Security Threats to your Android Device

As you know, Android phones are becoming more and more popular. Just like Microsoft Windows, the more popular they become, the more attractive a target they are to cyber criminals.

Don't underestimate the power in your hands.

Your phone is basically a computer, and it has the same limitations and weaknesses as any other computer. Take the same precautions that you would use with a Windows PC.

What would you do if you lost your phone?

Most use these devices to access email, facebook, twitter, and other online accounts, some of which may be synced to your phone.

Security Reports

F-Secure said in Q2 2012 more than 5,000 pieces of malicious Android software were received, which represents a massive 64 percent increase of Android malware during the quarter over Q1 2012.

http://www.f-secure.com/weblog/archives/MobileThreatReport_Q2_2012.pdf

McAfee said that in Q2 2012 mobile malware increased 700 percent in the last one year, mostly targeting Android. Symbian was at the second spot.

http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2012.pdf

Technical Assistance Group (TAG)

E-mail: tag@uah.edu
Phone: 256-824-3333

i.t.solutions
uahuntsville

E-mail: itsolutions@uah.edu
Web: http://its.uah.edu

National Cyber Security Awareness Month

Securing an Android Device

A guide to security information regarding your Android device.

UAHuntsville
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Securing Your Android Device

Android is at the top of the list for highest targeted mobile platforms. You are at risk!

Android Security Apps and Protection

www.mylookout.com — Remote wipe and remote lock, available for the premium (paid) version.

www.mobiledefense.com — Free remote wipe, lost phone locator, and malware protection.

www.avast.com — Free remote wipe/lock, lost phone locator, and malware protection.

wheresmydroid.com — Free tracking app.

How to Secure Your Android

- Try to avoid the temptation to "Root" your device unless you know what you are doing.
- Add PINs (passcodes) to your screen lock. — Usually under Settings > Location and Security > Set up Screen Lock.
- Don't answer text messages from unknown entities; otherwise, you might end up with malware.
- Set up screen timeout options to a low option so your device shuts off and locks itself. — Usually under Settings > Display.
- Put your name and contact information on your device. Android 3.0 or higher allows you to add owner information to the lock screen under Settings > Location and Security.
- Always apply the latest updates, as some of them may be security related.
- Be wary of public Wi-Fi hotspots. Make sure you are connecting to the coffee shop's access point (SSID) and not a rogue hacker. If in doubt, ask the coffee shop for the name of the SSID to connect to. Don't go to your banking site unless using a VPN (like HotSpot Shield).
- Record your phones IMEI and ESN numbers, and store them in a secure location. This will help your cell phone provider possibly locate or track your stolen/lost phone.
- Install a Remote Wipe app. This will allow you to wipe the data off your device remotely if your phone is lost or stolen.
- Shut down BlueTooth, Wi-Fi, and GPS when not in use.
- Install a Missing Device app. This will help you locate your device, via GPS, if it is lost. You must leave the GPS turned on for this app to work.
- Install an Antivirus/Malware app. This will help you protect your device from those pesky rogue apps.
- Consider using a cloud-based password manager, like Last Pass.
- Protect your phone from unknown applications. — Usually under Settings > Applications > uncheck the "Unknown Sources" box.
- Check user reviews of apps to get clues of any security issues.
- Uncheck the option "Make Passwords Visible." — Usually under security settings.
- Encrypt your data (available for 3.0 or higher) — Usually under Settings > Location and Security > Encrypt.
- Back your device to Google or Lookout Mobile.
- Don't just click on apps' requests for permissions (like accessing GPS or contacts) without fully understanding the reason why the app would need this.
- Be sure that apps come from the right developers. Some people create fake or pirated apps which often cost much less. Check user reviews for verification.