Mobile Phone Security Awareness and Practices of Students in Budapest

Iosif Androulidakis

Jožef Stefan International Postgraduate School
Jamova 39, Ljubljana SI-1000, Slovenia
sandro@noc.uoi.gr

Gorazd Kandus

Department of Communication Systems
Jožef Stefan Institute
Jamova 39, Ljubljana SI-1000, Slovenia
gorazd.kandus@ijs.si

***Abstract*—**The present paper presents the results of a survey about users' security practices regarding mobile phone usage that took place in 4 Universities of Budapest in February 2010. We targeted an extended pool of respondents reaching 959 answers. The general users' feeling is that mobile phone communication is secure and this possibly leads to a relaxation. As results indeed further showed, students are unaware of the necessary measures to avoid a possible unauthorized access and/or sensitive data retrieval from their phones and that they lack proper security education. There was also a statistically important difference in the answers, depending on the type of operating system (modern or not). Since users fail to secure their phones they should either be educated or preferably presented with transparent security features, built in their phones, in order to mitigate the dangers**.**

Keywords-mobile phone security; security practices; user interface security; questionnaire survey; mobile phone usage

I. INTRODUCTION

Mobile devices are becoming a critical component of the digital economy, a style statement and useful communication device, a vital part of daily life for billions of people around the world. Modern mobile phones' enhanced capabilities allow them to be almost as versatile as a computer becoming a valuable business (mobile applications) and entertainment tool (mobile games, m-commerce). At the same time users store and process more data including sensitive information in their phones. A few years ago the only concern of a mobile phone user would be his communication privacy.

This is not the case anymore. Users have to be protected from unauthorized third party access to their data. Apart from the traditional security measures such as PIN (Personal Identification Number) usage and voice encryption, users have to take extra security measures and to follow new best practices. Unfortunately, as the survey revealed, users aren't adequately informed about security issues in regards to their mobile phones' options and technical characteristics and fail to follow proper security measures and practices. In Section II, related work is examined. The methodology used for the survey is described in Section III. Results are presented in Section IV, closing with conclusion and future work in Section V.

II. RELATED WORK

Although there have been quite many theoretical studies concerning mobile services, a significant means for investigating and understanding users' preferences is asking their opinion via specific questioning techniques. The vast majority of these surveys indicate the growing importance of mobile phones in everyday life and the increased popularity of new features [1].

In any case, the security of mobile phones is proven not to be adequate in many research papers [2][3]. There also exist several survey studies in this direction. Some of these surveys studies focus on mobile phone's security issues [4][5] while others on mobile phone services, touching also security issues [6][7]. Modern smart phones, specifically, are open to more security risks [8].

A recent survey [9] published in November 2008 focused on mobile phones security issues and in which degree these issues concern the users. The conclusion was that a major part of the participants are extremely concerned about security and don't want any of their private data to be available to 3rd party unauthorized users.

It is interesting to note that according to other surveys [10] a major part of the participants is interested in mobile services adoption only if the prices are low and the security framework tight enough. At the same time, cyber security and safety education is left out from the educational system [11] and users do not know if their phones are secure or not [12]. Given the fact that mobile phones could be a dominant feature of future classroom, special security awareness and training courses, presenting the necessary guidelines, should definitely be implemented in schools. This is why the present paper tries to address users' security awareness and practices, as an enabler for greater mobile services market penetration.

III. METHODOLOGY

A very useful evaluation method for surveying user's practices is the use of multiple-choice questionnaires (i.e. in person delivery or e-mail questionnaires) [13][14]. Our survey was conducted using in-person delivery technique, with a total of 959 respondents participating in this survey. This method was selected from other alternatives because is more accurate and has a bigger degree of participation from

 ISBN: 978-1-61208-127-4

the respondents (e-mail questionnaires usually treated as spam mail from the respondents or they might misunderstand some questions). Data entry took place using custom software [15]. Due to lack of financial resources the survey was limited to Europe. An interesting approach would be to use social networks such as Facebook to amend the results of the survey, especially targeting students from United States and other continents.

The target group of the survey was university students from ages mostly 18-26, incorporating both younger and older youth segments (24-26 years old percentage was 25.5%) because these ages are more receptive to new technologies. They also understand better the technological evolution than older people who use mobile phones mostly for voice calls.

In the analysis of the security feeling and the security knowledge a simple mathematical formula was developed to produce numerical values. We weighted the responses with the following weights: Very Much: 4, Much: 3, Moderately: 2, Not much: 1, Not at all: 0 and then divided by the number of occurrences, in order to get a mean value.

