DID YOU KNOW?

44%

of small businesses reported being the victim of a cyber attack, with an average cost of approximately $9,000 per attack.[1]

NEARLY

59%

of U.S. small and medium-sized businesses do not have a contingency plan that outlines procedures for responding to and reporting data breach losses.[2]

RESOURCES AVAILABLE TO YOU

US-CERT.gov

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.

SBA.gov

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.

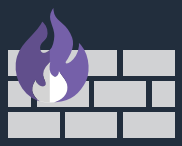
USChamber.com

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.

SIMPLE TIPS

1 

Make sure all of your organization's computers are equipped with antivirus software and antispyware. This software should be updated regularly.

2 

Secure your Internet connection by using a firewall, encrypt information, and hide your Wi- Fi network.

3 

Educate employees about cyber threats and how to protect your organization's data. Hold employees accountable to the Internet security policies and procedures.

4 

Establish security practices and policies to protect sensitive information.

5 

Require employees to use strong passwords and to change them often.

6 

Invest in data loss protection software, use encryption technologies to protect data in transit, and use two-factor authentication where possible.

7 

Protect all pages on your public-facing websites, not just the checkout and sign-up pages.

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.onguardonline.gov/file-complaint.
- » Report computer or network vulnerabilities to US-CERT via the hotline: 1-888-282-0870 or www.us-cert.gov.

[1]2013 Small Business Technology Survey, National Small Business Association

[2]www.staysafeonline.org/about-us/news/new-survey-shows-us-small-business-owners-not-concerned-aboutcybersecurity, 2013

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/stopthinkconnect.

Homeland Security

gurusentry

STOP | THINK | CONNECT™
dhs.gov/stopthinkconnect