JOURNAL OF AWARENESS

E-ISSN: 2149-6544

Cilt:3, Sayı:Özel, 2018 *Vol:3, Issue:Special, 2018*

http://www.ratingacademy.com.tr/ojs/index.php/joa

*SMARTPHONE SECURITY AWARENESS AND PRACTICES OF USERS IN ALBANIA**

Esmeralda KADËNA
Óbuda University, Doctoral School on Safety and Security Sciences
Budapest/HUNGARY,
*E-mail: **kadena.esmeralda@phd.uni-obuda.hu***

ARTICLE INFO

Keywords:
smartphones; questionnaire survey; security practices; security awareness

DOI:

10.26809/joa.2018548618

ABSTRACT

Nowadays smartphones security problems are not just a matter of technological factors but human factor is involved as well. The aim of this study is to investigate smartphone security practices of users in Albania and how is presented their security awareness. To accomplish the objectives, a questionnaire was conducted. The results from 103 participants are presented and analysed.

1. INTRODUCTION

In recent years, the smartphone usage raised significantly because they provide users with a wide range of services like phone calls, Internet services, sharing and keeping data, on/off-line games and some entertaining applications while tracking personal data of the users such as location, private messages, contact lists and more. On the other hand there are some challenges in terms of security and privacy as well. The dawn of the planet of the smartphones might be considered from2007 when Steve Jobs presented the first model of iPhone (Leaders, 2015).

Every country is experiencing technological changes. The facilitated communication with smartphones has changed. Moreover there is a huge amount of information about what we do with these devices and when we use them. While talking about the security in this field we have to put human factor in the first line. The user can influence over the mobile device. In most cases he can harm or prevent from harming himself.Due to the growing number of smartphones in the hands of people, the internet penetration rate is increasing more and more. According to Internet World Stats, North America has the largest internet penetration rate (88.1%) followed by Europe with 80.2% and Australia/Oceania with 69.6%. Africa is ranked as the last with a rate of 31.2% (Miniwatts Marketing Group, 2017). In case of Albania statistics show that in 2017, there are 1,932,024 Internet users and the internet penetration rate is 66.4%. It was estimated that each inhabitant is using on average two mobile phones (Rrapaj, 2015).

The objectives of the study discussed in this paper are to have an understanding of the smartphones security and privacy awareness of Albanian users', to provide general information to help on addressing the problems and to give some suggestion with regard to educational and training strategies.The paper proceeds as follows: in second section a literature review of

**Bu çalışma, 19-21 Nisan 2018 tarihlerinde Çanakkale/TÜRKİYE'de gerçekleşen 2. Uluslararası Rating Academy Kongresi: Umut temalı kongrede sunulmuş aynı isimli bildirinin gözden geçirilmiş halidir.*

security and users' behaviour studies related to smartphones is presented. In third section is described the methodology used for the survey. Thereafter the collected data and findings are presented and analysed. The work concludes with conclusions.

2. LITERATURE REVIEW

2.1. Related research

Researchers are focused on examining whether users' protective behaviours are influenced by their technical knowledge and awareness of security threats (Rader & Wash, 2015), (Conolly & Aytes, 2003). Wash et al. found that users' security perceptions can be grouped according to their demographic groups and technological knowledge (Rader & Wash, 2015). Their observations showed that people with lower educational levels tend to make simpler security decisions (Rader & Wash, 2015).Spitzner showed that human behaviour on security awareness can be measured through some metrics that focus on the key human's risks to organization such as phishing emails (Spitzner, 2014).Kruger and Kearny developed a model to measure overall awareness level by focusing on three dimensions: attitude, knowledge and behaviour (Kearney & Kruger, 2006). Blythe et al.studied the factors affecting users' security related behaviours (self-efficacy, social influence, perceived severity, perceived susceptibility, attitude, response efficacy, response costs) in the workplace.

Researchers showed that peoples' willing to protect themselves against security risks affects their security practices (Larose, Rifon, & Lee, 2008). Other authors stated that privacy concerns of users are related to location tracking and sharing (Kelley, Benisch, Cranor, & Sadeh, 2011), (Smith, Consolvo, LaMarca, Matthews, Powledge, & Tabert, 2005). Wash argued that the privacy and security play roles in users' installation decisions. The result from the interviewed people was that they were cautious when installing new software because of malware concerns (Wash, 2010). In an experiment realized by Good et al., was found that people preferred applications with better privacy policies if the privacy is included in the cost of application functionality (Good, et al., 2005). Another critical point is the fact that cyber security and safety education is left out from the educational system (NCSA, 2010), (Lazarus Alliance, 2017) and users do not know if their phones are secure or not.

