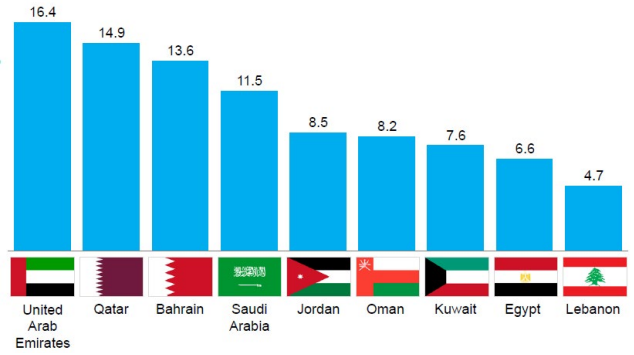

Figure 2. Smart phone penetration in Arab Countries (Source: Digital McKinsey)[28].

The research questions are:

1. Are Jordanians aware of the dilemma of apps espionage on their private information and the unrevealed functions of mobile devices to their private information stored or communicated via their smartphones?
2. In case they are aware of such breaches, what precautions do they take to protect their private information from illegally revelations action to a third party?

This study investigates the convenience of smartphone apps use by Joran youths associated with privacy and security awareness, and presents some recommendations to safeguard user's data and communication.

2. Smartphones Applications Overview

The app marketplace is filled with numerous free or low-priced app selections. Hundreds of thousands of apps are available for smartphones. According to[9], reported that

the accelerated use of smartphones has brought about emerging privacy and security concerns related to personal information protection. There are various vulnerabilities and risks associated with the use of smartphone targeting critical infrastructure assets[10]. Moreover[11] states that 95% of the tested apps have one or more vulnerability.

A smartphone user's privacy can be compromised in many different ways when using smartphone app such as infection by malware, which can embedded in applications that can modify or monitor information on smartphones. Apps may also collect information and share it with third-party companies. Many mobile users are unaware of the different ways in which their privacy can be breached and what steps they can take to protect their private information[12-14.]

The illegal collection of information is possible both through the installation of a malicious program on a mobile phone, the network, and undeclared functions installed on the mobile phone by its developer. Apps can collect all sorts of data and transmit it to the app-maker and/or third-party advertisers where it can then be shared or sold. As a customer to Internet service provider you may not be able to stop data collection, but you may be able to stop the data collected from being shared with third-parties (e.g. advertisers), because some service providers offer an opt-out agreement for certain types of advertising.

According to Privacy Rights Clearinghouse[15], smartphone service providers collect data of incoming and outgoing calls, incoming and outgoing text messages, and e-mails, and location data embedded onto image files can result in the tracking of the smartphone user, where more than 1 billion breaches were recorded since 2005.

According to the Federal Trade Commission[16], U.S. smartphone users had expressed concern about their privacy on mobile devices. 57% of all app users have either uninstalled an app because of concerns about having to share their personal information, or declined to install an app in the first place for similar reasons. About one-third of survey respondents reported feeling in control of their personal information on their mobile devices.

An exploratory study of users' smartphone security awareness conducted in South Africa showed that users are self-satisfied in their smartphone security behaviors, displaying high levels of trust towards smartphone app repositories. Users rarely consider privacy and security when installing new applications and also do not adequately protect themselves by adopting smartphone protection controls[7.]

According to Research[17], smartphone apps are collecting our personal details, including invisible 'cookies' tracking us online or location data revealing our whereabouts, where 61.1% of surveyed are being concerned about invasion of their privacy through new technology. In spite of that they continue to switch on, log in and hand over their credit card details.

According to the Centre for the Advancement of Social Sciences Research[18] which conduct a security survey among Chinese people, "70.3% of respondents did not know that apps might secretly access information they had not said they would".

According to Mobile Phone Security Awareness and Practices of Students in Budapest Research[12] the research shows that 40% of users use Antivirus in their mobile phone and 57% of users they store sensitive information in their phones, and a large percentage of the participants reaching 47% never perform a backup of their phone's data.

