

Recommended Security Practices for Small Businesses

Small businesses face the same online threats as large corporations. Whenever you and your employees are online, your business is exposed to security threats. By implementing these recommended security practices, you can help protect your information.

- **Install antivirus software** on all desktops, laptops, and servers to prevent virus infection.
- **Use a firewall** on all desktops, laptops, and servers to block intruders.
- **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 45-60 days.
- **Open email responsibly.** Never open attachments from unknown senders. DO NOT respond to spam.
- **Enable 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) that provides a private “tunnel” to your business.
- **Secure wireless connections** with a virtual private network (VPN) and install firewalls.
- **Follow routine physical security precautions** by using a screen-locking feature to lock down laptops with a cable.

Reference: www.symantec.com/small_biz1