IV. RESULTS

The questionnaire was divided in two parts. In the first part participants were asked some demographic data including gender, age and field of studies as well as some economic data including mobile phone usage, connection type and budget spent monthly on phone service. In the second part we proceeded to our main contribution, the specific questions related with their practices and security perceptions regarding mobile phones' security issues.

A. Demographics

56.3% of the participants were females and 43.7% were males. Most of the respondents, in turn, were aged 18-26 (82.4%). The main body of respondents was studying Economics or Business Administration (30.1%) Following in the sample there were students of Humanities or Philology (22%), Engineering, Mathematics or Natural Sciences (13.7%), Medicine (13.2%), Law (10.8%) and other fields (10%).

Regarding mobile phone usage, 60.3% of them are using daily a single mobile phone, with some 21% using two phones regularly and even 10% using more than two phones. Nokia is the favourite brand, reaching one third of students (34.3%) followed by Sony-Ericsson (21.3%) and Samsung (17.6%) (Figure 1). Apple's iPhone (which is expected to have a higher percentage in the US market) has a very descent 7.8% of penetration given the generally low budgeted section of the population targeted. It is immediately apparent that focusing on Nokia and Sony-Ericsson phones a security awareness campaign would immediately target more than half of users yielding a very high return. Of course the brand itself is not enough to categorize attack vectors and practices, since there is also the feature of the specific operating system running on each phone.

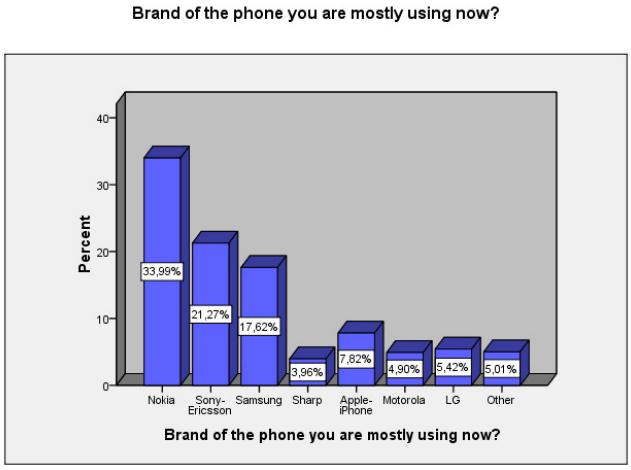

Figure 1. Favourite brands.

B. Economics

Proceeding to economics, participants were asked whether they are using a pre-paid or post-paid (contract) mobile phone connection. Half of students are using a contract based subscription, a rather high percentage, while 17.2% have both prepaid and postpaid SIMs (Subscriber Identity Module).

Answering how much money they spent monthly, student mobile phone users had a wide range of financial capabilities. The leading 25.7% spends 11-20 Euros (currency converted) monthly while almost equal parts of 20% spend 21-30, 31-40, or more than 40 Euros per month.

C. Security Specific Questions

The objective of this particular subsection and the main contribution of our research were to determine whether our participants acknowledge some security related features of their phone and what is their security feeling. The results are analysed in the following paragraphs.

Our fundamental research question was whether students are informed about how the options and the technical characteristics of their mobile phones affect the security of the latter and whether they are taking the necessary measures to mitigate the risks. The results that follow are totally in line with the initial response of students that only 29.6% believe they are much or very much informed while 42.6% state that they are not at all (a large 20.4%) or not much (Figure 2).

 ISBN: 978-1-61208-127-4

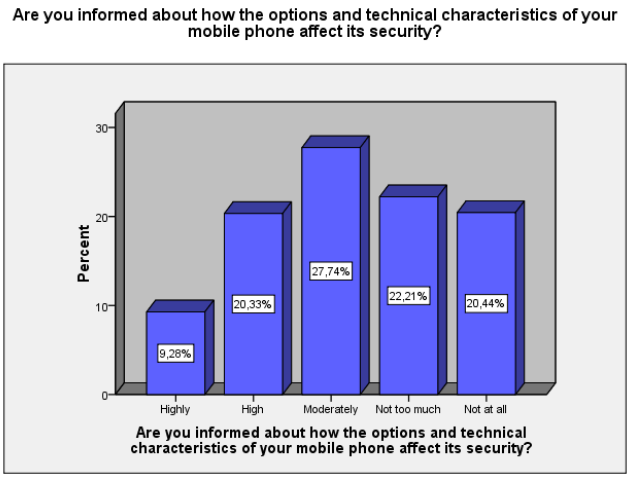

Figure 2. Knowledge of mobile phone security aspects.