2.2. Smartphone Security Risks

Due to the increased processing power and memory of smartphones and tablet computers, increased data transmission capabilities of the mobile phone networks, and open and third-party extensible operating systems for mobile devices, they have become an interesting target for attackers (Costantino, Martinelli, Saracino, & Sgandurra, 2013). Many related articles and news on smartphone security, try to give a prediction on the future through a statement like "The wireless epidemic" (Kleinberg, 2007), "Is it finally time to worry about mobile malware?" (Lawton, 2008), "Planet of the phones" (Leaders, 2015), etc. Smartphones has become the gateway of personal details both local and those who are delivered to a third party "in the cloud". But in inevitable way, they lead tracks, not only details regarding to the owner of the phone but also to his friends and colleagues, their contacts, messages, appointments, notes and locations.

Permission given to applications should be considered; users tend to ignore or do not understand them (Ha, Felt, Egelman, Haney, Chin, & Wagner, 2012). Moreover, permission prompts are troublesome to experience of users as they "help" on teaching users to ignore and click them (Motiee, Hawkey, & Beznosov, 2010). As a result users give many permissions to applications and later on vulnerabilities are shown, especially in case those applications use the permissions in suspicious way.

"Jailbreaking" (in iOS case) or "rooting" (in Android) on the mobile devices which are not using a firewall.Jailbreaking is the method used for obtaining an application that does not belong to Apple or due to some restrictions from any other source cannot be downloaded. Through this method allows attackers to have access to the OS of the mobile and as a result creates vulnerability. Furthermore these devices do not receive the necessary security updates and become vulnerable to threats (Ruggiero & Foote, 2011).

If the device is lost or stolen and if is not protected with any screen lock method, the disclosure of information caneasily happen (Causey, 2013). Confidential data like e-mail, documents, reports, files, applications, usernames and passwords, installed certificates, banking information, and web accounts can be accessible if the device is lost or stolen. Moreover Bring-Your-Own-Device (BYOD) development is another potential risk. Employees are encouraged to access organization resources like corporate e-mails, calendars and scheduling, documents, applications, etc., with their personal devices, either for work or for personal use (Gajar, Ghosh, & Rai, 2013). But on the other hand if an attacker could gain access both personal and work data might be compromised.

3. METHODOLOGY

In this study were used both quantitative and qualitative data. The qualitative data was obtained from the primary sources of data through administrating questionnaire. While the quantitative data was collected from both primary and secondary sources of data obtained from reports, manuals, and different journals, publications for assessing existing findings, internet, books and documents.

A questionnaire was used to collect data. It was generated by Google forms in local language (Albanian) for easy understanding and simplicity. The link was send by email and social networks (Facebook, Whatsapp, Viber). The structured questionnaire itself was designed so as to make it easy to answer and developedaround the idea of exploring Albanian users' practices and how aware are they with regard to security while using smartphones.

The respondents were smartphone users andrandomly selected, aged between 20 years old and more than 50 years old. It was conducted from December 1st 2017 until December 31st 2017 and contained a brief self-administered demographics questions that collected basic information including gender, age, study level, monthly incomes, and employment status. That was mostly intended to give a better understanding of the respondents included in the study. On the other part were specific security questions.

It is important to note that there are some limitations. Respondents may not tell the truth when asked or they might misunderstand some questions. The use of the questionnaire will give in general at least an indication of security practices and awareness.

4. RESULTSAND ANALYSIS

4.1. Demographics

A total of 103 recorded questionnaire responses were received. Age frequencyis given in the table 1.

Table 1. Age frequency of participants

Age	Number of participants
<20	8
20-30	60
30-40	16
40-50	11
>50	8

There has been a significant difference between the group ages that use the smartphones. The majority of participants (58.3%) were between 20-30 years old followed by group ages 30-40 and 40-50 years old. Participants less than 20 years old and more than 50 years old have the same distribution (8 participants). There is a slightly difference between the number of males and females participated in the questionnaire, 57.3% were male and 42.7 % female.

