

Mobile Security Practices of Faculty and Students in a Philippine State University

Niel Francis B. Casillano*

Department of Information Technology Eastern Samar State University, Philippines;
nfcasillano@gmail.com

Abstract

Objectives: This study aimed to determine the various practices of faculty members and students of Eastern Samar State University in terms of mobile phones security. **Methods/Statistical Analysis:** This research used the descriptive research design and adapted a questionnaire from Androulidakis and Kandus (2011) in their study entitled "What University Students Do (or don't) Know about Security in their Mobile Phones". The respondents of the study were faculty members and students of Eastern Samar State University. Weighted mean and percentage were used to interpret the gathered data. **Findings:** It was determined that most of the faculty members and the students saved sensitive data (ATM pins, passwords, images, videos) in their mobile phones without using any encryption methods. It was discovered further that more than 50% of the faculty and students were not aware of the security features in their respective mobile phones therefore exposing their sensitive data to hacking, intrusion and data theft. **Application/Improvements:** The results of this research can be used as inputs in the conduct of a University-wide Mobile security awareness campaign to increase the over-all knowledge of students and faculty members on mobile security.

Keywords: Data Security, Confidentiality, Information Assurance, Mobile Security, Passwords

1. Introduction

Phones have drastically evolved from a basic call and text device to an advanced mobile computing system. The world is becoming smaller every second because of the tremendous advancements in the mobile phone technology. With the integration of advanced operating systems, phones that were merely used as handsets for calling and texting can now be used as a camera, music player, web browser, TV and many other innumerable uses¹.

There are over 4 billion users of mobile phones worldwide comprising almost two thirds of the world's population. In industrialized countries, increase in mobile phone usage means increase in the demand of data services². This leads to an increase of sensitive data being stored on mobile phone³. Old mobile phones security problem was only communication breach but this is

not the case anymore. More and more phones become advanced which makes more people store many types of data in their devices. Transactions such as mobile banking and online shopping, which involves highly sensitive data, attract hackers. Also, increase in available applications also increases the chances of installing a malicious program that might corrupt, delete or expose sensitive data⁴.

This study aimed to determine the mobile phone security practices of the faculty members and students of the College of Computer Studies - Eastern Samar State University Main Campus.

2. Objectives

This study aimed to determine the various practices of faculty members and students of Eastern Samar

*Author for correspondence

State University – College of Computer Studies in terms of their mobile phones security.

Specifically, this study aims to determine:

1. Practices of faculty and student-respondents in terms of their mobile phones:
 - 1.1 Physical security
 - 1.2 Data Security
2. Types of sensitive data kept in their mobile phones
3. Awareness on how mobile technical characteristics can affect security.

3. Materials And Methods

3.1 Research Design

In this study the researchers determined the practices of faculty and students in terms of their mobile phones' security. Descriptive research design was used in this study.

3.2 Respondents

The researchers distributed a total of 215 questionnaires (203 randomly selected BSIT and BSCS students, 12 faculty members of the College of Computer Studies).

3.3 Instrument

The instrument that was used in this study is a questionnaire adapted from the study of Androulidakis and Kandus, 2011 entitled "What University Students Do (or Don't) Know about Security in their Mobile Phones"⁴. The same questionnaire was also used by the same authors in the study "Mobile Phone Security Awareness and Practices of Students in Budapest"⁵. The questionnaire was modified to fit the needs of the researchers.

3.4 Data Analysis

The descriptive statistics using the frequency and percentage was employed to present the Demographic characteristics of the respondents and level of the students' knowledge on Mobile security.

4. Results

Results from the survey were analyzed and the following were deduced:

Table 1 shows the extent of knowledge and practices of faculty and student-respondents in terms of their mobile

phone's physical security. Question 1 indicates that few of the respondents (faculty, 33%; students, 26%) lost their phones. Mobile phones that were lost or stolen may contain important and confidential data that can cause harm to the owner. One of the ways to mitigate such problem is through blocking the phone using the IMEI Number. Questions 2 and 3 indicate that a huge percentage of the respondents didn't know what IMEI is for and how it was accessed.

