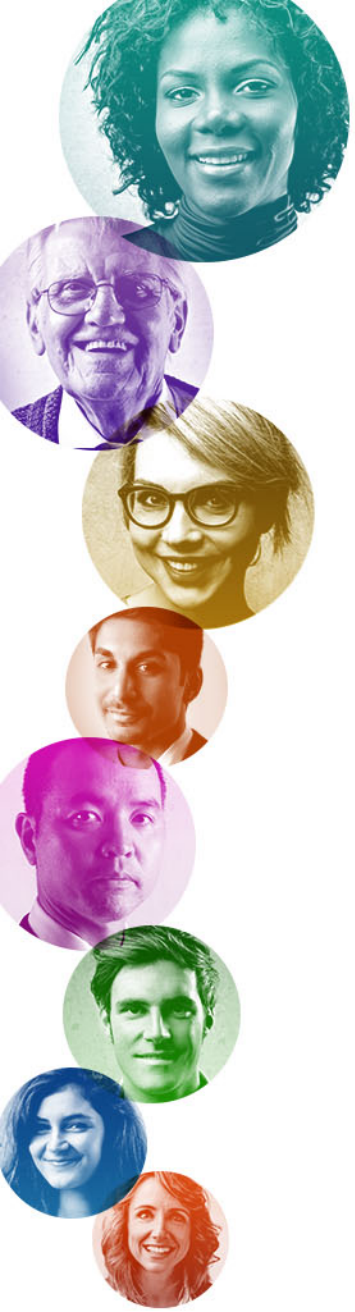

STOP.THINK.CONNECT™
NATIONAL CYBERSECURITY AWARENESS CAMPAIGN
SMALL BUSINESS PRESENTATION
Homeland Security
STOP | THINK | CONNECT™

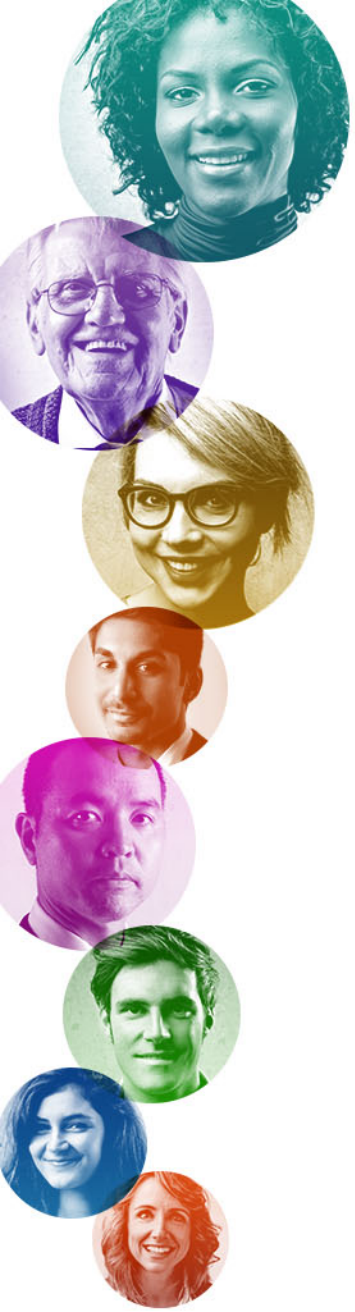


ABOUT STOP.THINK.CONNECT.™

In 2009, President Obama issued the *Cyberspace Policy Review*, which tasked the Department of Homeland Security with creating an ongoing cybersecurity awareness campaign–Stop.Think.Connect.–to help Americans understand the risks that come with being online.

Stop.Think.Connect. challenges the American public to be more vigilant about practicing safe online habits and persuades Americans to view Internet safety as a **shared responsibility** in the home, in the workplace, and in our communities.

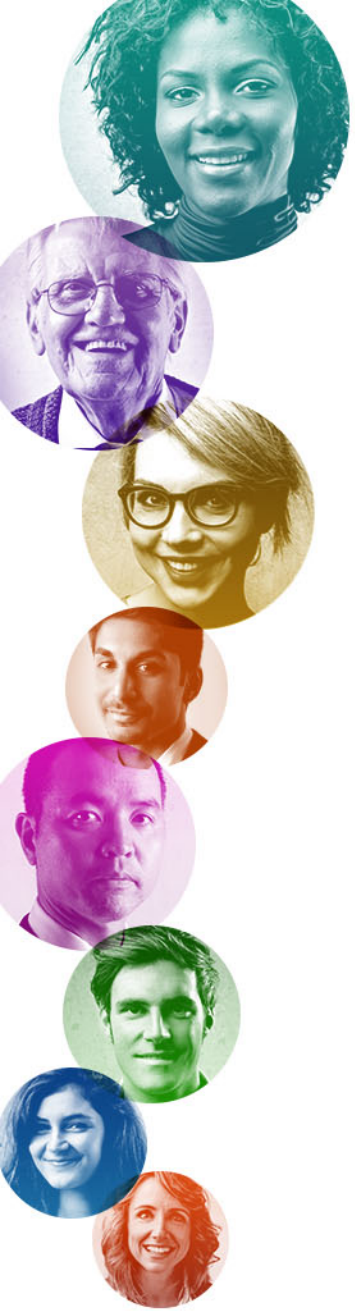
STOP | THINK | CONNECT™ | Homeland Security