The major part of Albanians have a Master degree (44%) followed by 31% who have a Bachelor one and 18% have a secondary education level. 69 respondents were employed, 25 were student and the rest (9 respondents) unemployed.

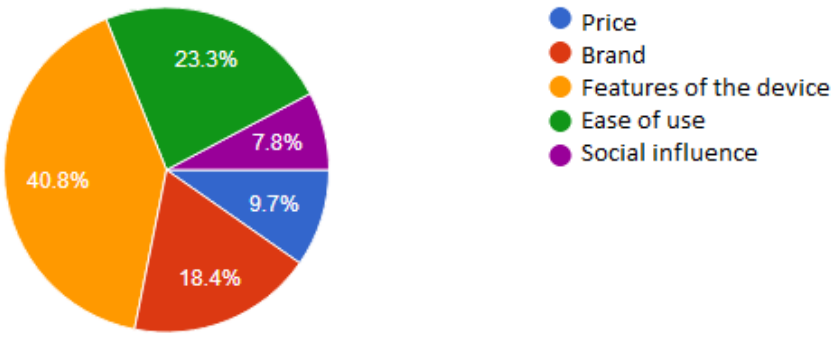
The frequency of their monthly income (in ALL- Albanian Lek is the official currency of Albania) is shown in table below:

Table 2. Frequency of monthly income

Monthly income (in ALL)	**Number of respondents**
<20.000	15
20.000-50.000	35
50.000-70.000	28
70.000 - 100.000	15
>100.000	10

4.2. Mobile device's selection, using purposes and its importance

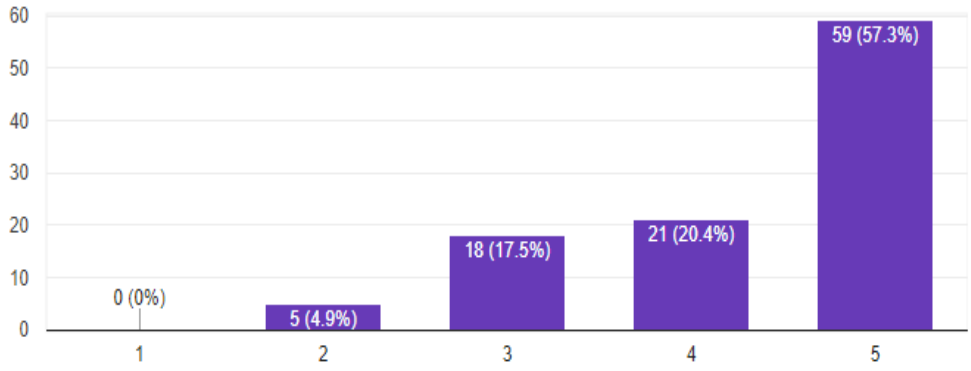
Figure 1. From which factor are influenced the most when choosing a mobile device



In the figure above (fig. 1) is shown from which factor are the respondents influenced the most when choosing a smartphone. The majorty of Albanian participants are influenced by the features of the device. In these features can be mentioned: long lasting battery, processing speed, display screen, camera, storage space, biometric sensors.

These can be seen also from the fact that approximately 50% of them are using iPhone, followed by 39% Samsung users and the rest LG, Nokia, Sony, Huawei, HTC, Blackberry have no significant frequency. Moreover they were asked about what might be the next selection (the above mentioned brands were not changed in the question) if they will change smartphones and approximately 61% would prefer to have an iPhone and 23% Samsung. Again the other brands have no significance. The result about how important is their smartphone is presented in the figure below (fig. 2):

