CPA
Practice Advisor

If you are not yet concerned about hacking, the most recent news from the world of Network Security may not bother you. But it scares the hell out of me.

Consider a couple simple points:

1. A sustained cyber attack was launched last fall against hundreds of commercial websites and government sites, successfully penetrating the security of those systems and wreaking havoc on our ecommerce and defense systems.
2. Law enforcement services successfully shut down a hacking network that in just 30 days penetrated 2,411 corporate computers, ripping from them all sorts of individual and corporate details of financial records and passwords.

We've heard stories like this so often that it has almost become like the "Boy Who Cried Wolf." After all, these are sophisticated hackers who have powerful skills and would never bother with small and mid-range companies, right?

Wrong.

The Internet underground has advanced to the point where anyone with $325 and even basic computer skills can hack their way into corporate data systems and steal critical information.

Here's the problem, according to security firm SecureWorks: There is a powerful, simple-to-use hacking program called 'ZeuS' — usually used as a 'Trojan virus' against banks — that is readily available on criminal forums.

Current versions of the ZeuS hacking tool sell for up to $10,000, and are used by elite cyber gangs to wire funds from the online banking accounts of small- and medium-sized businesses to their own accounts. But older, free versions of ZeuS work just fine for turning an infected PC into a bot and harvesting all the PC's account logons that

obediently harvest, according to SecureWorks.

In today's economy, that is a powerful inducement to become a hacker and try to probe corporate networks. Not the ones operated by the big guys, who are likely to have sophisticated security departments. But the smaller companies, like the ones most accountants have as clients. Amateur crooks may already be at work plundering your clients of their cash. And because we refuse to believe they can do it more easily than ever before, they may well get away with it.

So how does an accounting firm protect itself and its clients from these attacks? The answer lies in four fairly simple precautions, though it is amazing how often these are overlooked or ignored. Here they are:

> **1. Use a firewall to filter all Internet traffic and email.** For smaller offices, this means using not only the firewall built into your security software (Norton, TrendMicro, Microsoft, etc.), but also checking to see that these are set at a high enough level to do the job. All too often, users will turn down or turn off this protection because it interferes with browsing some sites. For larger offices that have their own routers and servers, make sure that the router firewalls are operating, and consider using an industrial-strength firewall device (such as the Barracuda devices) to elevate the level of protection.
>
> **2. Protect your email as well.** Antivirus protection for email can be awkward because it does slow down some operations. You're just going to have to live with it. It is vital that every incoming message is scanned, every attachment is scanned, and every outgoing message is scanned. If your email provider does not also scan all email passing to your computers, switch vendors to finds one that does.

3. **Turn off your workstations every night.** I know this runs contrary to

viruses and Trojans and should be banned on work computers for that reason. The rules should be simple but strictly enforced: No shopping sites for personal shopping, no social networking sites, no adult content, and no personal email to the work email account. Employees who break the rules put the entire company at risk, and should be disciplined accordingly.

You have every right to be scared about what is going on in the hacker world today. But that fear is only useful if it provokes a healthy response — protecting the firm from hackers, watching for their incursions, and moving swiftly to get help if your system is ever hacked. A few simple rules are a good place to start.

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.