https://doi.org/10.48009/2_iis_2013_329-335
Issues in Information Systems
Volume 14, Issue 2, pp.329-335, 2013

TOOLS AND TIPS FOR TEACHING SMARTPHONE SECURITY

Lynn R. Heinrichs, Elon University, lheinrichs@elon.edu
Beth H. Jones, Western Carolina University, bjones@email.wcu.edu

ABSTRACT

The growth of smartphone ownership has been no less than explosive, but so has the growth in mobile security threats. Organizations that embrace BYOD (bring your own device) policies place their information assets at risk if employees cannot or do not manage the security of their personal devices. Today's students are tomorrow's employees who will likely have access to sensitive data using their smartphones or other mobile devices. How can IS educators prepare their students to be responsible information stewards? In this paper, the authors share three teaching tools and tips for increasing student awareness of smartphone security: an interactive presentation, a discussion survey, and a video/poster project.

Keywords: Information Security, Smartphones, Mobile Devices, Education and Awareness

INTRODUCTION

The growth in smartphone device adoption has been astounding. According to research firm Flurry Analytics, the rate of iOS and Android device adoption is 10 times faster than the 1980s PC, twice as fast as the 1990s Internet boom, and three times faster than social media adoption [14]. And while these devices are invaluable for a wide-range of activities such as banking, getting directions, checking weather, and entertainment [15], they are also the target of unprecedented security attacks such as malware, phishing, spyware, and theft to name a few.

Unsecured mobile devices put both organizations and individuals at risk. A joint study by McAfee and Carnegie Mellon [10] of more than1500 respondents in 14 countries noted the following:

- Ninety-five percent of companies have mobile device policies in place.
- Less than one in three employees are aware of the policy.
- Fewer than half of companies reported that employees understand their mobile device access/permissions.

Furthermore, the McAfee/Carnegie Mellon study also revealed that, unless mobile devices are issued by large organizations with security policies in place, employees tend to use their own personal phones for work-related tasks placing a greater burden on individuals to practice information stewardship.

According to Howard Schmidt, former cyber-security coordinator of the Obama Administration, educating individuals is the key to keeping systems safe from attacks. "Business schools today need to be teaching this to the future CEOs [17]." Their ability to use smartphone technology in a secure manner determines the degree to which they put themselves and their organizations at risk.

Today's students are tomorrow's employees. Are they prepared for the responsibilities of protecting an organization's information assets? Information systems educators can help prepare students for their future security responsibilities. This paper describes three tools that the authors have used for increasing student awareness of smartphone security threats and prevention practices: an interactive slide presentation, a discussion survey, and a video/poster project. By sharing these ideas, the authors hope to encourage other faculty members to also include smartphone security instruction in their curricula.

SMARTPHONE THREATS AND SECURITY PRACTICES

Over the last few years, mobile device security has emerged as a top concern of those involved with protecting information assets. For example, in 2011, the American Institute of Certified Public Accountants [1] identified "the

control and use of mobile devices" as the top technology on its initiative list followed by "information security." The list includes "technologies that IT decision makers should be aware of over the next 12 – 18 months." More recently, Richard Clarke, former cyber-security chief for the White House, described smartphones as posing the "newest and largest vulnerability in corporate America now [12]."

Smartphone threats can arise from both legitimate day-to-day use such as map services, banking, and social media (see Figure 1) to well-publicized cyber-attacks perpetrated through malware ([6], [10]). Unintentional sharing of data in either case can put an individual at risk. And in a day of BYOD policies, an organization's information assets also may be at risk.

