Educating the End User on Mobile Device Security

Dr. Karen Paullet
American Public University System

Mobile Device

- Mobile device refers to any mobile phone, tablets, e-Readers such as Kindle, GPS

Bring Your Own Device (BYOD)

- A phrase that has been adopted for employees who bring their own computing devices such as smartphones, laptops and tablets to the workplace for use and connectivity on the secure corporate network.

Mobile Devices are Attractive Targets

PERSONAL DEVICE

- Contact List
- Photos
- Calendars
- Email Accounts
- Notes
- PIN Numbers

WORK DEVICE

- Corporate email
- Customer Information
- Corporate Information
- Network/Login Credentials
- Confidential Information
- Access to Database

Four Common Mobile Vulnerabilities

1. **Lost or Stolen**
2. **Malware**
3. **Unsecured Network**
4. **Gaps in Mobile Management/Policy**

Lost or Stolen Devices

- 123 Cell Phones/Smart Phones are lost or stolen each minute
- 120,000 mobile devices are lost annually in Chicago Taxi cabs
- Major city transit authorities receive over 200 lost items per day

Cash for Device Machines

Malware and Mobile Apps

- 82% of applications are tracking the end user
- 80% collect location information
- 55% continuously track location while the device is turned on
- 36% know the users device information
- 35% contain malware

Example App Agreement

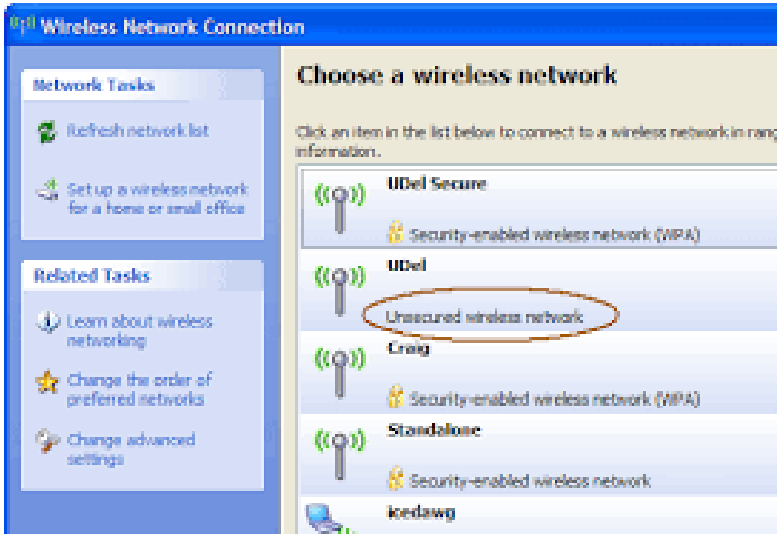
- Terms of use agreements create a legal agreement between end user and company
- We can collect, use and share your personal information
- You give us permission to use your personal email and contacts to network with your friends

Symptoms of Malware

- There is a sudden increase in your phone bill without cause
- The device has emails and messages in the sent folder that you did not send
- The user interface changed

Connecting to Unsecured Networks

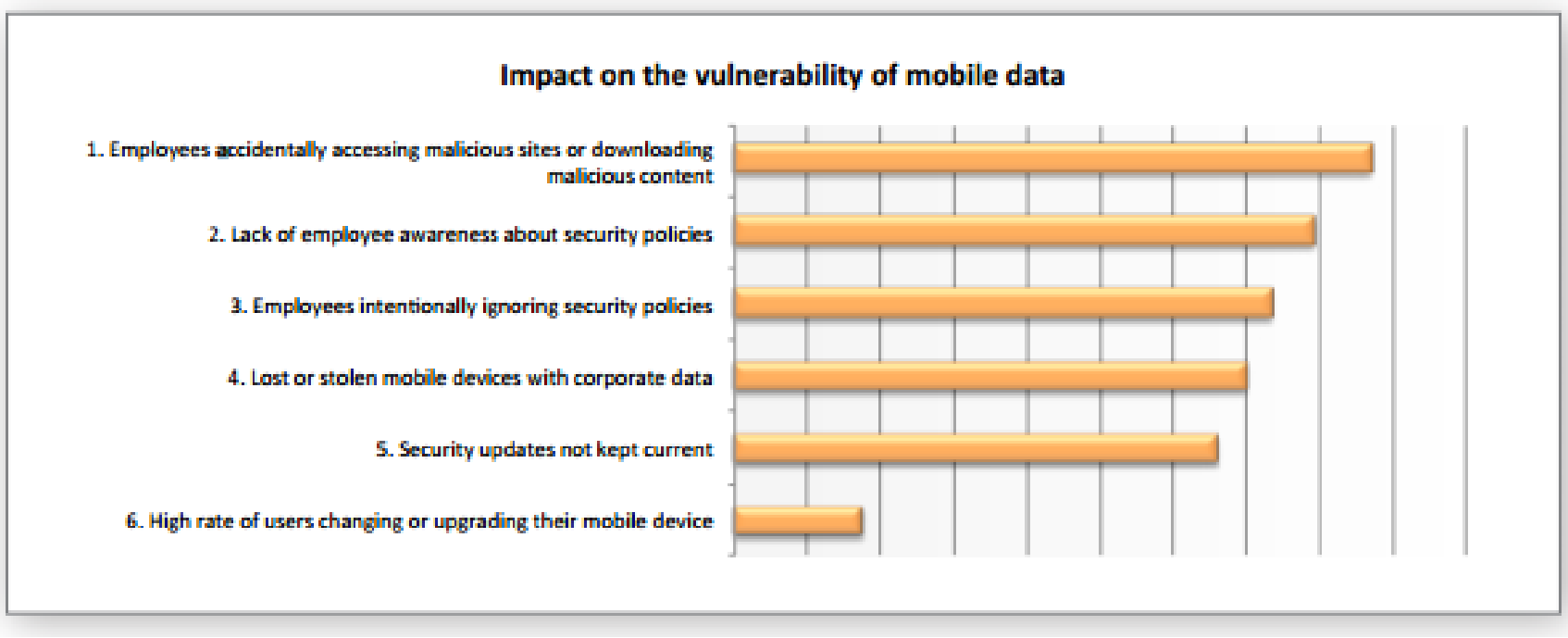
- Automatically connecting to Wi-Fi
- Leaving Bluetooth setting to "ON"
- Connecting to a Hot Spot that is not password protected