Regulatory agencies have attempted to preserve user privacy in the app marketplace. *Smartphone owners are generally more active in managing their mobile data, but also experience greater exposure to privacy intrusions.* According to the survey conducted by Pew Research on Internet and technology[19], conducted in 40 nations among them Jordan, nearly one third of cell owners have experienced a lost or stolen phone, while one in ten have had someone access their phone in a way that they felt invaded their privacy. *More than half of app users have uninstalled or decided to not install an app due to concerns about personal information. In addition, Cell phone owners take a number of steps to protect access to their personal information and mobile data and* one in five cell owners have turned off the location tracking feature on their phone, and one in three have cleared their cell phone browsing or search history.

According to the Pew Research survey[19], Jordan ranks 17 on Smartphone penetration and ranked second in Internet usage in the Arab world. The availability of smartphones in Jordan has significantly increased the number of social media users and this trend is expected to continue to grow. Using mobile phones to send text messages is the most popular activity among mobile users in Jordan, with 71 per cent of them using their phones to text.

According to the Ponemon Institute[20], 75% of respondents are very concerned about the security of their personal data when using smart devices. 66% are concerned about their security when using social media such as Facebook and Google.

Another study carried by[21], revealed that mobile security company found that ads from advertising networks running on some apps may change smartphone settings and take contact information without your permission. The study tested 384,000 apps and found that 19,200 of those apps used malicious ad networks.

Yovel research on smartphone applications[6] indicated that among the top paid and free mobile applications:

- 56% of the top 100 paid apps for Apple iOS had been hacked,
- 73% of popular free apps on Android had been hacked,
- 53% of popular free apps on Apple iOS had been hacked, and
- 100% of the top 100 paid apps on the Google Android platform had been hacked.

3. Smartphone User Privacy Protection

Smartphone can provide entertainment, information, and useful services. However, other through smartphones can invade our privacy through looking into the contact list, email, track the location, and enter or copy files without our knowledge. There are various threats to mobile phone users' privacy. Unfortunately, laws have not kept pace with changing technology. The first iPhone was released in 2007 and was accompanied with security and privacy threats. The main threats include the following: Signal Interception, access to text messages, access to user records, and access to stored information on smartphone sets[4,22]. The major smartphone attacks came from WLAN access where the IP address of smartphone users and may be detect by invaders. In addition, Bluetooth attack is a very common attack among the smartphone users. There are many kind of the Bluetooth attacker some of them may read your SMS, access your mobile setting, update your calendar, and more[23].

Moreover, another famous attack is by phishing, it occurs by installing a malicious application or webpage which looks the same as the original one, so the user install the fake application or give his personal information to untrusted person unintentionally[24.] Androulidakis[25] found that, 75% of the mobile user does not use a screen-lock for their device and 24.5% do not know if their mobile have this option or not.

3.1 Legal Safeguard

According to the Federal Trade Commission[16], app developers should have a privacy policy and make sure it is easily accessible through the app stores. The Federal Trade Commission provides various relevant resources regarding mobile privacy policies, which includes:

- Mobile Privacy Disclosures: Building Trust through Transparency;https://www.ftc.gov/reports/mobile-privacy-disclosures-building-trust-through transparency federal-trade- commission.
- Children's Online Privacy Protection Protect (CORPA): Websites that are collecting information from children are required to comply with CORPA: https://www.consumer.ftc.gov/articles/0031-protecting-your-childs-privacy-online.
- In most of the Middle East countries including Jordan, Laws designed primarily to protect privacy do not typically exist as laws in their own right, it such as may be found in the context of other laws. For example, the privacy of an individual is protected under general provisions of laws not specifically focused on the issue of privacy[26].
- The government of Jordan has pursued a proactive strategy of economic diversification, including substantial emphasis on ICTs. These efforts have resulted giving the Kingdom of Jordan a relatively high e-Government readiness rating of 0.52[19]. Every mobile app should have a Terms of Service /Terms and Conditions or in some instances as a Disclaimer. The content of the Terms of Service will vary based on the mobile app itself, its functionality, and the specific issues it poses.

