Scientific and Practical Cyber Security Journal (SPCSJ) 2(1):72-83
Scientific Cyber Security Association (SCSA), 2018 ISSN: 2587-4667

A PERSUASIVE SYSTEM FOR INFLUENCING MOBILE PHONE USERS' LOCKING BEHAVIOUR

S. Agholor, D.O. Aborisade and A. Onuodafin
Federal College of Education, Abeokuta, Nigeria
Federal University of Agriculture, Abeokuta, Nigeria
College of Education, Eki-Adolor, Nigeria

ABSTRACT: The ease of usage of mobile phones led to its adoption by the users as personal digital assistant. This adoption, no doubt made it a lucrative target for cyber-criminals. A mobile phone can get into the hands of criminals through theft or loss. When this happens, the stored data can easily be compromised if the mobile phone is not protected with a password. To avoid this, developers of the mobile phone operating system included various screen lock options as the first line of defence to prevent unauthorized access to the mobile phone and by extension, the stored data. Various studies on the use of these screen lock options revealed that most end-users do not generally make use of it. To solve this problem, an Auto-reminder Persuasive System (APS) was developed. The system was implemented using Android SDK and JAVA. A pilot test was carried out using purposive selection of 1000 participants randomly divided into two equal groups of 500 members labeled A and B for experimental and control groups respectively. In the experimental group, APS was installed on the mobile phones of the members, while in the control group there was no installation of APS. At the end of the three months of the pilot test, the mobile phones of members of the two groups were collected and attempts were made to use the phones. The result from group A showed that 98.40% of members of the group passworded their phones as against the 24.00% from group B. With this result, it showed that APS is a highly promising method of persuading end-users to use password in protecting their mobile phones against unauthorized access.

KEYWORDS: Android Operating System, Auto-reminder Persuasive System, Countermeasures, Passwords, Screen Lock Options

1. INTRODUCTION

In recent years, cell phones have evolved spectacularly from supporting telephony only to supporting multiple features, ranging from capturing and playing digital media, to e-mail access and e-banking [1, 2], as well as remote access to personal files [3]. This has led to an unprecedented expansion in the usage of mobile phones. For example, over the last decade, the number of mobile phone subscribers in the United States alone has more than doubled with the projection that it will soon surpass the number of people in the United States [4]. Similarly, in Nigeria the number of connected lines are over 192 million, while the number of active lines are over 140 million with a 100.59 teledensity [5]. From the foregoing, one can say that the number of subscribers in Nigeria are more than her population, which implies that there is ubiquitous use of mobile devices in Nigeria. The world-wide phenomenal expansion in the use of mobile phones also made it a great target for attackers.

Unfortunately, most users' refusal to make use of the first line of defence on their mobile phones to protect their stored data despite its vulnerabilities calls for serious concern. It is against this background that we proposed an Auto-reminder Persuasive System (APS) whose sole aim is to persuade end-users to use the basic security facility on their mobile phones in protecting the stored data in case of theft or loss.

In this work, smartphones, all handheld phones and the traditional multifunctional mobile phones mean the same and are collectively referred to as mobile phone(s) or mobile device(s) or simply called device(s) or phone(s). They are used interchangeably.

The rest of the paper is organized as follows. Literature review was treated in Section 2 in which threats to the use of mobile phones and the countermeasures being put in place against these threats were discussed. It also highlighted why end-users choose convenience to security. The proposed system to overcome the issues raised in Section 2 was discussed in Section 3, while implementation and evaluation were handled in Section 4. Finally, recommendation and conclusion were discussed in Section 5.

2. LITERATURE REVIEW

The unique property and usage pattern of a mobile device subject it to threats that are often higher than those of personal computers.

First, mobile devices allow storage and retrieval of many types of sensitive data and services, including personal photos, email, text messages, GPS traces, social media feeds, bank accounts, and corporate infrastructure [6]. Always-on with smooth access to services made it easy for attackers to leverage on one account to gain access to another. For example, an attacker that gained physical possession of a mobile device can request a password re-set for one service, which sends a reset message to an email account on that mobile device [6], especially when the mobile device is not passworded.