Figure 2. The importance of smartphone in a scale from 1-5



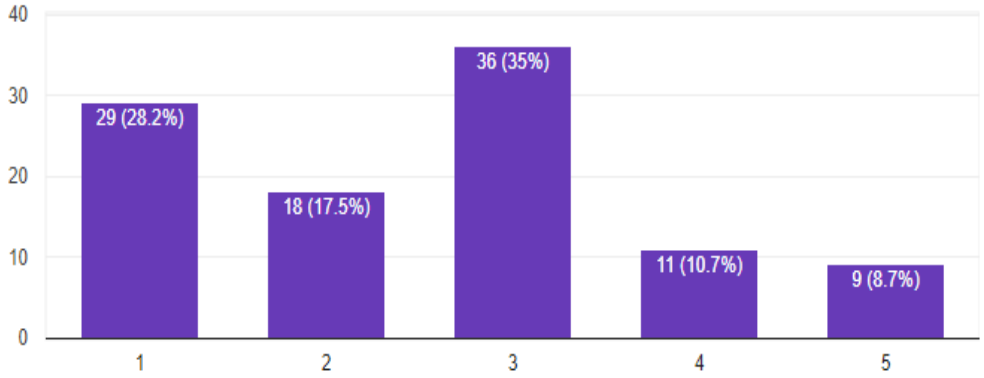
So it is clearly shown that more than half of participants consider their smartphones as very important. Only 1 respondent consider it not important at all. The results show that 71% of them use the smartphone for both personal and business purposes and the potential risks are increased because if an attacker could gain access on smartphone, both personal and work data might be compromised.

4.3. Security part

The aim of this part and the main contribution to this work is to investigate whether theparticipants have knowledge on some security features of their smartphones and how is presented their awareness. The results are analysed as follows.

The research question consist on whether smartphone users are informed about how the security options and characteristics of their devices affect the security of it and if they are taking any measure to address the risks. They were asked if are informed about how the options and technical characteristics of smartphones affect the security (in a scale 1-5 where: 1-Not informed at all; 2-Not too much; 3-Moderately; 4-Informed; 5-Well informed) and the major part of respondents (35%) feel moderately informed followed by not informed at all response by approximately 30%. Only 8.7% feel that are very much informed. The results are presented in figure 3.

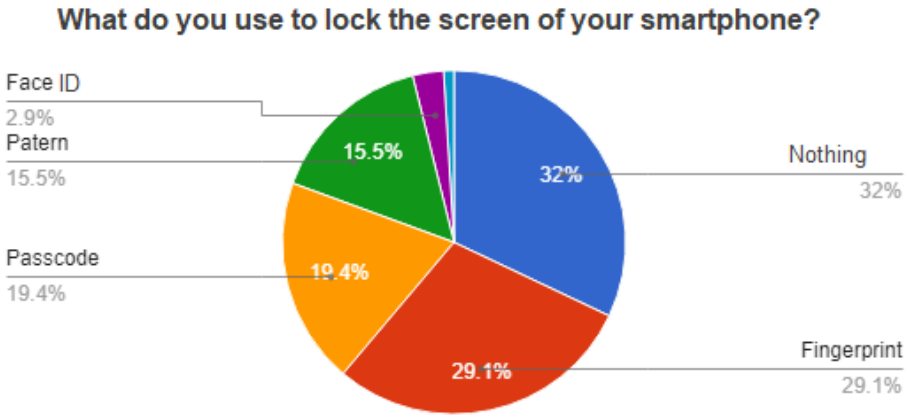
Figure 3. Knowledge of how smartphone options and technical characteristics affect the security



Correlating their responses to the age of respondents show that the younger respondents have statistically (Pearson Chi - square) better knowledge on security aspects than those who are older (weak negative association, r=-0.14).

The negative finding that Figure 4 presents is that the major part (32%) do not use anything to lock/unlock the screen and the main reason for that was "I found it faster way". These respondents are in a high risk and seem not aware on the potential risks. This could be the first line of the defence. In such cases, an attacker can gain access to the phone by downloading specific software.

