Protecting Your Computer: Part 2 - Firewalls

January 10 2006

by Philip Dunn **[** Part 1 **]**
While rather new to computing in comparison to antivirus programs, in today's Internet connected world firewalls are actually more important.

A firewall is a barrier between your computer and the outside world – be it other computers on a network or the Internet.

To communicate with other computers, your software is equipped with thousands of virtual ports. These ports or communications channels allow different programs to communicate with each other. Each program looks for a response on a specific port.

For example, port 80 is used by your web browser "see" pages on the Internet. Popular chat programs often use port 1214. Some file sharing programs use port 6385. Each program is different and some are

configurable as to which port they use.

Understanding these ports exist is more important than knowing which one each program uses, however. Unfirewalled ports are constantly listening for attempts at communications from other computers.

Hackers know this and often scan the Internet for computers with listening ports. Once found, they initiate communications and quickly – a matter of milliseconds - gain full access to your computer. This process is completely automated and hackers can scan thousands of computers in less than an hour.

Once connected, they can do virtually anything you can - read files, install programs – mostly viruses and worms - and even monitor your keystrokes. Keystroke monitoring is dangerous because it allows them to capture your passwords and credit card numbers. Worms are used to infect other computers.

The best defense against this is to block access to these ports. When a hacker scans a firewalled computer, he gets no useful information to carry out an attack. The ports are closed.

In response to this defense, hackers have devised clever programs that you must install to get around the firewall. This leads us to the firewalls second role: blocking outgoing communications from your computer.

When you install any new program that tries to access the outside world, the firewall will inform you of this activity and ask you what you want to do: allow or deny access.

Programs can receive for two types of access: client - outgoing communications only and server – two-way communications. Programs that need to register themselves via Internet often ask for client

permission. Chat and file sharing software need server access to work properly.

Be very careful about giving server access to any program. This access can allow the software to modify your system, see files on your hard drive and install software. If you're not sure, deny access to the program. If the program continues to work properly, it does not need internet access.

Programs that fail to work require that you adjust the firewall to allow access. Some firewalls, like Norton Internet Security, scan your computer during the install process and give the appropriate permissions automatically. If not, try to discover what privileges the program needs. Does it need to access the Internet? Is two-way communications required? Give the lowest possible permission to allow it to function – you can always adjust it later if needed.

One good way to find out what a program is doing is to Google it. If it's a virus, somebody has discovered it already.

Firewalls can be chatty at times, constantly warning you of outside attacks. These messages can be turned off or ignored. Rest assured its doing its job. Most messages are generated by harmless routers and web servers.

Remember that firewalls protect you from all other connected computers, not just ones on the Internet. This can cause headaches when connecting your computer to a local area network at you home or office. Good firewalls, like Zone Alarm, normally detect the new networks and ask for permission for access. If you wish to allow print and file sharing, give server permission, if not, give client permission – enough for web browsing, for example.

If you are on an organized network at work, you may be protected by a proxy server with a hardware firewall and a proxy server - ask your network administrator.

Don't even think about connecting your computer to the Internet until you are sure a firewall is installed at some point between you and the Internet.

Firewalls, like antivirus programs, need to be kept up to date. They normally do this in the background automatically. Still, it's a good idea to check them and make sure they are loading at startup and updating automatically.

Windows XP version 2 has a built-in firewall that, although not the best, is enough to protect you from most common attacks.

Experts recommend more. Get a dedicated firewall like Zone Alarm (free at www.zonelabs.com) or Norton Internet Security (www.symantec.com) – which also includes its famous antivirus program.

[Protecting your Computer: Part 3 – AntiVirus][/