3.2 Technical Safe Guards

In addition to tradition security measures of using user-id and password, to access user account on electronic devices such as smartphone, tablet and other devices,

many other technical safeguards can add more security including the following:

- *Network Authentication:* some devices such as IMSI catcher and femtocells can be utilized as faked base stations and permit others to get access to the smartphone users' information. This problem can be eliminated by introducing network authentication to the smartphones as smartphones are authenticated by the network with new protocols and software upgrading for the in mobile phone sets and the network as well.
- *Protection against Viruses/Spyware:* Mobile security software Products which include, AVG, McAfee, and Norton. Some products are downloaded with small fee or free of charges. Depending on the used software, you may be able to protect against malware, back up your smartphone data, store data elsewhere, track your phone if it is lost or stolen, protect against certain viruses, lock your phone remotely, and wipe your data remotely. However, as with anything else you download on your smartphone, be sure to research mobile security companies and software before you download it. Don't allow someone to exploit your trust just because they say they are providing you with a security service. Also, research privacy policies—the company may be giving free security software so that it can get your personal data.

1. *Password/Fingerprint Sensor:* majority of smartphone users do not use passwords to protect the stored information on their mobile phones despite the fact that a considerable percentage of users save personal and confidential information on their mobile phones. The fingerprint sensor (available in some new models of mobile phones) is considered more effective than passwords. Users, who store sensitive information in their smartphones, should consider adopting such protection measures.
2. Encryption of stored data and transmitted messages.

4. Research Hypothesis

The research hypotheses are as follows:

Attitude towards Smartphone Apps:

- H1: Attitude towards smartphone apps is positively associated with Perceived Privacy,
- H2: Attitude towards smartphone apps is positively associated with behavioral control, and
- H3: Attitude towards smartphone apps is positively associated with Perceived security.

Perceived Privacy:

- H4: Perceived Privacy is positively associated with the Subjective norms,
- H5: Perceived Privacy is positively associated with the Perceived Security, and
- H6: Perceived Privacy is positively associated with the IT Expertise.

Apps Installation:

- H7: Apps Installation is positively associated with Subjective norms,
- H8: Apps Installation is positively associated with Attitude towards smartphone apps, and
- H9: Apps Installation is positively associated with Perceived Usefulness.

5. Mobile Phone Users Survey

5.1 Survey Design of Research

The population of this research covers all the Jordanians who are 18 years or older, and covers different Jordanian communities with different level of educations. Items of the research are shown in Table 1.

Table 1. Items of the questionnaire

Mobile apps are reliable.	29
Using Mobile apps, I can rely on service providers to protect my privacy.	29
Smartphone apps cannot be trusted; there are just too many uncertainties.	29
Smartphone apps has the chance of fraud.	29
I believe my transmitted information will only reach the intended recipient.	29
I believe that the security system does not allow unauthorized access to my apps accounts.	29

I believe that the security system stops any unauthorized changes to my apps accounts.	29
I only use app is from a trustworthy source when I download software to my smartphone.	30
I am a Security savvy user (knowledgeable about smartphone security).	30
I am an IT expertise.	30
I have a Privacy Concern when using smartphone apps.	30
I install anti-virus program to protect my data.	30
I Use security software in smartphone to protect my data.	30
I Use encryption.	30
I Use device password lock.	30
I Use remote data wipe.	30
I Store personal data on my smartphone.	30
I Search and use free smartphone security software.	30
I am aware of the apps access rights to information on my smartphone.	30
I install anti-theft program.	New
I am concerned about data leak outside my smartphone.	New
I believe that there is a privacy risk using smartphone apps.	New
I believe that am being tracked when using smartphone apps.	New
Smartphone Apps save money.	New
Smartphone Apps makes it easier for me to call Worldwide.	New
Smartphone Apps provides me prompt and efficient services.	New
Smartphone Apps provides means to Keep in touch with others.	New
Smartphone Apps gives the joy of controlling my contact list.	New

To develop a questionnaire that can provide enough information about the level of user awareness about protecting their privacy while using the smartphone. Some of the Instrument Items were established by this research, and the rest were adopted from several published instruments as indicated in Table 1.

The questionnaire was reviewed by a number of experts in order to be modified, developed and to add important items to it. Total of 3 experts reviewed the questionnaire were mainly academic at different Universities of Jordan. After receiving feedback few questions were added and some others were modified based on discussion with the expert professional.

