Mobile security: Tips and tricks for securing your iPhone, Android and other mobile devices

Presented by
Michael Harris
[MS, CISSP, WAPT]
Systems Security Analyst
University of Missouri

Overview

- What data needs to be protected, what should we avoid storing on mobile devices.
- What habits, settings and applications can help make your mobile devices more secure.
- Settings for iPhones, Android and flash drives will be discussed.

Division of Information Technology

What information is to be protected

- Data classification
  - http://doit.missouri.edu/security/data-classification
  - DCL1—Public
  - DCL2—Sensitive
    - Business, financial and research data
  - DCL3—Restricted
    - 12 elements of FERPA
    - PCI
    - Red flag
    - GLBA
    - 18 elements of HIPAA
    - Other personally identifiable data
  - DCL4--National Security Interest (NSI)

Division of Information Technology

FERPA protected elements

- Course Roster
- Couse grades
- Courses taken
- Schedule
- Test scores
- Advising records
- Educational services received
- Disciplinary actions
- Student identification number
- Social Security number
- Student private email (with exceptions related to business processes)
- Some medical details (if paid by federal program)

Division of Information Technology

PCI & Red FLAG

- PCI
  - Full card number (unencrypted)
  - Card verification number
    - (3 or 4 digits back of card)
  - UM eCommerce Security Guide
  - http://doit.missouri.edu/security/inspection/eCommerceSecurityGuide.pdf
- Red Flag
  - Based upon Identity theft program
  - SSN
  - Credit score
  - Credit card details
  - Tax details
  - http://www.ftc.gov/bcp/edu/microsites/redflagsrule/faqs.shtm

Division of Information Technology

Graham Leach Bliley Act (GLBA)

- Employee financial account information
- Student financial account information (aid, grants, bills)
- Individual financial information
- Business partner and vendor financial account information

Division of Information Technology

HIPAA protected data elements

- Names
- All geographical details, including street address, city, county, precinct, zip code,
- All elements of dates (except year) and all ages over 89 (including year)
- Phone numbers
- Fax numbers
- Electronic mail addresses
- Social Security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images and
- Any other unique identifying number, characteristic, or code

Division of Information Technology

Why worry?

- Sophos survey
  - 22% had lost a phone or mobile device
  - 70% do not password protect phone
- Google intelligence survey
  - 40% of organizations are planning to deploy mobile phone data encryption
  - 33% are already protecting their mobile phones with encryption products and services

Division of Information Technology

Using mobile devices more securely

- iPhone
- Android
- Common across platforms
- USB flash drives & other stuff

Division of Information Technology

iPhone

- Enable auto lock
- Enable passcode lock
- Wireless
  - Use WPA and WPA2
  - Only use WEP as last resort
  - WEP better than nothing
  - Disable when not needed
  - Choose wisely what wireless you attach to
  - Don’t act as access point for others
  - Rogue GSM rare but possible
- Use VPN whenever possible
- Take care loaning to others (kids, others)
- Use native device usage restrictions
- Find My iPhone / Remote data wipe
- Docking phone may allow access in spite of encryption or Passlock

Android

- Set a screen lock password or pattern
- Turn on SIM card lock if available
- Take care docking or tethering devices
- Do not act as an access point (hotspot)
- Disable Bluetooth when not in use
- Take care downloading from Market
- Review application access for new apps
- Take care were you store backups of your phone
- Often androids tied to Gmail & Google accounts with stored password

Division of Information Technology

Common platform vulnerabilities

- Cautious browsing
- Not all browsers offer HTTPS(SSL) support
- Sun Java
- Flash Player
- FLV Player
- QR Code ➔
- Jail breaking
- Rogue Wi-Fi
- Rogue GSM
- Same social media abuses as on PC

http://doit.missouri.edu/security

Division of Information Technology

Flash drives and other USB stuff

- Limit where used to minimize risk
- Password protect when appropriate
- MacAfee encryption product for mobile devices soon
- Virus check flash drives when used somewhere new
- Attach to keychain or lanyard to avoid loss
- Label exterior of device with return address or phone number
- We are working on policy to mandate level 3 data be encrypted on mobile devices too.
- Report loss of flash drives containing UM information

- Other devices to protect? Cameras, MP3 players etc…

Division of Information Technology

Best practices

- Devices storing data must have ID and Password
  - (8 Character Upper-Lower-Number-Symbol etc.)
- Level 3 data should be protected with strong encryption
- User and other trusted individual should have encryption keys if not centrally managed
  - (IT Pro, Co-PI, boss… someone trusted to see the data)
- Keep devices patched and up to date
- Run antivirus and keep it up to date
- Take great care with mixing of personal and professional information
- Lost & stolen devices containing UM information must be reported
  - http://infosec.missouri.edu/hr/mandatory-reporting.html

Division of Information Technology

Common Helper apps

- Antivirus
- Antitheft
- Firewall
- Lost device locator
- Data scrub when lost

Division of Information Technology

Last Thoughts

- Set a non-trivial numeric device passcode
  - Not 123456, 111111 etc.
- Use passcodes consisting of additional character sets or greater lengths whenever possible.
- Set an inactivity timeout to automatically lock the device after ten minutes
- Use data storage encryption If possible especially for level 3 data.
- Automatic data wiping after ten failed passcode entry attempts.
- Enable the ability to remotely wipe data from lost/stolen devices
- Prohibit other users from modifying or disabling security safeguards

Division of Information Technology

Questions

References

- http://doit.missouri.edu/security/inspection/eCommerceSecurityGuide.pdf
- http://www.ftc.gov/bcp/edu/microsites/redflagsrule/faqs.shtm
- http://infosec.missouri.edu/hr/mandatory-reporting.html
- http://www.pcworld.com/businesscenter/article/152128/six_essential_apple_iphone_security_tips.html
- http://securityevaluators.com/content/case-studies/iphone/
- http://www.mulliner.org/ipahone/
- http://resources.infosecinstitute.com/android-tips-and-settings/
- http://informationsecurityhq.com/android-security/
- http://www.slideshare.net/ronaldotcom/the-current-state-of-mobile-security
- http://www.pcworld.com/businesscenter/article/152128/six_essential_apple_iphone_security_tips.html
- http://lifehacker.com/5738171/common-sense-security-for-your-iphone
- http://www.sandisk.com/media/226716/enisa-whitepaper.pdf

Division of Information Technology