Wireless Security

Protect yourself and your data when you are away from home.

Jeremy Childress
Network Administrator
Nothing is Private on public Wi-Fi

- Anything you do on a public Wi-Fi network is easily intercepted, it’s similar to having a conversation in a crowd using a loudspeaker.
- Even a public encrypted network is not completely safe.
- Just because you pay for public Wi-Fi doesn’t mean it’s safer
- UNKSecure uses enterprise level encryption, not Pre-Shared Keys (PSK)
Protecting Your Computer

- **Turn Off Sharing**
  - Windows Control Panel -> Network and Sharing Center -> Advanced Sharing Settings
  - Mac OS X – System Preferences -> Sharing

- **Turn Off Network Discovery**
  - Windows – it is a checkbox under sharing
  - Mac OS X – it is called “stealth mode” under the firewall advanced settings
Turn on Your Firewall

- Windows Control Panel -> System and Security -> Windows Firewall
- Mac OS X – System Preferences -> Security -> Firewall
- To allow exceptions-
  - Windows – “Allow a program or feature through the firewall”
  - Mac OS X – “Firewall Options”
Use a VPN

- Routes all your activity through a secure private network
- vpn.unk.edu is available for access to UNK resources
- To prevent creating security vulnerabilities, access to external resources is restricted
- For access to the UNK VPN, contact the helpdesk to setup your account.
Shut it Off

• If you aren’t using wireless — shut it off
  • Most PC’s have a switch or key combo
  • Mac OS X – System Preferences -> Network -> Wi-Fi

• On iDevices/Android, turn off automatically connect to network options.

• Turning off Wi-Fi reduces battery load.