Table 2 shows the practices of the faculty and student respondents in terms of their mobile phones' data/software security. A question 3, 4 and 5 tackles software components that can be optimized to improve phone security. Results indicate that only few of the faculty and student respondents (faculty, 17%; student, 7%) activate their SIM cards pin. SIM cards can contain vital information such as contact numbers, card numbers and messages that may be considered confidential. Results from Question 5 indicate that most faculty respondents (75%) use passwords as screensaver while only 31% of the student-respondents use password as screensaver. It was also determined that although most of the respondents' mobile phone have antivirus (faculty, 93%; students, 83%), most of them do not optimize its functions.

Table 2 also shows that a huge percentage of the respondents (faculty, 75%; students, 65%) store important data such as card numbers, passwords and etc. It was figured out that only 22% of faculty and 2% of student respondents use encryption methods of their important data. Encryption of data is important because it converts important files into an unreadable format and only authorized users can retrieve these data.

Figures 1 and 2 shows the types of sensitive data respondents store in their mobile phones. It was determined that most of the faculty and student respondents store Photos (faculty, n = 7; students, n=180), videos (faculty, n = 7; students, n = 170), documents (faculty, n = 6; students, n = 80), passwords (faculty, n = 3; students, n = 110) and PIN (students, n = 80) and with the result of Table 2 – Question 9, these data are exposed to data loss and theft.

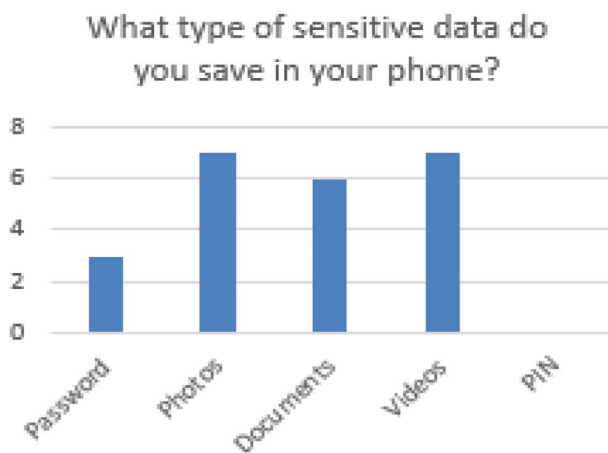
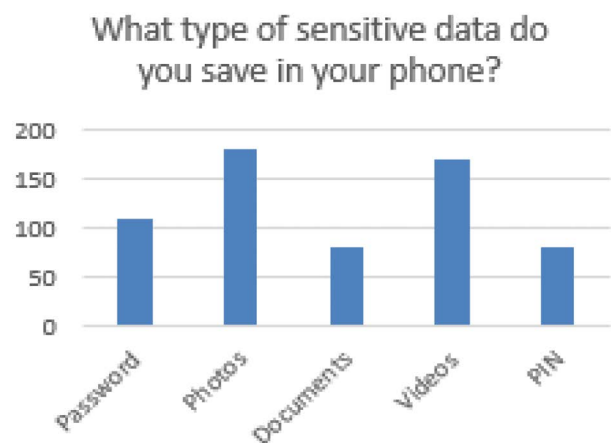
Figures 3 and 4 shows that a large percentage of respondents were not aware about the security characteristics of their mobile phones (Faculty, 41%; Students, 54%). The unawareness of the user in terms of their mobile phones security could lead to exposure of their personal and confidential data.

Table 1. Phone security

No.	Questions	Faculty (n=12)				Students (n=203)				Total
		Yes		No		Yes		No		
		f	%	F	%	f	%	f	%	
1	Was your mobile phone ever lost or stolen?	4	33%	8	77%	53	26%	150	74%	215
2	Do you know what International Mobile Station Equipment Identity (IMEI) is for?	3	25%	9	75%	8	4%	195	96%	215
3	Do you know how to access your phone's IMEI?	3	25%	9	75%	3	1%	200	99%	215

