White Paper

# Securing Home Wi-Fi® Networks: A Simple Solution Can Save Your Identity

Wireless-WP200-x

This white paper explains the need for securing Wi-Fi networks and the type of security best suited for use in the home. Several setup options exist, but the simplest solution is also the most secure.

May 18, 2005

## Introduction

Home computer users increasingly are taking steps to bolster Internet security, for several reasons. Well-publicized incidents of disk-crashing worms and viruses scare consumers into protecting their computers with firewalls and antivirus software. Also, the growing prevalence of uninvited spyware has spawned a fast-growing class of applications designed to protect computers from these performance-sapping nuisances. Ever-present fears of identity theft and credit card fraud remain serious concerns as well.

But while many consumers are securing their Internet connections, only a fraction of them take the time to protect their networks. As a result, they are still leaving gaping security holes for intruders to access personal information and destroy data.

Home users who leave their Wi-Fi networks unsecured do so for a variety of reasons. Some are not aware of the risks or the security options available to them. But research shows that the vast majority of them don't secure their wireless LAN simply because they find the task too complicated.

This white paper describes the security risks of leaving a home Wi-Fi network unsecured, and details the options that are available to protect it. As readers will discover, solutions with painless security installations can also make it easy to set up a Wi-Fi network or add devices to an existing network.

## Security Risks with Wireless LANs

LAN communication using wireless is, by nature, much more difficult to restrict and control than when using wired media. Wired phone conversations, for example, are quite difficult to intercept, but any hobbyist with a radio scanner can eavesdrop on radio transmissions between a police dispatcher and an officer on patrol. The same is true for wireless LANs: Any computer, handheld or other device in range has the potential to join the network, provided it has Wi-Fi capability, as Figure 1 illustrates.

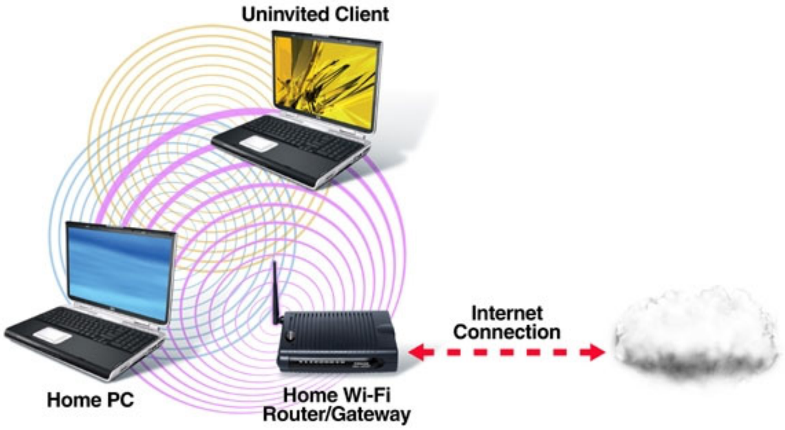


Figure 1: Though a home Internet connection may be secured by a firewall, antivirus software, and other protection alternatives, an uninvited computer in range is free to join an unsecured wireless network. This can introduce a host of security problems.

What sort of vulnerabilities does an unsecured Wi-Fi network open? The most common reason for uninvited guests to join an unsecured home wireless LAN is to gain access to an Internet connection. Though not irrevocably harmful, an unwelcome client can sap a household’s limited Internet bandwidth, slowing everything from sending e-mail to downloading programs and music.

Increasingly common is a practice in which hackers tap into a Wi-Fi network to use it as a temporary base for spam and other unethical or illegal activities. By hijacking an Internet address, they remain anonymous because the activity would be traced back to the home network.

Though less common, malicious users can easily damage or delete files on household computers that are connected to the Wi-Fi network. In rare cases, intruders are in a position to collect passwords, account numbers, and other personal information – activities that put personal finances and identities at risk.

Workers who bring a laptop computer home from the office could inadvertently expose company secrets by connecting it to an unsecured wireless network.

With such glaring holes, the motivation for implementing security on home Wi-Fi networks should be apparent. And yet, according to a recent study by the Farpoint Group, fewer than one-fourth of all home wireless LAN consumers activate the security features that are built into their hardware. Judging from technical support calls and product returns, a major reason that nontechnical consumers haven’t implemented security on their wireless LANs is that the process was too complex for them.

