

DON'T UNDERESTIMATE ONLINE RISKS TO YOUR SMALL BUSINESS

As your business grows, so does your responsibility to protect it.

As your business evolves, so do the online security risks you face. Small businesses are no less vulnerable to online threats than large businesses are; however, the staff and budgets of many small businesses are already stretched to the limit, and security may not be given high priority. But it should. Investing in Internet security now can protect your business' reputation and save you time, money and grief in the long run.

Consider these recent findings:

- In a 2004 survey* of American businesses, 78 percent of respondents reported having experienced a virus outbreak. Viruses can cause nagging problems like slow system performance, or worse, destroy customer, accounting, or project files.
- According to the National Cyber-Security Alliance, 90 percent of PCs connected to the Internet have some form of spyware installed on them. Spyware poses a risk to businesses by enabling external sources to monitor a user's or business' activity without consent.
- As much as 65 percent of all email traffic in 2004 was spam, according to the Symantec™ Brightmail Probe Network. Sorting through spam is a daily time-waster, impacting employee productivity.

Online threats pose a wide range of risks to your business, including hardware damage, altered or lost business data, and even loss of customer confidence due to a missed deadline or a virus-infected email sent from your business. Some threats are simple nuisances that cause distractions, but do no tangible harm. Others can bring business to a halt for hours and even days, destroying critical business data in the process.

The days when antivirus software alone provided sufficient protection are long gone. However, the good news is that many of the preventative steps you can take won't cost you a dime. By implementing the following security practices, you can help protect your information:

- If you haven't already, install antivirus software on all desktops, laptops, and servers to prevent virus infection and keep the antivirus software updated. Some antivirus software will also provide spyware protection. Be sure you have antispyware on all systems that use the Internet.
- Use a firewall on all desktops, laptops, and servers to block intruders. A good firewall will make your computers invisible to external threats.
- Keep current with operating system and security software updates to ensure you have the latest protection.
- Create strong passwords with at least eight characters combining alphanumeric and special characters. Change passwords every 45 to 60 days.
- Open email responsibly. Never open attachments from unknown senders. Don't respond to spam.
- Enable the security settings on your web browser and do not enable file sharing.
- Back up important data regularly and store extra copies offsite.
- Secure all remote computers with antivirus and personal firewall software. Evaluate the benefits of a virtual private network (VPN) to provide a private "tunnel" via the Internet to your business that helps keep communications secure.
- Secure wireless connections with a VPN and install firewalls.
- Follow routine security precautions, from setting up a screen saver password in Windows® with your display options to locking down laptops with a cable.

**Source: 2004 CSI/FBI Computer Crime and Security Survey*