CHAPTER I

INTRODUCTION

1.1: Introduction

Communication tools are part of our daily life. Using a smartphone nowadays has far exceeded the use of computers. Recently, the smartphone was one of the fastest growing technologies in the world. The phone shipments grew to more than one billion in 2012, and the phone shipments are expected to grow to two billion (Llamas and Restivo, 2012). Smartphones combine functions of mobile phones and computers. The first device that combined phone and computer was made in 1973. First Smartphone was released to the public in the 1993 which was produced by IBM. The term of "Smartphone" first appeared in 1997. Smartphones can be defined as handheld mobile telephone devices that integrate advanced information processing functions with conventional mobile phone capabilities.

With a large number of products equipped with touch screens, Smartphones characteristically offers users the ability to customize their handset as they please, enabling unrestricted installation of desired applications in much the same manner as PC. Smartphones offer functions that are not available on PCs, including HD video cameras, GPS function and other accessories, and in light of this, Smartphone allows people to stay connected to internet networks, also it allows everyone to write up a quick Word document and easy to check their emails. There is a need to be mindful of the fact that although Smartphones offer a high level of convenience, there is always the possibility of new risks emerging as a result of this convenience factor.

Also the applications for the Smartphones are not as powerful as on the regular computers. Popularity of smart phones is constantly growing together with a number of third-party applications and Smartphone applications, such as Google play and Ovi store, according to (Mylonas et al., 2013).

Smartphones connect to the internet in two ways; they can connect to wireless networks or connect through smartphone SIM card. And they might download malware and viruses from the web and disseminate it to network devices. Also smartphones are beyond IT control. It is very hard for IT specialists to control what users do with their smartphones, and how these devices expose confidential data to security threats, therefore users are unaware of these malwares and viruses and hence, security features are very important to eliminate this issue.

Smartphones can be used at any age, the two largest groups using the smartphone are adults between 18-29 and 30-49 years (Brenner, 2013). People in these age groups are university students and early career professionals. Also the PEW Research in 2011 reported that college-aged students are among the largest group of smartphone users. Also, Verizon (2012) affirmed that college students are one of the largest of smartphone users. As long as college campuses are open to the public, it could lead to high cybercrime. Various studies reported that cybercrime costs organizations between 110 billion to one trillion dollar every year, according to (Hyman, 2013). Cyber criminals exploit this vulnerability by hacking personal information, or transmitting files which lead to malware infections, identify theft, data tampering and denial of service.

The lack of smartphone security on campuses can permeate academic systems due to the unsecured wireless device which connects to campus resources, like the network

server. This lack of smartphone security makes those resources vulnerable to threats and attacks. If students are not aware of the security of their smartphone, and how to deal with security threats and countermeasures that lead to more attacks such as spoofing, man in the middle can access to their data. Also the confidential information of students and the university system can be accessed and tampered, also their confidential information can be sold. Therefore, this research focuses on students' awareness on smartphone threats and security features.

1.2: Problem Statement

Smartphone devices are exposed to different types of security threats like malicious programs which include virus and worm, vulnerabilities of smartphone, information theft, damage and spam (Kim and Leem, 2005). With the increase of communications and sending information through wireless channels and increase the use of wireless technique between smart phone users, this leads to an increase and generate new threats; and how secure the information security become a critical issue to smartphone devices, and it becomes a source of concern for the smartphone users like the computer users (Bouwman, et al., 2006)

Educational organizations are making every effort to protect information asset from damage, loss, theft, etc. and try to have a strong security mechanism to maintain their assets. But having a strong mechanism is not enough without a high level of security awareness among the students. As Siponen (2000) confirmed that the organizations focus on having advanced technology and assign security experts to deal with security issues while they neglect security awareness which is the basis through which people will be aware of their device's security. However the results from previous studies that looked into the correlation between user awareness programs and

user behavior have shown that, in spite of the implementation of user awareness programs, the organizations still have security problems (Kruger et al., 2003).

In this research, the problem has been determined. Usually students are obsessed with advanced technology such as smartphones, which offer many features and requirements for them. At the same time they are vulnerable to various security threats according to Androulidakis (2010). By using smartphone devices without any security knowledge and lack of awareness and thinking that the smartphone is secure, that will lead students' smartphone being exposed to security risks. This will harm their smartphones and personal or confidential information could be stolen. Therefore, educational institutions should implement information security education (Hentea, 2005). It is also important to conduct further research into security awareness in order to know the current level of user awareness towards the smartphone security threats and how secure their devices by using smartphone security features, and to better understand what factors that contribute and effect the user awareness level. Finally, the relationship between the identified factors should be measure in order to come up with a good security model.

1.3: Research Questions

Q1- What is the level of students' awareness on smartphone security threats and features?

Q2- Which factors (gender, age, educational level, academic specialization and smartphone experience) that affect the students' awareness level?

Q3- Is there any relationship between the factors and students' awareness level on smartphone security threats and smartphone security features?

1.4: Objective of Research

The purpose of this study will focus on two main objectives:-

1- To assess user awareness level of smartphone security threats and security features.

2- To explore the factors (gender, age, educational level, academic specialization and smartphone experience) which affect the user awareness level on smartphone security.

3- To measure the relationship between the factors and students' awareness level on smartphone security threats and smartphone security features.

1.5: Hypotheses

H1: There is a relationship between gender and users' awareness level on smartphone security threats and features.

H2: There is a relationship between age and users' awareness level on smartphone security threats and features.

H3: There is a relationship between educational level and users' awareness level on smartphone security threats and features.

H4: There is a relationship between academic specialization and users' awareness level on smartphone security threats and features.

H5: There is a relationship between smartphone experience and users' awareness level on smartphone security threats and features.

1.6: Scope of Study

The target group of this research is the Zawia University students, between the age of 18-33 years old who use the smartphones, because the college campuses are open to the public that lead to high cybercrime and this is a good reason for choosing the students for awareness research. Also, this population comprises different cities, and not limited to a specific city. So that, it can be said the population, to a great extent, is representative of Libyan citizens. The scope of this study is to assess the level of users' awareness of smartphone security threats and features, also to explore the factors (gender, age, educational level, academic specialization and smartphone experience) which affect the user awareness level on smartphone security. This study

uses the quantitative method which through the questionnaire. The aim of using the questionnaire is to measure the user awareness level on smartphone security threats and features. Also to come up with a relationship between the awareness level and the factors.

1.7: Significance of the Research

This research was studied on smartphone security awareness. Smartphone usage continues to increase. The mobility and wireless connectivity make internet access easy and the smartphone is often preferred over a laptop or personal computer. However, the data transmitted through the open airwaves are inherently unsecure. Cyber criminals are beginning to target smartphone consumers and exploit the weakness in open airwaves. The college students, the next generation is the largest consumers of smartphone (Verizon, 2012). Androulidakis and Kandus (2010) observed the lack of security awareness on a smartphone. Additional research was necessary to fully understand the security awareness level on smartphone threats and features. The significance of this research was determined in the following:

- Level of user awareness toward the smartphone security threats and features have been identified.
- The factors that affect the security awareness level have been identified.
- The relationship between the factors also have been measured.

1.8: Thesis Outline

The thesis is encompassed of five chapters. Chapter I offers the introduction and defines the problem statement; thereby research questions and the purpose of this study and the significance of the Research. Chapter II, then reviews the literature on smartphone security awareness, and reviews the research being carried out and looking into what already has been done. Chapter III presents the methodology used and the questionnaire that employed in this study. Chapter IV presents the results of this study. Finally, chapter V concludes the overall work.