## Security Options for Home Wi-Fi Networks

Wi-Fi products offer a multitude of security alternatives, including both industry-standard and proprietary protection schemes. The industry standard approaches have evolved from Wired Equivalent Privacy™ (WEP) to Wi-Fi Protected Access™ (WPA).

WEP was part of the original IEEE 802.11 wireless specification in 1997. WEP-enabled wireless LANs require a secret key code from computers before they can join the network. WEP quickly proved to be easy to crack, because the code is not terribly complex, and because it is static. Researchers have since found other cryptographic flaws in WEP.

The 802.11 committee – the IEEE standards-setting body for wireless LAN – formed the 802.11i security task force to define a more robust system for protecting Wi-Fi networks. After several years of deliberation, the IEEE ratified the 802.11i standard in July 2004.

In the meantime, businesses and security-minded consumers demanded more robust security than what WEP provided, and they weren't willing to wait for the new specification to become finalized.

To meet the demand for better security in the interim, the Wi-Fi Alliance, an independent industry association, worked together with the 802.11i task force to produce Wi-Fi Protected Access™, or WPA. Unveiled in April 2003, WPA provides far better authentication than WEP, as well as an encryption scheme to confound intruders from deciphering network traffic.

Once authenticated, WPA encrypts data traffic with a scheme called TKIP or temporal key integrity protocol. WPA's TKIP employs a complex algorithm that regularly replaces security keys before would-be intruders have a chance to crack them.

### Wi-Fi Security Terms

**802.11i**: Industry standard for Wi-Fi security approved in 2004. The 802.11i standard adds AES encryption to WPA. Some large businesses and government agencies require AES.

**AES**: Advanced Encryption Standard. The government standard for encrypting data communications.

**WEP**: Wired Equivalent Privacy. The original wireless security standard. Generally thought to be insufficient in protecting Wi-Fi networks.

**WPA**: Wi-Fi Protected Access. Adds a means for authenticating computers on a Wi-Fi network and provides an algorithm for encrypting communication called TKIP.

**WPA2**: Any Wi-Fi hardware based on 802.11 that has been certified as 802.11i compliant by the Wi-Fi Alliance.

WPA has now replaced WEP as the de facto standard for home Wi-Fi network security. In fact, WPA support is now required in order for Wi-Fi network hardware to receive the Wi-Fi CERTIFIED™ seal of interoperability.

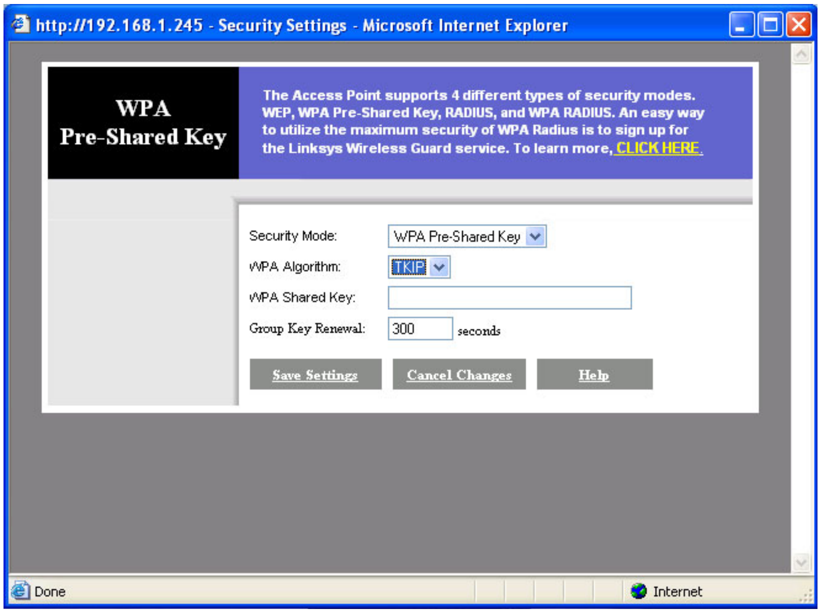
## What's the Best Way to Activate WPA for Home Wi-Fi Networks?

As discussed, the most common approach among consumers is to do nothing to protect their wireless networks – typically because configuring security is too complicated.