Using the simple formula described in Section III (Methodology), the mean "security knowledge value" was 1.76, in the 0-4 scale (0 not at all, 4 very much). Further correlating their responses to the type of operating system–O/S (modern or not) proved that students owning phones without modern operating system have statistically (Pearson Chi-Square) better knowledge of security aspects than those who actually own a phone with modern O/S (Figure 3). As it was expected users that do not know the type of their O/S were the least informed about security.

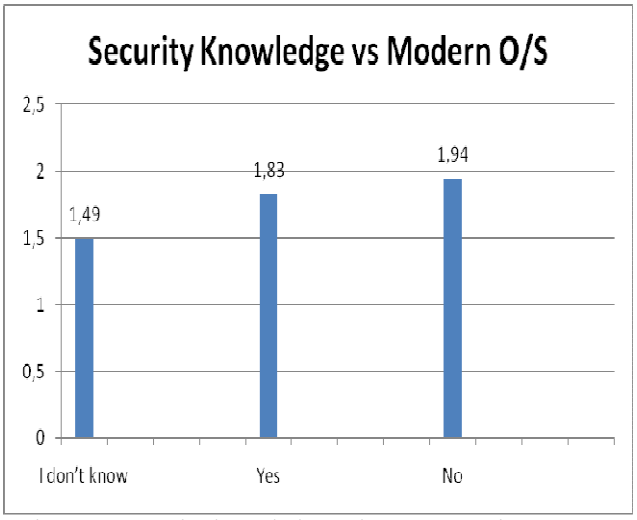

Figure 3. Security knowledge value vs. operating system.

Continuing with a general question about how "safe" mobile phone users feel, the majority (30%) replied "high (much)" followed by 26.7% "moderately" (Figure 4). On the other hand, some 27.9% felt not too much or not at all sure they are safe. This general feeling of security in turn leads to an over-relaxation of students in regards to security practices as following answers reveal.

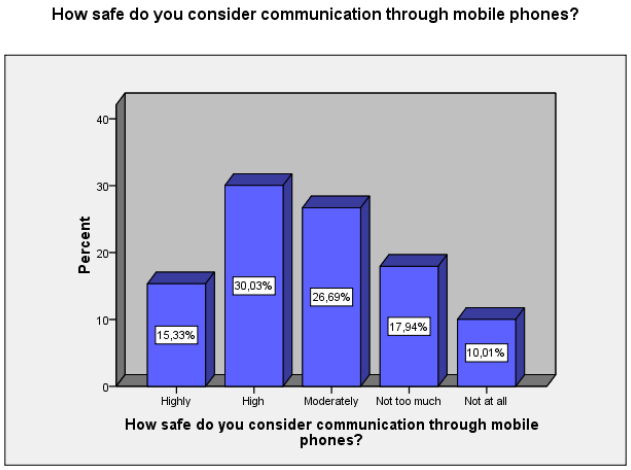

Figure 4. How safe do you consider communication through mobile phones?

Using the same methodology, the mean "security feeling) value was 2.22 in the 0-4 scale. The correlation to the operating system showed that users without modern O/S feel statistically (Pearson Chi-Square) the least secure while users that do not know the type of O/S are more "relaxed" (Figure 5).

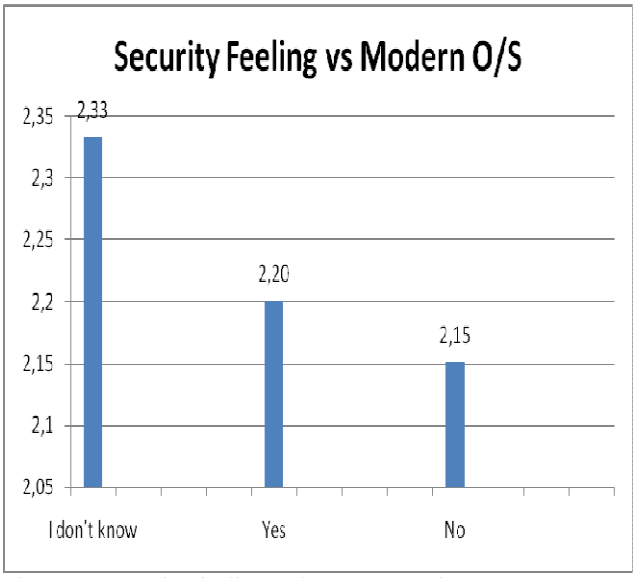

Figure 5. Security feeling value vs. operating system

In regards to operating system itself, a significant percentage of the participants (33.2%) doesn't know about the capabilities of his phone's operating system. Almost the same percentage (31.6%) of students is using mobile phones