SHARED RESPONSIBILITY

For small business owners, business growth is the name of the game. It's important to establish a cybersecurity protocol early that can grow with your business to protect your most critical assets.

- Not only do businesses rely on technology to perform daily functions, but the Internet provides easy ways for businesses to stay connected and informed.
- However, with these increased conveniences comes increased risks.
- Many of the crimes that occur in real life are now facilitated through the Internet, including human trafficking, credit card fraud, identity theft, and embezzlement.
- No country, industry, community, or individual is immune to cyber risks, and no single government agency, company, or individual can solve our cybersecurity challenges.
- We all have to work together to secure cyberspace.

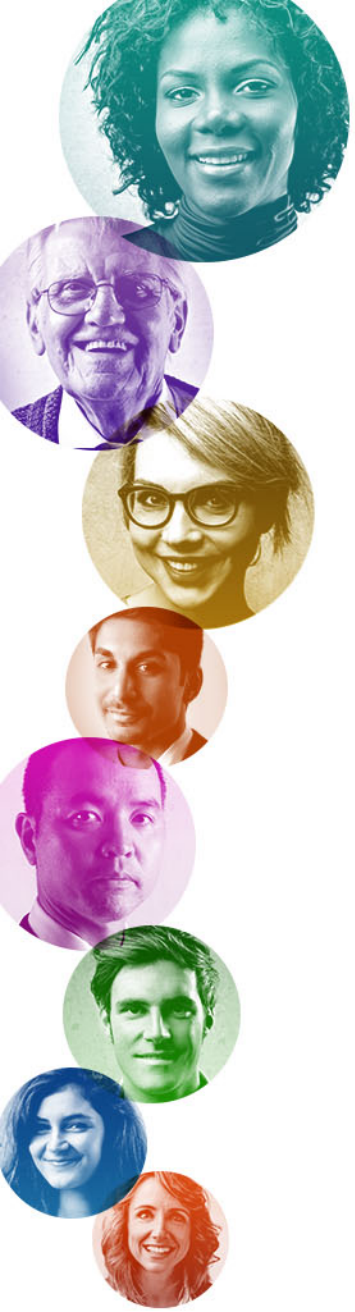


DID YOU KNOW?

In 2012, 50 percent of all targeted cyber attacks were aimed at businesses with fewer than 2,500 employees.[1]

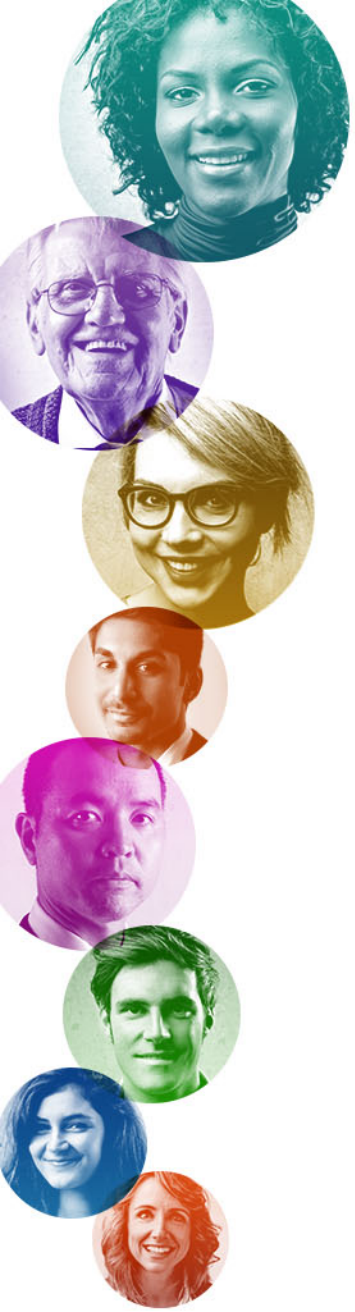
- The largest growth area for targeted cyber attacks in 2012 was businesses with fewer than 250 employees.[2]
- Forty-four percent of small businesses reported being the victim of a cyber attack, with an average cost of approximately $9,000 per attack.[3]
- Nearly 59 percent of U.S. small and medium-sized businesses do not have a contingency plan that outlines procedures for responding to and reporting data breach losses.[4]

