Security Basics For Small Businesses

The news has been filled for several weeks with the security breach of some large companies. Could that happen to your small business? From what I hear and read, small business is now a prime target of hackers and data thieves intent on stealing credit card and other sensitive information.

Think you aren’t vulnerable or that it can’t happen to your business? Think again. Major credit card companies now estimate that 95 percent of data theft they uncover happens at the very smallest businesses that accept credit cards (and thus have customer credit card information; if only briefly). In fact we have seen reports that a small business could have been the source inroad to the Target security problem.

The data theft divisions of Verizon (which operates data transmission networks) and the U.S. Secret Service, which investigates cyber crimes, saw data theft reports at small businesses jump 400% last year.

The reason is simple: Hackers find small businesses to be easy targets. Even a local hair salon, pizza shop or dental office has names, addresses and credit card data. And with more small businesses now storing information electronically, the opportunities for data theft have soared. And it will get worse before it gets better.

The problem is tricky because it takes so many different forms. One common hacker tactic is to plant malicious software programs called “malware” on small business computers. These programs, sometimes sent to employees as email links or attachments, can steal information and send it undetected over the web. Point-of-service credit card terminals are an increasingly common target as well.

Daniel Kehrer, Founder & Managing Director of BizBest Media Corp., is a nationally-known, award-winning expert on small and local business. I respect his work and insight. He shared the following ways to protect your business:

- **Keep security software up to date:** If you do nothing else, installing (or updating) the latest versions of anti-virus and anti-spyware software will provide some protection.
• Use a secure wireless connection and a good firewall: Many small businesses use unsecured wireless networks. That’s asking for trouble. The old standard, known as WEP, is useless. What you need is WPA2 Encryption, the current standard in data protection.

• Segregate your sensitive data: The fewer places your sensitive information is stored, the less you have to worry about. For example, credit card information should be segregated from other data and from your network as well.

• Revise and rethink your passwords: Many small businesses are victimized by data theft and other computer crimes simply because they have weak passwords. Change passwords regularly, and use strong ones that are not predictable. Some experts suggest using three-word or more password “phrases.” These can actually be easier to remember and quicker to type.

• Don’t leave computers unsecured: Require logins for all computers and laptops, and set them to return to the login screen after five or ten minutes of inactivity. Only download or install applications that come from trusted sources.

• Avoid direct connections to the Internet: Many small businesses don’t have networks or routers and simply plug directly into the Internet. But business owners can block many common threats by using a quality router, such as a Netgear or Buffalo brand router and making sure to change the router password from the default setting.

• Upgrade security policies and email standards: In this age of social media it’s more important than ever to set policies and standards on what types of information can be shared online. And many businesses still treat email as confidential communication, which it isn’t. Think of emails more like postcards, and not sealed letters.

• Protect tablets and mobile devices, too. Mobile phones, iPads and similar devices should also be password protected and kept in secured storage when not in use. Avoid storing any sensitive data on these devices.
Use a secure SSL connection for sending or receiving data: Secure Sockets Layer (SSL) is an encrypted Internet connection for sending data safely over the Internet.

Get help: OnGuard Online (www.onguardonline.gov) offers practical tips on computer security from tech specialists. SANS (www.sans.org) is one of the world’s most trusted sources for information security training.

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