 ISBN: 978-1-61208-127-4

with an advanced operating system. In any case, apart from the relaxation in security awareness that was previously shown, the ignorance of the type of operating system renders users more vulnerable to hacker attacks with the use of exploits specifically targeted for their phones.

Similarly, in Figure 6, only a very small percentage of the participants (less than 24%) knows his/her phone's IMEI (International Mobile station Equipment Identity) and has noted it somewhere. IMEI is very significant because if the phone is ever stolen, using this serial number the provider can block access to the stolen phone effectively mitigating stealing risks. Almost half of students are completely unaware of its existence. Knowledge of this feature would possibly help 41.1% of them who unfortunately had their phone stolen once or more (Figure 7). Similarly high percentages are noted by other studies too [16][17].

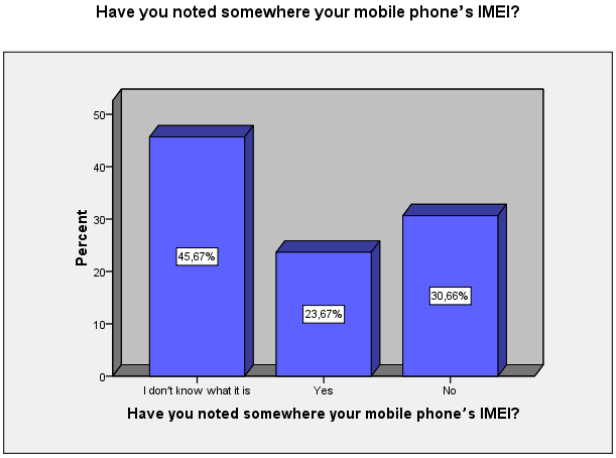

Figure 6. IMEI knowledge.

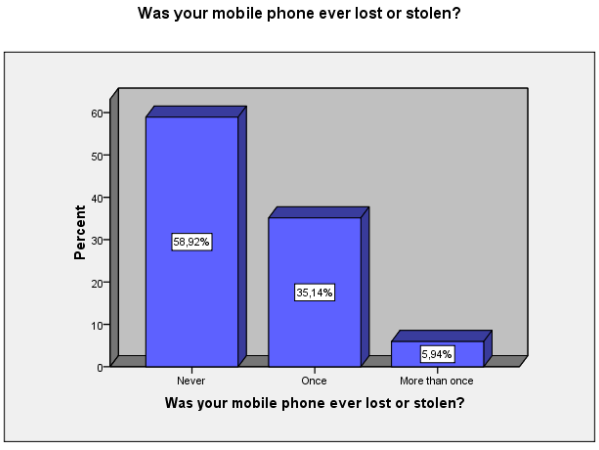

Figure 7. Lost or Stolen phone.

At the same time, 71% of users are not aware of the existence of the special icon that informs the user that his/her phone encryption has been disabled [3]. Ignorance of this security icon leaves users vulnerable to man in the middle attacks since they can't recognize the attack taking place. This was probably the most expected result as even professionals are not aware of this feature and another hint that user interfaces should help and not obscure security.

Users, as expected, are actively (almost 70%) using SIM's PIN code. The negative finding that Figure 8 reveals is that only a small percentage (24.5%) uses screen-saver password while similar percentages do not know if their phone has such an option. That leaves 75% of users without a screen saver password, and their phones ready to be manipulated by "malicious" hands. An attack can take place in a few minutes by downloading specific software to the phone; this is why it is not enough to protect the phone only by PIN but also by a screen saver password.

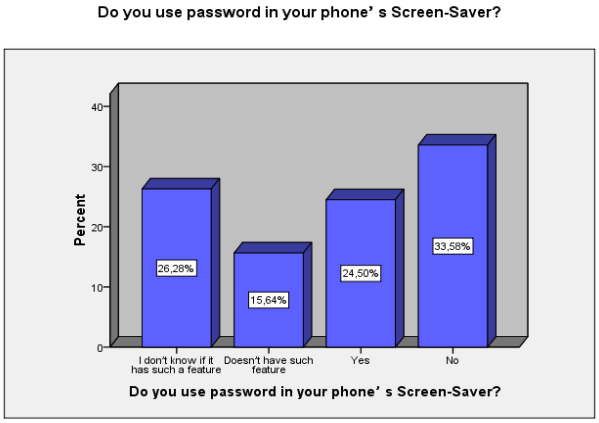

Figure 8. Screen-saver password.

