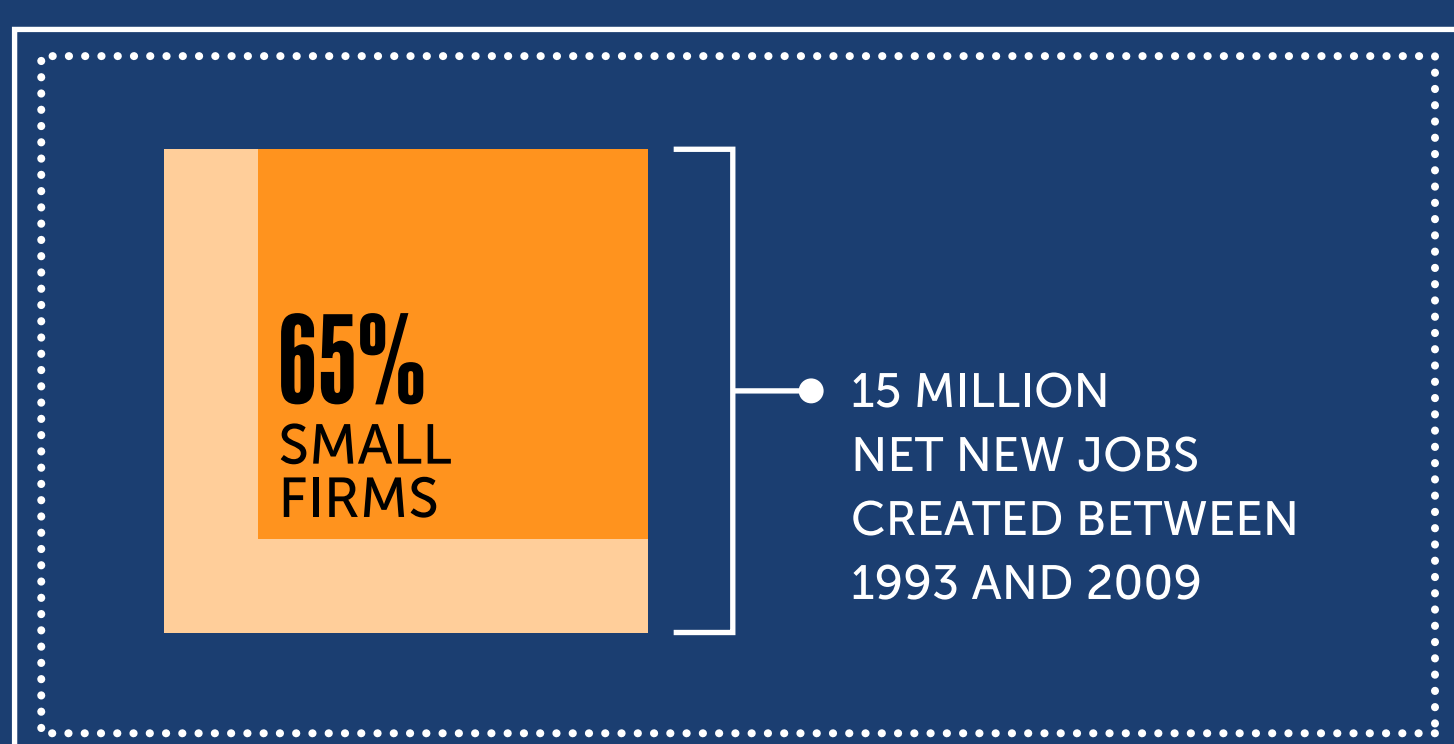
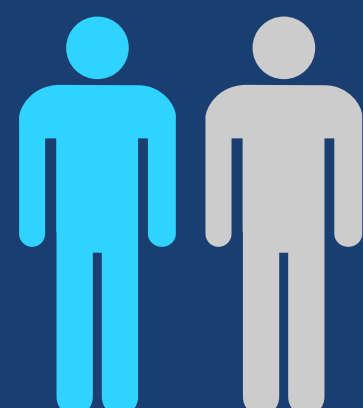


AMERICA'S SMALL BUSINESSES MUST TAKE ONLINE SECURITY MORE SERIOUSLY

SMALL BUSINESSES FORM BACKBONE OF U.S. ECONOMY

1 IN 2 AMERICAN WORKERS ARE EMPLOYED IN A SMALL BUSINESS

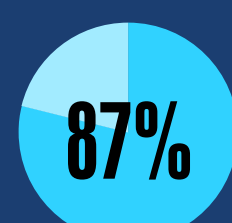


THE INTERNET IS A CRITICAL RESOURCE FOR U.S. SMALL BUSINESSES



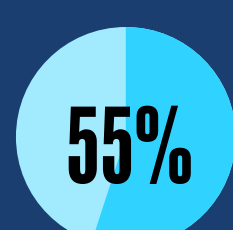
73%

SAY A SAFE AND TRUSTED INTERNET IS CRITICAL TO THEIR SUCCESS



Have one or more employees who use the Internet for daily operations

Say that the loss of Internet access for 48 straight hours during a regular business week would be disruptive to their business—38% say it would be extremely disruptive



