It’s not just big businesses who are at risk for cyber attacks–small businesses are at risk too, and the consequences can be significant.

**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 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. Use and regularly update anti-virus and anti-spyware software on all computers; automate patch deployments across your organization to protect against vulnerabilities.
2. Secure your Internet connection by using a firewall, encrypting information and hiding 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 that employees use strong passwords and regularly change them.
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.

**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.

---

\(^1\) Symantec Internet Security Threat Report, April 2013.
\(^2\) Ibid.
**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.

**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](http://www.ic3.gov).

Stop.Think.Connect.™ is a national public awareness campaign aimed at 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](http://www.dhs.gov/stopthinkconnect).