



MIKE HALE
S H E R I F F

(205) 325-5900 www.JeffCoSheriff.net

IDENTITY THEFT: Firewalls & Computer Safety

By ITRC Staff
Compiled by Linda Foley, Executive Director, ITRC
Copyright August 2003, all rights reserved

Identity Theft Resource Center
P.O. Box 26833, San Diego, CA 92196, 858-693-7935
Email: itrc@idtheftcenter.org Web: www.idtheftcenter.org

This copyrighted document may be copied for personal use only. The text of this document may not be used or altered without express authorization of the Identity Theft Resource Center, other than for personal use. This fact sheet is an information source and should not be considered professional advice.

DIRECT CONNECTIONS TO THE INTERNET: Protecting Yourself Against Intruders

Today people use the Internet to see what movie is playing at a nearby cinema, shop, do homework, pay bills and even for banking. For many of us, email has not only taken the place of postal mail, but also telephone calls. There is an increasing group who has direct connections to the Web through cable modem or DSL, which means you may be hooked up 24 hours a day, 365 days a year.

There is one major drawback to being hooked up to the Internet that many of us have either overlooked or are not aware of. Some Internet Service Providers (ISPs) are neglecting to tell you just how vulnerable you are to being hacked.

The Internet is like the rest of the world. It is populated with the same kind of people society deals with on a daily basis, including criminals and those who wish to create havoc and chaos. It used to be people would get a kick out of hacking a company's homepage or Website in order to change some graphics. The object was to simply to prove you had the skill to "break into" another computer. Today, computer and database breaches have become more criminally focused.

Leaving your computer hooked up to a direct connection without firewall protection software is like leaving your house unlocked all the time. Worse yet, you have a sign hanging out front saying, "Come on in!" When you are connected to the Internet, you literally have access to the world. What some people forget is that this is not a one-way mirror. If you can see out, that means anyone on the Internet, with the right program, can see into your computer as well. Not only that, but they can plant a program into your computer so that they can access it not only at that very moment, but in the future as well.

Once a thief gains access to your computer, they can gather all the personal or sensitive information you have stored on the hard drive unless your information is securely encrypted. Social Security Numbers, credit card numbers, bank account information, your budget, and your electronic tax returns - any and all are up for grabs. Identity theft is on the rise, and these pieces of information are the keys that imposters seek. Leaving your computer openly connected to the web without firewall protection, be it via software or hardware, is just asking for trouble.

DEFINITIONS:

Virus: A virus is a program that reproduces itself by infecting other programs on the same computer. Viruses can do serious damage, including erasing files or an entire hard drive. Others may just do silly or annoying things such as popping up in a window that says, "Ha, ha, you are infected!" Viruses are transferred by electronic contact and usually are attached to a data file. You send it to a friend or coworker by sending a file or an email that contains the virus. Typically you need to open an infected file to activate the virus.

Worm: Like a virus, a worm is also a program that reproduces itself. Unlike a virus, however, a worm can spread itself automatically over the network from one computer to the next without attaching itself to another file. Typically worms do not destroy a computer or files. They just take advantage of automatic file sending and receiving features found on many computers. However, a worm can send a virus through your computer to others using this auto-send feature.

Trojan horse: Trojan horse attacks pose a serious threat to computer security. The name comes from the hollow, wooden horse the Greeks used to smuggled soldiers into the fortified city of Troy. In today's computer world, a Trojan horse is a malicious, security-breaking program that is disguised as something benign, such as a screen saver, game or joke. It might send itself to everybody on your email address book or IRC channel, erase or modify your files or download another Trojan horse program designed to steal your passwords. Many Trojan horses also allow hackers to take over your computer and "remote control" it. Trojan horses have become more sophisticated in recent years, as hackers use them to scan your system for vital information (credit card numbers, SSNs, bank account numbers), and use the retrieved information to open accounts, run up huge credit card debt, or drain the bank accounts of unsuspecting victims.

Trojans can be spread in the guise of literally anything people find desirable, such as a free game, nude picture, MP3 song, etc. You might have downloaded the Trojan from a website or file transfer without even knowing it. That is why it is important to always know what you are downloading and who is sponsoring the program.

Hacker/Cracker: When used properly, this term refers to an elite breed of "good guys" who are talented computer programmers. They enjoy solving challenging problems or exploring the capabilities of computers. Like a carpenter wielding an axe to make furniture, the hacker does good things with his skills. True hackers subscribe to a code of ethics and look down upon the illegal and immoral activity of crackers (defined

above). When the press uses "hackers" to describe virus authors or computer criminals who commit theft or vandalism, it is not only incorrect, but also insulting to true hackers. The correct term for a hacker that uses this skill for criminal purposes is "cracker."

