Smart Phone Security Practices: 
Item Analysis of Mobile Security Behaviors of College Students

Scott Mensch, Indiana University of Pennsylvania, USA
LeAnn Wilkie, Indiana University of Pennsylvania, USA

ABSTRACT

Hand-held cell phone technology has been around for quite some time, however when Apple introduced the iPhone in 2007, the widespread adoption of smartphones took off. Smartphones allow users to communicate via talk, text and video; access personal and work e-mail and the Internet; run applications; make purchases; manage bank accounts; take pictures - and for many of us are an integral part of our everyday (The Privacy Rights Clearinghouse, 2018). Smartphones are “essentially tiny computers, we reach for these devices when we first wake up, bring them with us into the car, and often keep them with us during our most private moments (The Privacy Rights Clearinghouse, 2018). Many users rarely turn off their smart phones.

KEYWORDS

Hackers, Mobile Device, Security, Smartphone

INTRODUCTION

Hand-held cell phone technology has been around for some time (The Washington Post, 2014); when Apple introduced the iPhone in 2007, the widespread adoption of smartphones began. Smartphones allow communication via talk, text and video; access of personal/work e-mail and the Internet; run applications; make purchases; manage bank accounts; take pictures - and for many of us - are an integral part of our everyday (The Privacy Rights Clearinghouse). Smartphones are “essentially tiny computers…” Users rarely turn off their smart phones and while they have lots of useful tools, most users don’t realize the large amount of personal data they contain and stored. This article represents in an in-depth analysis of specific security behaviors based on mobile security scores derived from an exploratory study.

LITERATURE REVIEW

Studies show that U.S. smart phone usage has increased dramatically in the past half-decade; the volume of cellular data related to Internet searches and e-commerce has also increased. Smith (2015)
found that 64% of American adults owned a smartphone, and smart phone usage is expected to increase by 38 million users in 2018. Also, 87% of Americans ages 30-50+ and 91% of 18-28-year-olds check email via their cell phone (Smith, 2015). The reliance on cell phones and the necessity to feel continually linked are evidence, as 46% of users say they can’t live without their smart phone (Anderson, 2015); “…their mobile phone is the first and last thing they look at each day;” 84% keep their mobile phone next to their bed or in the same room while they sleep (Statistic Brain Research Institute, 2017). Generations Y and Z (born 1997 to present) want instant gratification and have “…less patience for delay of any kind” (Tapscott, 1998, p. 109; Tari, 2011).

Perceptions about mobile device security from both physical and digital security breaches seems to have lagged per Pew Research Center’s study, finding that 28% of all smart phone owners took no measures to secure their devices (Anderson & Olmstead, 2017); see Table 1 for additional findings about users and smart phone security.

The Prevalence of Mobile Computing and Smartphones

Mobile computing usage allows communication and computing without restriction to physical location. There are security vulnerabilities related to mobile computing including transmission of data over wireless networks, and storage of information and data on mobile devices (Alotaibi, Mustafa & Hoque, 2016). Wireless networks are susceptible to eavesdropping, spoofing, message interception and other issues, a particular concern for college students, as 82% connect to the Internet wirelessly through cell phones, laptops or other Internet-connected devices (Zichur, 2010).

Security threats to mobile devices are growing; apps classified as malware grew from 7 million in 2013 to 1 million in 2014, and 17% of all Android apps are malware (Symantec, 2015, p. 11), and the number of new malware variants increased by 54% from 2016-2017. Grayware apps (non-malicious, annoying or inadvertently harmful apps) are an increasing threat, growing to 2.3 million in 2014 and increasing by another 20% from 2016-2017 (Symantec, 2017); 63% of these apps “…leak the device’s phone number” and another 37% leak the device’s location (p. 6, 10). Approximately 24,000 malicious apps are blocked each day in 2017 (Symantec, 2017, p. 6). Mobile ransomware was first discovered in 2014 (Symantec, 2015) and is among the top two most significant threats to organizations in 2017 (Neely, 2017). Ransomware locks users and forces them to pay money or bitcoin to unlock the device (Harman, 2015), and a watering hole employers an exploit kit to infect only users from a pre-selected IP range to get users to visit a compromised website (Symantec, 2017).

According to Jones, Chin, & Aiken (2014), a 2011 Carnegie Mellon University/McAfee study found that, while 95% of companies have a mobile device policy in place, less than one third of employees were aware of the policy, and less than half of companies say that employees understand mobile device access/permissions. Users aren’t keeping mobile devices updated; “…only 20 percent of devices are running the newest major version and only 2.3 percent are on the latest minor release” (Symantec, 2017, p. 6).

Table 1. How Smart Phone users secure their phones (Anderson & Olmstead, 2017)

<table>
<thead>
<tr>
<th>How Smart Phone Users Secure Their Phones</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set a screen lock with a PIN</td>
<td>25%</td>
</tr>
<tr>
<td>Thumbprint Scanner</td>
<td>23%</td>
</tr>
<tr>
<td>Password</td>
<td>9%</td>
</tr>
<tr>
<td>Pattern Dots</td>
<td>9%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
</tr>
<tr>
<td>No Screen Lock</td>
<td>28%</td>
</tr>
</tbody>
</table>
The Language of Leaders: Identifying Emergent Leaders in Global Virtual Teams
[www.igi-global.com/chapter/language-leaders-identifying-emergent-leaders/25566?camid=4v1a](www.igi-global.com/chapter/language-leaders-identifying-emergent-leaders/25566?camid=4v1a)

The Influence of a Program Based on Hidden Curriculum on the Concept of Citizenship for Students in Al Majmaah University
[www.igi-global.com/article/the-influence-of-a-program-based-on-hidden-curriculum-on-the-concept-of-citizenship-for-students-in-al-majmaah-university/224013?camid=4v1a](www.igi-global.com/article/the-influence-of-a-program-based-on-hidden-curriculum-on-the-concept-of-citizenship-for-students-in-al-majmaah-university/224013?camid=4v1a)

Automatical Emotion Recognition Based on Daily Gait
[www.igi-global.com/chapter/automatical-emotion-recognition-based-on-daily-gait/211045?camid=4v1a](www.igi-global.com/chapter/automatical-emotion-recognition-based-on-daily-gait/211045?camid=4v1a)