International Journal of Information Management 35 (2015) 561–571

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt

# On the efficacy of smartphone security: A critical analysis of modifications in business students' practices over time

Beth H. Jones [a,*], Amita Goyal Chin [b]

[a] College of Business, Department of Accounting, Finance, Information Systems and Business Law, Western Carolina University, Cullowhee, NC 28723, United States

[b] Department of Information Systems, School of Business, Virginia Commonwealth University, PO Box 844000, Richmond, VA 23284-4000, United States

ARTICLE INFO

*Article history:*
Received 5 March 2015
Received in revised form 18 June 2015
Accepted 18 June 2015

*Keywords:*
Smartphone security
Business students
Mobile devices
Cell phones
Gender

ABSTRACT

Perhaps no prior technology has more expediently and more ubiquitously usurped the landscape than mobile technology. Smartphones are used for social interactions, financial transactions, to increase employee productivity, and in academic pursuits. Smartphones have established omnipresence on college campuses, where students are using them for all aspects of their daily life. With such significant usage, concerns for the security of data and personal information become paramount. This study employs a survey instrument to assess undergraduate student use of smartphone security practices in 2014, and compares this behavior to results from the same survey instrument when administered in 2011. Results indicate a worrisome trend, for while more students have smartphones and a higher percentage use them for financial purposes, risky behavior continues and, in several cases, has worsened. When good security practices are not followed, their efficacy is diminished and users are left more vulnerable than ever.



## 1. Introduction

Perhaps no prior technology has more expediently and more ubiquitously usurped the landscape than mobile technology. Mobile technology includes phones, tablets, personal digital assistants (PDAs), gaming consoles, and e-readers (Harris & Patten, 2014). At 7.22 billion, the number of mobile devices exceeds the number of people in the world, which is approximately 7.19 billion (Boren, 2014). According to the Pew Research Center, as of January 2014, 90% of adults in the US have a cell phone, 58% of which are smartphones (Pew Internet, 2014). From 2004 through 2015, the growth rate of mobile phone ownership has consistently exceeded the combined growth rate of desktop and laptop computer ownership (Pew Internet, 2014). It is expected that by 2020, "90 percent of the world's population over six years old will have a mobile phone (Fried, 2014)."

Feature phones, smartphones, and tablets have become dominant devices for business, academic, and social exchanges. The retronym feature phone, or dumb phone, refers to a genre of mobile phones that were relatively simple in their functionality. Typically, these phones allowed users to make traditional phone calls, exchange text messages, and exercise some rudimentary multimedia functions, and had limited or no internet connectivity. The most advanced of these phones evolved to include higher speed processors, significant on-board storage, and wireless network capabilities to both local WiFi and high-speed cellular networks. These smartphones, which are essentially standalone computing devices with sophisticated operating systems, akin to desktop computers, are designed to be constantly connected, and possess the ability to run applications (Dadwal, 2014), commonly referred to as "apps." These applications have gradually increased in complexity and sophistication. Additional essential functionalities of smartphones include, but are not limited to, ready access to email, internet browsing, touch-screen interactivity, and high end camera and video capabilities. The inclusion of a location sensor (i.e., GPS), motion sensor, and environmental sensors (e.g., for temperature) has also become commonplace (Mylonas, Kastania, & Gritzalis, 2013a; Mylonas, Meletiadis, Mitrou, & Gritzalis, 2013b).

Though still in its infancy, mobile technology has been pervasive and has rapidly become a dominant medium for consumers for conducting business, for education, and for social interaction. It has drastically impacted when and how we work and play, as well as how we behave and interact with others. For example, mobile devices provide easy access to retailers' websites, facilitating online purchasing from any location at any time of day. On Black Friday 2014, 29% of the online purchases were made from mobile devices (Adobe Reports, 2014). And, evidence from industry suggests this

* Corresponding author. Tel.: +1 828 227 3465; fax: +1 828 227 7584.
*E-mail addresses:* bjones@email.wcu.edu (B.H. Jones), agchin@vcu.edu (A.G. Chin).

http://dx.doi.org/10.1016/j.ijinfomgt.2015.06.003
0268-4012/

increased reliance on mobile devices for online shopping is going to continue to grow (Holmes, Byrne, & Rowley, 2014).

While the omnipresence of mobile technology has afforded invaluable convenience to consumers, thereby improving human and organizational performance, it has raised significant cause for concern for consumer safety (Zonouoz, Houmansadr, Berthier, Borisov, & Sanders, 2013; Zhao, Zhang, Ge, & Yuan, 2012; van Cleeff, 2008; Wang, Streff, & Sonell, 2012). This is because, as with desktop computers and laptops, mobile devices are susceptible to multifarious forms of malicious IT infringements. However, data-centric security for mobile devices has largely been limited (van Cleeff, 2008) and no governmental regulations or other compulsory measures have been instituted that compel users to proactively implement security measures. In fact, smartphone safety and security has largely been neglected altogether (Gupta, Kumar, & Loothra, 2014). While organizations may require that specific security procedures be followed when using company computers and/or accessing company data, they lose control when company-confidential information is accessed and stored on personal mobile phones, which are commonly used for this purpose (Leavitt, 2013), also known as the BYOD (bring your own device) phenomenon.