Firewall: A firewall is a device, either software or hardware driven, that enforces an access control policy between two networks. A PC connected to an ISP, for instance, represents a bridging of two networks. A firewall can be thought of as a pair of guards: one blocks traffic and the other permits traffic. Some firewalls place a greater emphasis on blocking traffic, while others emphasize permitting traffic. The most important thing to recognize about a firewall is that it implements an access control policy. That means you have control over what program or website is allowed to mingle with your computer. Even if you are unsure as to what kind of access you want programs or websites to have to your PC, it is vital as a cable modem or DSL user that you employ a firewall. Most firewalls manufactured today come with pre-set recognitions of those popular programs that most folks tend to have on their PCs, and therefore take much of the guesswork out of a user having to determine what programs should communicate via the Internet (and either send or receive information) or not. Even dial-up Internet users, should they be of the sort who remain online for hours on end, should have some sort of firewall protection, just in case. For such folks, there are a good number of free firewall programs available to suit their needs.

Software-driven firewalls: A software firewall is okay for one computer connected to the web. Windows XP includes a limited firewall. You probably should consider adding an extra level with another program as well. There is an excellent free software firewall available from www.zonelabs.com/zonealarm. It is easily configured and can be tailored to meet your needs. There are many others but at this time (Aug 2003), Zonealarm still ranks as the best free program.

Hardware-driven firewalls: If you have a small home network (two or more computers) you should look at a hardware-based firewall. A hardware firewall is vastly superior to software solutions because a computer running Firewall or other protection software is still visible on the Internet. There are several good ones available. D-Link makes a Cable/DSL Router which has a configurable firewall built right into it. The D1-701 looks like your computer on the Internet to hackers and it hides your real computer. Like a decoy, it stays visible so any attacks will be directed at it. The only thing the hackers see is the router, and they can try to hack that all they want. This should prevent damage to your expensive computer, as well as protect valuable personal information. Routers cost \$400 to \$500 dollars just a year ago. You can now pick one up like the D1-701 for less than \$100. If you would like to read more about the D1-701 go here: <http://www.dlink.com/products/broadband/di701/>

HOW TO PROTECT YOURSELF:

- Install a firewall to protect your information. Remember that your ports are open doors that allow traffic in and out when your computer is connected to the Internet. Many people believe that if the company they shop with or bank with is protected, their own PC is protected. That couldn't be further from the truth. You still need to put a firewall around your PC to keep crackers and hackers out when you are online. This has nothing to do with the transactions you do with a bank or merchant. When your computer is online it can be tapped by anyone at any time, completely separate from the transaction you have just completed. Crackers can see any part of your hard drive: your tax records, the account numbers you placed in the computer for record-keeping, your bank information, even your letter to Aunt Mary.
- Install reputable anti-spam and anti-virus software. Most reputable anti-spam software programs today are also programmed to identify known viruses, which could contain Trojan horses as well.
- Keep your anti-virus, firewall and operating systems updated. Run an update at least every two weeks. You may need to do this more frequently if there is an alert about a particular virus. If you see a "time to update" notice sent by the supplier of your operating system, do so.
- Be certain of BOTH the source AND content of each file you download! Don't download an executable program just to "check it out." If it's a Trojan, the first time you run it, you're already infected! In other words, you need to be sure that you trust not only the person or file server that gave you the file, but also the contents of the file itself. Remember that a virus or Trojan horse might cause your friend's computer to automatically send you the questionable file. In general, there is no reason for even a friend or colleague to send you an executable file. When in doubt, ask them first. Be aware that "free" programs or spam might also contain a troublesome file. If you download commercial games or other software from unknown shareware sources or "spam," it's just a matter of time before you fall victim to a Trojan.
- Be cautious of dealing with pop-ups. This is a perfect place to plant a virus or Trojan program. You never know who wrote the program or that person's intent.
- Beware of hidden file extensions! Windows by default hides the last extension of a file, so that innocuous-looking picture "susie.jpg" might really be "susie.jpg.exe" - an executable Trojan! To avoid being tricked, unhide those pesky extensions .
- Don't be lulled into a false sense of security just because you run anti-virus programs. Many of anti-virus programs do not protect against all viruses and Trojans, even when fully up-to-date. You need both virus protection and firewalls programs to be fully protected against identity thieves.



- If you are an online multi-gamer type, do not publish your I.P. address on websites or newsgroups, unless you are very sure that you are fully protected. You would be much better off logging into others' game servers, than inviting others to log onto your game server at a precise I.P. address.
- Backup your system! One of the best ways to protect yourself in the result of a virus attack is to have a clean set of backup disks/tapes/CDs that will fully restore your system (without the virus) and the applications you are using. Too often, home computer users fail to protect themselves in this manner. With CD burners and accompanying software being relatively inexpensive, a full system backup can quickly restore your computer in the event that your hard drive has to be reformatted.
- Turn off your computer when not in use. If you are not connected to the Internet, you cannot be infected, hacked or hijacked.
- Use common sense. When in doubt, assume the unknown attachment is a virus. Pay attention to virus alerts. Don't even consider trying to outsmart those who have created these malicious programs. Reconsider storing personal information in your computer. Transfer it to a CD and use the CD when you need the information. This is especially true of passwords, SSNs, tax and financial records.

In closing, jumping on the direct connection bandwagon can be safe and fun as long as you protect yourself adequately from unwanted intruders by using either a software or hardware firewall, practicing safe techniques and keeping virus protection updated. For further information on firewalls visit the following links:

- <http://www.firewallguide.com/>
- <http://www.howstuffworks.com/firewall.htm>
- <http://www.greatcircle.com/gca/tutorial/bif.html>