

# Router Configuration & Security

Demo using Verizon Actiontec  
MI424WR menus

# Why?

- Because most routers default to lowest security std
  - To minimize personal identity theft
  - To minimize use of your Internet connection for illegal activity
  - To minimize loss of bandwidth & speed of connection
- Security breach reality check
  - Probability small
  - Consequences can be significant



The Actiontec MI424WR

# What config issues? Page 1

- Router access & default UID & PWD
  - HTML, Telnet, & SSH access
  - WAN & LAN access
  - Ethernet (cable) & wireless access
  - Changing the MI424WR settings
    - <http://www.howtogeek.com/howto/35374/how-to-reset-or-change-the-password-for-your-verizon-fios-router>
  - Finding default UID & PWD for routers
    - Organizationally Unique Identifier (OUI)
    - <http://www.routerpasswords.com>
  - Using Belarc

# What config issues? Page 2

- Wi-Fi config
  - Radio on/off
  - a/b/g/n protocols on/off
  - n-protocol 2.4GHz & 5GHz bands
  - SSID (Service Set ID) - to hide or not
  - Encryption
    - none, WEP, WPA, WPA2
    - Google "Cracking WEP"
    - Old & new devices consideration
- Wi-Fi scanning
  - BSSID (MAC, Basic SSID) & OUI

# What config issues? Page 3

- Ports
  - Port forwarding (including triggered, etc.)
  - UPnP (Universal Plug 'n Play) on/off
    - Typically used by games & media software / devices
    - Malware concern
- MAC (Media Access Control) filtering
- DHCP address space
- Static DHCP vs Static IP