A great attack vector of the past, Bluetooth, seems not to be the problem anymore (Figure 9). Just one out of five students has Bluetooth switched on and visible (leaving the phone vulnerable), while 42.3% of users have it switched off. It is not clear whether this is a security practice or a social practice that stemmed from the continuous harassments messages over Bluetooth caused upon users.

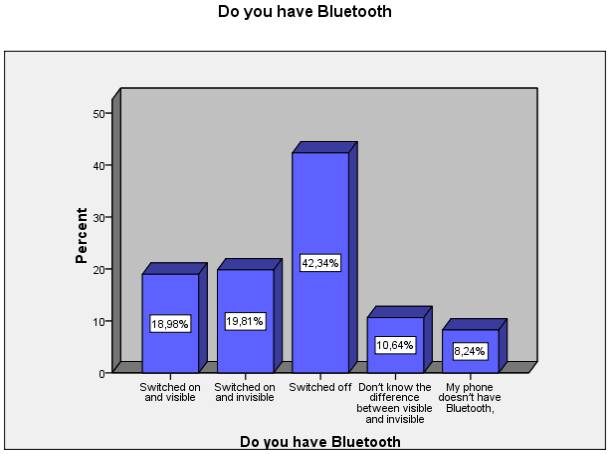

Figure 9. Bluetooth.

 ISBN: 978-1-61208-127-4

In a question that touches upon issues of politeness and openness, 44.7% of students are lending their phones, but only while they are present (Figure 10). This is a major factor that compromises the phone's security even if the participant is present, because a single minute is needed for someone to install malicious software in the phone. In that respect 36.2% of them refuse to lend their phone in any case being better safe and "impolite" than sorry.

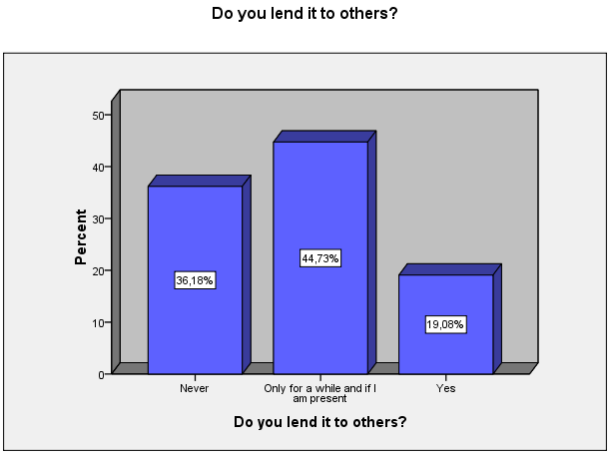

Figure 10. Phone lending.

Following, in Figure 11, with a question of both security and economic importance, almost 60% of participants don't download any software at all. There is also a 13% that actively downloads ringtones or logos, a 16% that tries applications and just 11% of "gamers". It is well interesting to note that security considerations is one of the hindering factors of mobile phone downloading [2]). In the antipode, getting familiar with downloading users are being more vulnerable to downloading and using unauthorised software that can harm their phone.

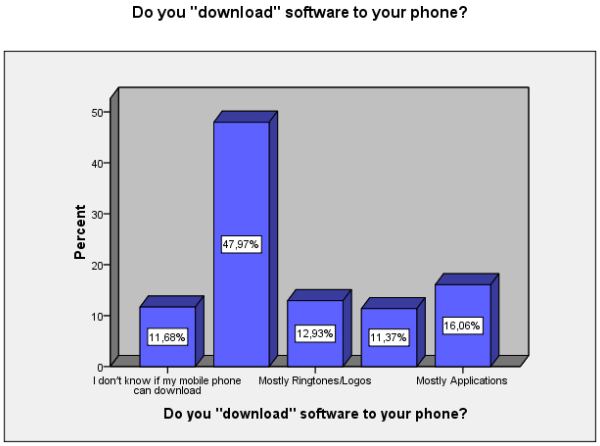

Figure 11. Software downloading.

