

Wireless Networking Security Tips



www.cybersciencelab.com

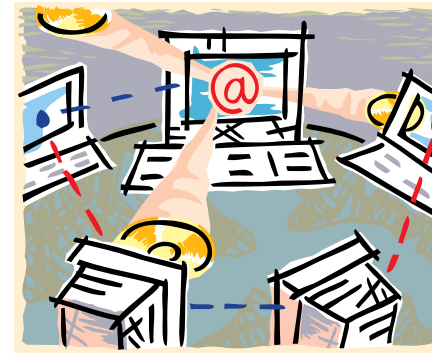
A Program of the National Institute of Justice

*This is to be used as an informational guide only.
Please refer to our disclaimer at www.cybersciencelab.com.*



Wireless Networking Security Tips

- Set up **access points** (APs) in the center of the building if possible, or use a directional antenna to direct the RF signals into the building (not the parking lot)
- Have some form of **authentication** (e.g. Active Directory or RADIUS)
- Connect APs to the net via **switches** instead of hubs to minimize traffic sniffing threats



- Utilize **MAC Access Lists** to control WLAN access
- **Change** the AP's important **default settings** from their well known, factory configurations; Subnet, Password, SSID, and WEP key
- Change all **passwords**, especially the administrator, on a regular basis
- Survey your site regularly for **Rogue APs**, as they can pop up anywhere and at anytime
- **Separate** your WLAN from your regular network and place it outside the firewall or behind its own
- **Encrypt** all WLAN traffic (e.g. VPN, TTSL, SSL, IPSEC, LEAP, and EAP)
- Enable the **highest WEP encryption** possible
- Disable DHCP and use **static IP** assignment
- **Disable** Beacon or Broadcast SSID
- Increase WLAN user and administrator **awareness** through better training