



The Latest News from More Power Computers

War Driving; It's Not About Slaying Zombies Using Cars This Time

War Driving. It's not a new video game that your kids want this Christmas. It's the drive-by hacking of wireless networks. For some, it's a game, like the lottery. The more unsecured spots they find the better they are at the game. The goal is to find out who does not have pass-



word protection on their wireless network or who can be hacked. For others, it's about using the internet by finding free wireless connections. But for a few, it's about activities that

range from menacing to criminal, and if they're using your network, it could be traced back to you. Businesses that allow employees to work from home are very concerned about this trend because an employee's wireless home network, if unsecured, means the business network is at risk too. So what can you do to protect yourself and your business? Wireless networks broadcast data in segments or packets. Attached to each packet is a Service Set Identifier (SSID), a code that identifies the network so all within range can see the network. If SSID is disabled then it's harder for hackers to find your network and less likely a casual drive-by hacker will find you. If you need to have SSID enabled for use on a wireless LAN, do not

use the SSID default; use something that is not obvious or easy to guess. Another way of making your network more secure is to use Media Access Control (MAC) filtering. A MAC address is a number assigned to each computer or device. Restricting access only to known addresses means the hacker would have to learn the address number of a legitimate computer on your network to gain access. Encrypting your network can be another way to safeguard your data. You can only use one method at a time. Whether you use Wi-Fi Protected Access (WPA) or Wired Equivalent Privacy (WEP) you need to change your password and encryption key on a regular basis. For more on encryption, read the article that follows.

Encryption Security: WPA Versus WEP

The Federal Bureau of Investigation (FBI) has brought together security professionals to find possible threats to security. One such group, called the InfraGard Program, deals with information security and cyberspace. A recent alert came when European hackers found a way to break through WEP encryption within seconds. Since what hackers do on your internet connection can get traced back

to you, you want to get the best internet security possible. The FBI recommends using several layers of security and switching to a more secure protocol such as AES, TKIP, or WPA2. Whether you go with WPA, WEP, or something else, change the security settings (do not use the default settings) and set up a difficult to guess password. If you are not sure how to do that, a good first step is a mixture of letters,

numbers, and other characters, but be sure to check the website of the manufacturer of your wireless router. Many will have a section devoted to internet security.



More Power Computers, Inc.

Serving The Lower Columbia
Region Since 1994.

Special points of
interest:

- > Keeping Yourself Safe From A Drive-By Hacking.
- > SSID, MAC, WPA; Learning The Alphabet Soup Of Internet Security
- > European Hackers Found A Way To Break Through WEP Encryption Within Seconds.
- > What Hackers Do On Your Internet Connection Can Get Traced Back To You!

