5 SIMPLE STEPS FOR INTERNET SAFETY

Businesses today are always looking for ways to improve their access to information. The quicker information is received and processed the better we are able to efficiently run our business. To this end, internet use has become the easiest and quickest way to process and maintain information. Along with this convenience however, there needs to be a discussion about how to manage the risks associated. Many smaller business owners assume that large corporations are more vulnerable to internet security threats. However, it is often the other way around. Because they have a false sense of security and assume theyôre not at risk, many small business owners do not adequately protect their computers and networks from spy ware, viruses, worms and hacker attacks. Computer safety is usually far down on the to-do list. Small and mid-sized businesses need to take the most basic security precautions, such as installing antivirus and anti-spy ware.

Fortunately, there are plenty of ways to protect your business from internet security threats. These are five questions that should be asked when looking at internet security.

Have a full understanding of the security you need vs. what you currently have. The good news is you probably have more than you think. Most local area network routers include a built-in firewall that blocks intruders from accessing the computers network.

Have the basics. At a minimum, all your business computers should be protected by a hardware or software firewall and antivirus and anti-spy ware protection program.

Does computer security seem like a complicated and time consuming task for you to handle? If so, hire a consultant to perform a security audit of your business systems and network making recommendations on improvements that may be needed.

Have a detailed written security plan that includes policies and procedures as well as technology requirements. This is particularly important for businesses that have employees. If a plan is written it is not so easy for an employee to dispute or disregard.

Regularly update my internet security. New internet threats are cropping up daily. Your security solutions will not be effective if they are not updated. Fortunately, most software is automatically updated but a plan must be in place to make sure.

A secure network provides businesses with benefits beyond protection from internet threats. Inherently, a security network is a foundation that can support new technologies and reduce operating costs.

Along with securing your network there are best practices that can be put into place to protect your identity and information. Along with the convenience of banking, shopping and interacting online comes the ease with which other people can now steal your information. Here are a few strategies to mitigate this risk:

Don’t use lazy passwords. Come up with longer passwords that contain both letters and numbers/characters preferably one that references something significant only to you.

Read the fine print. When signing up for, installing, and/or agreeing to anything. This is a way to avoid being put on telemarketing lists or to receive junk mail.

Control the information you are sharing. Only negotiate with companies and persons that you know. The more information you give out the more you could become vulnerable to identity theft.

Be aware of online scams. Be careful of spoof emails claiming to be from the bank or companies that you trust. These reputable companies will not ask for personal or sensitive information.

While the internet provides a convenient and easy way to do business it also comes with greater risk and responsibility. Ultimately, when your business is secure, itôs stronger and more agile, and definitely, more competitive.