Figure 4. Measures taken for locking the screen of smartphones



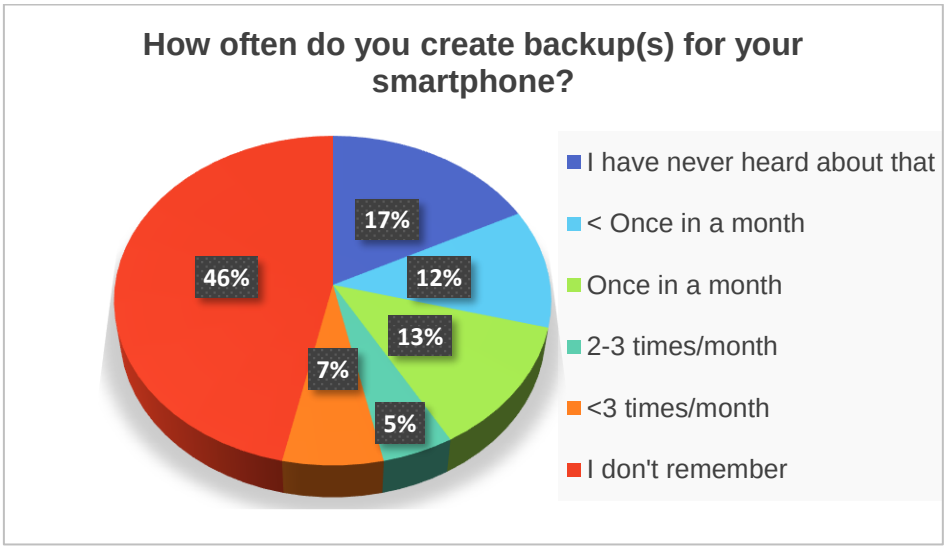
What if the mobile device is stolen or lost? Everyone can gain easily access on it if the screen is not locked. The participants were asked also if their phone have lost and only 15% had experienced that. Moreover another reason to activate the mobile phone screen locker is because of the amount of the sensitive data people save and store there. Approximately 79% agreed that store sensitive data. 46% of participants save passwords of their important accounts (i.e. bank account, email), 47% do not save and the rest appears as careless as they do not pay attention if they do that.Between this variable and the knowledge on security aspects of smartphones, exists a moderate negative relationship r = - 0. 34.

Encryption is an essential measure when it comes to security.With data like bank card information, passwords, sensitive data (messages, photo, video, etc.), encrypting the data on

smartphone keeps most personal information secure. A good defence practice against hackers can be the use of a strong password. The longer the password, the stronger the encryption key.The respondents were asked if they are aware about this term and the results show that the major part (60%) are not aware. The correlation between their awareness on existence of this term and their knowledge on security aspects of smartphones statistically (r = 0.36) proves that they who are aware on encryption have better knowledge on security aspects.

Making regular backup(s) is very important. As in smartphones are stored and saved important files and sensitive data, people should do regular backup(s) in order to stay in the safe side in case the device is lost, stolen or damaged. It means that the data should be transferred somewhere else. The cheapest and easiest way is by taking advantage of free cloud services. Respondents were asked about how often they create backup and the results in figure 5 show that the major part of them (46%) might be careless as they do not remember how their practice is.

Figure 5. Frequency of backup(s)

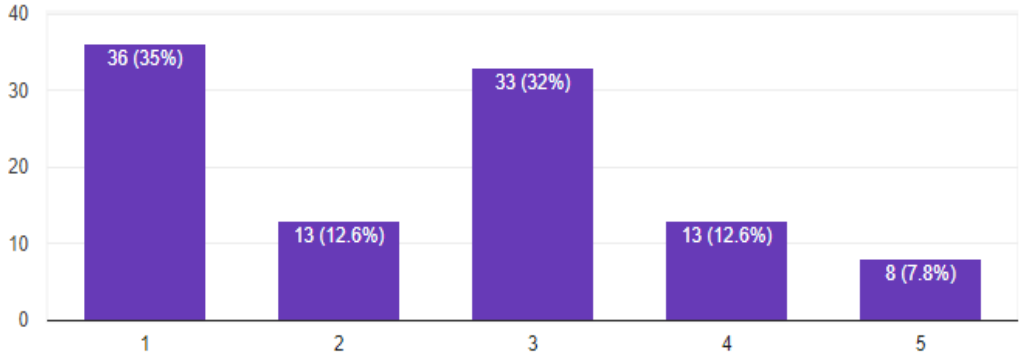


Following with another question about security practices. The results for the question from where they download applications showthatmost of them (~ 60%) use only official stores, while the rest do so also from third-party app stores. Even though there is no significant difference in numbers, they are prone to be surveyed and hacked. Actually many of the apps that can be downloaded from a third - party app store can collect information about owner of device and serve ad banners regardless of what the owner is doing on his device.