1. Symantec Internet Security Threat Report, April 2013
2. Ibid
3. 2013 Small Business Technology Survey, National Small Business Association
4. www.staysafeonline.org



THE REALITY OF CYBER ATTACKS

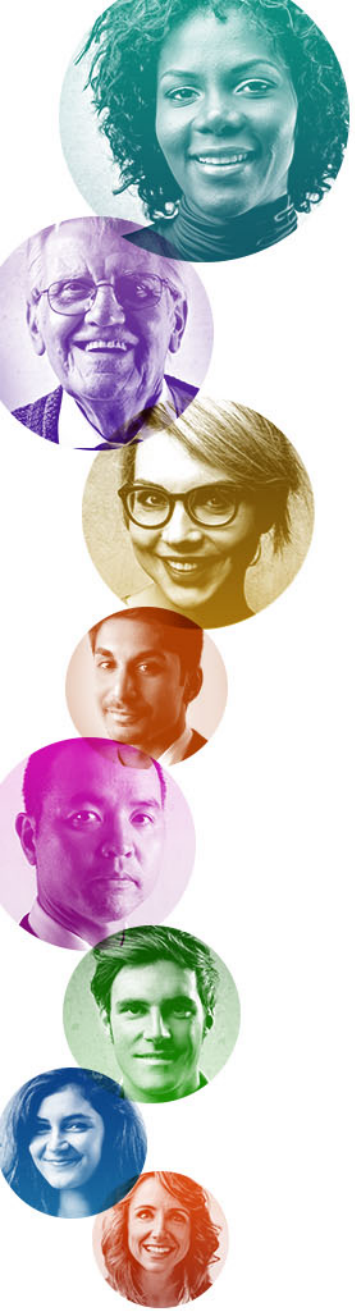
- All businesses, regardless of size, are at risk. Small businesses may feel like they are not targets for cyber attacks either due to their size or the perception that they don't have anything worth stealing.
- Only a small percentage of cyber attacks are considered targeted attacks, meaning the attacker group is going after a particular company or group of companies in order to steal specific data.
- The majority of cyber criminals are indiscriminate; they target vulnerable computer systems regardless of whether the systems are part of a Fortune 500 company, a small business, or belong to a home user.



SMALL BUSINESS BREACHES

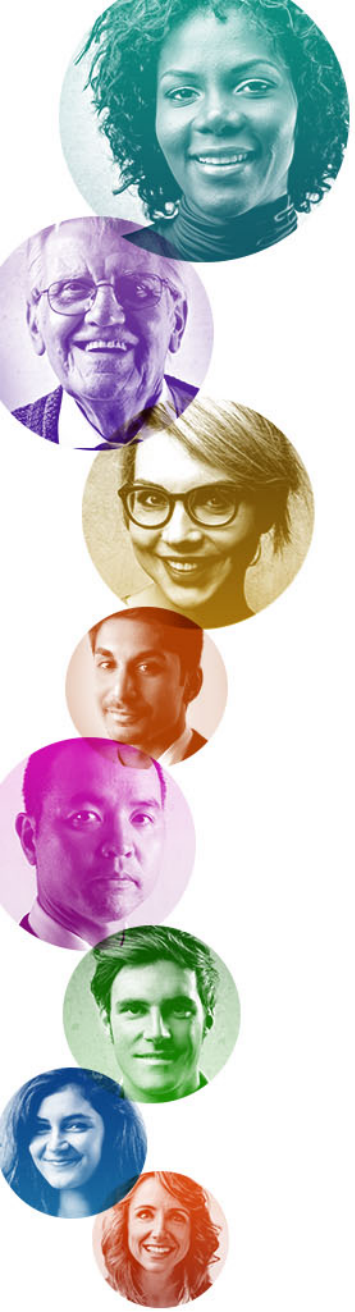
Small businesses, which are making the leap to computerized systems and digital records, are attractive targets for hackers.

- Small businesses store significant amounts of sensitive data from customer information to intellectual property.
- While large businesses can dedicate resources to cybersecurity, small businesses face the same cybersecurity challenges and threats with limited resources, capacity, and personnel.
- In 2010, the U.S. Secret Service and Verizon Communications Inc.'s forensic analysis unit, which investigates attacks, responded to a combined 761 data breaches, up from 141 in 2009. Of those, 63 percent were at companies with 100 employees or fewer.
- Visa estimates about 95 percent of the credit-card data breaches it discovers are on its smallest business customers.



