

Do you dream of downloading files off the Internet at blazing speeds, being able to easily check your e-mail, or playing the latest game across the Internet without slowing down? Well, the answer, to this question is broadband and approximately 18 million people in the US currently use it.

But is there any disadvantage to retiring your slow dial-up connection for a blazing fast cable modem or DSL line? For the most part, the answer is no. Broadband is far superior to a dial-up connection for just a few dollars more per month. The only real disadvantage to broadband is something generally overlooked by the average Internet user, i.e. security.

Every security problem associated with a broadband connection is not unique to broadband; dial-up users face the same security concerns. So why is security considered to be a "broadband problem" then? The answer is "bandwidth." The always on, high bandwidth, connection that cable modems and DSL lines give their users make them alluring targets for unscrupulous people more so than the slow dial-up connections.

Bandwidth is alluring for two main reasons. First, the simple fact that a broadband connection is always on makes it easier for malicious hackers to "find you" on the Internet. Second, few people actually utilize the full potential of their Internet connection all the time.

The security concerns

An unprotected computer system that is hooked up to a broadband connection is a sitting duck waiting to be victimized. Why? It has to do with the protocol that is used to connect to the Internet. Every device that connects to the Internet, e.g. computers, printers, PDAs and phones, is given its own unique address on the Internet. This is known as an IP (for Internet Protocol)

address. Your ISP, or Internet Service Provider, is responsible for "leasing" IP addresses out to you when you connect

does not give up its IP address as easily. Since you are always connected to the Internet, you must maintain an IP address, or your connection to the Internet is lost. Usually, broadband ISPs will periodically change your IP address. But this address change will not happen nearly as often as it does for dial-up users.

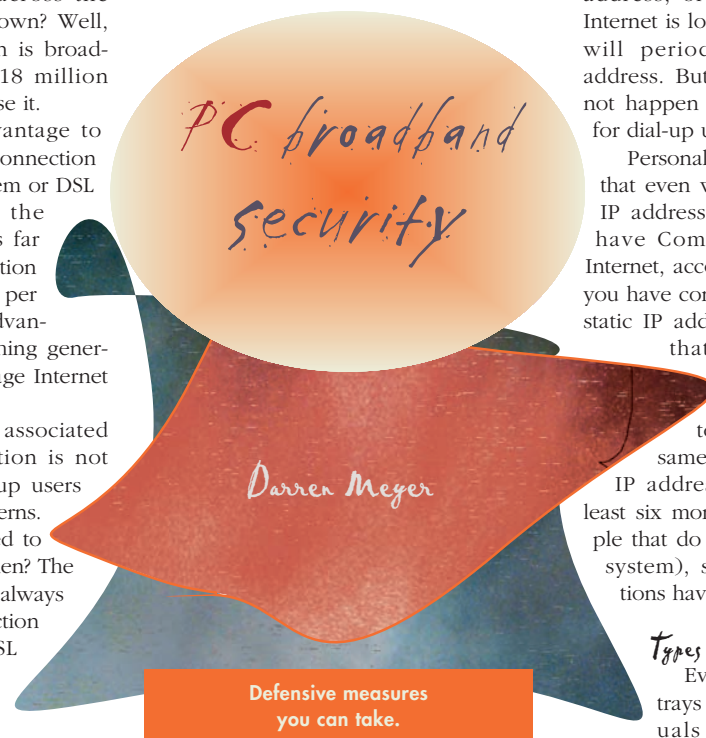
Personal experience has shown me that even when ISPs say they change IP addresses, they don't. I currently have Comcast (AT&T) Broadband Internet, according to their web site, "If you have configured your system with a static IP address, there is a possibility that when IP addresses are reassigned (as they are regularly), another customer will be assigned the same IP address." My system's IP address has not changed in at least six months. Even worse (for people that do not protect their computer system), some broadband connections have permanent IP addresses.

Types of attackers

Even though Hollywood portrays these folks as elite individuals who break into the Department of Defense's computer system to get missile codes to sell to terrorist nations. The truth is that most attackers are ordinary people in the computer industry and they are usually not looking for codes to start World War III.

On the web site <Extreme Tech.com>, Brett Glass lists three main reasons that your broadband connection may be a target. The first reason is your bandwidth. Hackers like high bandwidth connections because typically users are not pushing the limits of their connections. Therefore, the hacker's presence will likely go undetected.

As a result, the hacker/cracker may want your system to help launch a much larger attack, such as a distributed denial of service (DDoS) attack. This is



to the Internet. If a hacker/cracker finds your system a joy to work with, but your IP address changes, it will be harder to find/use your system again. But if your address doesn't change often, finding/using it again just increase the rapture.

With a dial-up connection, such as AOL (with a member base of over 34 million users), you connect via your modem and get an IP address. When you are done using the Internet, you return your IP address back to AOL for another person to use. The next time you connect to AOL, whether you reconnect in 5 minutes or 5 days, the chances of getting the same IP address are small.

