



Susan-Says® Protect Your Business From Cyber-Sabotage.

By: Susan Wilson Solovic, CEO SBTV

Many small business owners believe their computer network is too small and uninteresting to be targeted for a cyber-attack. Nothing could be farther from the truth. Cyberspace saboteurs often look for small, unknown companies with less sophisticated security systems as an opportunity to test their skills before they move on to more challenging systems.

“Small and medium sized companies typically don’t have the budget or resources to retain full-time security and audit personnel on staff, which sets the stage for information compromise, hacks and intrusions,” explains Glenn Miller, CEO of Countermeasures Information Security, Inc..

Known as computer hackers, these cyberspace criminals use unauthorized access to systems for the purpose of stealing and corrupting data. According to a report published by E-Commerce Times in 2000, hackers cost U.S. corporations \$266 million in 1999 which was double the losses suffered the previous three years.

To protect your firm and the integrity of your customer’s information:

First, make sure your small business has an antivirus system and that it’s up-to-date. New viruses emerge daily so regular updates help ensure these new viruses will be recognized. And you should install firewalls which create a protective wall between your computer and the outside world. They work by filtering out unauthorized or potentially dangerous types of data from the Internet. Firewalls also ensure unauthorized persons can’t gain access to your computer while you’re connected to the Internet. Laptops should have their own firewalls if you use Wi-Fi connections at public places such as airports, hotels and coffee shops. Finally, most experts recommend installing an intrusion detection system. This type of program will notify you when someone has tried to tap into your network.

Create a password policy for your company to minimize the risk of unauthorized users accessing your system. Set up separate passwords for all your databases and require your employees to periodically change their passwords. Passwords should be at least eight characters with both upper and lower case letters. However, even inexperienced crackers can obtain programs to help them easily identify your password so make them difficult to guess.

Notwithstanding any provision in any documents available here, you are permitted to download an entire, unchanged copy (including any copyright notice and author attribution) to a computer and make a print copy of internal use.

This material is intended to provide a general overview and does not purport to provide all specific requirements for any person. MasterCard provides this material AS IS for the convenience of its members and cardholders.

“Don’t choose words that apply to your pets or your hobbies,” says Suzanne Magee Joyce, president of Techguard Security. “Try using words that aren’t commonly found in the dictionary and ones that are unrecognizable. Include numbers and punctuation marks for greater protection.”

Back up your data regularly and store it on a removable media. This should include your file registry which contains all of the settings and operating instructions for your computer. File registries are a common target for attack. A popular type of backup device is called a tape backup unit, or tape drive. A tape drive puts your data on a tape that resembles a standard music cassette tape, which you can then take with you and put in a safe place.

Consistently re-evaluate your computer protection systems. “You need to determine if the strategies you have been using are working successfully. But you also need to know what advances have been made and keep up. Malicious hackers don’t stop. They keep evolving their art so when it comes to the security of your computer system, you have to do the same thing,” explains James Joyes, Chief Technical Officer for Techguard Security.

Make sure you keep your software is updated. Hackers like to find and exploit bugs and loopholes in popular software products. Some do it for money, some to make a statement, some simply to cause trouble. And they can cause trouble - exposing customer credit card numbers on a Web site or stealing passwords in a computer. The impact on a business can be fatal.

Finally, never open emails from an unknown source. Sounds like a simple rule, but because most viruses are spread via email, it doesn’t hurt to remind ourselves and our employees. Even if you know the person sending you an email, you should exercise caution if the message seems strange and is unexpected, particularly if it contains unusual hyperlinks.

For more information on protecting your business go to:

<http://www.sba.gov/beawareandprepare/cyber.html> or

<http://www.microsoft.com/security/default.msp>.

Notwithstanding any provision in any documents available here, you are permitted to download an entire, unchanged copy (including any copyright notice and author attribution) to a computer and make a print copy of internal use.

This material is intended to provide a general overview and does not purport to provide all specific requirements for any person. MasterCard provides this material AS IS for the convenience of its members and cardholders.