

How safe is your wireless network?

What you should know

Wi-Fi "hotspots" are popping up in a growing number of homes, businesses, hospitals, and even parks. But are they safe?

With many users unaware of free firewall protection and a built-in feature that scrambles data (called "encryption") on their wireless devices, the answer is too often "no."

National studies show that at least one-third of all wireless networks are unsecured. That means the confidential data they carry and store can be picked up by electronic eavesdroppers hacking in from as far as a mile away.

Securing your network isn't difficult or expensive. It just involves reading your owner's manual and following a few easy steps, many of which are outlined here for you to follow.

Understanding the Risks

Because of the very nature of wireless communications - that they occur in the open air and can be easily intercepted - Wi-Fi networks are more vulnerable to security problems than wired forms of networking. Hackers or intruders don't need physical access to your hardware to disrupt operations. Anyone within radio range can theoretically tap into your wireless network and steal confidential data. This means that intruders may be sitting in your parking lot or in the apartment complex across the street.

Anyone who uses a wireless network should understand the potential risks:



Freely available tools allow anyone to pinpoint insecure networks. Intruders inside your network may corrupt your data, consume network bandwidth, reduce network performance, launch viruses and attacks that prevent authorized users from accessing the network, or even attack other networks.



Exploiting wireless networks is one of the many ways hackers can gain access to your personal information and commit identity theft. In 2004, 9.3 million Americans - or one in every 23 adults - were victims of the crime, according to the Better Business Bureau and Javelin Strategy and Research. A survey by the Federal Trade Commission estimates that identity theft crimes tallied \$52.6 billion in costs in 2004.



While there are security features built into wireless networking products, most manufacturers turn them off by default because it makes the networks easier to set up. This effort to make wireless networking more user-friendly has rendered most equipment completely unsecure from the moment it comes out of the box.

Part of the problem is that most software and service providers responsible for installing wireless equipment have no incentive to advise users of the risks. That is why Westchester County is encouraging both residents and businesses to take a proactive stance in safeguarding their networks from possible intruders.

Basic Steps You Can Take

There are a number of steps that even non-technical users can take to make a wireless network more secure. *Some general instructions follow, but you will need to refer to the owner's manual for your wireless equipment for more specific instructions.*

1

Use personal firewalls. One of the easiest ways to guard a network from attack is to set up a personal firewall. Top firewall software products include ZoneAlarm Pro (free to download at www.zonelabs.com), Norton Personal Firewall and McAfee Personal Firewall Plus. If you are running Windows XP, Microsoft's built-in firewall may already be turned on. Check also with your computer manufacturer to learn if firewall software has already been installed and enabled on your machine.

2

Change your name. Most systems use a default SSID (network name) such as "wireless" or "default." Hackers know that the popular LINKSYS product uses the name "linksys" as its SSID. Be sure to change default names to something unique that will not attract unwanted attention.

3

Disable SSID broadcasting. Doing this hides the presence of your wireless network or at least obscures the SSID itself which is critical for a device to connect to your network. By turning off the broadcast SSID function, a hacker will have to guess your network's name to get in.

4

Scramble your data. In order to protect your data from prying eyes, you should scramble or "encrypt" it so that nobody else can read it. Most recent wireless equipment comes with both WEP (wired equivalent privacy) and WPA (Wi-Fi protected access) encryption tools that you can enable. WPA is more robust and should be used if supported by your equipment.

5

Block casual intruders. Each network device has a unique identifier called a Media Access Control (MAC) address, similar to a serial number. Some wireless devices allow users to create an "authorized MAC address table" which means only devices with serial numbers you've approved are allowed on the network.

Remember that even with all these steps, there's no way to guarantee 100 percent security for a wireless network. Since protecting your wireless network is all about improving the odds that you'll be safe, the more steps you decide to take the better off you'll be.



**Message from
County Executive
Andy Spano**

Wireless technologies have become increasingly popular in our everyday business and personal lives. Internet setup and access are easier and more convenient than ever. Unfortunately, this convenience may be exploited by malicious individuals who want to hack into private networks and steal confidential data.

Nobody likes to imagine that there is someone prying into their affairs or grabbing a free ride at their expense. But if you have a wireless network – and information you'd like to keep confidential – then a little extra caution will serve you well.

Westchester County has broken new ground by passing a first-of-its-kind law requiring all commercial businesses using wireless networks to take basic security precautions when dealing with sensitive customer data. Businesses offering public Internet access must post a sign advising customers that they should also install their own protective measures.

As part of the new law, the County is also committed to increasing public awareness about the need for network security. The information in this brochure will help you understand the risks of using a wireless network and learn what you can do to ward off potential “data thieves.”

Resources

For further ways to protect your wireless network consult a qualified network specialist. Listings of local consulting firms are found online or through the yellow pages.

You may also visit your computer manufacturer's website or call the consumer technical support line for assistance setting up a firewall and other security measures. Wireless service providers also offer helpful information on their websites on how wireless works and additional ways to secure your computer.

For additional information on wireless security and identity theft, visit www.westchestergov.com/idtheft.

The Federal Trade Commission has also created a one-stop resource to learn more about the crime of identity theft and the many resources available to consumers and businesses: www.consumer.gov/idtheft.

Wireless Networks...

You May Be More
Vulnerable
Than You
Think



Westchester
gov.com

Andrew J. Spano, Westchester County Executive
County Board of Legislators