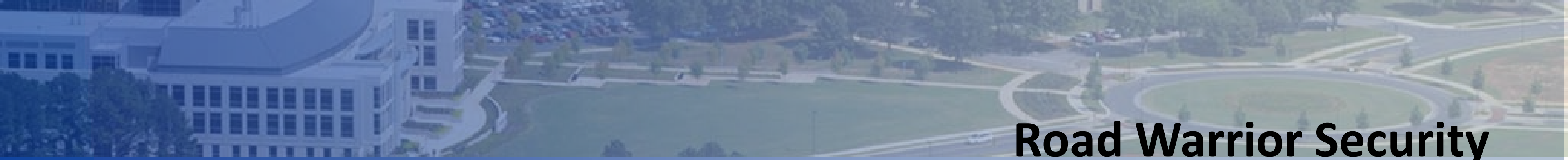
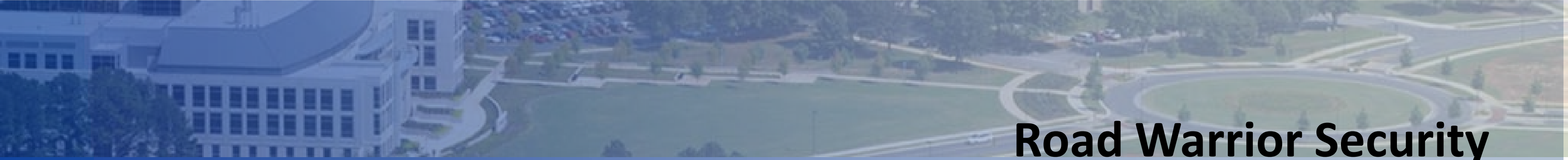


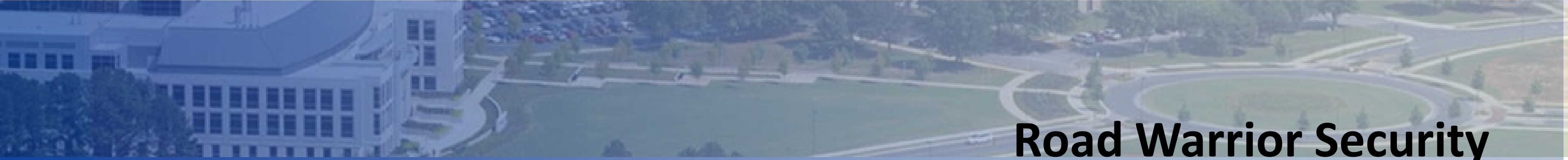
IT Security for the Road Warrior

Staying Secure Online While Traveling



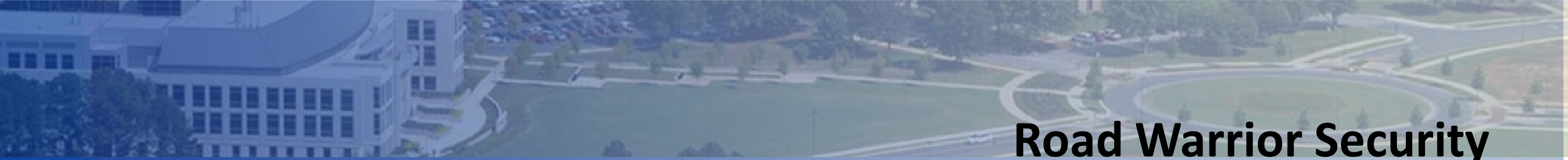
WHY WORRY?

- We have no knowledge or control over how the networks are defended
- We don’t know who the other users are on the network
- Do we even know that the network we’re connecting to is legitimate?
  - Attackers often set up their own wireless in hotels and airports. So is “Hilton1” or “DFWDterminal” real?