This is where a mobile phone Antivirus would help. In our case (Figure 12), 19% of users acknowledge it exists such a product but don't use it, while 44% do not know whether such a product exists. That leaves 12.3% using it. Compared to PC users where nowadays everybody is using (at least) an antivirus shows a clear lack of security education and different mind-set. Organizations, in turn, show an increase in mobile phone antivirus tools usage [18]

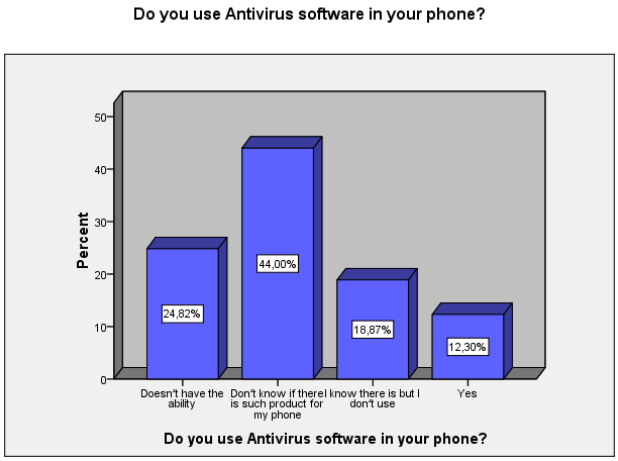

Figure 12. Anti-virus usage.

Being young, 57% of university students keep sensitive information into their mobile phones (Figure 13). It seems that we consider our mobile phone to be a very personal device and we save equally important and sensitive information there. Such kind of information should be protected but again, the results from our survey show that users fail to do so. The consequences from a breach of data of this type could be devastating for the life of the victim.

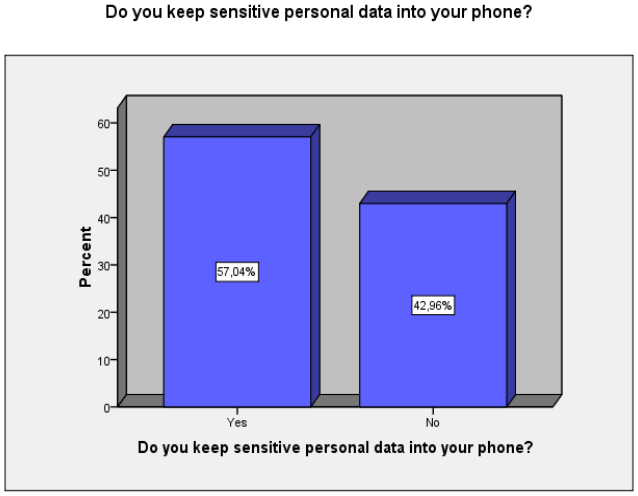

Figure 13. Sensitive information kept in phone.

 ISBN: 978-1-61208-127-4

In a rather alarming finding, 21.6% of users (Figure 14) keep passwords saved in plain in their mobile phone. At least, another 22% is using some form of encryption (i.e. letter scrambling). Since users generally follow the notion of encryption in these saved passwords, it is expected that they would be able to do the same with private information (i.e. photos) kept in the phone, should they be provided the necessary software. Once again, the issue of better designed user interfaces surfaces.

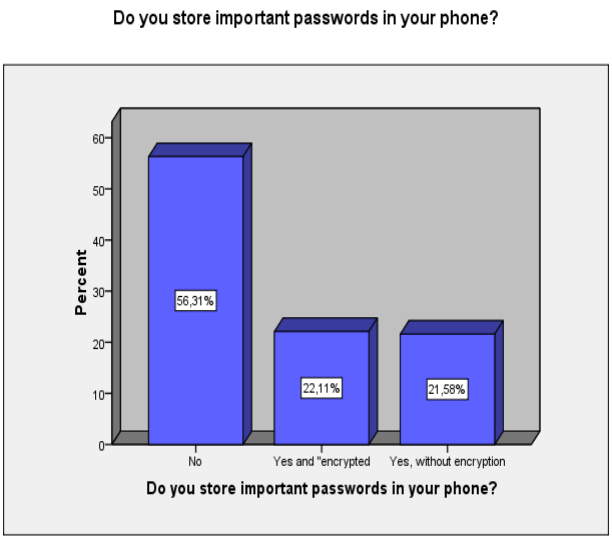

Figure 14. Important passwords kept in phone.

