

SECURITY - Now ...more than ever!

Cyber Security - Disaster Recovery - Continuity of Government



DTI eSecurity News - Are hackers using your Internet connection from down the street?



How do wireless networks work?

Wireless networks, also commonly referred to as “WiFi” networks (short for Wireless Fidelity), allow computer users to connect to the Internet without relying on wires. A transmitter, known as a wireless router, acts as a bridge between your wireless enabled computer and a wired network. Some of the common router manufacturers are LINKSYS, D-Link, and NETGEAR.

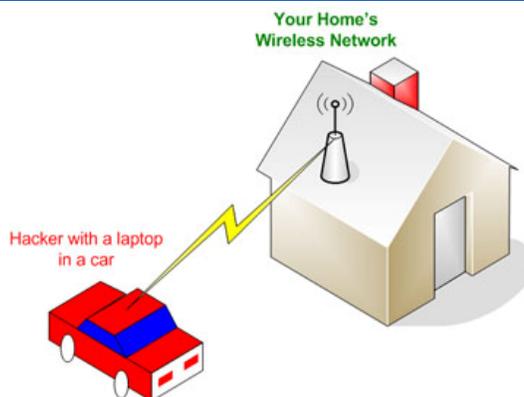
Depending on its settings, a wireless enabled computer may either connect automatically to wireless networks it discovers or require the user to specify which network to connect to. All wireless networks are identified by their service set identifier (SSID). The SSID is basically the name of a wireless network.

What are the risks of running a wireless network?

A wireless network, with a high speed connection, can easily be setup at home by purchasing a wireless router from a retail outlet, such as Best Buy or Circuit City. Wireless networks are popular because they provide internet access throughout a home, and for multiple computers within the home, without the need to run hard wiring from one room to another.

However, if set up improperly, these wireless networks can be a security nightmare for your home computers. If someone gains access to your wireless network, they may also be able to access any of the computers on your network. While wireless routers include functionality to protect your computers from internet threats, they do not commonly provide protection from computers that may have gained access to your own home network.

Even if a malicious user is not after your home computer, they may use your internet connection to hack other systems, send large amounts of spam, or launch virus and worm attacks. If such illegal attacks were traced, the results would point back to your account!



How do I secure my wireless network?

The most important steps in securing your wireless network are to: 1) take the time to read the manual that accompanies your wireless router and 2) take advantage of all security options when configuring the network for the first time. Always change the default router password, and pay attention to these other key configuration items:

- **Encryption:** Wired Equivalency Privacy (WEP) is acceptable for home networks. However, if your router supports WiFi Protected Access (WPA or WPA2), you should use it. It is one of the newest wireless standards, and it is based on the Federal Government Advanced Encryption standard. It provides very strong security.
- **Access Control Lists:** These lists provide your router with a list of specific computers permitted to connect your network. All other requests are denied. The manual will provide further details as different routers vary.
- **Router SSID:** Configure your router so you are NOT broadcasting the SSID. This step hides your wireless network's name, which makes it more difficult for hackers to connect.

Questions or comments?
e-mail us at
eSecurity@state.de.us