Gaps in Mobile Management

- Management of network
- Authentication of devices
- Policies and implementation
- Enforcement of policies

Employee Actions and Mobile Data



(Dimensional Research, 2014)

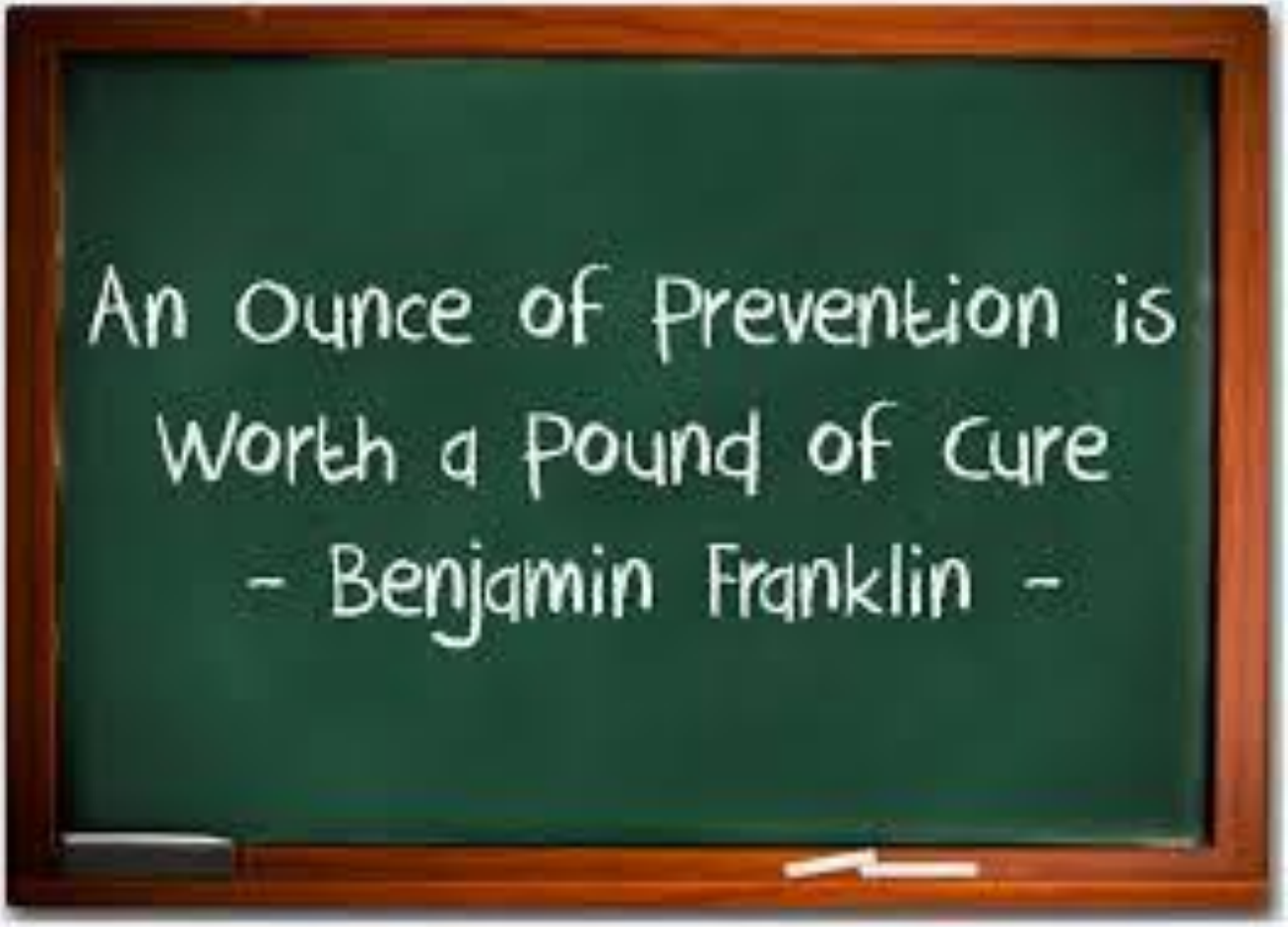
Preventative Measures

- Keep your mobile device with you at all times
- Turn on the security features on the device
- Set a password of PIN
- Install anti-malware/anti-virus software
- Turn Bluetooth to “OFF” when not in use
- Turn Wi-Fi “OFF” when not in use
- Record the International Mobile Equipment Identifier (IMEI) on the device

Preventative Measures

- Check your phone bill for unusual activity
- Backup data on a regular basis
- Set the device so that it automatically locks
- Stick with reputable sites when downloading from the Internet

Questions


An Ounce of Prevention is
Worth a Pound of Cure
- Benjamin Franklin -