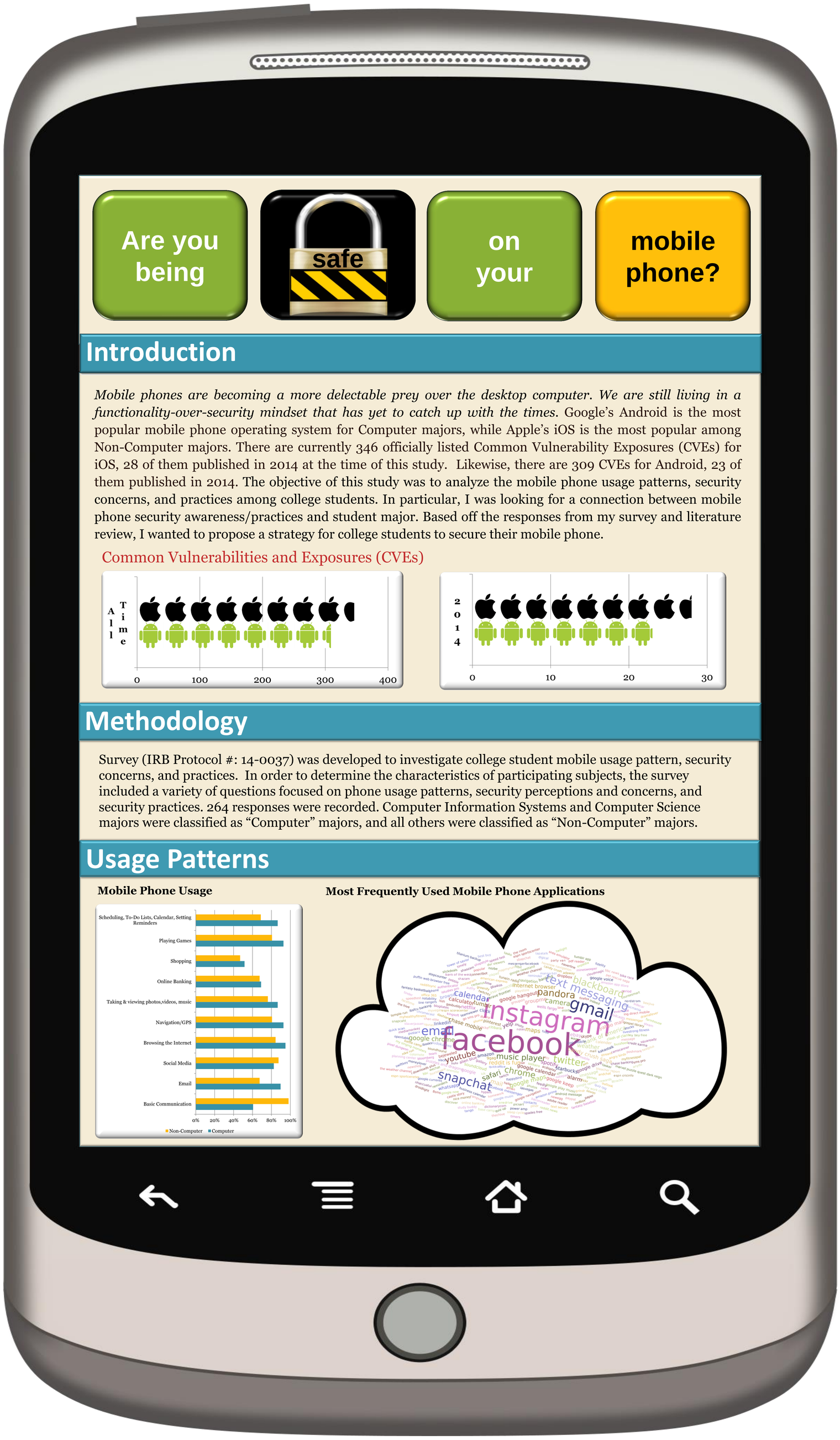
Mobile Phone Security Practices, Usage Patterns, and Recommendations for College Students

Saree Costa, Computer Information Systems

Mentor: Dr. Sonya Zhang

Kellogg Honors College Capstone Project



Introduction

Mobile phones are becoming a more delectable prey over the desktop computer. We are still living in a functionality-over-security mindset that has yet to catch up with the times. Google's Android is the most popular mobile phone operating system for Computer majors, while Apple's iOS is the most popular among Non-Computer majors. There are currently 346 officially listed Common Vulnerability Exposures (CVEs) for iOS, 28 of them published in 2014 at the time of this study. Likewise, there are 309 CVEs for Android, 23 of them published in 2014. The objective of this study was to analyze the mobile phone usage patterns, security concerns, and practices among college students. In particular, I was looking for a connection between mobile phone security awareness/practices and student major. Based off the responses from my survey and literature review, I wanted to propose a strategy for college students to secure their mobile phone.

Common Vulnerabilities and Exposures (CVEs)

Methodology

Survey (IRB Protocol #: 14-0037) was developed to investigate college student mobile usage pattern, security concerns, and practices. In order to determine the characteristics of participating subjects, the survey included a variety of questions focused on phone usage patterns, security perceptions and concerns, and security practices. 264 responses were recorded. Computer Information Systems and Computer Science majors were classified as "Computer" majors, and all others were classified as "Non-Computer" majors.

