

Company Contact: Bob Jewell

Media Contact: Codie Breitbarth

Wireless Warning

Businesses should take steps to secure their wireless computer networks.

Hundreds of Kansas City businesses run the risk each day of exposing company secrets and customer information, and losing money. And they don't even know it. The reason: an unsecured wireless network.

More local businesses are joining the wireless technology explosion, but they are failing to take proper security measures. Small businesses can easily purchase wireless devices from retailers and install the device themselves. Wi-Fi can save companies money and time. However, many companies that are using the technology fail to take precautions to protect themselves from hackers skilled in "war driving."

War drivers use a laptop computer, software and a wireless card to pick up unsecured Wireless Local-Area Network (WLAN) signals. The software, such as Netstumbler, is available for free on the Internet. At a minimum, hackers war drive wireless networks for anonymous and free high-speed Internet access. In the worst-case scenario, war drivers can steal company secrets or customer information, place a virus on a network and ultimately cost businesses millions.

There are several ways you can limit access to keep strangers off your Wi-Fi network.

Change your default SSID

Wi-Fi access points and routers ship with a pre-defined network name — a Service Set Identifier (SSID) — set by the manufacturer. The SSID can be accessed from within these products' Web-based or Windows-based configuration utilities. To improve the security of your wireless network, change the SSID to a name different from the default. An SSID can be changed at any time, as long as the change is also made on all computers within the wireless network.

Don't broadcast your SSID

This is by far the easiest way to prevent someone from accessing your Wi-Fi network, but it's far from secure. By default, most products broadcast their presence through their SSIDs, but you can reconfigure the base station to not broadcast the SSID. While this will keep out most uninvited guests, a stranger who already knows your Wi-Fi network name can still gain access.

Change the default password that comes with the equipment

Manufacturers set both the account username and password at the factory. To improve the security of a Wi-Fi network, you should immediately change the administrative password on your wireless access point or router when installing the unit. The default passwords for popular models of wireless network gear are well known to hackers and often are posted on the Internet.

Encrypt your wireless network password

Wi-Fi access points can be open or secure. If the access point is open, anyone with a Wi-Fi card can access the network. If it is secure, in order to connect the user needs to know a Wired Equivalent Privacy (WEP) key — a security protocol used to encrypt the data stream. To limit access to your wireless connection, set up your equipment's WEP encryption. Usually, the higher

the value, the better. For example, setting your wireless access point to use 128-bit encryption will provide better protection than if you set it to 64-bit.

Configure your access point to allow only your computer MAC address

Every computer is identified by a unique number called a Machine Access Code (MAC) address. You can instruct your Wi-Fi base station to allow access to only certain MAC addresses. The MAC address of your wireless card can be found on the card itself. This is a slightly more labor-intensive task, but it can be very effective, because MAC addresses are hard to guess.

Most new wireless network devices include detailed instructions that outline the appropriate steps businesses or consumers can take to secure a network. The larger and more complex a wireless network, the harder it is to secure. It's always a good safeguard to seek professional advice when it comes to network security issues.

Ask the IT Experts

If you still have questions or uncertainties about your network's security, consider contacting an IT professional. The IT professional you select should be able to help your company take advantage of wireless technology without risking your network's security. Ask the professional to provide detailed findings outlining potential dangers within your network, and to recommend ways to reduce security risks without reducing customer **convenience**.

Bob Jewell is senior vice president of Network Integration Services Inc. of Lenexa. He can be reached at (913) 492-3055 or rjewell@netisinc.com.