Reading privacy statements when downloading and installing an application is asecurity practice that users prefer skipping to do it. The results showed that the majority (44 respondents) rarely read them, followed by 40 respondents who never read, 16 do it usually and only 3 read them always. The correlation between feeling that have knowledge on security aspects and reading privacy statements is positive but weakr = 0.23.

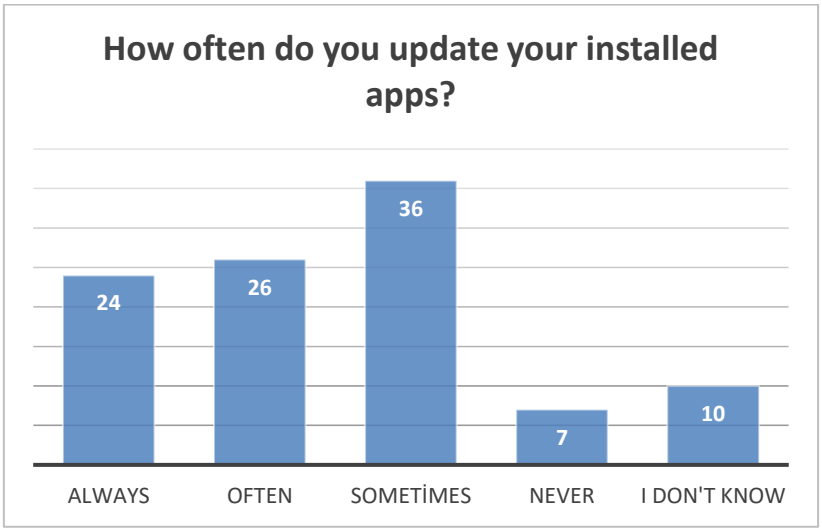
Moreover, in figure 6 are presented the results of the question “How aware are you of the permissions you give, when downloading and installing apps (i.e. location, personal information, network access, email address book, etc.)?”. There is no significant difference between those who feel unaware (35%) and those who think have a moderate awareness. Further correlating their responses to their knowledge on security aspects proves (r = 0.48) that people who are aware about the permissions given when downloading and installing have better knowledge on security than those who are not aware.

Figure 6. Frequency of the awareness level about permissions given when downloading and installing apps



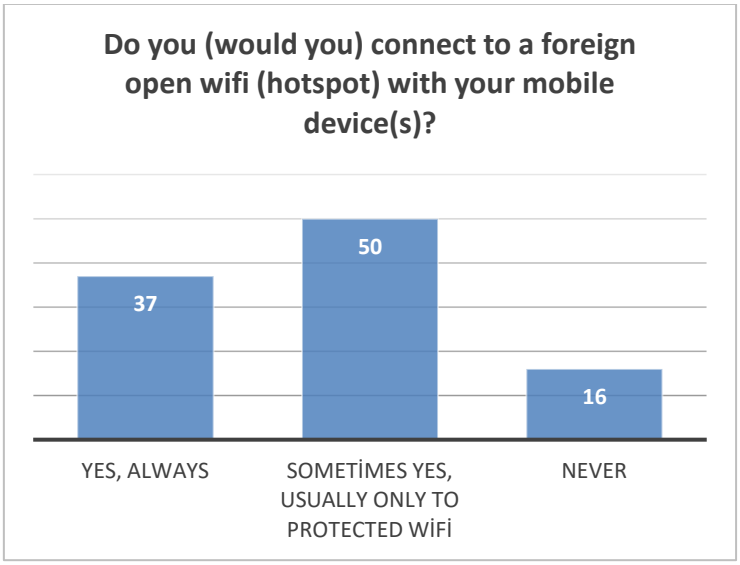
As we live in a world where cyberattacks are becoming so common, updating installed applications is a very essential. Every update has some new features (including here also security aspects) or some bug fixes. Users answers are presented as follows (figure 7). The results are good. Some mobile devices can do it automatically and users do not have to pay attention on that. Most of the respondents are aware that should check and do it sometimes. But here the type of the smartphone should be considered.

