Protect your wireless network from hackers

By Xiao Ming Wu, CNET Freelancer
2/25/2005
Filed in: Networking and Wi-Fi
Level: Intermediate | **160 out of 160** users found this tip helpful

TALES FROM THE CRYPTOGRAPHER

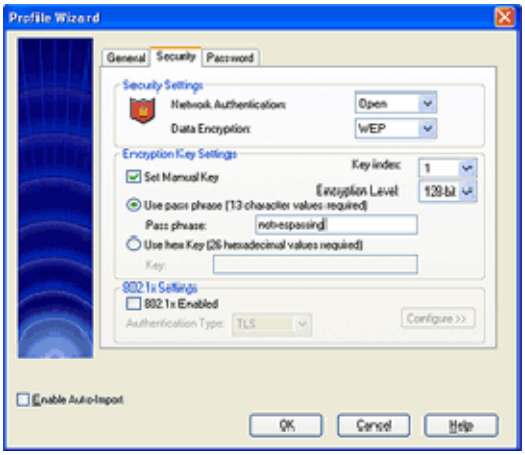
It would send chills down your spine to learn how easy it is for others to connect to your Wi-Fi network and put your computers under their spell. If your computer has been acting funny lately, working fine at times while slowing to a crawl at others, it may have crossed over to the dark side and could be spamming your friends and scamming your parents.

A home network brings many benefits, but it can also expose new evils. Both your Internet connection and your wireless router are potential points of entry for the bad guys. Hackers can probe for your computers over the Internet and turn them into zombies if they are unprotected. Worms and viruses can slither their way through your network, burrowing more holes into your PC than a maggot-infested corpse, and the thief parked on the street where you live can set up shop with the help of your Wi-Fi connection.

Here are a few tips that will keep hackers and freeloaders at bay.

1. Use encryption to protect your wireless network. It sounds trivial, but consider this: wireless data is transmitted over the air. This makes it far more exposed than data transmitted over a cable. To hack into an Ethernet network, you either need to force entry through an Ethernet connection or you need access to the Ethernet cable, which you can lock behind a door; but to pry into a wireless network, you need only be within range. A would-be intruder can park in the street where you live and do her dirty work from the privacy of her car, without risking the unpleasantries of breaking and entering.

You can protect your wireless network by encrypting it. Virtually all Wi-Fi gear supports an encryption scheme called WEP (Wired Equivalent Privacy). WEP scrambles data transmitted over your network, making it difficult to decipher. Even better, setting up WEP is easy. In most cases, you merely enter a passphrase into the configuration settings of each device on your network. The devices use the passphrase to generate a WEP key, which is used to encrypt and decrypt data transmitted over the network.



Use a passphrase to configure WEP.

2. Lock down your LAN. An always-on broadband connection is convenient, but it's also a magnet for hackers and script kiddies, giving them a target that is open 24/7. You can use a firewall to thwart attacks on your network that use your Internet connection as their point of entry. Most wireless routers come with an integrated NAT firewall. NAT stands for *network address translation* and is used to hide the IP addresses of the PCs on your network behind your router's IP address. From the Internet, your network appears to consist of only one device, your router. This makes it more difficult for intruders to identify the computers on your network. NAT, however, is relatively dumb. It maps the addresses of the computers on your network to the IP address of the router, but it doesn't inspect the data inside the packets passing through your router. For that, you need a second firewall that performs *stateful packet inspection,* or SPI. An SPI firewall can determine if an incoming data packet is a legitimate response to a request from one of your computers. Not all routers include an SPI firewall, so keep a lookout for it when you buy your gear.

Configure the computers on your network with static IP addresses.

3. Don't make it easy for criminals. Most consumer networking gear is designed to be easy to use out of the box. Easy setup might leave you with a warm fuzzy feeling after the initial setup, but a foolproof setup routine can also leave your network vulnerable to unwanted visitors. For example, routers use DHCP, *dynamic host configuration protocol,* to automatically handle the IP address information for the computers on your network. But handing out IP address information automatically makes it easy for unwanted guests to join your network. Consider manually assigning static IP addresses to your computers and turning off your router's DHCP server. To manually configure an IP address, right-click the Network Neighborhood icon and select Properties. A window appears listing your network adapters. Right-click the adapter you use to connect to your LAN and select Properties. In the "Local area connection properties" window that appears, select Internet Protocol (TCP/IP) and click the button marked Properties. This window allows you to use a prespecified IP address, subnet mask, default gateway (in this case, your router), and DNS server. Check Wednesday's nightmare for more information about assigning IP address information.

If you have a wireless router, it probably advertises its network name, or SSID, at regular intervals to any device within range, making it easy for others to join your wireless network. Some routers let you turn off the beacon that puts your SSID on the air for everyone to see. Since your computers presumably already know your wireless network's SSID and have profiles instructing them to use it for their connection, consider turning off your router's beacon. Though not all routers let you turn the beacon off, many do. Check the router's browser-based configuration tool for a beacon switch.

Tags: encrypting network, wireless network

---

160 out of 160 users found this tip helpful

Did you find this tip helpful? Yes