Pilot testing took place in three stages. The first stage consisted of developing and testing the terms used in the instrument as well as the instructions of how to use the instrument. The second stage was a test of the instrument by asking participants to take the survey online. The third and final stage was to test the reliability of the instrument. To test the internal consistency and reliability, the pilot test included a stage to calculate the internal consistency reliability coefficient.

The questionnaire was distributed to 500 different smartphone users in the Jordan community. The survey was distributed different group through paper formats (face-to-face using hard copies in different Jordanian's malls) as well as through the social media especially WhatsApp, and Facebook (200 questioners face-to-face and 300 questioners through the social media). The overall total of the response was 338 that have been collected through different data collection method (61.8% overall respond).

6. Analysis of Results

6.1 Demographic Data

The majority of the participants were between the ages of 18 and 30 years of age (71%). The respondents' age groups are illustrated in Figure 3.

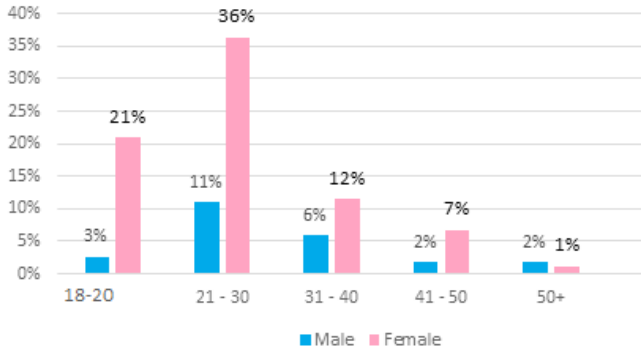

Figure 3. Respondents age group.

6.2 Descriptive Statistics

Calculated and analyzed mean and standard deviation of all the construct have been presented in Table 2. The result revealed the mean score: Apps installation is 4.774, Perceived Security is 3.564 and Perceived Privacy is 3.765. Similarly, the mean values for IT Expertise is

2.672, the Subjective norms is 2.593, Perceived behavioral control is 3.576, and Attitude towards smartphone apps is 3.415, which indicates that smartphone apps users are understand the security and privacy issues, and yet have a positive attune towards smartphone apps, because they believe that they are in control.

Table 2. Descriptive statistics

Variables	Min	Max	Mean	Standard deviation
Apps Installation	1	5	4.774	0.720
Perceived Security	1	5	3.564	0.145
Perceived Privacy	1	5	3.765	0.231
IT Expertise	1	5	2.672	0.817
Subjective norms	1	5	2.593	0.231
Perceived behavioral control	1	5	3.576	0.125
Perceived Usefulness	1	5	4.745	0.151
Attitudes towards smartphone apps	1	5	3.415	1.453

6.3 Inferential Statistics

In this section the results of the inferential statistical techniques used in the study are presented.

6.4 Attitude towards Smartphone Apps

Pearson correlation co-efficient is calculated in Table 3. The result shows that Perceived behavioral control, Perceived Usefulness and Perceived behavioral control have strong significant impact on Attitude towards smartphone apps as coefficient values indicate r= 0.467, r=0.457 and r = 0.379

Table 3. Correlation matrix

Variable	Attitude towards smartphone apps	
	Pearson correlation	significance 0.05 (2-tailed)
Perceived behavioral control	0.467	0.965
Perceived Usefulness	0.457	0.765
Perceived behavioral control	0.379	0.832

6.5 Perceived Privacy

The result of Table 4 reveals that subjective norms have a negative relationship with Perceived Privacy, confirming that subjective norms are insignificant in measuring Attitude towards smartphone apps. Whiles Perceived Security and IT Expertise have a positive effect on Perceived Privacy.

Table 4. Correlation matrix

Variable	Perceived Privacy	
	Pearson correlation	Significance 0.05 (2-tailed)
Subjective norms	-0.212	0.734
Perceived Security	0.303	0.402
IT Expertise	0.423	0.643

6.6 Apps Installation

In Table 5, subjective norms have negative and in significant relationship with APPS installation, where Attitude towards smartphone append Perceived Usefulness shows significant effect on APPS installation.

