



The United States Internet Crime Task Force, Inc.
A Non-Profit / Government-Assist / Victim Advocate Agency

**A Guide For
Buffalo Wireless
Routers**

Securing Your Wireless Network Using WEP

Secure Your Network In Seven Easy Steps

- 1.) Attach the router to your computer
- 2.) Connect to your router
- 3.) Login to the router
- 4.) Access the "Advanced Settings"
- 5.) Change your SSID
- 6.) Change your wireless security settings
- 7.) Change the router password

Securing Your Wireless Network

Introduction

Welcome to the wireless age. Gone are the days of dial-up Internet and home networks that require many cables to be run throughout your home. A wireless network provides an unparalleled freedom to connect many of your own computers to the Internet, while also allowing for a convenient method of sharing files and printers among wirelessly connected devices. Although this type of networking is becoming a popular means by which many users are connecting technologies and transmitting data, the wireless network you depend on everyday may also become a hindrance if it is not properly secured.

Imagine an entire neighborhood of homes, many with wireless networks. Consider that each wireless network is probably sharing a connection to some sort of high bandwidth Internet access. Assuming that 90% of all of these homes have unsecured wireless networks, anyone with a wireless connection card can connect to a multitude of devices in different homes with access to each Internet connection and possibly to all of information stored within each computer. In the wrong hands your wireless network can be a staging point for an infinite amount of potentially destructive activities.

Since each user's network is inherently different, wireless routers often come packaged with all of the embedded security features turned off. Even more, most routers come with default passwords that can easily be found in the Internet manuals published by each router's manufacturer. In knowing that these specific conditions exist, someone can gain access to your network and in most instances you may never notice.

However, viruses (especially worm viruses) travel through networks and infect unsecured devices without malice. The effects of one devastating virus on only one of your computers can cost you all of the information you once had stored on the infected device. Predators also lurk on the Internet and thrive on performing various criminal acts on unsuspecting users, and sometimes even preying on children. Crimes committed via the Internet are often traced back to the originating Internet connection, sometimes leading the authorities back to an innocent household with an unsecured wireless network that has been misused by someone else in the area.

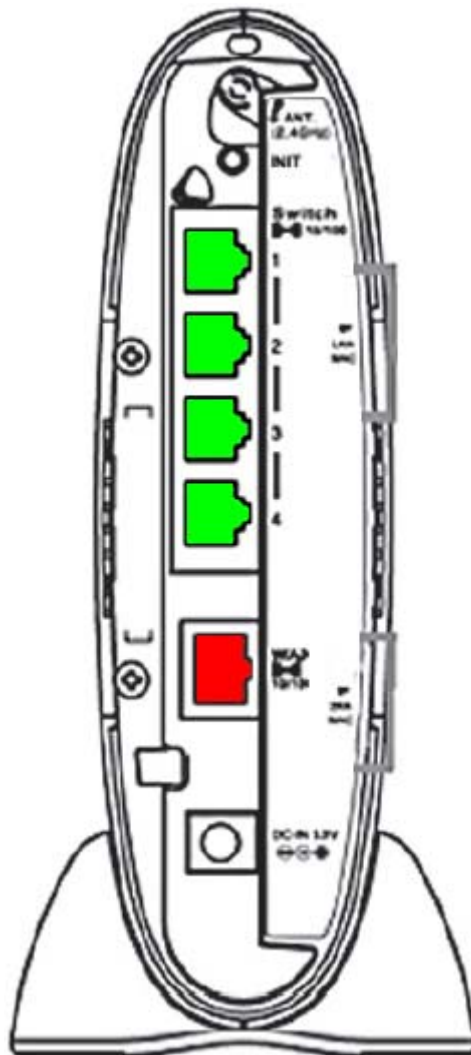
Many reasons exist for simply taking a few moments to secure your wireless network. In the following segments you will be guided, step-by-step, through the process of implementing the necessary restrictions on your router. For more information on this and other technology concerns, keep checking in with the United States Internet Crime Task Force, Inc. at www.usict.org.

Securing Your Buffalo Wireless Router

Note: This document is based on the Buffalo WBR2-G54 wireless router owner's manual, which can be found at www.buffalotech.com. Since many of Buffalo's wireless routers have the same (or similar) user-interface, this series of instructions can be used as a guide for most of the Buffalo routers on sale at the time of this publication. If your specific router cannot be configured using this set of instructions, please go to your manufacturer's web site for model specific instructions, or browse the United States Internet Task Force, Inc. website at www.usict.org and follow the instructions for your corresponding device manufacturer.

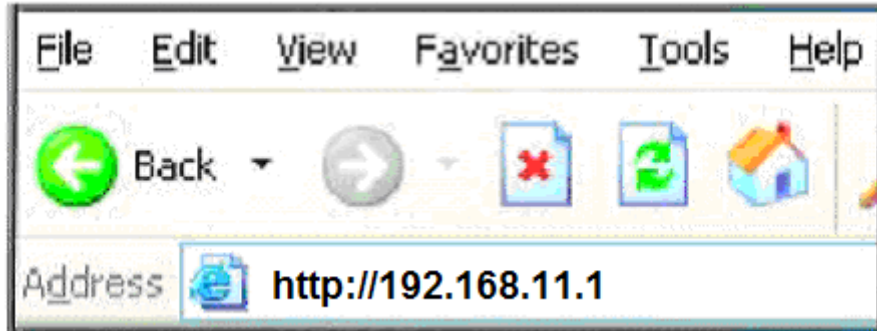
Step One: Attach your wireless router to your personal computer.

Simply take an Ethernet (network) cable and plug it into any one of the open ports on your router, except for the one marked "Internet". Attach the other end of the cable to the back of your computer in the network card (or NIC, which stands for Network Interface Card).