For consumers that decide to tackle security, there are three common methods to activate WPA on their home wireless networks:

1. Manually configure the settings on their devices
2. Run a configuration wizard or
3. Press a special-purpose security setup button

To manually activate WPA, users first need to configure their access point or router manually by entering the shared key code. Many access points available today enable configuration - through an embedded web page - like the one shown in Figure 2. Once the access point is configured, the user must enter the chosen WPA key into their PC or other device in order to be added to the network.



http://192.168.1.245 - Security Settings - Microsoft Internet Explorer

WPA Pre-Shared Key

The Access Point supports 4 different types of security modes. WEP, WPA Pre-Shared Key, RADIUS, and WPA RADIUS. An easy way to utilize the maximum security of WPA Radius is to sign up for the Linksys Wireless Guard service. To learn more, CLICK HERE.

Security Mode: WPA Pre-Shared Key

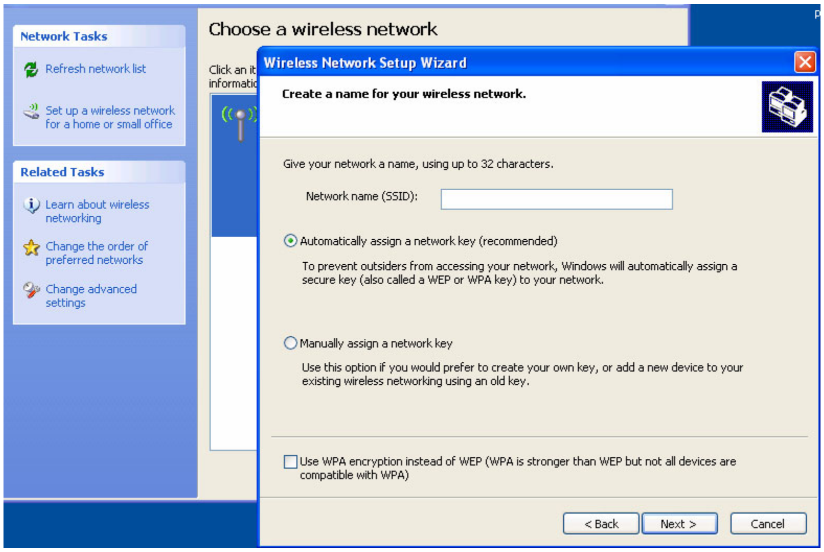
WPA Algorithm: TKIP

WPA Shared Key:

Group Key Renewal: 300 seconds

Figure 2: To enable WPA on a home network, users select the preshared key option. (Large businesses may assign a dedicated system, called a RADIUS server, to the task of authenticating computers.) Then, users must enter a common key code into both the access point configuration page and on computers and devices joining the network.

Some Wi-Fi hardware ships with configuration wizards designed to simplify setup. In fact, Microsoft has built a wizard into the latest edition of Windows XP (Service Pack 2), which is shown in Figure 3 below. The Microsoft implementation relies on a USB flash drive to transfer settings to additional computers that home users would like to include on the network.


Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Click an it
informatic
Wireless Network Setup Wizard
< Back
Next >
Cancel

Create a name for your wireless network.

Give your network a name, using up to 32 characters.

Network name (SSID):

● Automatically assign a network key (recommended)

To prevent outsiders from accessing your network, Windows will automatically assign a secure key (also called a WEP or WPA key) to your network.

○ Manually assign a network key

Use this option if you would prefer to create your own key, or add a new device to your existing wireless networking using an old key.

□ Use WPA encryption instead of WEP (WPA is stronger than WEP but not all devices are compatible with WPA)

Figure 3: Installation wizards, like this one from the latest version of Windows XP, help simplify setup and securing a home wireless network. There are still choices to make, though, and pitfalls remain as a result.

A third option is emerging as suppliers of Wi-Fi network hardware, computers and peripherals make setting up a wireless LAN and installing WPA security as simple as pushing a button. Hardware without displays, such as wireless access points, printers, and other consumer networked devices – feature actual buttons such as those pictured in Figure 4. Wireless-enabled computers or notebooks using a wireless PC Card will present consumers with a button-like icon to click during installation.