Figure 7. Frequency of updating installed apps



In the end they were asked if (would) connect to a foreign open Wi-Fi (hotspot) with their mobile device. When connecting to a foreign open Wi-Fi there are some risks. Someone spying could easily pick up passwords or other private information. Attackers/intruders might set up their own Wi-Fi hotspot with a general name to tempt people to connect (i.e. public Wi-Fi) and they can gain any data he/she send. These can be done easily without any kind of special equipment, a laptop or smartphone is more than enough. The results presented in figure 8, show that the major part do it usually to protected Wi-Fi. But still protected Wi-Fi has vulnerabilities. The hacking methods are becoming more and more sophisticated, for instance it can be threatened by weak passwords/passphrases that can make it easier for attackers to compromise the systems.

Figure 8. Connecting to a foreign open Wi-Fi frequency



5. CONCLUSIONS

This work shows that users in Albania do not pay the proper attention to privacy and security of their smartphones. The findings confirm that they store and save a considerable amount of (sensitive) data while their practices indicate that do not adequately protect themselves. Those who are younger seem to have a better knowledge than the older. Users seem to display high level of trust on smartphones and applications store. Furthermore they refuse to take the first line of defence, "locking the screen" and it means that all data (for personal and business purposes) is freely available in case the smartphone is stolen, lost or damaged. In general it is necessary to increase their security awareness as it is far from being perfect.

This work could be a good basis to further investigate on their security awareness, behaviours and comparing with other countries. Another concern is related with the lack of education on this field. Therefore it is very important to build up security training(s) to make them more conscious. This study should be viewed in light of its limitations. Participant behaviour and practices were self-reported. The size of the sample was small and the questionnaire was only available via internet. Therefore a study with a larger population should be considered for future research. Other instruments for measuring their behaviours might be employed to have a better understanding and results.

REFERENCES

CAUSEY, B., 2013. *Strategy: How to Conduct an Effective IT Security Risk Assessment,* InformationWeek Reports.

CONOLLY, T. & AYTES, K., 2003. *A Research Model for Investigating Human Behavior Related to Computer Security.*

COSTANTINO, G., MARTINELLI, F., SARACINO, A. &SGANDURRA, D., 2013. *Towards enforcing on-the-fly policies in BYOD environments.* Gammarth, IEEE, pp. 61-65.

GAJAR, P. K., GHOSH, A. &RAI, S., 2013. Bring Your Own Device (BYOD): Security risks and mitigating. *Journal of Global Research in Computer Science,* April.4(4).

GOOD, N. et al., 2005. *Stopping spyware at the gate: A user study of privacy, notice and spyware.*

HA, E. et al., 2012. *Android Permissions: User Attention, Comprehension, and Behavior.* Washington DC.

KEARNEY, W. D. &KRUGER, H. A., 2006. A prototype for assessing information security awareness. *Computers and Security,* Volume 25, pp. 289-296.

KELLEY, P. G., BENISCH, M., CRANOR, L. F. &SADEH, N., 2011. *When are users comfortable sharing locations with advertisers?.* Vancouver, pp. 2449-2452.

KLEINBERG, J., 2007. The wireless epidemic. *Nature,* p. 287–288.

LAROSE, R., RIFON, N. &LEE, D., 2008. Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology,* 27(5), pp. 445-454.

LAWTON, G., 2008. *Is It Finally Time to Worry about Mobile Malware?*, IEEE Computer.

LAZARUS ALLIANCE, 2017. *It's Time to Get Serious About Education Cyber Security.* [Online]
Available at: https://lazarusalliance.com/education-cyber-security/
[Accessed November 2015].

LEADERS, 2015. Planet of the phones - The smartphone is ubiquitous, addictive and transformative. *TheEconomist.*

MINIWATTS MARKETING GROUP, 2017. *World Internet Users Statistics and 2017 World Population Stat.* [Online]
Available at: http://www.internetworldstats.com/stats.htm
[Accessed 2017].

MOTIEE, S., HAWKEY, K. & BEZNOSOV, K., 2010. *Do Windows users follow the principle of least privilege? Investigating user account control practices..* New York.

National Cyber Security Alliance (NCSA), 2010. *State of Cyberethics, Cybersafety, and Cybersecurity Curriculum in the U.S*: NCSA.

RADER, E. & WASH, R., 2015. *Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users.*

RRAPAJ, A., 2015. *Market Overview and Regulation in Albania.* [Online]
Available at: http://www.infocomalbania.com/presentations-2015/rapaj.pdf
[Accessed November 2017].