Step Two: Connect to your router.

Open your Internet browser and type the following in the address bar: 192.168.11.1



Step Three: Login to your Buffalo router.

Once the connection is completed a login screen will appear. By default the router has no password name. Simply type "root" in the blank next to "User Name" and leave the password blank, then click on "OK".



Step Four: Access the advanced setting of the router.

A screen will now appear with three buttons. Click on the "Advanced" button (highlighted green).



Step Five: Change your SSID.

Your SSID (which stands for Service Set Identifier) is a code that gets attached to each piece of data (or “packet”) that will identify the information you send or receive as part of the network. When your computer displays wireless networks that are available for connection, the name of each network shown is the SSID. If you leave the SSID at the default setting (the AirStation’s MAC address) then other users may know which type of router you are using, which may leave your security at a disadvantage. From the main screen, choose “LAN Settings” from the tabs along the left side of the screen. Then choose “Wireless”. Type a name for your SSID in the “Custom” blank (highlighted green in the example). Click “Apply” when you are done.

Note: Another very basic method of security includes turning off the router’s broadcasting of your SSID. This can be done by removing the check next to “Broadcast SSID” in the previous screen. Doing this will make your wireless network “invisible” to other wireless users, but it does not mean that your wireless network will be impossible to find. If you wish to stop your SSID from being broadcast then you will have to manually specify which SSID each of your computers will connect to, as your network will not appear in the standard wireless network discovery wizards that come with Microsoft Windows or Apple Macintosh computers. For the purposes of this document, the steps will go in accordance with the SSID broadcasting active (enabled).

BUFFALO **AirStation**
Wireless LAN Access Point

▲ Basic Settings

LAN Settings

- Wireless
- Wireless LAN Security
- LAN Port
- DHCP Server
- Wireless MAC Filtering
- Wireless Bridging

WAN Settings

Network Settings

Management

Logout

Wireless Settings

Wireless Radio ?	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Wireless Mode ?	Mixed ▾
SSID ?	<input type="radio"/> AirStation's MAC Address <input checked="" type="radio"/> Custom <input type="text" value=""/>
Wireless Channel ?	Channel 11 ▾
Privacy Separator ?	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
BSS Basic Rate Set ?	Default ▾
Frame Bursting ?	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
802.11g Protection ?	Enable ▾
DTIM Period ?	1
Wireless Output Power ?	100 ▾

Step Six: Change your wireless security settings.

Under the “LAN Settings” tab, choose “Wireless LAN Security”. Set your “Data Encryption” to WEP. The key your wireless devices will use can be derived one of two ways. You can either type your own HEX keys in the blank next to “Key 1” (hexadecimal keys use only letters A – F and numbers 0 – 9). Another type of key is ASCII. With ASCII keys, you can type a word or series of numbers into the blank for key 1. The keys you create have to be manually input into each computer that connects to your network. Write down the keys you create for future reference. The keys you create have to be manually input into each computer that connects to your network. Write down the keys you create for future reference. Click “Apply” when you are done.

The screenshot shows the Buffalo AirStation configuration interface. The top header includes the Buffalo logo and 'AirStation Wireless LAN Access Point'. The left sidebar contains navigation tabs: Basic Settings, LAN Settings (selected), WAN Settings, Network Settings, Management, and Logout. Under LAN Settings, 'Wireless LAN Security' is selected. The main content area is titled 'Wireless Security Settings' and includes a 'Broadcast SSID' toggle (set to 'Enable'). Below this, there are radio buttons for 'Disable', 'WEP' (selected), and 'TKIP'. The 'WEP' section has a 'WEP Key' field with four keys (1-4) and a 'Data Encryption' dropdown set to 'WEP'. The 'TKIP' section has a 'WPA-PSK Pre-shared Key' field and a 'WPA Rekey Interval' set to 50 seconds. An 'Apply' button is highlighted at the bottom.

Note: While this manual calls for the use of WEP, there are other methods of wireless security. Specifically there are WPA (WiFi Protected Access) and WPA2 which are far better than using WEP. However, WPA and WPA2 are only supported on select devices, usually coupled with driver updates performed for each wireless connection card and operating system updates. Both types of WPA are only currently supported in Windows XP (and only with a patch).

Step Seven: Change your router’s administrator password.

Having completed the necessary security changes on the router by implementing WEP, only one other task will be required for completion. From the options along the left of the screen click on “Management” and then “Change Password. At this point in your configuration of the router it is vital to set an administrator password that is different from the password your router was packaged with. If you made the changes to WEP and did not change the password on the router, another user could very easily login to the router and get the keys required to access your network, in many ways defeating the purpose of the WEP configuration. In the first blank “Administrator Password”, type a new password and then retype the password in the second blank “Confirm Password”. Be sure to write this password down, or simply use a password that you are sure to remember. You will need this password every time you need to login to change a setting on the router. Click on “Apply” when you are finished.

▲ Basic Settings

LAN Settings

WAN Settings

Network Settings

Management

System Information

Change Password

Time Setup

Administrator Name and Password

AirStation Name ?	<input type="text" value="AP000740C66A8C"/>
Administrator Name ?	root (fixed)
Administrator Password ?	<input type="password"/>
	<input type="password"/> Confirm Password

Note: Choosing a password with a higher degree of complexity will also help to strengthen your security. To make a password harder to break, use a combination of letters and numbers. For example, the password “1234” is very easy to break in comparison to the more complex password “Unbr3akAB|3”.

References

Editor’s Note: The basic instructions and images in this document came in part from the Buffalo WBR2-G54 manual which can be found on the manufacturer’s website at www.buffalotech.com.

Buffalo Technical Support: (866) 752-6210 www.buffalotech.com/support

Wireless Security Information: United States Internet Crime Task Force, Inc.: www.usict.org.