Cyber Attacks on Small Businesses

Computer hacking has become front-page news lately, but many small business owners assume that because they’re small potatoes, have a firewall, and use anti-virus software they’re immune to a cyber attack. They’re dangerously wrong.

And what’s striking are the kinds of businesses that have been hit: small manufacturers, building contractors, credit unions, hotels, diners and restaurants, coach and limo services, trucking companies and law, accounting and venture capitalist firms. In other words, if you have a website, you’re vulnerable.

Over the last five years there have been 78 major cyber attacks and tens of thousands of small ones against American business, government and educational organizations. Sony just spent $170 million mopping up after the PlayStation disaster. Security experts agree that a cyber 9/11 is likely; indeed, some say the only reason it hasn’t happened already is lack of terrorist leadership. What’s more, there’s evidence that foreign-made computer components are being manufactured to make it easier to launch cyber attacks.

This is precisely the reason that SCORE and the Small Business Development Center are trying to help small businesses in the area to deal with this looming threat by offering a workshop session on June 19th. This is designed to give small businesses practical help to secure their company’s data.

In the meantime, here are a few of my tips that you can do to help secure your business and mitigate loss if (when?) you're the target of a hacker attack.

Use strong passwords and change them regularly
Build the passwords you use, a different one for each log-in, with a pattern that you can remember without writing them down. Small businesses often have high turnover, and that means they need to change passwords regularly to prevent a former employee or contractor from logging in and reading e-mails or mining your system for customer information.

Fear E-mail attachments
You know those cute pictures and interesting PowerPoint presentations people send you? They’re one of the most common ways bad guys pass around computer viruses. And just because an e-mail comes from someone you know, doesn’t mean it they actually sent it. A lot of e-mail addresses have been stolen lately and you really can’t be sure. Be particularly suspicious if the e-mail is sent to a long list of strangers.

Update anti-virus signatures
Anti-virus programs look at the contents of a file and search for a specific pattern of characters known
as a virus signature. When a new threat crops up, anti-virus program companies create an updated set of virus signatures. Make sure your program is set to update automatically.

**Back up, back up, back up**

If a hacker ruins your computer system or website by destroying software, files, or folders, you have to recover quickly. Can you cope for several days while your systems are repaired and information is rebuilt manually? Backups are your best insurance against intruder attacks (or a natural disaster). Especially when you keep copies off site.

**Make sure you have insurance coverage**

Cyber risks are not covered by standard property and casualty policies. Cyber insurance, however, is available to cover privacy and security liability, crisis management, business interruption, denial of service, lost income, cyber extortion and media or Web content liability.

Nine of 10 businesses have been the victim of some form of cyber crime. If yours hasn’t, you’re lucky. Or could it be you just don’t know yet?

____________________

Dean L. Swanson  
Southeast Minnesota SCORE  
c/o Rochester Area Chamber of Commerce  
220 South Broadway, Suite 100  
Rochester, MN 55904  
*Dean is a volunteer SCORE Mentor and District Director of SCORE Minnesota*