HOOVERING UP YOUR DATA: WHAT THE APPS CAN ACCESS

	Location data	Internet history	Text messages	Contact book	Online account IDs	Who you are calling	May intercept calls	Can access camera
Flickr	x		x	x		x		x
Flixster	x				x	x		
YouTube					x	x		x
Foursquare	x				x	x		
TweetDeck	x				x	x		
Netflix		x						
Facebook	x		x	x	x	x		
Ancestry.co.uk	x							x
Badoo	x		x	x		x		x
Angry Birds	x					x		
Yahoo! Messenger			x	x	x	x		
Shazam	x					x		
My Fitness Pal				x		x		x
My Remote Lock				x		x	x	

Figure 1. What Data Can Smartphone Apps Access? Source: Kelly [8]

There are many smartphone security practices available to protect users from hackers. Most simply require diligence and awareness. For those individuals motivated to learn the nuts and bolts of securing their personal devices, information on mobile device security practices is readily available online ([2], [3], [5]). One helpful and reliable list comes from the Internet Crime Complaint Center , a partnership between the Federal Bureau of Investigation (FBI) and National White Collar Crime Center (NWCCC), and includes the practices shown in Table1 [6]:

Table1. Recommended Smartphone Security Practices
(Source: Internet Crime Complaint Center)

• Turn off features that are not needed. • Use encryption (if available) to protect personal data. • Look at the reviews of the developer/company who published the application. • Review and understand the permissions you are giving when you download applications. • Use password protection. • Obtain malware protection. • Be aware of applications that enable Geo-location.	• Don't jailbreak. • Do not connect to unknown wireless networks. • Wipe the device (reset it to factory default) when selling or trading in. • Apply updates. • Avoid clicking on or otherwise downloading software or links from unknown sources. • Use the same precautions on your mobile phone as you would on your computer when using the Internet.

Even though today's generation of students is "born mobile [8]", there is no guarantee that they follow recommended security practices such as those published by the IC3. In fact, prior research on students and security justifies concern regarding their attentions to risk-mitigating practices. Teer, Kruck, and Kruck [16] examined the computer security practices of undergraduate students and concluded that "students are leaving their personal computers vulnerable to viruses. (p. 109)" Lomo-David and Shannon [9] surveyed students regarding the relationship between familiarity and usage of 10 security practices. In four areas, familiarity did not translate to usage: passwords on email attachments, biometric authentication, intrusion detection systems, and multifaceted authentication systems. The authors recommended that educational institutions disseminate more information to students on safe computing. Finally, Mensch and Wilkie [11] compared security practices of college students with respect to several factors including, but not limited to, gender, age, class, and identity theft victimization. They reported a "troubling disconnect" among information security attitudes, behaviors, and tool usage among college students.

Less research is available on students and mobile security than on PC security. However, there is some indication that students are not any more attentive to securing their smartphones than they historically have been to securing their PCs. The authors [7] surveyed business students about their smartphone security practices and examined differences by gender, age, class, and financial utilization. Students were found to be lax in their security with men more willing to engage in risky behaviors than women. There were no differences in behaviors based upon age, class, or use of smartphones for financial transactions.

TOOLS AND TECHNIQUES FOR TEACHNING SMARTPHONE SECURITY

Okenyi and Owens' [13] research shows training and awareness reduce risks to organizations and are essential to prevent hacking success rates at both the individual and organizational levels. Information systems educators can and should play a key role in security awareness and training. Security awareness efforts focus on keeping users mindful of information security practices; training goes a step further than awareness to include detailed information and hands-on instruction [18].

The authors are strong advocates for increasing student awareness of smartphone security practices. They have developed several instructional resources for use with undergraduate audiences including an interactive slide presentation, a discussion survey, and a video/poster project based upon the EDUCAUSE Information Security Awareness contest. Each of these "classroom tested" ideas is described below.

Interactive Slide Presentation

The 27-slide presentation entitled, "Smartphone Security: How Safe Are You?" is an introduction to smartphone security basics. To stimulate student interest, the presentation begins with the question, "If a hacker got into your phone, what would you NOT want him/her to see and/or copy?" The next slide lists what a hacker might see and in some cases even alter: calendars, address books, contact lists, photos, music files, text messages (old, new, even deleted ones), phone call details, and web browsing details and history. In addition, all subsequent phone calls/texts could be recorded and forwarded to a third party! The next slides briefly describe other types of possible mischief, such as hackers using your phone to call expensive international or 900-numbers, possible dangers of financial transactions, and distributed denial of service (DDOS) attacks. The next slide describes the easy ways malicious software can be introduced to a smartphone.

