New!

The Rules of Internet Security

When it comes to a secure computer network, there are certain truths that seem so irrefutable that any company would be a fool to not follow them. So, am I a fool – *yes*! Why? My network was attacked a couple of months ago.

The theory as to why we suffered this "brute force attack" was that I had recently changed the administrator password and had made access to our system too easy. Hackers have programs that go out and ping all online servers to bust into networks that have easy passwords and holes. We had 50-60 holes in our system, relatively a lot considering we only have seven or eight folks online at any one time.

After the hackers got in they installed a mass mailing program that only could be detected by file size, not by name. It was very clever and well hidden. Then they uploaded 113,000 e-mail addresses and proceeded to send out spam via our server. It took AOL about three to five days to shut us down and blacklist us. It took another three to five days to get off the blacklist. I knew something was wrong when all of our e-mails were getting kicked back via these "blacklists." My clients didn't appreciate this at all. If this ever happens to you, it can be undone, but it takes a lot of effort, is a big hassle and costly.

Jack, my favorite Information Technology guru, says that 60% of such attacks, worms, viruses, etc., come from Russia, Korea or China. He suggests that all networks be audited several times per year using audit programs that can trace, track, and discover inconsistencies. It took him a good three hours or so of auditing to find the mass mailing program and figure out we had been attacked because the data was so well hidden. Here are some of Jack's tactics for best practices for securing your computer network:

- **Avoid** all risky web-browsing behavior. Surfing to gambling or porn sites can get your network hacked.
- Password security is important. The **more complicated** the better.
- Permanent passwords are risky. Pay attention to **password expiration.**
- Keep your antivirus and spyware components **current.** (My personal favorite spyware components are AdAware and SpyBot 1.4.)
- Invest in a reliable **hardware firewall.**
- Allow only your **most trusted** individuals remote access to your network. Use firewall VPN clients if possible, and use encrypted RDP sessions to your network if you have SSL certificates on your server(s).
- **Do not** use POP3 mail. These transmit passwords and usernames in clear text. Use RPC/HTTP mail (128 bit encrypted) instead.

continued on page 71

>> By Cathy Costarides, LS

Costarides, *continued from page 72*

- Be careful about letting **guests** plug into your network. Make sure they have up to date antivirus clients.
- **Delete accounts** of former employees, vendors, consultants when they no longer have business needs to access your network.
- Do not allow employees to download software from the network unless it is approved by the company. This is one of the biggest holes I see in most networks. Remember, the **computers belong to the company,** not the employee.
- When you get up from your computer press Control, Alt, Delete and **lock the machine** so a password will be required to use it again.
- **Do not share passwords** or write them on sticky notes attached to your monitor, keyboard, etc.
- Be careful of people **standing behind you** when you type in your password.
- Do not open attachments from people you do not know before **scanning them for viruses.**
- **Do not shop** on the Internet during business hours. Most of these sites are reputable, however some may not be.
- Let employees know that if their computers get infected, hackers may gain access to the network, **causing downtime for the company** (and possibly lessening the likelihood of a raise!)
- Put company policy regarding computers **in writing.** Security can only start with senior management.
- Do not click on any "warning" that claims your computer has been infected and if you "click here" then everything will be okay. **Doing so may install spyware** – *not* anti-spyware.
- Finally, when it comes to your network – **paranoia is good.** Everyone is out to get you. Remember this.

Many of these suggestions are just good common sense. You may also want to find an IT guru like Jack in *your* neighborhood and tattoo his phone number on your arm. All the best!

Cathy Costarides is president and owner of both CC Land Surveyors, Inc. and SurveyingZone.com. Licensed in Georgia since 1992, she has been surveying for 25 years as well as designing residential and commercial projects.