Refreshing Mobile Devices for the New Year
January 17, 2012

Brad Wilson
Technology Support Services
Today’s Agenda

• Mobile Device Overview
• Smartphones
  – Understanding Your Device
  – Security Features
  – Best Practices and Usage Tips
• Tablets
  – Understanding Your Device
  – Security Features
  – Best Practices and Usage Tips
• Laptops
Mobile Devices

• Smartphones, tablets, e-readers
• Provide mobile access to wide variety of services
  • E-mail
  • Cloud storage
  • Internet
  • Literary content
  • Thousands of apps that range from GPS services to remote access to your desktop
Smartphone Overview

• Multiple manufacturers and operating systems
  – Apple, Samsung, Blackberry, LG, Nokia, etc.
  – iOS, Android, Blackberry OS, Windows Phone 7, etc.
• Wide range of capabilities
• Users are now integrated more than ever
Get to Know Your Smartphone

• Be aware of your device and prompts it displays
  – If it is prompting you to install something unusual, ask or investigate
  – Know how to tell if your device is connected to WiFi and if it is protected
  – Research apps before downloading; know what they will run or access on your phone

• Use online guides, YouTube, retail stores, to learn about your device
Smartphones: Know the Risks

• Software updates are essential
  – Security changes and improvements are constantly released by developers

• Understand the risks of using a mobile device for certain tasks
  – Mobile banking
  – Remote access
  – Storing passwords or personal information
Smartphones: PINs and Passcodes

• Immediately set up a PIN or passcode
  – Make sure it is a code you will remember—but not easily guessed (1111, 1234, abcd, etc.)
  – Personal information stored without a password is easily accessed by thieves
  – Do not place the passcode on the back or inside the battery door of your phone

• Accessing Collaboration Services requires a PIN or passcode on your device
Smartphones: Tracking Services

- Most smartphones have a tracking, remote wipe, remote lock system available
- Practice makes perfect! Use the track and remote lock services before you need them
- These services can be incredibly helpful in the event your phone has been lost or stolen
Smartphones: iOS Tips

• Register “Find my iPhone” service
  – Perform a test “track” to understand how the service works

• Browse WiFi menu to understand what a secure and unsecure network looks like

• Contact your IT department to receive more information regarding VPN use on your iOS device
Smartphones: Android Tips

- Be wary of third party apps
- Use app closing software to increase battery life and decrease the number of programs running in the background
- Depending on the manufacturer, a tracking service may be available
  - Motoblur, HTC Sense, etc.
- Install software on your computer to allow for backups and syncing
- Be cautious of “rooting” or “jailbreaking”
Smartphones: Windows Phone 7 Tips

• Install Windows Phone 7 sync software for efficient backups
• Learn how to tell if a WiFi network is secure
• Register and test tracking service with Windows account
• Set a passcode lock
Tablet Overview

• Tablets have increased mobile productivity greatly; can be used as a limited laptop but may also increase your security risk
• Various manufacturers and operating systems
  – Apple, HTC, Samsung, Acer, Asus, Blackberry, and many more
  – iOS, Android, QNX, WebOS, etc.
Get to Know Your Tablet

- Set up a passcode or PIN to secure your device
- Try to be aware of what your device is accessing, downloading, etc. at all times
- Simplicity does not mean security! Be aware when using your device
- Tablets can give you the ability to remotely access your desktop; before attempting this consult your local IT support
Tablets: iPad Best Practices

- Keep your iPad applications organized using folders and pages
- Use the double-click feature to see what apps are running in the background
- Refrain from purchasing or entering any personal information on a Web page on an open WiFi network
• Android tablets are still open source, which can pose a risk if you download questionable applications
• Refrain from storing personal information on your tablet
• A large variety of helpful resources are available with tablets, do your research before making major changes
Laptop Best Practices

• Use a strong password and change it periodically
• Always lock your computer when leaving your desk
• Keep anti-virus software up to date
  – Download University-provided software at www.it.northwestern.edu/software/sav
• Install operating system and other software updates when available
• Connect to secure networks whenever possible
General Security Tips

- Be mindful of where you browse and how you connect your mobile device to the Web
- As devices make it easier to store information, this makes it simpler for thieves to steal
- Ask a reliable source whenever you are entering unfamiliar territory
Questions?

The NUIT Support Center is mobile too!

Call: 847-491-HELP (1-4357)
Self-service: itsm.northwestern.edu/SM7/ess.do
E-mail: consultant@northwestern.edu
IM: www.it.northwestern.edu/supportcenter/livechat.html
Visit: www.it.northwestern.edu/supportcenter/index.html
Tweet: www.twitter.com/NU1HELP