A broadband connection, however,



an attack where the hacker takes over many computer systems and directs all the computers to send requests to a particular server at the same time. The goal is to overwhelm the attacked server and, thus, bring it down. Your bandwidth may also allow a hacker to use your system in a series of hard to trace attacks on other systems. In fact, it will look as though *you* are attacking the other computer system.

The second reason is that the person is after your computer's resources. A hacker could break into your system and use it as an Internet relay chat (IRC) server. This person is after your bandwidth, CPU processing time, memory, and other system resources. One resource that is attractive is your hard drive space. These folks have been known to take over a computer and store files on it, such as illegal copies of Microsoft Office, Microsoft Windows, or even movies! Because of the always on, high bandwidth connection that your cable modem or DSL line provides, uploading or downloading the files is not a problem. What's more, few people would notice the loss of bandwidth or loss of hard drive space, especially now, when even the cheapest computer typically comes with at least a 20 gigabyte hard drive.

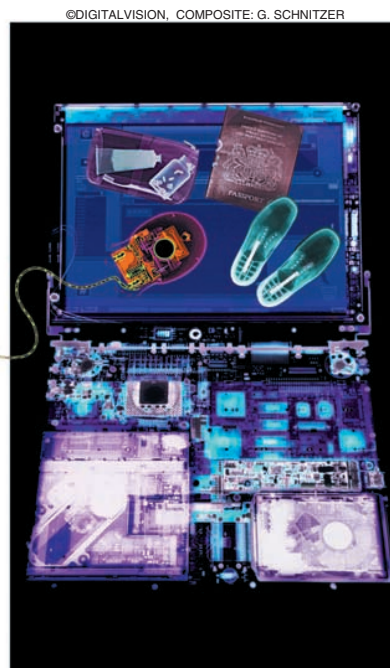
The third and last reason is what many of us equate to as being "hacked." Brett Glass lists "your personal data, your identity, your reputation, and/or the contents of your bank account" as the third item malicious hackers are after. This is the category that scares most of us. While some people may think that there is not any information on their computer that can be used, they are probably mistaken. If you have ever prepared your taxes on your computer, used online banking, paid a bill online, or just bought something from an online store, chances are your computer holds enough data for an evil hacker to access the personal information you want to protect.

While there are laws to protect you from identity theft, such as the Fair Credit Billing Act, identity theft can be detrimental to your life. Even if you are able to prove that you have been the victim of identity theft, it may take months or even years to completely recover all your losses.

Other threats that exist to Internet users include viruses, the threat that is most likely to affect you. According to Symantec's web site (the maker of the

popular Norton Antivirus program), there are over 60,000 viruses currently active. Along the same lines, there are Trojan horses. These are small files that try to hide their mischievous activities, typically anti-virus software will also search for this type of threat.

Finally, another threat that is becoming more popular is called "spyware." Spyware is software that is installed on your computer, unknown to you. Spyware will actually broadcast back to a web site information about what you have been doing. Even if it just reports what web sites you have visited, the damage can be substantial. (It could potentially provide sensitive data such as bank account numbers or social security numbers).



Actually, some people consider Internet cookies to be a type of spyware. Cookies are small amounts of data that are placed on your computer when you are browsing the Internet. There are different kinds of cookies and different privacy policies applied by web sites. Some cookies can be privacy-intrusive (obtain data associated to the user's identity) other cookies are anonymous. Almost every web site uses them. Cookies, if used intelligently, can capture trends about your Internet activity and used for marketing purposes.

Another way spyware can get on your computer is that you actually install it! Kazaa, a popular P2P (peer-to-peer) application for downloading

mp3s, actually installs spyware on your computer. While it is common knowledge that Kazaa does this, many people would rather have access to millions of files to download, then have to worry about a "little" invasion of privacy.

Steps to take

There are many steps that can be taken to protect one's system. Most are easy to do and cost little to no money.

Every time you check your e-mail you have the potential of downloading a virus along with your messages. Some viruses are so advanced they can be activated by simply browsing the Internet. So the first piece of software to install is some type of anti-virus software. The more popular ones include Symantec's Norton Antivirus and McAfee Security's VirusScan. These software packages are typically reasonably priced. Also, almost all, new computers come with some sort of anti-virus application pre-installed. If you don't want to shell out any money for anti-virus protection, you can even find 100% free anti-virus software on the Internet, such as AVG Anti-Virus System available at <www.grisoft.com>.

So you have installed the latest version of some anti-virus suite, you are now officially safe. Yes, for about a week maybe. This is a mistake that many people make. You must update your anti-virus software on a regular basis (at least weekly). Every anti-virus program has its own update that can be downloaded from the Internet; these updates are called "signature" updates. As new viruses are discovered, the company that makes your anti-virus software will make new signature updates available for download. Remember you are only protected from these new viruses if you actually update your software.

Here is a tip to save you some money; many makers of anti-virus software will make you pay an annual fee to download virus signature updates. This fee usually will allow you to "automatically" update your software by simply clicking on "update" from within the anti-virus program itself. If you feel energetic, though, you can simply go to the site of your anti-virus vendor and download the updates for free. It takes a little more effort, but it will save you a few bucks.

