International Journal of Information Systems and Social Change
Volume 7 • Issue 3 • July-September 2016

The Influence of Students' Characteristics on Mobile Device Security Measures

Winfred Yaokumah, Department of Information Technology, Pentecost University College, Accra, Ghana

ABSTRACT

This study aimed at investigating the influence of students' characteristics (majors, maturity, and gender) on mobile device security practices in the context of a developing country. Focusing on graduate and undergraduate students from both public and private universities, participants' characteristics were measured against three approaches of mobile devices security practices (user-behavior and activities, device settings, and disaster recovery). The sample consisted of 375 students from two public universities and three private university colleges. The results found that Technology and Engineering students differ statistically from Business and Arts students in terms of mobile device settings and disaster recovery practices. The undergraduate students were less engaged in risky activities with their devices compared with the graduate students. Moreover, the younger students were more cautious than the older students regarding user-behavior and device settings. Finally, female students were more negligent when it comes to setting the devices to militate against security threats.

KEYWORDS

Device Settings, Disaster Recovery, Mobile Device Security, Threats, User-Behavior and Activities, Vulnerabilities

INTRODUCTION

Mobile devices such as cell phones, smartphone, and tablet computers are rapidly penetrating all human activities; causing changes in the way people work, learn, play, and interact with each other. International Telecommunication Union, ITU's (2015) recent figures show that the number of mobile phone subscriptions exceeds the world's population of about seven billion and the number of active mobile broadband subscriptions is in excess of 2.1 billion. One area where mobile devices are predominantly used is in higher education (Mtebe & Raisamo, 2014). Mobile devices have impacted students' learning process; students use these devices on daily basis to communicate with their peers and instructors, obtain Internet-based information for research and other purposes, complete assignments using applications such as wikis (Komlenov et al., 2013), and for social networking (Claybaugh & Haried, 2014) such as sharing information, photographs and videos. Even in some cases students use applications on the mobile devices to post inappropriate contents (Melton, Miller, & Salmona, 2012).

However, mobile devices are faced with various security attacks, mainly as a result of the user's behavior and activities that can make the device vulnerable to attacks. Another factor is the user's lack of knowledge of and familiarity with the device features and failure to apply device security measures. For instance, recent studies show that Android phone users have poor understanding of its security features (Felt et al., 2012; Kelley et al., 2012) and 62 percent of smartphone users fail to lock their devices with a password or a pin code (Javelin Strategy & Research, 2012). But, just like all other computing resources, mobile devices must comply with the core security principles of

DOI: 10.4018/IJISSC.2016070104

confidentiality, integrity, and availability, if they are to be relied upon. Accordingly, mobile device security strategies must cover the three security controls that have been implemented to protect information resources: *technical*, *physical*, and *administrative* controls.

While *technical* (logical) controls are the software or hardware components such as firewalls, intrusion preventive and detection systems, antimalware, encryption, identification and authentication mechanisms, *physical* controls are measures including cable locks, fencing, closed-circuit TV, and lighting that are implemented to protect facilities, personnel, and other resources (Shon, 2013). But, *administrative* controls are more management-oriented and deal with security policies and procedures, risk management, personnel security, effective hiring practices, and security awareness and training programs (Shon, 2013). Specific to mobile devices, the major operating systems developers, BlackBerry operating system (OS), iPhone OS (iOS), Android OS, and Windows Phone OS, have implemented security measures to protect the devices and the data they contain. These security measures can broadly be grouped under four layers. The *device security* layer prevents an unauthorized individual from accessing and using the device, *data security* layer protects the data stored on the device even if the device is stolen, *network security* layer provides tools that can encrypt data while being in transit across a network, and *application security layer* has mechanisms to secure the operating system and isolate applications while they are running (Apple Inc., 2014).

Though mobile operating systems and their applications have some levels of security measures (Perakovic et al., 2012), they have serious security concerns (Patten & Mark, 2013). For example, Juniper Networks (2013) reports on the rapid growth of mobile malware from 155% in July 2011 to 614% between 2012 and 2013. Also, Munro (2014) demonstrates the process of exploiting the Android operating system to uncover personal data and PIN codes that users stored on the devices. Consumer Reports (2014), a national representative survey, reports that 1.6 million mobile devices were stolen in 2012 and 3.1 million in 2013. Though device users can limit the vulnerabilities, research findings rather show that users represent the weakest link in security efforts (Crossler et al., 2013; Curry, 2011). To deal with this problem, there is the need to understand how users behave and the activities they engage in while using the devices and the extent of their familiarity and knowledge of device settings and disaster recovery processes. In doing so, attention should be focused on the category of users based on users' characteristics (area of study, maturity, and gender). In this way, an appropriate and targeted training and awareness programs can be developed to inform or educate users to bring about changes in attitudes and usage behavior (Imgraben et al., 2014).

Therefore, the purpose of this quantitative survey research is to investigate the influence of students' characteristics (majors, age, course-level, and gender) on mobile device security practices. Jones and Heinrichs (2012) classified mobile device security practices into three approaches, namely user-behavior and activities, use of device settings, and disaster preparedness. User-behavior and activities entail that users avoid harmful behaviors and activities as they use applications on their devices; device settings requires that users protect the devices through security setting features on the devices such as enabling and disabling applications, and installing add-on utilities and patches; and disaster recovery requires that users are prepared to recover their devices and the data they contain from disaster such as theft/lost, in case it occurs.

LITERATURE REVIEW

This section presents key mobile device security controls and reviews literature on three generally recommended approaches (Jones & Heinrichs, 2012) to securing the mobile devices.