Since the first mobile phone viruses emerged in 2004, smartphone users have reported significant malware attacks (Wang et al., 2012; Ingerman & Yang, 2011; Felt, Finifter, Chin, Hanna, & Wagner, 2011), and yet, most users are unaware of preventive measures (Paullet & Pinchot, 2014). Malware compromises can occur in the form of viruses, worms, Trojan horses (Gohring, 2006), and spyware. A compromised feature phone could divulge a limited quantity of personal data; however, an infiltrated smartphone has the potential for far-reaching havoc, for the perpetrator could potentially gain access to apps, personal information for all of the owner's contacts, banking information and passwords, email, texts, photos, video, etc. In addition to personal, financial, and professional losses, including those that could lead to impersonation and identity theft (van Cleeff, 2008; Arthur & Boggan, 2011), such malware attacks can have devastating repercussions for organizations (Liang & Xue, 2010), especially if the smartphone was used as a BYOD.

The purpose of this study is to continue our examination of the efficacy of smartphone security behaviors of undergraduate college students. College students were chosen because they represent a segment of the population that is generally zealous adopters of mobile technology. They use their phones to access academic resources such as Blackboard and online coursework, particularly since curriculums of higher education are increasingly incorporating new methods of teaching and learning that are based on mobile access (Minaie, Sanati-Mehrizy, Sanati-Mehrizy, & Sanati-Mehrizy, 2011). Many institutions also offer undergraduate and graduate level courses on mobile computing and even offer it as an area of research concentration for graduate students (Minaie et al., 2011). Students also use mobile technology to interact socially through email, text and social media sites, including Facebook and Instagram, and for personal activities including banking and other financial transactions. Therefore, it has become vitally important to "protect their information and systems from possible security attacks" (Kim, 2014).

## 2. Background

The extant literature on the security practices of college students signals that students are remiss in their behavior (Kim, 2014). Given the plethora of applications readily available at low- or no-cost from the internet, users routinely download unknown software onto their mobile devices, creating potential security breaches for malware and other infractions (Mylonas et al., 2013a, 2013b; Zonouoz et al., 2013; Jones, Chin, & Aiken, 2014; Zhao et al., 2012). Lee, Kim, Cho, Choi, and Park (2014) analyzed the security concerns of the Android OS and Guo, Wang, and Zhu (2004) examined the types of attacks that can be used to compromise smartphones. In addition to unsafe downloads, college students are particularly prone to leaving their cell phone on a desk in their classroom or at a seat during a social congregation. Theft of mobile devices is common, where "more than 40 percent of all robberies now involve cell phones (Theft of cell phones rise rapidly nationwide, 2012)." It has become "the fastest growing undetectable crime (Gupta et al., 2014)." Apart from the financial distress of losing a smartphone, the loss of contact information, passwords, calendars, and other data can cause particular setbacks in the daily lives of the device owners (Gupta et al., 2014). Another opportunity for a security infraction is that, as part of their social interaction, students often use Facebook Places, Foursquare, etc. to check-in, disclosing their current physical location and past movements. This information can be aggregated and mined and used maliciously to obtain personal information and knowledge about habits, making the device owner a prime target for robbery (Kaplan, 2012).

To more accurately gauge the smartphone security practices of college students and to determine the potency of these practices, several researchers have employed survey instruments and analyzed the collected data (Terzis & Economides, 2011; Padilla-Meléndez, Aguila-Obra, & Garrido-Moreno, 2013). Mylonas et al. (2013a, 2013b) conducted a survey to assess security awareness of smartphone users who download applications from the various application repositories such as Google Play, Apple's App Store, etc. and found that users exhibit a blind trust in such repositories and do not necessarily exercise caution when selecting, downloading, and installing applications. Mensch and Wilkie (2011) compared security practices of college students and reported a "troubling disconnect" among information security attitudes, behaviors, and tool usage. Kim (2014) implemented a survey instrument to gauge the security awareness of college students and concluded that additional security awareness training is needed. Harris, Furnell, and Patten (2015) surveyed college students who are nearing graduation and are about to enter the workforce as well as current IT professionals and determined that significant weaknesses exist in security practices, further establishing a need for security awareness and training programs. Patten and Harris (2013) proposed integrating mobile security education into the IT curriculum to help educate current students who will become future IT professionals. The previous research literature is consistent in that while students practice a rudimentary level of mobile security, this level is sorely ineffective against diabolical intentions.

The present study is a continuation of the work in Jones and Heinrichs (2012) and in Jones et al. (2014). In the former work, survey results collected from two hundred five undergraduate business students at a regional public university were analyzed. The study found that students were lax in their mobile security practices, with men more willing to engage in some of the risky behaviors then women. The present study extends previous work and contributes to the research literature in two important ways: first, this study presents an updated evaluation of the current security practices of undergraduate business students; second, we compare current results with those obtained in earlier studies and provide a comparative analysis of student behavior regarding smartphone security practices. This is an extremely important contribution because, while previous studies clearly show that students are lax in their security practices, these have been snapshots of behavior at one point in time. Our study uses the same survey in 2014 that was used in 2011 (Jones & Heinrichs, 2012), at the same university, therefore, we are afforded an opportunity to examine behavioral trends.