

## Whitepaper

# Understanding Home Network Security

## *Creating and Maintaining a Secure Home Network*

### Executive Summary

There are countless dangers lurking on the Internet, and routers are equipped to prevent some, but not all, of them. While implementing a router's security features can enhance a user's safety while using the Internet, the fact remains that **the responsibility of Internet security lies mainly with the online behavior of the user**, whether he/she visits unsecure or illegitimate web sites, opens email attachments from strangers, or falls for the latest phishing scam. A combination of common-sense user behavior and software security on the router or computer can prevent almost all Internet misfortune, but the battle rages on, and the bad guys keep getting smarter.

### Security Options Offered by Many Routers

Most routers offer a **two common basic security features**. One of these is the **firewall**, which acts like a gatekeeper and decides which traffic can or cannot enter the network. Usually, a firewall operates like this: most new connection requests coming from the outside are denied, but new connection requests coming from inside the network are approved. The majority of firewalls are set up to block everything but email and Web access. Firewalls often fail when malware is cloaked to resemble Web traffic, which the firewall allows into the network.

The other basic security feature found on most routers is **NAT** (Network Address Translation). NAT hides the IP address of all devices within the home network. Only one address is visible to outsiders: the IP address your ISP provided. This protects the individual computers connected behind the router by keeping their actual IP addresses hidden from outsiders.

**According to security expert John Viega, “These technologies (firewall and NAT) make it extremely difficult for someone from the outside world to break in to your machine WITHOUT you doing anything. You generally have to do something that results in your infection.”**

Viega continues, “Stick your users behind a (router using NAT), and...the outside world won't be able to get at your machines unless someone on the network does something to infect your network.”

**Routers often feature other security options, as well.** Content filtering using URL keywords is one type: this allows the user to create a list of keywords. If any of the keywords appears in the URL of a particular website, access to the website will be denied. Denial of Service (DOS) protection is another common router security feature. DOS protection prevents DOS attacks, which flood a network with so many outside requests, regular data flow is severely limited or even stopped. DOS attacks are usually targeted at Web servers. Many routers also offer intrusion detection. Passive intrusion detection systems monitor the incoming flow of traffic and alert the network's administrator if a potential security breach is detected, while reactive systems respond by resetting the connection or reprogramming the firewall.

Above and beyond the previously mentioned security features are **more enhanced security options**. One of these is a Stateful Packet Inspection (SPI) firewall. An SPI firewall keeps track of network connections and is configured to recognize whether packets (a formatted unit of data) from a particular outside connection are legitimate or not. Only packets matching a known connection state are allowed; all others are denied.

MAC address filtering is another advanced security option, used mainly on wireless networks. MAC address are unique identifiers assigned to every networkable device (such as computers). MAC address filtering allows the user to create a list of MAC addresses that are either allowed (whitelisted) or denied (blacklisted) access to the wireless network. If a whitelist is created, only those devices with the MAC addresses listed will be allowed to access the wireless network. If a blacklist is created, all devices except those listed will be allowed access to the wireless network.

A third advanced security option is VLAN (Virtual Local Area Network). This option allows the router to create two or more local area networks, thereby isolating one group of devices from another. This ensures that sensitive data is not passed along to the entire network.

## Security Risks Outside of a Router's Control

Despite all of these security features, **there are many scenarios in which routers provide little protection.** For example, a network user may download a piece of malware unintentionally, whether through email attachments or unintentional downloads from un reputable websites. Web browsers are also vulnerable. For example, a web browser can be instructed to download and install malware on your computer while simply visiting a particular website (known as a "drive by download"). Another web browser vulnerability is DNS rebinding. In this attack, a hacker creates a legitimate website, such as "attackprevent.com." The user sees an advertisement online for attackprevent.com and goes to the site. Initially, the browser connects to the site in the normal manner, but then it is redirected, without the user knowledge, to an identical website by changing the server address. At this second website, the attacker is able to access the computer and possibly the router and other devices on the home network. **"Web browsers are massive pieces of code and they're bound to have security problems, no matter how hard people look,"** says Viega.

## Suggestions on Protecting the Network & Personal Information

### Suggestions for Router Manufacturers

So how do you protect your router and network? Router manufacturers can help out by doing these four things, which some manufacturers have already implemented in their latest designs:

- Require the user to change the default password upon initial GUI access
- Provide unique default passwords on each router
- Ensure the ability for Service Providers to retrieve/change unit passwords via TR-69
- If the router is wireless, make sure that WPA2 encryption is turned on with a unique password.

By simply ensuring a unique user name and password, many of the common attack methods such as UPnP Exploitation will be thwarted, as the attacker will not be able to gain access to the router's administrative GUI.

