Mobile Device Security Training

Austin Polley
Information Technology Assistance Center (iTAC)
Kansas State University
Why Focus on Mobile Device Security?

- Idea of being just a “phone”
- Smaller size
- Increased mobility
- Increased functionality
- Value
Where are we going?

- A look at common security concerns with mobile devices
- Tips to secure your devices and keep your data safe
- What to do when security is compromised
- Questions and open discussion
Security Concerns

- Physical Access
- Staying safe while using device
- What to do before/after you lose your phone
Physical Access

- Always keep track of your mobile device
  - Never leave it unattended for any amount of time
  - Don’t leave it in the care of others
- When storing your device, you can never be too safe
  - Store in locked cabinet or drawer in office
Physical Access

- Check what security settings your device has
  - Pin number, password, swipe pattern unlock features
  - Wipe phone after x amount of failed login attempts
- Belt clips can be problematic, carry it securely
- Choose to leave phone at home when you don’t need it
Staying safe while using device

- Avoid public or open WIFI hotspots.
  - Use mobile data connection: tethering, mobile hotspot etc
- Use a VPN Client
- Turn off unnecessary features
Staying safe while using device

- Only keep the files you need
- Virtual Credit Card Numbers
- Reporting location in social networks can be dangerous
Malicious content

- Newer threat, especially to Android Devices
  - Apps collect user data, spam contact list, etc
    - Read about the developer, read reviews, don’t assume anything
  - Read Permissions before installing, App markets can be open and vulnerable.
- Don’t allow apps from unknown sources, 3rd party Appstores.
**Legitimate Application**

Steamy Window

Do you want to install this application?

Allow this application to:
- **Network communication** full Internet access
- **Hardware controls** record audio

Hide

[Install] [Cancel]

**Malicious Application**

Do you want to install this application?

Allow this application to:
- **Your messages** receive SMS
- **Your personal information** read Browser's history and bookmarks, write Browser's history and bookmarks
- **Network communication** full Internet access
- **Storage**

[Install] [Cancel]
Malicious content

• What’s the answer to android viruses?
  • Android antiviruses of course!
  • Many Popular AVs now have an android version
Preventative Measures

• Making preventative steps is the only way…

• Smartphones have find my phone, remote wipe, remote lock, remote “scream” abilities. Many 3\textsuperscript{rd} party options

• Varies for each device, learn what yours is capable of

• Find the solution that you think will work best for you and test it.
Preventative Measures

- Encryption

- Not all devices have it, even less have it as a built-in function and even fewer than that implement it well.

- Blackberry is known for good encryption

- Reports that iPhone encryption is poor, almost no encryption on Android. Possibility for this to change.
If your device is lost or stolen

• Use any systems you had in place to:
  • Find your phone, make sure it didn’t just get left at work
  • If its been stolen, remote wipe it if you can
  • Device has to have some type of connection to receive commands.
  • Contact Law enforcement and cell carrier.
Questions & Open Discussion
Thank You