Multi State Information Sharing and Analysis Center

Briefing Paper

Keeping Your Broadband Internet Connection Secure

August 2007

Broadband Internet Security

Keeping Your Broadband Internet Connection Secure

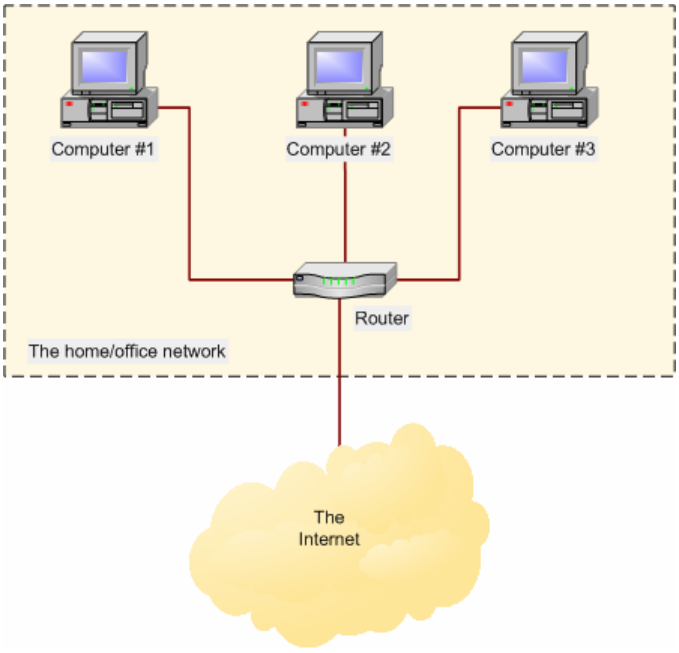
~ How to Prevent "Always-On" from Meaning "Always-Vulnerable!" ~

The Internet has become an integral part of life for many of us. Recent estimates indicate that the United States has more than 60 million broadband users. Many are individual home users using the Internet for a variety of reasons including accessing e-mail, shopping, banking, taking online courses, and more.

High-speed connectivity is becoming more prevalent with this increased Internet usage. Individual home users are the most highly targeted sector for cyber attacks, as they are generally less likely to have well-established security measures and practices in place. As such, they are much more vulnerable to identity theft, fraud and other cyber incidents.

Broadband – What is It?

Broadband Internet access is an "always on" connection to the Internet that allows a user high speed access. Simply put, broadband is a faster way for you to gain access to the Internet and the web sites or pages that you want to see.



Think of dialup connections like a garden hose. Only a certain amount of water can pass through it. Broadband is more like a fire-hose. More information moves through it in a shorter time.

Put more technically, the data rate of a broadband connection has information carrying capability in excess of 200 kilobits per second (Kbps) in both sending and receiving at the same time.

Broadband generally comes in three varieties:

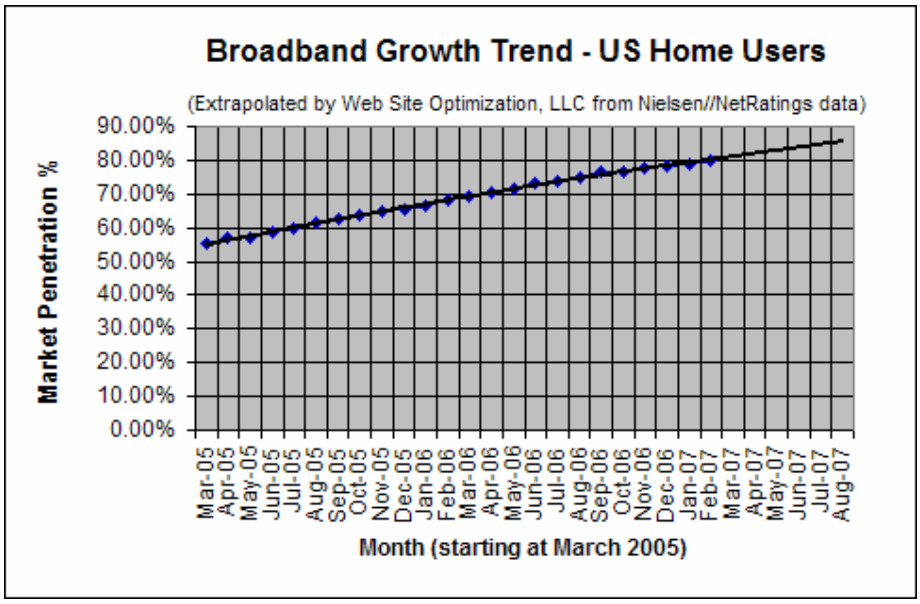
Cable - It is easily the most available and can be ordered through many cable television providers.