Table 2. Data security

No.	Questions	Faculty				Students				Total
		Yes		No		Yes		No		
		f	%	f	%	f	%	f	%	
4	Do you have SIM card's PIN activated?	2	17%	10	83%	14	7%	189	93%	215
5	Do you use password in your phone's Screen-Saver?	9	75%	3	25%	63	31%	140	69%	215
6	Do you have Antivirus software in your phone?	11	92%	1	8%	169	83%	34	17%	215
7	If yes to Q6, Do you use it?	11	100%	0	0%	82	49%	87	51%	181
8	Do you store important passwords in your phone (e.g. Credit cards passwords, ATM passwords)?	9	75%	3	25%	132	65%	71	35%	215
9	If yes to Q8, Do you use encryption methods?	2	22%	7	78%	2	2%	130	98%	141

**Figure 1.** Types of sensitive data stored in phone (Faculty).**Figure 2.** Types of sensitive data stored in phone (Students).

Are you informed about how the options and technical characteristics of your mobile phone affect its security?

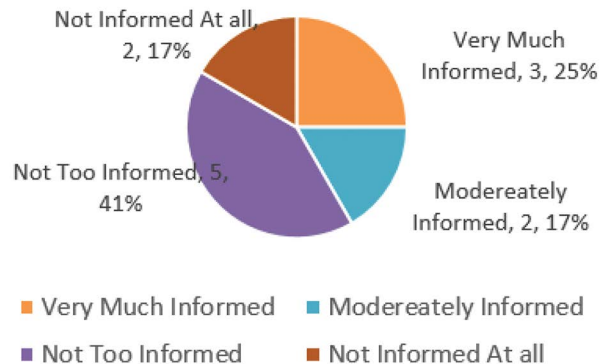


Figure 3. Level of information mobile phone security characteristics (Faculty).

Are you informed about how the options and technical characteristics of your mobile phone affect its security?

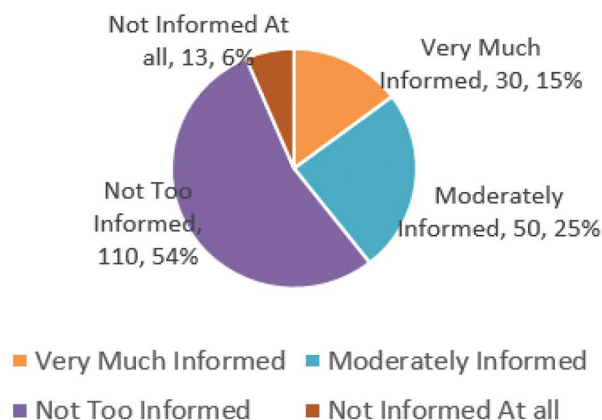


Figure 4. Level of information mobile phone security characteristics (Students).

5. Conclusions

After the interpretation of data, the following conclusions were drawn:

1. Most of the faculty and student-respondents were not aware of the IMEI number or how it was accessed.

2. Although most of the respondents use passwords as screensaver, most of them do not encrypt the data that they save in their phones. Furthermore, they do not activate their Simcard's PIN which exposes their contact numbers, passwords and messages to security breach and penetration.
3. Most of the respondents save important data in their mobile phones and although there is a presence of antivirus software, it is not used to protect these data. Furthermore, encryption methods are not utilized to secure personal data.
4. Some respondents save sensitive data such as images, passwords, videos and PINs in their mobile phones.
5. Most of the respondents were not aware of the security features their phones contain.

6. Recommendation

An Information Dissemination Campaign on Mobile Phone security must be carried out to inform both faculty and students of how critical and important information saved in their mobile phone are and educate them on different mobile security measures.

7. References

1. Breiting F, Nickel C. User survey on phone security and usage. Cased; 2011. p. 1–6.
2. Chintalapati JB, Rao ST. Remote computer access through android mobiles. International Journal of Computer Science Issues. 2012; 9(5):363–8.
3. Androulidakis I, Kandus G. Mobile phone security awareness and practices of students in budapest. The Sixth International Conference on Digital Telecommunications; 2011. p. 18–24.
4. Androulidakis I, Kandus G. What university students do (or don't) know about security in their mobile phones. Telfor Journal. 2011; 3(1):8–12.
5. Androulidakis I, Papapetros D. Survey findings towards awareness of mobile phones' security issues. Proceedings of the 7th conference on Data networks, communications, computers; 2008. p. 130–5.