Second, users carry and use mobile devices everywhere [6]. These small devices can easily be lost, forgotten, or stolen. For instance, in many major USA cities, over 40% of users have either lost their cell phones or have been victims of cell phone theft [7]. According to [8], the number of phones lost in USA have skyrocketed to thirty million. When we talk about the number of mobile phones lost or stolen in Nigeria, there are no relevant statistics to refer to as many victims do not report officially to the appropriate authority. However, [9] in a survey of 500 participants found that 10% of the respondents have experienced a case of mobile phone loss or theft.

According to [10], most data breaches on mobile devices are typically due to basic security failures such as weak or no passwords being in place, failure to encrypt data or falling victims to phishing or other social engineering attacks and yet the survey result of [10] showed that 67% of their respondents do not protect their mobile phones against unauthorized access with password.

Furthermore, industry surveys estimated that between 38% and 70% of smartphone users do not even lock their phones with passwords or PINs [11, 12, 13]. In a related study, a survey of 500 participants by [9] showed that 80% of the respondents do not password their mobile phones. In view of the foregoing findings, one is forced to ask: “why do users prefer insecure access on devices that are very useful and sensitive but prone to theft or loss?” One explanation offered by the users according to [6] is that entering passwords and PINs on virtual keyboards is time consuming, cumbersome, and error-prone. Similarly, [14] finding showed that 55% of their respondents choose convenience over security as their reason for not using the basic security facility provided by their mobile phone manufacturer. Another

explanation according to [6] is that users do not believe that passwords or PINs are needed to prevent unauthorized use of their phone since they are the only one using the phone forgetting that it can be misplaced or lost or stolen. It is therefore necessary to develop a system that will persuade end-users to make use of the basic security facility on their phones. This is the goal of this study.

2.1 Review of existing Security Measure for Mobile Phones

Over the last decade, efforts from industries and research communities have made significant progress in addressing the security of mobile phones [15, 16, 17, 18]. However, much is still needed to be done in addressing the issue of the majority of the end-users' refusal to make use of these security features. These security measures, which should be implemented proactively by mobile phone users are grouped into three categories according to [19]. These categories are briefly discussed in the following sub-sections.

2.1.1 Countermeasures against Theft/Loss

To counter theft/loss, the security countermeasures proposed by [19] are as follows:

(i) Password: Lock your device with a password. This will prevent unauthorized access to the device;
(ii) PIN: Lock your SIM card with a PIN. This serves as a measure to prevent unauthorized use of it;
(iii) If critical information is going to be stored/saved on the mobile phone, data encryption measures are required;
(iv) If your mobile phone has any expanded memory slot, do not carelessly store sensitive data in such memory. Flash memories such as SD card are electronic storage media which are difficult to completely delete data and therefore, the supposedly deleted data might be restored;
(v) For important data, back it up to a different storage and such back up media also require security countermeasures against theft/loss; and
(vi) It is advisable you use a service that can help you lock your phone or delete its data from a remote site. Most existing antivirus software have this facility.

2.1.2 Countermeasures against Infection

Apart from the aforementioned security measures against theft/loss, there are other security measures that should be considered for mobile phones. As stated earlier, users can freely install applications and use them for various purposes. For this reason, like personal computer users, mobile phone users might suffer damages caused by computer viruses or unauthorized access [20]. Furthermore, they might also be guided to an illicit site and fall for the phishing scam or one-click billing fraud. Once infected with a virus, it might allow for unauthorized access through the virus or the personal information stolen through the virus or even re-format the phone storage.

In order for your mobile phone to be self-defended against malware performing illegal operations and/or unauthorized access, it must be able to prevent virus infection without user intervention. Therefore, the following countermeasures against infection are recommended by [19]:

(i) Use security software/application (Anti-Virus Software);
(ii) Keep your application up-to-date, that is, enable "Automatic Update". This setting is highly recommended;
(iii) Keep the operating system of your mobile phone up-to-date;
(iv) Install applications from a reliable site;
(v) Disable "Allow Installation of Application from Unknown Sources" if you are using Android Operating System; and
(vi) For Android terminals, confirm the access permissions requested, prior to installing that application.