PREPARATION

- The key to using the Internet securely while traveling is to understand these additional risks, use caution, and be prepared.
  - Update your laptop and smartphone operating systems and applications to the latest version reduce their vulnerability to attack.
    - Automatic Updates
    - Secunia PSI

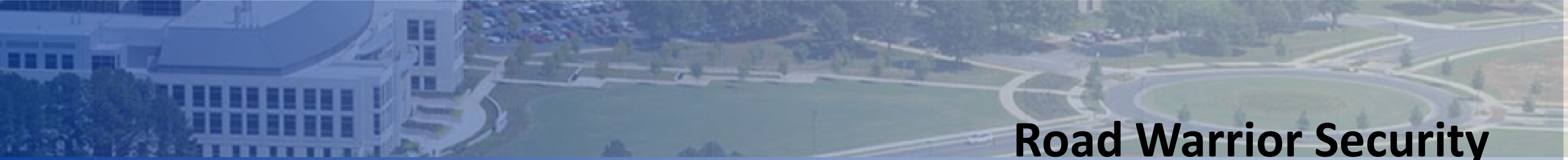


PREPARATION (Cont.)

- Make sure the firewall on your laptop is enabled. This helps prevent others from connecting to your laptop over the network.
- Check that your anti-virus software is up-to-date and is running.
- Laptops and smartphones are targets for thieves and easy to lose. Enable automatic screenlock on your laptop and smartphone using a strong password or, at the very least, a PIN code.

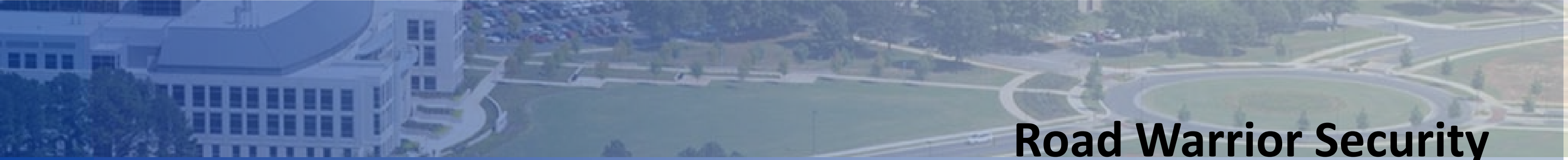
PREPARATION (Cont.)

- If your laptop or smartphone has personal or confidential information stored on it, consider encrypting the information or your entire hard drive before you leave.
  - ITS Offers Laptop Encryption (Contact TAG)
  - Takes 1-2 Days - Plan in Advance



CONNECTING TO PUBLIC NETWORKS

- Be cautions with Wi-Fi connections in airports, hotels, restaurants, and cafés
  - Look for signs with the name of the Wi-Fi network (SSID) displayed in the hotel lobby, airport terminal, or café – You can be sure you are connecting to a legit network
  - When possible use encrypted Wi-Fi networks (from best to worst: WPA2, WPA, and WEP)



CONNECTING TO PUBLIC NETWORKS (Cont.)

- Even with Wi-Fi encryption, your communications could still be intercepted by other users of the same Wi-Fi network
  - – Use HTTPS for Browser Sessions (look for padlock icon)
  - – Use VPN when available – UAHuntsville is planning a new VPN solution in 2012
    - VPN Creates an encrypted “tunnel” that all traffic passes though

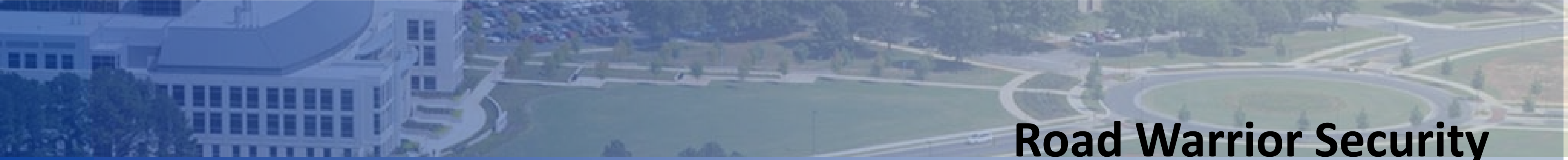
AVOID USING PUBLIC COMPUTERS

- Hotel business centers and internet cafes
  - Avoid them for anything other than casual web browsing
  - They are seldom monitored for tampering by malicious users and seldom patched
    - There have been numerous reports of keylogging software and other spyware discovered on public machines

Road Warrior Security

NEW OPTIONS

- Use your smartphone as a Wi-Fi access point
  - Several newer phones have this feature
- Choose your phone’s email and web browsing capabilities instead of public networks
- Read the security portion of the manual so your phone is configured securely
  - Smart Phone security is it’s own presentation, but the networks themselves are fairly secure



TRAVEL SAFELY!

Questions?