BY HON. JEFFERSON LANKFORD

Firewalls: Protection from Hackers

Hon. Jefferson Lankford is a judge on the Arizona Court of Appeals, Division I.

The need for protection from hackers—computer intruders—is greater than ever. Hacking seems to be a favorite pastime for a whole generation of tech-savvy teens. Leaving your computer unprotected is like leaving your car in a public parking lot with the doors open, the key in the ignition and the engine running: It invites mischief.

Although all computers connected to the Net are exposed, many people have increased their vulnerability with broadband (high-speed) Internet services. Broadband leaves the Internet connection "on" at all times, creating an open pipeline for hackers. (Turning off your computer protects you even when the connection is open, and it's a good idea to do so whenever you're not using it).

A firewall is a barrier against intruders. The simplest type—and sufficient for home computer use—is software that analyzes incoming and outgoing data and blocks or allows its transfer. The software applies "rules" to block or allow data. Firewalls also can alert the user to suspected intrusions, provide the intruder's IP address and record the details in a log file. The log enables users to report intrusion incidents to their Internet service providers.

Amazingly, competent firewall software is now free; that protection cost $50, $100 or more not long ago. Although neither ARIZONA ATTORNEY nor this column endorses software, reviewers often recommend **Zone Alarm**, available free for personal use at **www.zonelabs.com.** Businesses can evaluate the same software free on a 60-day trial and purchase it at modest cost.

> Don't give the hacker a chance to see your client's confidential documents.

Tiny Personal Firewall is a similar program available from **www.tinysoftware.com** (click on "products" from the home page). Also known as TPF, this too is free for home use and costs less than $40 for businesses.

And this software is easier to use than older firewalls. The user can choose a "ruleset" by designating a desired protection level from among several options.

The firewall's protection rules can be customized to suit the user's particular needs. Customizing those rules can be challenging. You may need a type of connection that the off-the-rack rulesets block. For example, online gamers and users of ftp (file transfer protocol) software may need to tell the firewall to allow the connections needed for those functions. That forces you to distinguish potentially malicious transmissions from those that are helpful or even essential to connectivity. Deciphering information such as "FTP Port 21 Source 107.233.421.56," required for some firewalls, may be daunting.

Fortunately, help is available in configuring the firewall. Even makers of free firewall software may reply to requests for help in installing or configuring the software. Your Internet service provider also may help you determine which types of connections (called "ports") are necessary.

Don't give the hacker a chance to see your tax files, your investment portfolio—or your client's confidential documents. Get a firewall and lock hackers out of your computer.

Questions or tips about the Internet? E-mail them to sidebar@cox.net.

These resources are complemented by more and better information on the Net about firewalls. For example, you can find straight, helpful and non-technical talk about firewalls at

www.firewallguide.com.

The site also offers reviews of software and links for downloads. Another worthy site with firewall tests, links and how-to's for installing and configuring numerous firewall programs is

www.firewall-net.com.

For a better understanding of how firewalls work, a basic explanation appears at **www.securityfocus.com/infocus/1182,** and a much more detailed one at **www.interhack.net/pubs/fwfaq.**