2.1.3 Countermeasures against the Leak of Information

In addition to the aforementioned security measures against theft/loss and infection, one other security measure that should be considered is countermeasures against information leakage. The measures to prevent information leakage as recommended by [19] are listed below:

(i) Avoid the shared use by multiple users;
(ii) For the communication of critical information, use secured line; and
(iii) If you are going to use mobile phone for your business operations at a company, follow the company established security policy (unauthorized use must be strictly prohibited).

2.2 Discussion on the Use of the Security Measures

From the three broad security countermeasures, one can conclude that the most common basic security approach is the screen lock, which enables a user to prevent unauthorized access to his device. For the purpose of this work, the Android Operating System which provides six types of screen lock options was chosen for case study. The Android Operating System was chosen because it runs on many phones such as LG, Techno, Samsung, Sony, Infinix, Philips, Ericson, Blackberry-manufactured smartphones, etc [21]. Furthermore, Android is the world's most popular smartphone operating system with more than 135 million users worldwide [20]. The six screen lock options are None, Slide, Voice Unlock, Pattern, PIN and Password. They are further explained below.

(a) None
This means none selection of any other protected means of locking the phone. It is the mobile phone manufacturer's setting. In other words, it is selected for the phone owner by the manufacturer. When this option that has been selected by the manufacturer is allowed to stay by the phone owner, it means that the mobile phone is not locked at all, hence no protection against unauthorized access.

(b) Slide
This is commonly used in place of PIN and password to prevent the phone from dialing when a button or number is unintentionally pressed. It is not an effective lock of the phone against unauthorized access as the screen will display how you can unlock it.

(c) Voice Unlock
It enables an end-user to use his/her voice in locking the phone. It is sparingly used by end-users for fear of voice variation/imitation. The snapshot is shown in figure 1.

Figure 1: Android Screen Lock using Voice Unlock

(d) Pattern

This method allows end-users to create patterns instead of digit- and text-based passwords. Android provides a pattern-based screen locking application that consists of a 3X3 grid of dots. The end-user then connects the dots together in some easily remembered pattern. To unlock the phone, the end-user is presented with the 3X3 grid and is asked to re-enter the pattern before access is granted. The pattern-based method may be easier to input on the small screens of mobile devices and also easier to remember but it has very low entropy which makes cracking it very easy. The snapshot of Pattern lock is shown in figure 2.

Figure 2: Android Screen Lock using Pattern

(e) PIN

This is similar to the Password but makes use of only numeric characters (digits). The end-user is presented with a numeric keyboard, resulting in PIN-like passwords. While PIN codes are more easier to use on mobile phones than passwords, they also offer a smaller key space which makes an offline dictionary attack easier. However, the use of digits are better than nothing. The snapshot of PIN lock is shown in figure 3.