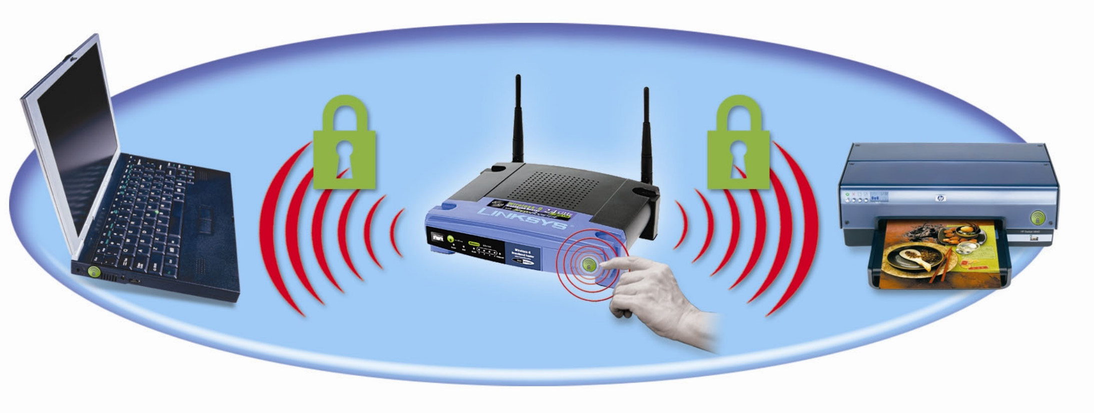


Figure 4: Wireless router and notebook with push button setup option.

With push button security, a consumer presses the button on the access point to get started. That cues the access point to prepare to configure a secure connection.

It then watches for signs from a PC peripheral or other device to be configured. Once the consumer clicks the button on the computer peripheral or other device, the access point establishes a secure communication link between the two devices, generates a WPA passkey, if one is not already established, and automatically provides the information to the device that is joining the network. To add another device to the network, the consumer would just repeat the push-button process.

Since the biggest challenge to Wi-Fi security has been turning it on, the simpler and more automated a solution is — the better the opportunity for the home user to activate security. A button is the easiest method for securing a home wireless LAN, as consumers are already accustomed to pushing buttons to pair up other wireless consumer electronics devices, such as garage door openers and in-car remotes.

With any of the methods used to activate WPA security, it is a good idea to store security settings in a safe location for future reference.

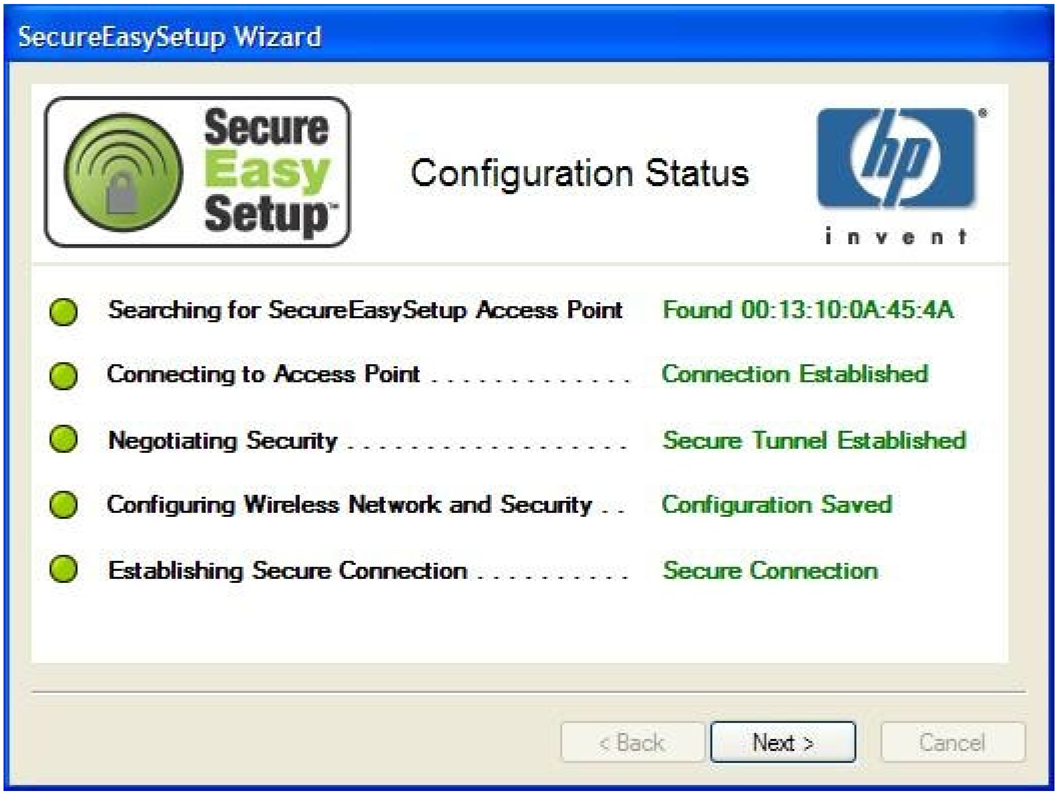
## Helping Consumers Install and Protect Their Wireless Networks with SecureEasySetup™

The leading push button setup and WPA security implementation in the industry is called SecureEasySetup™, a Broadcom innovation that is built into routers, gateways, access points and Wi-Fi cards from Linksys as well as consumer products including printers from Hewlett-Packard.  These leading vendors have collaborated to define the functionality of SecureEasySetup and to promote the SecureEasySetup logo shown in Figure 5

Figure 5:  Wireless LAN hardware with the SecureEasySetup logo pictured above features push button configuration and security.