Table 5. Correlation matrix

Variable	Apps Installation	
	Pearson correlation	Significance 0.05 (2-tailed)
Subjective norms	-0.312	0.765
Attitude towards smartphone apps	0.312	0.343
Perceived Usefulness	0.303	0.302

The value for the R-squared as shown in Table 6 is 0.724 which indicates that 72.4% of the variation in the dependent variable is explained by the independent variables of the model. The 27.6% variation in the dependent variable remains unexplained by the independent variables of the study.

Table 6. Goodness of fit for attitude towards smart phone apps

Model	R	R square	Adjusted R- Square
Attitude towards smartphone apps	0.932	0.724	0.421

The Least Square Dependent Variable of Attitude towards smartphone apps is illustrated in Table 7. The value for the F-statistic is 4.21 and is significant endorsing the validity and stability of the model relevant for the study. The other diagnostics suggest that the Perceived Usefulness and Perceived Privacy both have significant positive relation

with Attitude towards smartphone app., while, Subjective norms has a negative and insignificant effect on attitude towards smartphone apps. As shown in Table 7, the correlation is significant at the 0.01, 0.05 and 0.09 level.

Table 7. Least square dependent variable of attitude towards smartphone apps

Construct	Coefficients
Subjective norms	-0.021
Perceived usefulness	0.268***
Perceived privacy	0.289**
Adjusted R-squared	0.421
F-statistics	0.491*

7. Recommendations to Protect Users' Privacy

1. Provide user education materials on such topics as use of Wi-Fi networks and disposal of old cell phones in a manner that safely protects personal and sensitive information.
2. Research apps before you download them and to turn off location-tracking for the apps that is don't needed. Look at how many people have downloaded the app, read what they have said about it, determine who created it, and if you are skeptical do some further research such as app's privacy ratings.
3. Certain smartphones may ask you for specific permissions when you install an app. Read these, think about what the app is asking for permission to access and what it does for you. Learn where to go on your particular phone to determine what you will allow the app to access.
4. Look at a privacy policy and terms of service. If the app download screen doesn't show it, usually the app's webpage will, but you might have to ask. Is this app requesting access to only the data it needs to function? If the answer is no, don't download it.
5. In order for smartphone users to guarantee higher security and more privacy on their phone calls, users can always use external voice encryption devices such as TopSec Rohde and Schwartz. A separate device which can be connected to the mobile phone using Bluetooth technology or integrated in the mobile phone handsets.
6. Finally, the most effective way to improve the privacy of mobile phone users is to increase the awareness with the various threats that can compromise their privacy.

8. Conclusions

User awareness factors are considered the most important means of enhancing and improving information security. The study revealed more than 90% of users have installed apps on their smartphones and about 83% of them did not read the apps privacy policy before the installation. The study also found that 57% of smartphones apps users have no idea what personal data stored on their phones are accessed by apps service providers, and 71% of mobile phone social apps users are unaware that their contacts and social relationship data is being uploaded to a central server. In addition, while 89% of the users activated screen lock on their smartphone to protect their phones and personal data, only 42% of the users take the necessary steps to protect their phones against virus and similar malicious software.

The most effective way to improve the privacy of mobile phone users is to increase the awareness among the users with the various threats that can compromise their privacy. In regards to awareness, users that feel they are very much informed believe that communication is very much secure. On the other hand, users that do not feel informed are afraid that communication is not at all secure. Excessive confidence could lead to "relaxation" of security practices while excessive fear certainly hinders technology adoption and especially mobile downloading.

It is more than clear that the mobile security area is going to be the next battleground since mobile security is an emerging discipline within information security arena and security levels are not high enough. Users themselves are critically affected by security and privacy threats, and play a key role in protecting themselves and others, since they do not actively follow most of security best practices.

9. References

1. Sheila M, Faizal MA, Shahrin S. Dimension of mobile security model: mobile user security threats and awareness, International Journal of Mobile Learning and Organization. 2015; 9(1):66–85. crossref.
2. Nazri NB, Ali M, Ibrahim J. Survey on mobile and wireless security awareness: User perspectives, International Journal of Science and Research. 2013; 4(1):1287–92.
3. Mattord H, Whitman ME. Principle of Information Security. 4th Ed. Cengage Learning; 2015. p. 1–656.
4. Threats to Mobile Phone Users' Privacy Report. Memorial University of Newfoundland. Date accessed: 03/2009. Available at: crossref.