While having anti-virus software running on your computer is a great first step, it is only the first step. Typically, viruses are received via e-

mail and the user has to actually run the virus for it to infect a computer. Running anti-virus software is important, but it offers no protection against others snooping in on your computer. For protection from the outside, you must place a "firewall" between yourself and the outside world.

Firewalls

There are two types of firewalls that broadband users can install on their computer systems. The first type is a hardware firewall and the second type is a software firewall. Both types, if administered correctly, will keep people from being able to gain access to your computer through open ports. While no firewall is full proof, if a hacker finds two broadband connections, one with a firewall and one without, the person will go after the easier target.

If you are planning to share your broadband connection with others in your home or office, you will be well served installing a hardware firewall. Many of the most popular broadband routers have built in firewall protection, as well as other features such as built in DHCP (Dynamic Host Configuration Protocol)(stands for?) server functions. For example, most of the popular Linksys EtherFast series routers and D-Link Express Ethernet routers have a built in NAT firewall. NAT, which is short for Network Address Translation, will hide your internal LAN's IP addresses from the outside. Many of these firewalls also have port-filtering features. These filters will block outsiders from accessing your computer through many common ports, such as port 80, which is used for http, and port 21, which is used for ftp. You may even be able to block all incoming traffic.

The built in firewall that is found inside a cable modem router is probably enough security for the average home user. However, if you use a cable modem or DSL connection at your small business, you may want to get a full-blown firewall. A simple standalone firewall may sell for as little as \$150. The price can go up to several thousands of dollars for firewalls that will protect a corporate LAN. However, the companies that require \$10,000 plus firewalls are most certainly not using a cable modem or DSL connection. They would be using a T1 or better.

The other option for the broadband user is a software firewall. Most major anti-virus vendors also offer some sort

of software firewall, such as Norton Personal Firewall from Symantec Corporation or Personal Firewall Plus from McAfee Security. These firewalls can be quite useful, offering everything from port filtering to blocking certain IP addresses. They can also control what programs on your computer actually are able to access the Internet, such as blocking Windows from accessing the Internet in the background without your knowledge.

One major advantage that some software firewalls have over the built-in NAT firewalls found in broadband routers is logging. Logging is an important security feature that will allow you to view what IP addresses have been hitting your computer, what IP addresses have been blocked by your firewall, and what IP addresses have passed through your firewall. These logs can be especially useful if you feel you have been attacked; your ISP may be able to track the attacker down by using the logs created by your firewall.

Counter-spyware

By installing both anti-virus software and a firewall, you are a well-protected broadband user. However, there are still other measures that can be taken to protect your self against spyware. According to Steve Gibson, spyware is any software that uses a back channel connection to the Internet without the user's explicit permission. Steve Gibson is responsible for a program called "OptOut." It informs you when a back channel is being used and allows you to cancel the back channel connection and remove the spyware.

Another popular program that protects against spyware is Ad-Aware by Lavasoft. This program will scan your computer for known spyware and remove it. But be careful, removing some spyware may leave other software unusable. You may be forced to reinstall the damaged software.

Two important tools

Finally, installing firewalls, anti-virus software, anti-spyware software, and any other form of security measure must be combined with two other important tools, common sense and understanding. Do not randomly open executable attachments from anyone, even if you know them. Getting an executable attachment should send off warning flags, the same as if you

received a package in your mailbox that said "BOMB" on the side of it. Practicing common sense will protect you from many threats, especially viruses. You must also use common sense when surfing the Internet. This facet includes always making sure that you are using https (secure) connections whenever you purchase anything online, and only dealing with known, reputable companies.

You must also arm yourself with understanding. Keep up with the current virus information. Know what the likely subject line of an e-mail containing a virus will be. It may keep you from opening a potentially damaging attachment. You must also understand how to administer your firewall correctly; otherwise, you may as well not even have one. Luckily, most home firewalls have easy to use interfaces, explaining what each feature does. Also, it will not hurt you if you actually read the instruction manual. This way you can intelligently decide what features you want to turn on and which to turn off. A little time and effort up front can lead to your computer being a safe environment and more importantly, save you time, money and frustration in the long run.

Read more about it

- D-Link Home Page. <http://www.d-link.com>
- "Internet Security". AT&T Broadband Website. <<http://help.broadband.att.com/security/SecurityIndex.jsp>, (Web page is no longer available)
- "Got Broadband? You're Under Attack". ExtremeTech.com., <<http://www.extremetech.com/article/2/0,3973,23886,00.asp>>, Brett Glass, June 12, 2001
- Lavasoft Home Page. <http://www.lavasoft.de>
- McAfee Security Home Page. <http://www.mcafee.com>
- OptOut Home Page. <http://grc.com/optout.htm>
- Symantec Home Page. <http://www.symantec.com>

About the author

Darren Meyer is a Program Analyst at Magnetrol International, located in Downers Grove, IL. He holds a BS in computer science from North Central College in Naperville, IL. In his spare time he coaches track and field at Downers Grove South High School and enjoys rooting for the Chicago Cubs. Contact him at darren_meyer@hotmail.com.