CYBER TIPS FOR YOUR BUSINESS

- **Assess risk and identify weaknesses** – If you're sensitive information is linked to the Internet, then make sure you understand how it's being protected.
- **Create a contingency plan** – Establish security practices and policies to protect your organization's sensitive information and its employees, patrons, and stakeholders.
- **Educate employees** – Make sure that employees are routinely educated about new and emerging cyber threats and how to protect your organization's data. Hold them accountable to the Internet security policies and procedures, and require that they use strong passwords and regularly change them.
- **Back up critical information** – Establish a schedule to perform critical data backups to ensure that critical data is not lost in the event of a cyber attack or natural disaster. Store all backups in remote locations away from the office, and encrypt sensitive data about the organization and its customers. Invest in data loss protection software and use two-factor authentication where possible.
- **Secure your Internet connection** – Use and regularly update antivirus software and antispyware on all computers. Automate patch deployments across your organization, use a firewall, encrypt data in transit, and hide your Wi-Fi network. Protect all pages on your public-facing websites.
- **Create a continuity plan** – A continuity plan ensures that of nature, accidents, and technological or attack-related emergencies. Business functions can continue to be performed during a wide range of emergencies, including localized acts templates for this type of plan at http://www.fema.gov/planning-templates.

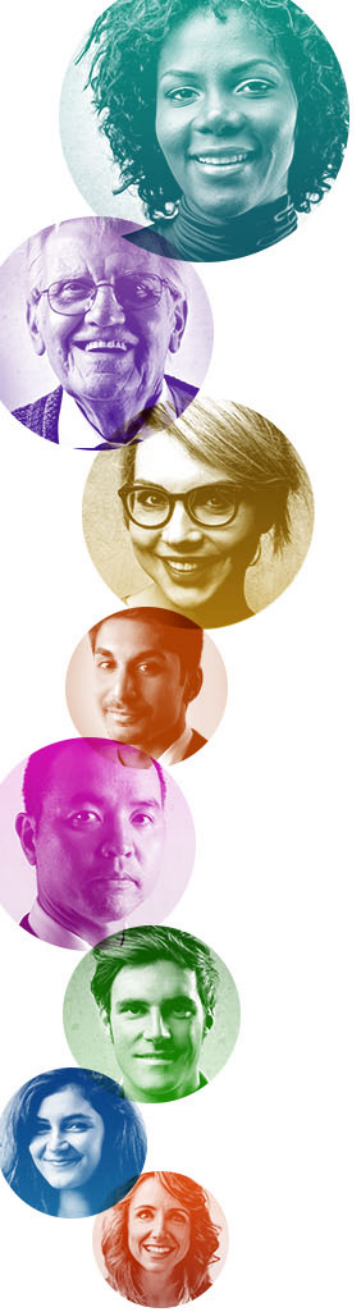


DO YOUR PART

Consumers are taking notice of how businesses secure their data and are more willing to trust and reward businesses for good security practices. Nearly 85 percent of consumers in a recent survey said they would increase their shopping at a store known for good cybersecurity practices. Only 20 percent said they would continue shopping at a store that had a recent data breach.[1]

- As a business owner, you can earn customer loyalty by promoting the security practices that you have implemented to protect their data.
- The losses resulting from cyber crimes, which can severely damage a business's reputation, often outweigh the costs associated with the implementation of a simple security program.
- By implementing a security program that involves both technical controls and cultural adjustments, small businesses can take a big step in fighting cyber crime.

1. Javelin Strategy & Research



CALL TO ACTION

Cybersecurity is a **shared responsibility** *that all Americans must embrace to keep the Nation secure. Become an advocate in your community to help us educate and empower the American public to take steps to protect themselves online.*

How to get involved:

- Become a *Friend* of the Campaign by visiting **www.dhs.gov/stopthinkconnect.**
- Make cybersecurity a priority. Discuss safe online practices with your fellow employees.
- Inform your community about the Stop.Think.Connect.™ Campaign and the resources available.
- Blog or post about the issue of cybersecurity and the Stop.Think.Connect. Campaign.
- Host a cybersecurity activity in your office.
- Download and distribute Stop.Think.Connect. materials, such as the brochure, bookmark, and poster, to your employees.


SECURING
CYBERSPACE STARTS
WITH YOU
Homeland
Security
STOP | THINK | CONNECT