Closing our survey, the issue of backup was examined. As it can be seen in Figure 15, a large percentage of the participants reaching 47% never performs a backup of their phone's data. At least some 53% do backup up, although the majority (19%) less often than once per month.

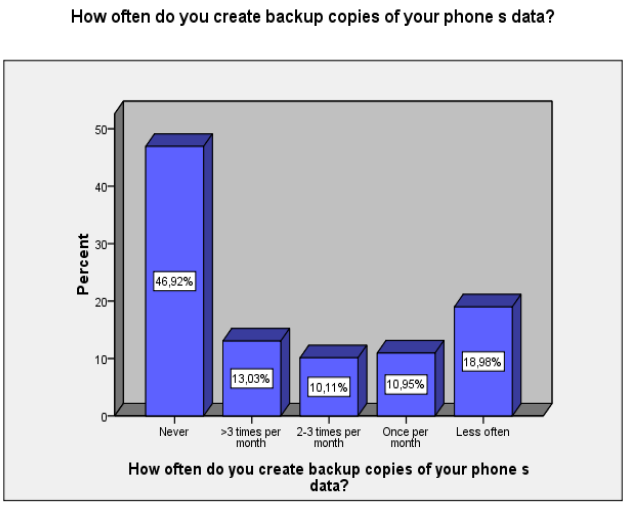

Figure 15. Backup frequency.

V. CONCLUSION AND FUTURE WORK

The majority of the respondents care about security issues and are concerned about data interception and the fact that an intruder could gain unauthorized access to their devices, as previous surveys have clearly showed. However, there is no culture of security and no advanced technical knowledge of their mobile phones.

A very high percentage of users didn't know there is an icon that informs them about the phone encryption status. Most of them don't take backups at all while at the same time would lend their phone that contains sensitive data and passwords to somebody else. Contributing to the problem, badly designed interfaces are an additional factor of hindering the development of security culture.

Students owning phones without modern operating system have statistically (Pearson Chi-Square) better knowledge of security aspects than those who actually own a phone with modern O/S. At the same time, they feel statistically the least secure while, on the other hand, users that do not know the type of O/S are more "relaxed".

In order to have comparative results, we have conducted a similar survey in more than 10 European countries reaching more than 7500 students and the results will soon be published. The preliminary findings however, show that users exhibit the same behaviour everywhere. Since students (who are young people and mostly receptive to technology and knowledge) do not actively follow most of security best practices then academia, phone manufacturers and operators must team up informing users, raising awareness level and building more secure systems and user interfaces with transparent security features.

REFERENCES

[1] Synovate, "Global mobile phone survey shows the mobile is a 'remote control' for life", Synovate survey, http://www.synovate.com, 2009 [accessed: 09/10/2010]

[2] Rahman, M. and Imai, H., Security in Wireless Communication, Wireless Personal Communications, vol. 22, issue, 2, pp. 218-228, 2002

[3] I. Androulidakis, Intercepting Mobile Phones, Article in «IT security professional» magazine, Issue 8, pp. 42-28, Jan-Feb 2009

[4] Trend Micro, *"Smartphone Users Oblivious to Security"*, Trend Micro survey, http://www.esecurityplanet.com, 2009, [accessed: 09/10/2010]

[5] Goode Intelligence, *"Mobile security the next battleground", http://www.goodeintelligence, 2009, [accessed: 09/10/2010]*

[6] Androulidakis, N. and Androulidakis, I. Perspectives of Mobile Advertising in Greek Market, 2005 International Conference on Mobile Business (ICBM 2005), pp. 441-444, 2005

[7] Vrechopoulos, A.P., Constantiou, I.D., and Sideris, I. Strategic Marketing Planning for Mobile Commerce

 ISBN: 978-1-61208-127-4

Diffusion and Consumer Adoption, in Proceedings of M-Business 2002, pp. CD, July 8-9, 2002

[8] comScore M:Metrics, *"Smarter phones bring security risks: Study"*, http://www.comscore.com, 2008 [accessed 09/10/2010]

[9] I. Androulidakis and D. Papapetros, Survey Findings towards Awareness of Mobile Phones' Security Issues, Recent Advances in Data Networks, Communications, Computers, Proceedings of 7th WSEAS International Conference on Data Networks, Communications, Computers (DNCOCO '08), pp 130-135, Nov. 2008