## Suggestions for Service Providers

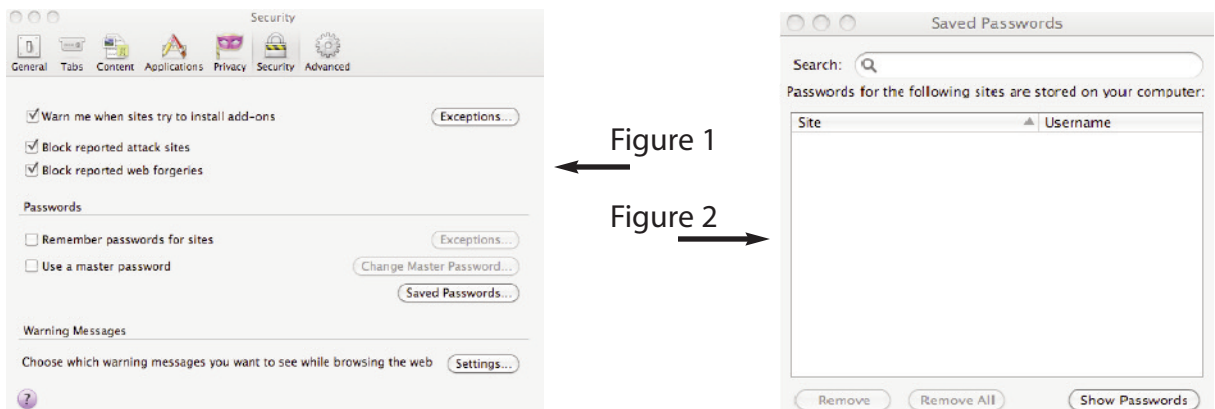
Service providers doing tech installs should be encouraged to change the default password on the router to something unique and leave a record of the new password with the user. Additionally, service providers allowing customer self-installs should encourage users to change the default passwords on all of their networked devices. Service Providers should also make sure that all of their major Internet access-related services, such as PPP, DHCP, and DNS servers, are upgraded and patched to protect against the latest known security vulnerabilities.

## Suggestions for End Users/Consumers

As for the user, there are several levels of security actions, that can be used to provide additional safety measures:

### 1st Level

Make sure you are using **unique passwords to access the router**. Also, make sure **your browser is configured so that it does not store any of your user names or passwords**. In the following two figures, we recommend not activating the “Remember passwords for sites” check box (as shown in Figure 1), and also making sure that no passwords are stored in the browser (as shown in Figure 2). Additionally, you might want to change the default LAN IP address scheme to something non-standard.



### 2nd Level

Make sure that all of your software is current and updated for the operating system, the web browser, and any plug-ins you might be using.

### 3rd Level

Use a software firewall on each computer connected to the Internet, such as Windows Firewall.

### 4th Level

Don't go to a website that you do not know. Use siteadvisor to determine if the site is legitimate or not. (Good sites are green.) Also, do not click on any email attachment if the email is from a corporation, even one you do business with, or from someone you do not know. Lastly, do not use any file-sharing applications.



### 5th Level

End users should consult with their Service Provider or Equipment Manufacturer to address any specific security concerns or for further suggestions on improving home network security.

Following these rules and using effective security systems can help you avoid compromising your network, but no system is completely invulnerable. As Viega cautions: "I don't believe that there is a 'silver bullet' for security..."

## About Actiontec

Actiontec Electronics develops broadband connectivity and broadband-powered solutions that simplify and enrich the digital life – delivering a unified experience that encompasses communications, entertainment, home management, and more. Actiontec offerings range from the market's broadest selection of IPTV-capable broadband home gateways for bringing IP-based video services into the home, to DSL modems, wireless networking devices, routers and digital entertainment devices. The company's carrier-class products are easy to install, manage, and use, and are sold through retail channels and broadband service providers. The company is committed to protecting the environment through energy efficient products and other green-friendly practices. Founded in 1993, Actiontec is headquartered in Sunnyvale, CA, and maintains branch offices in Colorado Springs, CO; Shanghai, China; and Taipei, Taiwan.

## Appendix: Resources and References

Active Defense: A Comprehensive Guide to Network Security by Chris Brenton and Cameron Hunt. 2001

Home Network Security Simplified by Jim Doherty and Neil Anderson. 2006

“Protecting Browsers from DNS Rebinding Attacks” by Collin Jackson, Adam Barth, Andrew Bortz, Weidong Shao, Dan Boneh. Stanford University. 2007

“Security Vulnerabilities in SOHO Routers” by Craig Heffner and Derek Yap.

The Myths of Security: The Ultimate Insider’s Guide to Network Security by John Viega. 2009