A One-Page Expert Guide from Ramon Ray

Editor & Technology Evangelist, Smallbiztechnology.com

8 Tips to Protect Your Business and Secure Its Data

As I learned in the Federal Bureau of Investigation Citizens' Academy that I graduated from, the digital hackers of 20 years ago often hacked into computer networks for the pure pleasure of showing off. However, today's hackers hack for the same reason their peers in traditional thievery steal: to steal money from someone. Sometimes they work alone, often they work in online gangs (or hacker groups or rings), and a growing number of them are backed by governments.

Digital thieves are constantly on the lookout for data to steal—personal information, financial records, intellectual property, or whatever valuable data they can get. They may then use this data to steal money from bank accounts or to set up credit cards, or they may simply sell the personal information to a third party. Your task is to do all you can to protect your precious business data from them. Your network, computers, mobile devices—you must protect everything from their attacks.

Remember that security is only one half of complete protection. It's vital that you also implement a proper backup strategy for your business. Security is great for keeping hackers away from your data, but if your data is corrupted or lost, how can you recover it? You can only recover it if it's backed up.

Here are eight simple things you can do to protect your business data:

1. Conduct a security audit.

If you don't know what parts of your business are vulnerable or what data you have that needs to be protected, you can't properly secure it. It is critical that you work with a professional to audit your entire IT infrastructure—computers, network, and mobile devices—to determine what you need to do to prevent hackers from accessing your network.

2. Make staff aware of the important role they play in security.

Your staff are your front line of defense when it comes to security. Sure, hackers can access your network remotely and siphon off data without setting foot in your office. However, vigilant employees (consultants, partners, and vendors, too) can ensure that human error—which is a big cause of data security breaches—is minimalized.

3. Use strong and multiple passwords.

Too many of us use simple passwords that are easy for hackers to guess. When we have complicated passwords, a simple "dictionary attack"—an attack by a hacker using an automated tool that uses a combination of dictionary words and numbers to crack passwords—can't happen. Don't write passwords down; commit them to memory.

4. Encrypt your data.

Encryption is a great security tool to use in case your data is stolen. For example, if your hard disk is stolen or you lose your USB thumb drive, whoever accesses the data won't be able to read it if it's encrypted.

5. Back up.

Security is important, but if your data is not backed up, you WILL LOSE IT. Ensure that your data is properly backed up, and test the backup to ensure that your data can be recovered when you need it.

6. Have security policies.

It's one thing to ask employees to work securely, but you must also have clear and simple policies in place for them to follow to ensure that they are working in a secure environment. For example, insist that all notebook computers connected to the corporate network have security software. Mandate that NO security information ever be given over the phone. Policies like this and more will help ensure that your staff are doing their part to be security aware.

7. Protect your mobile work force.

Your sales team of 10 years ago is probably nothing like your sales team of today. With the proliferation of the BlackBerry, iPhone, and other mobile devices, more of your staff are working away from the office—and away from the protection of your network security. They are operating "in the open" on your customers' networks, public networks at coffee shops, or free networks in the park. It is important to ensure that their mobile technology, often connected wirelessly, is as secure as possible.

8. Implement a multiple-security-technology solution.

Viruses that corrupt data are not the only security threat. Hackers, and their attacks, are more sophisticated than ever, and it is critical to have multiple layers of security technology on all your different devices (including each desktop, mobile device, file server, mail server, and network end point) to comprehensively secure your data. This multiple security will block attacks on your network and/or alert you to a problem so that you (or your IT expert) can take the appropriate action.

Securing your business's data is not easy, and it takes expertise. However, you can implement very practical and simple solutions (such as these tips) to ensure that when a hacker sniffs around your network or computers, he (or she) will move on to another victim—because your infrastructure is not worth the trouble of hacking into it. Think about your average street mugger. They want to steal a purse or wallet from the victim they think is most vulnerable, so they can get away with their crime as easily as possible. One of the most important things you can do is to educate your employees in security best practices and ensure that they know how important their role is in securing business data.

Ramon Ray is a Technology Evangelist with Smallbiztechnology.com and author of *Technology Solutions for Growing Businesses*.

Ramon is not "just" a technology writer, but, as a former small business technology consultant, he has years of hands-on experience in building networks, installing software, upgrading computers, and supporting the technology that small businesses use on a daily basis. He has written thousands of technology articles and news items for Smallbiztechnology.com and other media, including *Inc. Magazine*, *New York Enterprise Report*, *Black Enterprise Magazine*, *CNet*, *VAR Business*, *TechTarget*, *Entrepreneur.com*, *Small Business Resources*, and others.