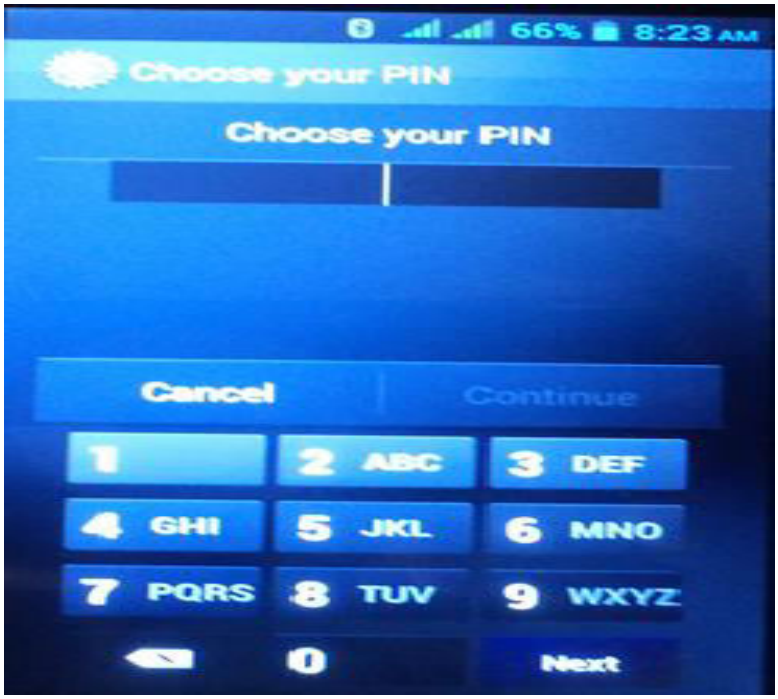

Figure 3: Android Screen Lock using PIN

(f) Password

This method allows end-users to employ a password similar to that used on a standard computer. The application of passwords may be difficult to use given the small screen and virtual keyboards on the mobile devices but they offer high entropy especially when the end-user makes use of at least eight characters consisting of the uppercase, lowercase, symbols and numeric. The snapshot of Password lock is shown in figure 4.

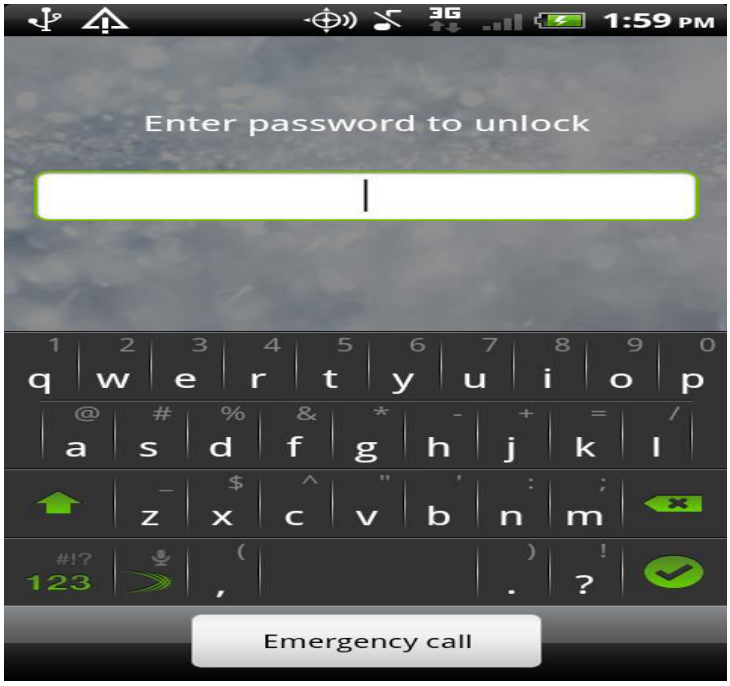

Figure 4: Android Screen Lock using Password

In summary, Screen lock is similar to password used to log onto a computer and is based on methods that fit within the different usage patterns of mobile devices. Furthermore, given that passwording a computer to prevent unauthorized access to data and programs is important, keeping a mobile device secured is considerably more important. This is true because mobile devices are gateway to a wealth of end-users' sensitive data stored on it. Thus, end-users need to be persuaded to use the basic security facility provided on their mobile phones through a system that will constantly remind them on the need to password their phones.

3. METHODOLOGY

From the literature, it was found that most end-users do not password their mobile phones, hence the need to persuade them to use the screen lock to prevent unauthorized access to their devices. In this study, we proposed a novel system called Auto-reminder Persuasive System (APS).

3.1 The Auto-reminder Persuasive System (APS)

The Auto-reminder Persuasive System was designed to influence end-users in applying the basic security facilities offered by Android Operating System. The simplified architecture is presented in figure 5.