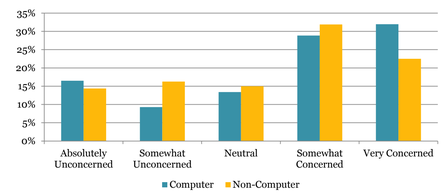
Usage Patterns

Mobile Phone Usage

Most Frequently Used Mobile Phone Applications

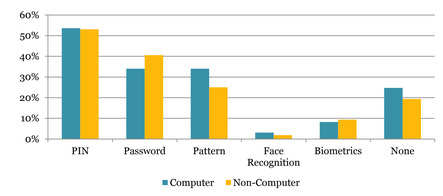
Security Practices

Concern with Security of Mobile Phone

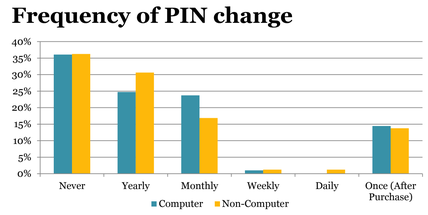


Most of the students expressed they were concerned about the security of their mobile phone. Further analysis indicated students were the most concerned with losing their phone, data theft, and losing contact information. Students mostly used PIN, Password and Pattern features to unlock their phone. About 20% have used no form of access protection.

Phone Unlock Features Used



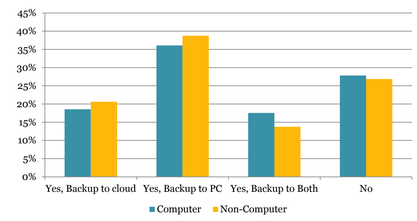
Frequency of PIN change



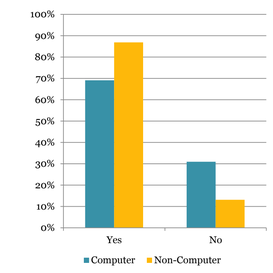
The majority of students indicated that they have never changed their password/PIN. Over 25% of students reported they did not backup their data, even though data loss was one of their top 3 concerns. Over 60% of students indicated that they connected to public Wi-Fi networks. Most students did not have remote wipe enabled, nor did they enable encryption on their mobile phone.

Overall, both Computer and Non-Computer majors shared similar patterns and security practices

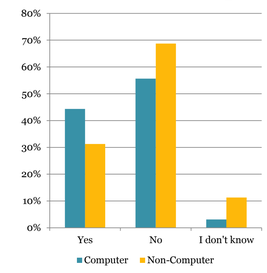
Data Backup



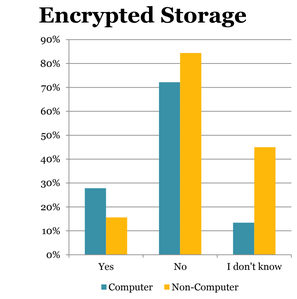
Connect to Public Wi-FI



Enabled Remote Wipe



Encrypted Storage



Recommendations

Protect access to your mobile phone
- Be aware of your surroundings and maintain physical control of your mobile phone
- Add a password, PIN, or pattern that's hard for others to guess
- Don't share your password with anyone, and change it regularly

Protect your data
- Regularly backup important data to your computer and/or 3rd party cloud service
- Enable full disk encryption

Keep an eye on Wi-Fi
- Connect only to secure networks
- Be sure you aren't automatically connected to insecure, public networks.

Update your OS and apps
- Update as soon as new patches become available
- Enable firewalls and security software

Be wary of the apps you download
- Download from trusted sources, research before you download
- Look at the permissions each app is requesting. Does it perform *only the functions you approve of*?

Prepare for the worst
- Insure your device
- Perform Factory Reset when disposing your phone
- Enable trusted anti-theft protection apps, and remote wipe in case your device gets stolen
  http://www.ctia.org/your-wireless-life/consumer-tips/how-to-deter-smartphone-thefts-and-protect-your-data

Stay informed
- Learn more about mobile phone security options available
- Check what CVEs are listed for your particular mobile phone's OS:
  http://web.nvd.nist.gov/
- FCC Smartphone Security Checker
  http://www.fcc.gov/smartphone-security

References

1. Enrollment by Level and Gender, Fall 2001 through Fall 2013. California State Polytechnic University, Pomona. Institutional Research & Academic Resources. Nov 12, 2013.
2. Kurkovsky, Stan. "Digital Natives and Mobile Phones: A Survey of Practices and Attitudes about Privacy and Security" 2010 IEEE International Symposium on Technology and Society. 2010.
3. Mannino, Jack. "The OWASP Mobile Top 10 Reboot." 2014.
4. "McAfee Labs 2014 Threats Predictions." McAfee. 2013.
5. National Vulnerability Database - Advanced Search. NIST, U.S. Department of Commerce. Retrieved May 2014, from http://web.nvd.nist.gov/view/vuln/search-advanced.
6. "Safely Disposing of Your Mobile Device." Ouch! Monthly Security Awareness Newsletter for Computer Users. The SANS Institute. May 2012.

CAL POLY POMONA

KELLOGG HONORS COLLEGE — Cal Poly Pomona — A community of scholars

Contact: costa@csupomona.edu

Scan above for full study

http://www.csupomona.edu/~costa/mobile-security.html