[10] I. Androulidakis, C. Basios, and N. Androulidakis, Surveying Users' Opinions and Trends towards Mobile Payment Issues, Frontiers in Artificial Intelligence and Applications - Volume 169, (Techniques and Applications for Mobile Commerce - Proceedings of TAMoCo 2008), pp. 9-19, 2008

[11] National Cyber Security Alliance (NCSA), *"Schools Lacking Cyber Security and Safety Education"*, http://www.staysafeonline.org, 2009 [accessed: 09/10/2010]

[12] McAfee, *"Most Mobile Users Don't Know if They Have Security",* McAfee-sponsored research, http://www.esecurityplanet.com, 2008 [accessed: 09/10/2010]

[13] Dillman, D. A., Mail and Internet Surveys: The Tailored Design Method, John Wiley & Sons, 2nd edition, November 1999

[14] Pfleeger, S. L. and Kitchenham, B. A. Principles of Survey Research Part 1: Turning Lemons into Lemonade, ACM SIGSOFT Software Engineering Notes, vol. 26 (6), pp 16-18, November 2001

[15] Androulidakis I., Androulidakis N. On a versatile and costless OMR system Wseas Transactions on Computers Issue 2, Vol 4, pp. 160-165, 2005

[16] CPP, *"Mobile phone theft hotspots",* CPP survey, http://www.cpp.co.uk, 2010 [accessed: 09/10/2010]

[17] ITwire, *"One-third of Aussies lose mobile phones: survey",* ITwire article, http://www.itwire.com, 2010 [accessed: 09/10/2010]

[18] Darkreading, *"Survey: 54 Percent Of Organizations Plan To Add Smartphone Antivirus This Year",* Darkreading article, http://www.darkreading.com. 2010[accessed: 09/10/2010]

APPENDIX

The Questionnaire used

1) Male (A) or Female (B)?
2) Age? (A < 18, B 18-20 , C 21-23, D 24-26 , E >26)
3) Are you studying: (A: Humanities-Philology, B Medicine, C Law, D Engineering-Computer Science, E Maths-Natural Sciences, F Economics-Business Administration, G OTHER
4) How many mobile phones do you use (daily)?
A) 1 B) 2 C) >2 D) None
5) Are you a contract subscriber or a prepaid subscriber?
A) Pre-paid (Card) B) Post-paid (Contract) C) Both
6) Your average monthly phone bill? (A up to 10 Euros, B 11-20 Euros, C 21-30 Euros, D 31-40 Euros, E >40 Euros)
7) Brand of the phone you are mostly using now? (A Nokia, B Sony-Ericsson, C Samsung, D Sharp, E Apple I-phone, F Motorola, G LG, H Other)
8) Does it have an advanced operational system (eg Symbian, Windows Mobile, Android)? (A I don't know, B yes, C no,)
9) Have you noted somewhere your mobile phone's IMEI? (A, I don't know what it is, B yes, C no,)
10) Was your mobile phone ever lost or stolen? (A Never, B once, C more than once)
11) Are you aware of the existence of a special icon in your telephone which informs you for the encryption's deactivation? (A Yes, B No)
12) Do you have SIM card's PIN activated? (A Yes, B No)
13) Do you use password in your phone's Screen-Saver? (A I don't know if it has such a feature, B, doesn't have such feature, C, Yes, D No)
14) Do you have Bluetooth: (A Switched on and visible, B Switched on and invisible, C Switched off, D don't know the difference between visible and invisible, E My phone doesn't have Bluetooth,
15) Do you lend it to others? (A Never, B Only for a while and if I am present, C Yes)
16) Do you "download" software to your phone? (A I don't know if my mobile phone can download, B No, C mostly Ringtones/Logos, D mostly Games, E mostly Applications)
17) Do you use Antivirus software in your phone? (A Doesn't have the ability, B Don't know if there is such product for my phone, C I know there is but I don't use D Yes)
18) Do you store important passwords in your phone (eg Credit cards passwords, ATM passwords)? (A No, B Yes and "encrypted", C yes, without encryption)
19) How often do you create backup copies of your phone's data? (A Never, B >3 times per month, B 2-3 times per month, C Once per month, D Less often)
20) Do you keep sensitive personal data into your phone (photos/videos/discussion recordings)? (A Yes, B No)
21) How safe do you consider communication through mobile phones? (A Very Much, B Much, C Moderately, D Not too much, E Not at all)
22) Are you informed about how the options and technical characteristics of your mobile phone affect its security? (A Very Much, B Much, C Moderately, D Not too much, E Not at all)

 ISBN: 978-1-61208-127-4