Securing a home Wi-Fi network with SecureEasySetup is not only easier than manual configuration, it also may be more secure. During manual setup, communication between a home computer and the access point may not be secure while passcodes are being set. While chances are remote, it is possible for a hacker, who is in the right place at the right time, to intercept the codes. SecureEasySetup eliminates that possibility by establishing an encrypted channel of communication between the access point and the network device undergoing configuration.

SecureEasySetup also has advanced mechanisms to detect and deflect intruders in the rare case that an outside hacker is trying to interrupt or hijack the setup process. A series of SecureEasySetup status messages keep the user informed every step of the way, as the following figure shows.



SecureEasySetup Wizard

Configuration Status

| | |
|---|---|
| Searching for SecureEasySetup Access Point | Found 00:13:10:0A:45:4A |
| Connecting to Access Point . . . . . . . . . . . . . . | Connection Established |
| Negotiating Security . . . . . . . . . . . . . . . . . . . | Secure Tunnel Established |
| Configuring Wireless Network and Security . . | Configuration Saved |
| Establishing Secure Connection . . . . . . . . . . | Secure Connection |

Figure 6: Easy-to-follow status messages keep users informed during SecureEasySetup installation.

During setup, SecureEasySetup establishes a strong, hard-to-crack WPA security key that is used to ensure the privacy of all subsequent network communication. Users tackling manual setup, on the other hand, may opt for pass phrases that are easy for them to remember – and thus make their home network more susceptible to discovery by dictionary-based, password-cracking bots created by hackers. To establish strong WPA encryption without SecureEasySetup, a user would have to take the time to create and enter a wireless network ID, or SSID, and a long passphrase.

SecureEasySetup is the best consumer option because it makes network setup simple without compromising security (designed for the non-technical home user), securely enables WPA, and is interoperable with a host of consumer devices that will display the SecureEasySetup logo. SecureEasySetup is supported by leading network device suppliers in the consumer market. To ensure simple push button setup, look for the SecureEasySetup logo on the devices/packaging to be connected. Networked devices that do not have the feature but support WPA can be added to the network and secured manually.

## Summary

The reasons for securing home Wi-Fi networks are apparent. And yet, the vast majority of consumers can't or won't activate the security that is built into their wireless hardware. Fortunately, new features such as SecureEasySetup are cropping up on wireless LAN hardware to simplify security setup.

With SecureEasySetup, implementing WPA – the best home Wi-Fi security option available – is a snap. Instead of navigating pull-down menus and entering key codes, consumers merely press the setup button on the access point and then click on a corresponding icon on their computer screen. Printers and other network peripherals may feature a physical setup button. That's it. The network does all the work to establish the Wi-Fi connection, as well as the security needed to protect network traffic.

Consumers looking for Wi-Fi hardware that is a breeze to set up and protect should look for products from both Linksys and HP with the SecureEasySetup logo on store shelves beginning this summer.

### Using SecureEasySetup to Extend a Secure Network

SecureEasySetup makes adding and securing peripherals like wireless printers to an existing home network easy. And it is much easier than adding and securing a wireless printer that doesn't have SecureEasySetup.

Without SecureEasySetup, users need to set up and secure a wireless printer either by navigating a web-like interface on a nearby computer or by maneuvering through menus on the device's control panel. SecureEasySetup greatly simplifies this process.

First, users push the SecureEasySetup button on the Wi-Fi router, alerting it that a new device is about to be added to the network. Next, they push the matching button or select the corresponding menu item on the printer.

That's all there is to it. The Wi-Fi printer is added to the home network, and it is protected with WPA security.

Phone: 949-450-8700
Fax: 949-450-8710
E-mail: info@broadcom.com
www.broadcom.com
www.54g.org

BROADCOM CORPORATION
16215 Alton Parkway, P.O. Box 57013
Irvine, California 92619-7013