5. Merlo A, Alessandro A, Verderame L. Considerations related to the use of mobile devices in the operation of critical infrastructures, International Journal of Critical Infrastructure Protection. 2016; 7(4):247–56.
6. Essential ways to protect my Mobile Apps. Date accessed: 07/05/2017. Available at: crossref.
7. Ophoff J, RobinsonM. Exploring end-user smartphone security awareness within a South African context, Journal of Information Security for South Africa (ISSA). 2014; 1–7.
8. Ghazal M. 95% of Jordanians own mobiles; 47% use the Internet, The Jordan Times. 2014.
9. Laura E, Gomez-Martin. Smartphone usage and the need for consumer privacy laws, Journal of Technology Law and Policy. 2016; 12:217–37.
10. Armando A, Merlo A, Verderame V. Security considerations related to the use of mobile devices in the operation of critical infrastructures, International Journal of Critical Infrastructure Protection. 2014; 7(4):247–56. crossref.
11. Valcke J. Best practices in mobile security, Biometric Technology Today. 2016; 3:9–11. crossref.
12. Androulidakis I, KandusG. Mobile Phone Security Awareness and Practices of Students in Budapest. The Sixth International Conference on Digital Telecommunications. Mont Blanc, France; 2011. 18–24.
13. Leavitt N. Mobile Security: Finally a serious problem? Date accessed: 06/2011. Available at: crossref.
14. Zhang Lei. Mobile Security Threats and Issues – A Broad Overview of Mobile Device Security. Tian Jin University, Tian Jin, China; 2016.
15. Privacy Rights Clearinghouse. Privacy in the age of smartphone (2005-2016). Date accessed: 19/12/2017. Available at: crossref.
16. Federal Trade Commission. Mobile Privacy Disclosures: Building Trust Through Transparency: A Federal Trade Commission Staff Report. Date accessed: 02/2013. Available at: crossref.
17. Digital Universe New Zealand: Privacy in the age of the smartphone, Roy Morgan Research. September 20 2013; Finding No. 5198. crossref
18. Centre for the Advancement of Social Sciences Research-CASR. Report on Privacy Awareness Survey on Smartphones and Smartphone Apps. Date accessed: 01/11/2012. Available at: crossref.
19. Boyles J.L, Smith A, Madden M. Privacy and Data Management on Mobile Devices, Pew Research Internet and Technology. 2012; 1–19.
20. Privacy and Security in a Connected Life: A Study of US Consumers. Date Accessed: 03/2015. Available at: crossref.
21. Mobile Ads Can Hijack Your Phone and Steal Your Contacts. Date accessed: 10/07/2012. Available at: crossref.
22. Mobile Device Security— Emerging Threats, Essential Strategies. Key Capabilities for Safeguarding Mobile Devices and Corporate Assets. Juniper Networks; 2011. p. 1–8.
23. Khadem, S. Security Issues in Smartphones and their effects on the Telecom Networks. Master of Science Thesis in the program Networks and Distributed Systems. Chalmers University of Technology; 2010. p.21–26.
24. Cyber Threats to Mobile Phones. Date accessed: 22/06/2012. Available at: crossref.
25. Androulidakis I. A Multinational Survey on Users' Practices, Perceptions, and Awareness Regarding Mobile Phone Security. In: Mobile Phone Security and Forensics; 2016. p. 15–28.
26. O'Connell N. Data Protection and Privacy Issues in the Middle East. Telecommunications Law and Regulation in the Middle East Conference; 2011.
27. Statista-2018. Number of mobile app downloads worldwide in 2016, 2017 and 2021 (in billions). Date accessed 15/2/2018. Available at: crossref.
28. Digital Middle East: Transforming the region into a leading digital economy. Digital Mckinsey Company. Date accessed: 10/2016. Available at: crossref.
29. Saleh ZI, Mashhour A. Consumer attitude towards M-Commerce: The perceived level of security and the role of trust, Journal of Emerging Trends in Computing and Information Sciences. 2014; 5(2):111–17.
30. Mylonas A, Kastania A. Gritzalis D. Delegate the smartphone user? Security awareness in smartphone platforms, Computers and Security. 2013; 34:47–66. crossref.