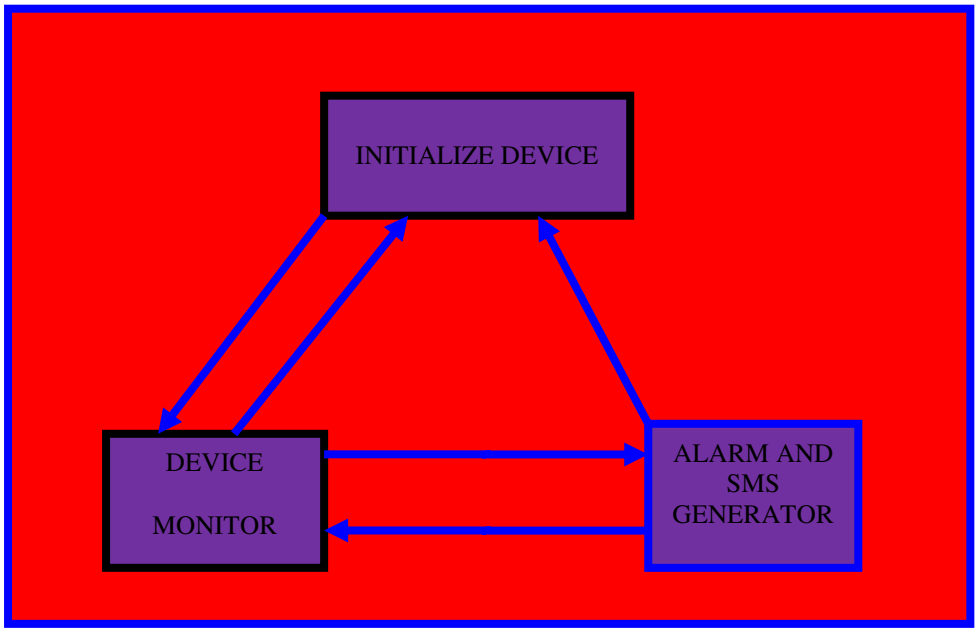

Figure 5: Simplified architecture of APS

3.1.1 Initialize Device Module

This Module checks if the device is switched on. If it is switched on, it communicates with the Device Monitor.

3.1.2 Device Monitor Module

On receiving communication from the Initialize Device Module, it checks if the device is passworded. If it is not passworded, it communicates with the Alarm and SMS Generator Module. Otherwise communication with Alarm and SMS Generator Module is terminated and the process is halted.

3.1.3 Alarm and SMS Generator Module

When this Module receives communication from the Device Monitor Module, it converts the following words “It is dangerous not to lock your phone. Lock it now with a password” into speech, which is referred to as sound message. After 10 minutes interval, it generates an SMS message with the following wordings “It is dangerous not to lock your phone. Lock it now with a password” and sends the SMS to the phone. The sound message and the generated SMS message will be alternated after every 10 minutes interval and will automatically stop once the phone is passworded. The sound message and SMS message are used to alert the end-user that his phone is not passworded, thereby persuading him to password it.

3.2 Algorithm of APS

```
1. Initialize the Device (D)
2. Let R denote the situation that D is passworded
3. onDeviceReady and R=False, then Goto 4 else 5
4. ∀ every 10 mins, alternate between 4a and 4b
    a. GET monitorPassword
```

```
      IF(monitorPassword=True) then
            deactivate app
            ELSE
            keep app running
            soundAlarm  "It  is  dangerous  not  to  lock  your
phone.
                        Lock it now with a password"
       ENDIF
   b. GET monitorPassword
      IF(monitorPassword=True) then
           deactivate app
           ELSE
           keep app running
           popupSMS "It is dangerous not to lock your phone.
                     Lock it now with a password"
       ENDIF
    GOTO 3
5. STOP
```

4. IMPLEMENTATION AND EVALUATION

4.1 Implementation

The Auto-reminder Persuasive System was implemented on Android Software Development Kit (SDK) with Android Development Tools (SDK) and JAVA.

