



CYBERSECURITY TIPS FOR SMALL BUSINESS OWNERS AND OPERATORS

TIP CARD

DID YOU KNOW?

- In 2012, 50% of all targeted cyber attacks were aimed at businesses with **fewer than 2,500 employees**.¹
- Nearly one-third [31%] of all cyber attacks targeted businesses with **fewer than 250 employees**, the largest growth area for targeted cyber attacks in 2012.²
- **Forty-four percent of small businesses** reported being the victim of a cyber attack, with an average cost of approximately \$9,000 per attack.³
- Nearly **59% of U.S. small and medium-sized businesses** don't have a contingency plan that outlines procedures for responding to and reporting data breach losses.⁴

SIMPLE TIPS

1. Make sure all computers within your organization [including those used off-site] are equipped with antivirus and antispyware software. This software should be updated regularly.
2. Secure your Internet connection by using a firewall, encrypt information, and hide your Wi-Fi network.
3. Establish security practices and policies to protect sensitive information; educate employees about cyber threats and how to protect your organization's data and hold them accountable to the Internet security policies and procedures.
4. Require employees to use strong passwords and to change them often.
5. Invest in data loss protection software on your network and use encryption technologies to protect data in transit.
6. Protect all pages on your public-facing websites, not just the checkout and sign-up pages.

¹ Symantec Internet Security Threat Report, April 2013.

² Ibid.

³ 2013 Small Business Technology Survey, National Small Business Association.

⁴ www.staysafeonline.org/about-us/news/new-survey-shows-us-small-business-owners-not-concerned-about-cybersecurity, 2013.

RESOURCES AVAILABLE TO YOU

FCC

The Federal Communications Commission (FCC), in collaboration with government agencies and industry leaders, created the Small Biz Cyber Planner, an easy-to-use, free online tool that will help you create a customized planning guide to protect your organization from cybersecurity threats.

US-CERT

The United States Computer Emergency Readiness Team (US-CERT) distributes bulletins and alerts for both technical and non-technical users, shares cybersecurity tips, and responds to incident, phishing, and vulnerabilities reports.

U.S. Small Business Administration

The U.S. Small Business Administration (SBA) helps Americans start, build and grow businesses. Through an extensive network of field offices and partnerships with public and private organizations, SBA delivers its services to people throughout the United States, Puerto Rico, the U. S. Virgin Islands and Guam.

Chamber of Commerce

The U.S. Chamber of Commerce has an Internet Safety Toolkit that teaches employees how to help protect company information, customer data, and their own personal information.

IF YOU'VE BEEN COMPROMISED

- Inform local law enforcement or the state attorney general as appropriate.
- Report stolen finances or identities and other cyber crimes to the Internet Crime Complaint Center at www.ic3.gov.
- Report fraud to the Federal Trade Commission at www.ongaurdonline.gov/file-complaint.
- Report computer or network vulnerabilities to US-CERT via the hotline: 1-888-282-0870 or www.US-CERT.gov.

Stop.Think.Connect.™ is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. The Campaign's main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family, and your community. For more information visit www.dhs.gov/stophinkconnect.



**Homeland
Security**

www.dhs.gov/stophinkconnect



STOP | THINK | CONNECT™