At this point, the slide presentation focuses on prevention and becomes more interactive. Slides are in pairs, with the first of the pair showing one to three recommended practices along with previously obtained survey results. These results are from a security practices survey conducted by the authors in 2011 [7]. Results show that good security measures were not being followed by all, or in many cases, even a majority of students. The second slide of the pair asks students to give reasons why people might choose not to follow a particular practice.

Figures 2a and 2b present one such pair. Figure 2a shows the results of two questions from the security practices survey for students to consider. Figure 2b poses a thought question. As students share their opinions, the instructor lists their responses on the PowerPoint slide. For example, the main reason given for not using a password was, not

surprisingly, simply the inconvenience of having to enter it each time the phone was used. Also, not being able to just hand your phone to a friend without having to give them the password (again, inconvenience). The entire slide show can be found here: http://paws.wcu.edu/bjones/SmartphoneSecurity.pptx.

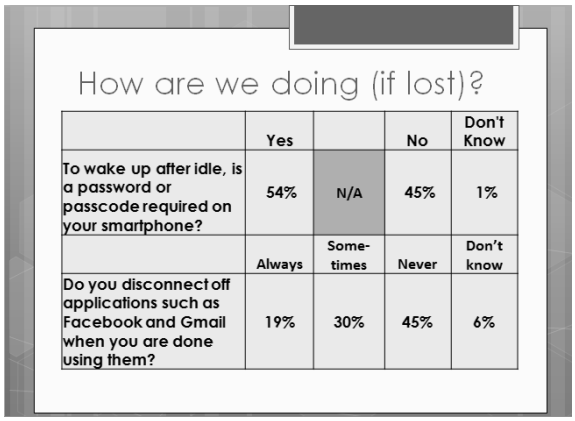

Figure 2a: Survey Results to Consider

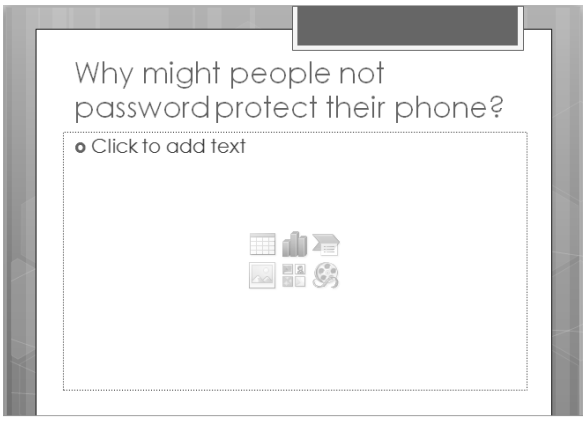

Figure 2b: Thought Question

The interactive slide presentation works best with classes in which students easily can engage in discussions. Faculty who teach first-year seminars in which personal/campus safety is a topic might find it useful. For larger or more mature groups of students, the next technique of using a discussion survey might be a better option.

Discussion Survey

Polling is a great technique for sharing information and engaging students in discussion. The beauty of polling is that it even works with large class sizes. A number of technologies are available for implementing surveys or polling activities:

- Course management systems such Blackboard or Moodle.
- Web-based survey tools.
- Clickers.
- Cell phones aided by a polling service (e.g., http://www.polleverywhere.com/).

To implement a smartphone security poll, the authors adapted a former research survey instrument. The questionnaire contains 30 items about students' perceptions of smartphone security (Table 2a) and their self-reported practices (Table 2b). The authors ask students to complete the survey anonymously first; then results are aggregated and discussed. Because results are aggregated and anonymous, the survey technique generates interesting discussion. To date, the authors have used course management software and Google forms to implement the classroom polling survey. Both have the ability to review aggregate survey results using charts.