Digital Subscriber Line (DSL) - Available only through your telephone company, although DSL has some limitations as to where it can be installed.

Wireless - Often slower than either cable or DSL, and the costs are generally higher.

Broadband Use: Popular At Home

Millions of American homes are now using broadband connections. The broadband penetration rate for homes in the U.S. homes was 78% in 2006, representing a jump from 65 percent in 2005, according to a recent study.[1]



Broadband Adoption Growth Trend - Home Users (US)
Extrapolated from Nielsen//NetRatings data

Not only are more people using broadband, but they are also staying online longer while using their broadband connectivity. Broadband users spent 33% more time online than dial-up users.[1] Broadband users also viewed twice as many web pages. Games, instant messaging, e-mail and social networking were among the leading activities among high-speed users.

Security Risks of Broadband Connections – and Steps You Can Take to Minimize Risks

"Always on" connections offer greater speed and may enhance a user's online experience. But, they also pose increased risk to your computer. Because your computer is always connected to the Internet, it is possible (if not certain) that someone will try to access your computer without your knowledge or approval. This risk can be greatly reduced through proper security.

Below are some steps that can be taken to lessen the risks associated with "always-on" Internet access:

- **Use anti-virus software**. It's the best way to keep your personal information safe and your computer clear of malicious programs. Free anti-virus software is available from a variety of sources.

- **Use a firewall**. A firewall can block malicious access attempts before they reach your computer.

- **Do not open e-mail attachments** or click on links sent by unknown individuals. They may contain viruses, worms and spyware.

- **Keep your programs up-to-date**. If you don't, there may be vulnerabilities in your programs that may be used by attackers to gain control of your system.

- **Back up your data**. Any information that you have on your computer that may be important should backed up regularly.

- **Disable Java, JavaScript, and ActiveX, if possible**. There are risks involved in running Java, JavaScript and ActiveX provided by web pages. A malicious programmer could use these tools to deliver worms, spyware or virus. This type of vulnerability can be avoided by disabling all scripting languages. However, it will limit the interaction you can have with some web sites. To disable or limit scripting, open your Internet Explorer browser, select Tools, and Internet Options. Then click on the Security Tab. Select Internet for your Web content zone and click on Custom Level for that zone. Scroll down and set the security level to medium or high. If you do not understand the choice, place your mouse on an option and right-click to see the description of that particular option.

- **Disable Scripting Features in E-Mail Programs**. Many e-mail programs use the same code as web browsers to display e-mail messages to look like web pages. Vulnerabilities that affect ActiveX, Java, and JavaScript

are often applicable to email as well as web pages. Therefore, users should disable these features in their email programs. Go to your e-mail Options and set your Spam Protection and General Preference to block images.

- **Set your security settings.** Spyware or adware infection could have modified your computer security settings. To restore your settings, open Internet Explorer and access the Tools menu. Select Internet Options. On the Security tab, select the Internet content zone icon and set the security level setting to Medium or High. Next, click the Privacy tab and set the privacy level setting to Medium or higher. Clicking OK will close the dialog box to activate your new security and privacy settings.

- **Make a boot disk** in case your computer is damaged or compromised. A boot disk is a diskette from which you can boot your computer. Normally, your computer boots from a hard disk, but if the hard disk is damaged (for example, by a virus), you can boot the computer from a bootable diskette. You must, however, create this disk before you have a security event. You can create a boot disk by going to http://www.smartcomputing.com and clicking on Tech Support Center. Click the Backups & Data Recovery link and select Create Emergency Boot Disks and follow instructions.

- **Shut down your computer when you are not using your PC**. Intrusions can't happen when your computer is turned OFF.

[1] Nielsen/NetRatings