4.2 Evaluation

The evaluation of the system was carried out using a purposive selection of One Thousand participants drawn from the second year students of the Federal College of Education, Abeokuta, Nigeria. The One Thousand participants were randomly divided into two equal groups of Five Hundred each. These groups were labeled A and B representing experimental and control groups respectively. The participants were then asked to write their names and group label on their phones for ease of identification. They were informed that a social media software called Telegram will be installed on their phones in which the lead researcher will pass lecture notes and exercises on CSC215 to them, in addition to the formal teaching. They were asked to come back to the laboratory after two hours to collect their phones. In addition to installing Telegram for all the participants, all the members of group A have their mobile phones installed with APS, while the APS was not installed for members of group B. At the end of the three months of the pilot test, the mobile phones of members of the two groups were collected and attempts were made to use the phones. The results of the pilot test are presented in tables 1, 2 and 3.

4.3 Results and Discussion

4.3.1 Demographic Analysis of the Participants

The result from the demographic analysis of the 1000 participants is presented in table 1.

Table 1: Demographic Analysis of the Participants

Sex	Number of Participants	Percentage
Male	540	54.00%
Female	460	46.00%
Total	1000	100.00%

Table 1 showed that out of the 1000 participants, 54.00% are males, while 46.00% are females.

4.3.2 Analysis of Use of Screen Lock Options by Group A

The analysis of the use of Screen Lock Options after the three months of the pilot test is presented in table 2. It should be noted that all members of this group have their mobile phones installed with APS.

Table 2: Analysis of use of Screen Lock Options by group A

Options	Number of Participants	Percentage
None	8	1.60%
Slide	0	0.00%
Voice Lock	0	0.00%
Pattern	0	0.00%
PIN	12	2.40%
Password	480	96.00%
Total	500	100.00%

After the application of Auto-reminder Persuasive System, the trend of not passwording the mobile phones was reversed downwardly as shown in table 2. From table 2, a high result of 96.00% of the end-users used password to lock their mobile phones, while 2.40% made use of the PIN option to lock their mobile phones. This brings the aggregate of the end-users who passworded their phones against unauthorized access to 98.40%. However, 1.60% still left their phones unlocked. The result showed that if APS is installed in the end-users' mobile phones, it will definitely yield positive result in persuading them to password their phones.

4.3.3 Analysis of use of Screen Lock Options by Group B

The analysis of the use of Screen Lock Options after the three months of the pilot test is presented in table 3. It should be noted that APS was not installed on the mobile phones of the members of this group.

Table 3: Analysis of use of Screen Lock Options by Group B

Options	Number of Participants	Percentage
None	300	60.00%
Slide	80	16.00%

Voice Lock	0	0.00%
Pattern	40	8.00%
PIN	45	9.00%
Password	35	7.00%
Total	500	100.00%

Table 3 showed the various Screen Lock Options that end-users used to lock up their phones. It is highly disturbing and worrisome to find out from table 3 that 60.00% of the participants do not lock their mobile phones at all, while 16.00% make use of Slide option. The slide option is not a protection against unauthorized access, hence the aggregate of end-users that do not password their phones were 76.00%, despite the confirmation from them that they use the phones for email, social media and banking transactions among others. This finding validated the results of [9], [14], [10] and [23] who reported that among their participants, 80%, 55%, 67% and 83% respectively do not password their mobile phones. On the other hand, 24.00% of the members of this group passworded their mobile phones.

Drawing inference from tables 2 and 3, it showed that with APS installed on their mobile phones 98.40% of the participants passworded their mobile phones as against 24.00% that passworded their mobile phones when APS was not installed.

5. RECOMMENDATION AND CONCLUSION

5. 1 Recommendation

In view of the huge success of the Auto-reminder Persuasive System in persuading end-users to make use of the security features found on their mobile phones as evidenced from the result in table 2, the paper recommends that mobile phone operating system developers should as a matter of neccessity incorporate APS in their design.

5.2 Conclusion

The result from the pilot test showed that with Auto-reminder Persuasive System, 98.40% passworded their mobile phones against unauthorized access in the event of loss or theft. On the contrary, 24.00% passworded their mobile phones against unauthorized access when APS was not applied. The result from this study showed that APS is a highly promising method of persuading end-users' to lock their mobile devices against unauthorized access..

