

Exploring The Need For A Firewall

What are they?
Where do I get them?
How much do they cost?
Do I even care?



Let's answer that last question first. Yes, you had better care. And, we'll add that it doesn't matter how much they cost because you had better care about what they can do for you; and by the way, you need one.

Before we continue with this discussion, here's a little background on the subject. Since we began this column in *Agency Sales* last September, we've received a number of requests related to problems/questions that our readers face with the technological tools they use to run their businesses on a daily basis. One subject we've frequently been asked about relates to computer firewalls. A surprising number of reps indicate they didn't know what they were — although they've heard of them — or how important they could be.

What better place to get a few

answers on the subject than with a MANA member who knows about them. According to Drew Elliott, CPMR, CSP, "Everyone with a computer needs a firewall!"

Elliott, Demo Sales Co., Portage, Michigan, who writes a tech column for the North American Representatives' Association's (NIRA) newsletter, explains that "Firewalls keep outside, unwanted influences from poking around your computers, your server or network. Those outside sources can steal personal and business information, implant viruses or set up a 'zombie' type of arrangement where your computer winds up sending out viruses."

Blocking Hackers

Elliott is hardly alone with his cautionary words. MANA-associate member Bill Perry, PerTel

Communications, Inc., Mission Viejo, California, notes, "The firewall sits between your computer and the Internet and it fends off direct probes into your computer. The probes I'm talking about come from hackers and others who can pose a threat to you and your business." Perry's business helps representatives post and maintain their line card on the Internet as well as increase productivity by solving rep e-mail, computer, database and programming problems.

Perry continues that Internet users that make use of a fast connection with either a DSL connection or a cable modem, are especially susceptible to the problems such connections can bring. Among the problems he describes are somewhat of a worst-case scenario "where an external user or other type of hacker can take con-

trol of someone's computer, use it as a clone, and ultimately execute a denial of service or some sort of blackmail attack."

The business press, not to mention various sites on the Internet, go on at length concerning the types of attacks that Internet users can find themselves susceptible to. Among the more common problems that can accompany Internet use without the protection afforded by a firewall are:

- **Denial of service** — As already detailed by Perry, this type of attack is nearly impossible to counter. What happens is that a hacker will send a request to the server to connect to it. When the server responds with an acknowledgment and attempts to establish a session, it cannot find the system that made the request. By flooding a server with these unanswerable session requests, a hacker causes the server to slow to a crawl or eventually crash.
- **Spam** — As detailed in previous articles in *Agency Sales*, spam is relatively harmless but always annoying. However, it can be dangerous. Often it contains links to various web sites. Users should be wary of clicking on these because they may accidentally accept a cookie that provides a backdoor to your computer.
- **Viruses** — Who among us haven't received virus warnings or a virus itself. A virus is a small program that can copy itself to other computers. It can spread quickly from one system to the next. They range from harmless messages to being able to erase all of your data.
- **E-mail bombs** — Usually this is a personal attack. Someone sends you the same e-mail hun-

If there are any subjects that you feel should be explored in Tech for Reps, or if you have any comments about this subject, please contact the Tech Talk editor at: alaplante@MANAonline.org.

dreds or thousands of times until your e-mail system cannot accept any more messages. According to Perry, sometimes the attack persists until the victim acquiesces to the hacker's demands.

- **SMTP session hijacking** — This is the most common method of sending e-mail over the Internet. By gaining access to a list of e-mail addresses, a person can send unsolicited junk e-mail (spam) to thousands of users.
- **Remote login** — This is when someone is able to connect to your computer and control it in some form. This can range from being able to view or access your files to actually running programs on your computer.

If we've defined what a firewall is, what it does and why it's important, what remains is for the Internet user to take action. According to Elliott, "I assume people are already making use of virus software, the most common of which are Norton and McAfee. Both of them, which are easily attainable and relatively inexpensive, have firewall service. In addition, most wireless routers have a firewall built into them. Windows XP also has a firewall that should be activated at all times."

Additional Help

Both Elliott and Perry note, however, that sometimes assistance is needed in this area beyond that which is provided in a commercially available product.

When that need arises, Perry urges that the "Internet user seek out someone who is aware of your computer use and the needs of an independent manufacturers' rep." He cautions, however, that "there are a lot of people, including high school students, who do what I call 'finger-pokin,' and they aren't looking out for your best interests. You need to work with someone who is technically astute. Sure, you can install a firewall yourself, but if a problem develops, you'd better make sure you find someone who can truly help you."

A couple of other areas he suggests are seeking recommendations from a network of cooperative reps in your area, such as through a MANA local networking chapter. In addition, he points to an organization he joined in Southern California (www.SMBTN.org) that can provide recommendations. "Users should seek similar organizations in their territories."

Following up on those suggestions, Elliott mentioned seeking help from the IT department of a local community college or even hiring an intern for your company that has some IT experience.

In any event, both men suggest taking action. As Perry says, "It's important to take the time now to fix something that could turn into a major problem. If you don't do something now, you could conceivably have to pay someone to reload your entire operating system, and that's very expensive in terms of time and money." □