Table 2a. Smartphone Security Survey – Sample Items Part I

Part 1. Respond True or False to the following statements.	
	1. One in five smartphone users has experienced some type of security threat with their device.
	2. Mobile device security is now one of the top concerns for information security professionals.
	3. Mobile device security is now one of the top concerns for *individuals* who own smart phones.
	4. Malware (such as viruses and worms) can totally break your phone – to the point where you can never use it again.
	5. It is possible for malware to be placed on a cell phone without the owner's knowledge.
	6. Malware can forward everything stored on a smartphone (contact list, notepad, calendar, texts etc.) to nearby users via Blue Tooth
	7. Someone can set up a fake Wi-Fi "gateway" to which the latest generation of mobile phones will automatically connect. Once a connection is established, all the information passing through can be stolen.
	8. Malware can be installed on a smart phone by clicking on links in emails or texts.
	9. Malware exists that, once placed on a smartphone, can forward to another phone a copy of all text messages received and sent
	10. Your phone can get infected by malware that automatically calls premium-rate telephone numbers (900 numbers such as adult chat lines and tech support), giving you quite a surprise when the bill comes in

Table 2b. Smartphone Security Survey – Sample Items Part II

23. Have you installed or enabled remote wipe software on your smartphone?	a Yes	b No	c Don't know
24. Have you installed or enabled remote lock software on your smartphone?	a Yes	b No	c Don't know
25. Have you installed or enabled your phone's locator feature? (Tracks phone's whereabouts if it's lost or stolen.)	a Yes	b No	c Don't know
26. Have you installed anti-virus software on your smartphone?	a Yes	b No	c Don't know
27. If you ever disposed of a smartphone, did you (or someone else) first remove the memory card and wipe all personal data (texts, contacts, etc.?)	a Yes	b No	c Don't know
28. To wake up after idle, is a password or passcode required on your smartphone?	a Yes	b No	c Don't know
29. Do you store confidential financial info such as credit card numbers and pin numbers in your phone (e.g. bank account pin numbers typed in as contacts so you can look them up)?	a Yes	b No	c Don't know
30. Have you set the idle timeout (so that the screen goes dark) to a shorter time than the factory default?	a Yes	b No	c Don't know

Video/Poster Project

For instructors who are looking for a more creative option that works well in a group context another option is to develop an assignment based upon the EDUCAUSE Information Security Video and Poster Awareness Contest [4]. The contest solicits posters and videos for raising student awareness of information security issues. Entries to the contest cannot receive direction from faculty members; however, designing a class project that incorporates the same guidelines for purely instructional use is an easy alternative.

One of the authors used the EDUCAUSE awareness poster project as part of an information security course requirement in Spring 2013. The project was completed in three phases: proposal, conceptual design, and final product with presentation. In the proposal phase, students worked individually to research information security topics and propose a poster idea. Students were grouped into five teams following review of the proposals. In the conceptual design phase, each team selected one proposal idea to implement and developed an initial poster concept. After receiving feedback on the conceptual design, students implemented an electronic version of their poster and presented it to the class. Although the final posters were not limited to only smartphone awareness issues, two of the five posters were related to mobile device security: password/passcode protection and jailbreaking.

The criteria for evaluating results can follow those of the actual contest, or be modified. Students can work individually or in teams to propose a message and medium, develop the idea, and generate a final product. An instructor has the option of using a panel of experts for reviewing completed submissions.

Limitations of Tools

One limitation of the interactive slide presentation and survey discussion tool is the problem of currency. The smartphone areas changes so rapidly that these tools can become outdated very quickly. This is less of a problem with the video/poster project where students develop their own messages about security. To help keep the discussion survey up-to-date, one of the authors asked for assistance from students in an upper-level information security course – so, even maintaining a survey can be a learning experience.

CONCLUSIONS

The growth of smartphone will continue to be accompanied by mobile security threats. Organizations that embrace BYOD (bring your own device) policies place their information assets at risk if employees cannot or do not manage the security of their personal devices. Today's students are tomorrow's employees who will likely have access to sensitive data using their smartphones or other mobile devices. Their awareness and use of information security practices is paramount.

The purpose of this paper was to share ideas on ways to raise smartphone security awareness. The authors see smartphone security as relevant preparation for today's workplace. Increasing student awareness of potential risks as well as appropriate security practices will help prepare them for their future roles as information stewards. The authors will share any of the resources they have created that are referenced in the paper and hope to generate discussion regarding others' classroom experiences.

