International Journal of Mobile Human Computer Interaction
Volume 10 • Issue 1 • January-March 2018

Mobile Phone Usage Patterns, Security Concerns, and Security Practices of Digital Generation

Sonya Zhang, College of Business Administration, California State Polytechnic University, Pomona, CA, USA
Saree Costa, College of Business Administration, California State Polytechnic University, Pomona, CA, USA

ABSTRACT

As the digital generations have grown up with high-tech gadgets and become avid users of mobile phones and apps, they are also exposed to increasing mobile security threats and vulnerability. In this paper the authors discuss the impact of recent mobile technology advancements on mobile threat environment and mobile security practices. They also conducted a survey to 262 college students to examine their mobile phone usage patterns, security concerns and practices. The results show that students use their mobile phone frequently for various productivity and entertainment purposes. They are generally aware of and concerned about mobile security, not only on losing the phone physically but also on data theft, web threat, and mobile malware. Students also practice security to some extend - most change PIN and passwords regularly, download their apps mostly from official app stores, and generally keep their OS and apps up-to-date. The authors also found significant correlations between mobile security practices and personal attributes, including major, gender, and technology aptitude.

KEYWORDS

Digital Generation, Mobile Phone, Mobile Security, Mobile Usage, Security Awareness, Security Concern, Security Practice

1. INTRODUCTION

With the ease of connectivity, always-on accessibility of online content and services, the explosion in the number and variety of apps, mobile phones today offer many advantages not only in communication but also in increased productivity, entertainment, and ubiquitous availability of personal and business data. The number of mobile phone users in the world is forecast to reach 4.77 billion by 2017, and pass the five billion mark (65% of world population) by 2019. Also by 2019 over 80% of the mobile phone users will be smartphone users (Statista, 2016a). 92% of people aged 18-34 years in the United States owned a smartphone in 2015. During June 2016, users aged 25 to 34 years accessed mobile apps via smartphone for an average of 85.6 hours, or 2.85 hours per day (Statista, 2016b).

As mobile phones usage continues to grow exponentially, security threats, attacks and vulnerability targeting mobile phones have also skyrocketed. In 2014, more than 3 million Americans lost their smartphones, another 2 million had their smartphones stolen, many of which weren't sufficiently protected with as much as a simple passcode to keep the phone's data safe according to Consumer Reports National Research Center. In 2015 Q3 and Q4, McAfee Labs (McAfee, 2015) detected

DOI: 10.4018/IJMHCI.2018010102

37 million malware in app stores, including increase in not only new malware (72% increase from Q3), but also the sophistication and complexity of mobile malware. Ransomware, bank fraud and remote access tools (RATs) all have an increased presence on mobile devices. Mobile devices run rapidly evolving and heterogeneous operating systems of which the security is yet to be rigorously established. In addition, the proliferation of mobile apps, easily downloaded and installed by mobile phone users at low price, opens the platform up to malware. Key vulnerabilities of mobile devices also include frequent loss and theft, misuse by employees, and unwillingness by management to take the appropriate policy and enforcement steps to ensure mobile security governance is enforced (Couture, 2010). McAfee Labs (2015) predicted that in 2016 as applications and prominent operating systems are hardened from attacks, those attackers shift their focus to less prominent but critical surfaces, innovative styles, and new device types. As enterprises strengthens their complex security defenses and comprehensive policies, attackers would target the weak security of employees working remotely, as well as develop more sophisticated attacks through firmware, espionage malware, and detection evasion.

2. MOBILE THREAT ENVIRONMENT

Mobile threat can come from multiple sources. Couture (2010) broadly classified mobile threats into three categories: 1) threats resulting from the physical nature of small and highly portable mobile devices, 2) threats stemming from their ubiquitous connectivity and 3) threats originating with the prevalence of mobile software applications and malware.

2.1. Physical Loss or Theft

Physical loss or theft of the mobile device can result in not only the loss of personal information but also copies of corporate data stored in email retrieved via mobile apps. As many of the lost phones will be found by individuals who have no interest in compromising the data within, it will be a good practice to include a contact telephone number or address labeled on the device, but not give away the personal identifiable information or the organization name. Assuming a subset of those who find lost devices are at least somewhat interested in the data, screen login pins and max-attempt lock out policies will become useful. A smaller subset of thieves may have the skills and motivation to attack the device with specialized software or techniques, sometimes even bypassing the screen lock. This reinforces the important need to encrypt valuable phone data, as well as to enable remote erase of phone data, either automatically after a certain amount of failed login attempts or when the lost phone becomes unlikely to be retrieved.

The physical Subscriber Identity Module (SIM) card inside the mobile phone used to connect to network may hold subscriber data, contact list and SMS messages and should be considered in mobile security policy. Devices should be managed such that data on these SIM cards are either encrypted or non-essential.

2.2. Mobile Network Security

Wi-Fi security threats are well-known and multiple vulnerabilities have been published, including severe weakness in WEP protocol encryption and man in the middle (MITM) attacks. Should a WEP network password be cracked, or should a mobile phone connect to an open WI-FI hotspot, the entire range of threats typically aimed at mobile devices become relevant.

Unlocking or “jailbreaking” of iPhones is also known to open security vulnerabilities. Users intend to gain more control over their devices hack their own devices in the process, permitting them to apply patches that disable manufacturer and network operator controls. As such, many of these jailbreaks open up root-level login accounts with default passwords and the phone begins broadcasting the availability of a remote SSH login service, which makes a successful malware installation far more likely and gives any malware root access to perform any manner of trouble.