RUGGIERO, P. & FOOTE, J., 2011. *Cyber Threats to Mobile Phones,* s.l.: United States Computer Emergency Readiness Team (US-CERT).

SMITH, I. E. et al., 2005. *Location Disclosure to Social Relations: Why, When, & What People Want to Share.* Portland, Oregon.

SPITZNER, L., n.d. *Measuring Change in Human Behavior.* Mosone Center, San Francsico.

WASH, R., 2010. *Folk Models of Home Computer Security.*

APPENDIX

Questionnaire about smartphone security awareness and practices of users in Albania
(Translated from Albanian to English)

(*required)

1. **Your Age: ***
   - < 20
   - 20-30
   - 30-40
   - 40-50

2. **Gender: ***
   - Female
   - Male

3. **Your education: ***
   - Secondary School
   - High School
   - Bachelor Degree
   - Master Degree
   - Higher Degree

4. **You are: ***
   - Student
   - Employed
   - Unemployed
   - Self employed
   - Retired

5. **Your status: ***
   - Single
   - Married
   - Divorced

6. **Your monthly incomes: ***
   - <20.000 Lek
   - 20.000-50.000 Lek
   - 50.000-70.000 Lek
   - 70.000 - 100.000 Lek
   - >100.000 Lek

7. **The brand of your smartphone is? ***
   - Apple
   - Samsung
   - LG
   - Nokia
   - Sony
   - Huawei
   - HTC
   - BlackBerry

- Other:_____

8. If you would change your smartphone, what could be the next choice? *
- Apple
- Samsung
- LG
- Nokia
- Sony
- Huawei
- HTC
- BlackBerry
- Other: _____

9. Would you use a smartphone that somebody before you used it? *
- Yes
- No

10. For what purposes are you using your smartphone? *
- Personal
- Business
- Both

11. From which factor are influenced the most when choosing a smartphone?
- Price
- Brand
- Features of the device
- Ease of use
- Social Influence

12. How important is your smartphone for you? *
(Where 1- Not important; 5- Very important)
- 1
- 2
- 3
- 4
- 5

13. Have you ever lost it? *
- Yes
- No

14. Do you let it in the others hands? *
- Yes
- No
- Only when I trust to the person

15. Are you aware about the term "encryption"? *
- Yes
- No

16. What are you using to lock the screen? *
- o Passcode
- o Fingerprint
- o Face Unlock
- o Pattern
- o Nothing

17. If you do not lock the screen of your smartphone, what is the reason?
- o I do not pay attention
- o I cannot remember
- o It is quicker
- o Other: _____

18. Your applications are downloaded: *
- o Only from official stores
- o From other sites as well

19. Do you save on your smartphone password(s)/PIN(s) of important accounts (i.e. bank account, email, social networks, etc.)? *
- o Yes
- o No
- o I don't know

20. Do you have sensitive data (like photo, video, phone calls recordings, private docs, etc.) in your smartphone? *
- o Yes
- o No

21. How often do you backup your device? *
- o I don't know what is this
- o <1 Once in a month
- o Once in a month
- o 2-3 times/month
- o >3 times/month
- o I don't remember

22. Where do you save your data during backup(s)? *
- o Cloud services
- o External memory
- o Export to other devices like PC, tablet, laptop
- o I don't know

23. Have your device ever been hacked? (i.e. virus, malware, etc.)? *
- o Yes
- o No
- o I don't know

24. Have you installed an antivirus? *
- o Yes
- o No

25. Are you informed about how the options and technical characteristics of smartphones affect the security?*

(Where: 1-Not informed at all; 2-Not too much; 3-Moderately; 4-Informed; 5-Well informed)

- 1
- 2
- 3
- 4
- 5

26. How often do you read privacy statements when downloading an application? *

- Always
- Often
- Sometimes
- Never

27. How aware are you of the permissions you give, when downloading and installing apps (i.e. location, personal information, network access, email address book, etc.)*

(Where: 1-Unaware and 5-Very aware)

- 1
- 2
- 3
- 4
- 5

28. How often do you update your installed apps? *

- Always
- Often
- Sometimes
- Never
- I don’t know

29. Do you (would you) connect to a foreign open Wi-Fi (hotspot) with your mobile device(s)?*

- Yes, always
- Sometimes yes, usually only to protected Wi-Fi
- Never