REFERENCES

1. AICPA (2011). *Top Technology Initiatives*, American Institute of Certified Public Accountants, retrieved on January 4, 2012 from http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/TopTechnologyInitiatives/Pages/2010TopTenInitiatives-Complete.aspx.
2. Baker, P. (2011, February 9). "Top Ten Smartphone Security Tips", CIO Update, retrieved on May 11, 2010, from http://www.cioupdate.com/trends/article.php/3924241/Top-10-Smartphone-Security-Tips.htm.
3. Chickowski, E. (2009, February 26). "10 Best Practices for Mobile Security," *Baseline Magazine,* retrieved on May 11, 2010, from http://www.baselinemag.com/c/a/Mobile-and-Wireless/10-Best-Practices-for-Mobile-Device-Security/.

4. EDUCAUSE (2013). Information Security Awareness Video & Poster Contest. http://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-initiative/community-engagement/information-security-awareness-.
5. Erlanger, L. (2011, October 10). "Smartphone Security Best Practices," McAfee Blog Central, retrieved November, 04, 2011 from http://blogs.mcafee.com/enterprise/security-connected/smartphone-security-best-practices-2.
6. IC3 (2012, October 12). *Smartphone Users Should Be Aware of Malware Targeting Mobile Devices and Safety Measures to Help Avoid Compromise*, an Intelligence Note from the Internet Crime Complaint Center, retrieved on February 12, 2013 from: http://www.ic3.gov/media/2012/121012.aspx
7. Jones, B. and Heinrichs, L (Winter 2012). "Do Business Students Practice Smartphone Security?" *Journal of Computer Information Systems*, pp. 22-30.
8. Kelly, T (2012, February 27). "Free apps 'can spy on texts and calls': Smartphone users warned of privacy dangers," *Mail Online*, retrieved on 2/17/2013 from http://www.dailymail.co.uk/sciencetech/article-2106627/Internet-firms-access-texts-emails-pictures-spying-smartphone-apps.html
9. Lomo-David, E. and Shannon, L. (2009). "Information Systems Security and Safety Measures: The Dichotomy Between Students' Familiarity and Practice," *Academy of Information and Management Sciences Journal*, (12:1), pp. 29-47.
10. McAfee (2011, May 24). *Mobility and Security: Dazzling Opportunities, Profound Challenges*, a report commissioned by McAfee and produced by Carnegie Mellon University's CyLab, retrieved on February 12, 2013 from: http://www.mcafee.com/us/resources/reports/rp-cylab-mobile-security.pdf.
11. Mensch, S. and Wilkie, L. (2011). "Information Security Activities of College Students: An Exploratory Study," *Academy of Information and Management Sciences Journal*, (14:2), pp. 91-116.
12. Messmer, E.(2011, September 19). "Former Cybersecurity Czar Clarke Says Smartphones, Digital Certificates Create Huge Security Problems," *Network World*, September 19, 2011, retrieved on September 19, 2011 from http://www.networkworld.com/news/2011/091911-clarke-cybersecurity-251014.html.
13. Okenyi, P.O., & Owens, T.J. (2007). On the anatomy of human hacking. *Information Systems Security,* 16, 302–314.
14. Reisinger, D. (August 27, 2012). "Android, iOS growing 10 times faster than PCs did in the 1980s," CNET News, retrieved on 6/19/2013 from http://news.cnet.com/8301-1035_3-57500961-94/android-ios-growing-10-times-faster-than-pcs-did-in-the-1980s/.
15. Smith, A. (August 15, 2011). *Americans and Their Cell Phones.* A report from the Pew Internet and American Life Project, Retrieved 10 28 2011 from: http://www.pewinternet.org/Reports/2011/Cell-Phones.aspx?src=prc-headline.
16. Teer, F., Kruck, S., and Kruck, G. (Spring 2007). "Empirical Study of Students' Computer Security Practices/Perceptions," *Journal of Computer Information Systems*, pp. 105-110.
17. Thompson, C. (2013, January 31). "Businesses Facing Increasing Cyber Threats: Security Experts," CNBC Technology, Retrieved from: http://www.cnbc.com/id/100421313.
18. Whitman, M.E. and Mattord, H.J. (2012). Principles of Information Security, .Course Technology, Cengage Learning, Boston, MA.