REFERENCES

1. Halmiton, A (2007) Banking Goes Mobile. From wwww.time.com/time/business/… Date visited 07/03/2015
2. Tiwari, R., Buse, S and Herstatt, C (2007) Mobile Services in Banking Sector: The Role of Innovative Business Solutions in Generating Competitive Advantage. *In International Research Conference on Quality, Innovation and Knowledge Management*, New Delni, pp. 1-17
3. Sabzevar, A. P and Sousa, J. P (2008) Inproving the Security of Mobile-Phone Access to Remote Personal Computers. *In International Conference on Software and Data Technologies*, pp. 96-103

4. CTIA (2012) U.S. Wireless Quick Facts. From ctia.org/… Date visited 03/03/15
5. Nigerian Communications Commission (2015) Subscribers Statistics. From www.ncc.gov.ng/. Date visited 03/03/2015
6. Fischer, I., Kuo, C., Huang, L and Frank, M (2012) Smartphones: Not Smart Enough? In ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM) pp. 1-6
7. Lookout Blog (2011) Lost and Found: The Challenges of finding your lost or stolen phone. From www.blog.mylookout.com/blog/... Date visited 03/03/2015
8. Jaroslovsky, R (2012) Help for Lost Cell Phones. From www.businessweek.com/magazine/ content/… Date visited 06/06/12
9. Agholor, S (2015) The Use of Screen Lock Options in Securing Mobile Phones. *In Akoka Journal of Vocational and Science Education*, Vol. 3, No. 2, pp. 231-237.
10. Lyne, J (2011) 67 Percent of Consumers Don't Have Password Protection on Their Mobile Phones. From www.sophos.com. Date visited 03/03/2015
11. Retrevo Blog (2011) iPhones, backups and tablets, what is the connection? From www.retrevo.com/content/blog... Date visited 07/03/2015
12. Norton (2011) Norton Survey reveals one in three experience cell phone loss/theft. From www.symantec.com/about/news/release/... Date visited 07/03/2015
13. Sophos Blog (2011) Survey says 70% do not Password-Protect their Mobile Phones. From www.nakedsecurity.sophos.com/... Date visited 07/03/2015
14. Confident Technologies (2014) Survey Shows Smartphone Users Choose Convenience Over Security. From www.confidentTechnologies.com/survey. Date visited 07/03/15
15. Apperian (2011) Solving Android Multiple Personality Disorder: No Drugs Required. From www.apperian.com/... Date visited 03/03/15
16. Fraunhofer (2012) BizzTrust Two Smartphones in One. From www.sit.fraunhofer.de/en/ bizztrust/… Date visited 03/03/15
17. iGillottResearch (2006) Security Mobile Devices on Converged Networks. From www.trustedcomputinggroup.org/... Date visited 03/03/15
18. Anderson, C. L. and Agarwal, R (2010) Practicing Safe Computing: A Multi Method Emperical Examination of Home Computer User Security Behavioural *Intentions. In MIS Quarterly*, Vol. 34, No. 3, pp. 613-643
19. Information-Technology Promotion Agency (2012) Security Measures Guide For Smartphones. From www.ipa.gov.jp/security... Date visited 07/03/2015
20. Chris, R (2012) Smart Phone, Dumb Security. *In Review of Business Information Systems*, First Quarter, Vol. 16, No. 1, pp. 21-26
21. Agholor, S (2017) An Improved Approach for Managing Multiple Passwords. An Unpublished Ph.D. Thesis submitted to Dept of Computer Science, FUNAAB, pp. 1-289
22. Gikas, M (2014) Most Americans Don't Secure their Smartphones. From www.cnbc.com/101611. Date visited 07/03/15
23. Bojinov, H., Bursztein, E., Boyen, X., and Boneh, D (2010) Kamouflage: Loss-Resistant Password Management. From www.cryto.stanford.edu. Date visited 11/12/2014