A CYBER SECURITY DISCONNECT: MAJORITY OF U.S. SMALL BUSINESSES SATISFIED WITH THEIR ONLINE SAFETY MEASURES...



77% say their company is safe from cyber threats such as hackers, viruses, malware or a cyber-security breach

66% say they are not concerned about external threats (like a hacker or cyber-criminal stealing data) or an internal threat (like an employee, ex-employee or contractor/consultant stealing data)

47% believe a data breach incident would have no impact on their business and it would be treated as an isolated incident

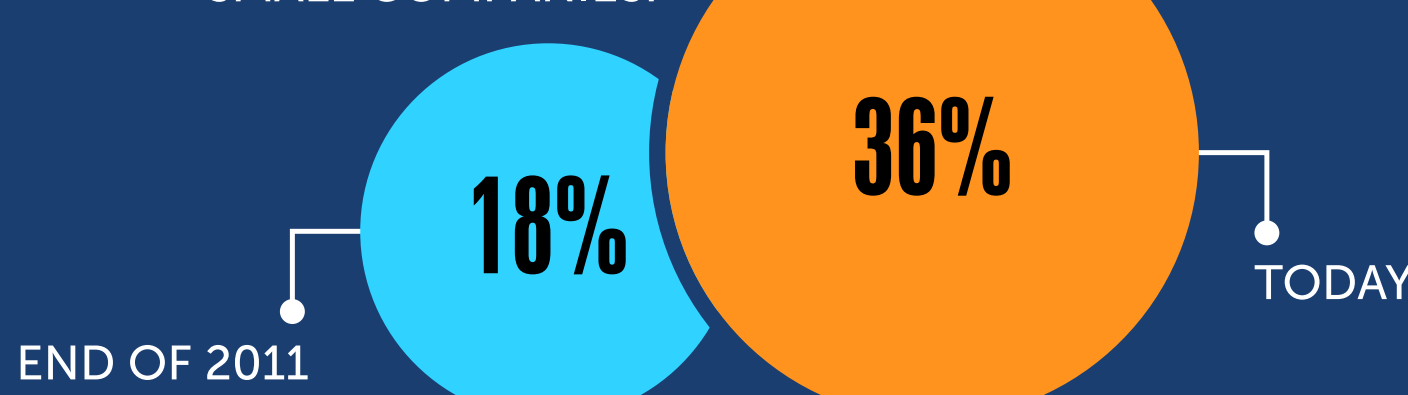
18% say they would not know if their computer network was compromised

YET MOST U.S. SMALL BUSINESSES CAN IMPROVE THEIR ONLINE SECURITY PRACTICES

According to previous Symantec research:



CYBER ATTACKS AIMED AT SMALL COMPANIES:



87% nearly 9 in 10 do not have a formal written Internet security policy for employees



69% do not have even an informal Internet security policy for employees



59% do not have a contingency plan outlining procedures for responding and reporting data breach losses



75% do not have policies for employee social media use on the job while 23% have established policies



60% do not have a privacy policy that employees must comply with when they handle customer or employee information

WHAT BUSINESSES CAN DO TO BETTER PROTECT THEMSELVES:

STOP. THINK. CONNECT.

Small businesses can improve their online safety practices, starting with these steps:

- **KEEP A CLEAN MACHINE.**
Keep all workplace machines clean and protected from malware, viruses and infections.
- **PROTECT YOUR INFORMATION.**
Secure your accounts by making passwords long, strong and unique.
- **PROTECT YOUR COMPANY'S ONLINE REPUTATION.**
Set security and privacy settings to your comfort level of sharing.
- **EDUCATE YOUR EMPLOYEES.**
Teach your employees basic best practices; such as if an email, social network post or text message looks suspicious, even if you know the source, delete it.



STOP | THINK | CONNECT™



National Cyber Security Awareness Month

VISIT WWW.STOPTHINKCONNECT.ORG AND WWW.STAYSAFEONLINE.ORG FOR MORE TIPS AND INFORMATION.

SOURCES

National Cyber Security Alliance, Symantec, U.S. Department of Commerce, U.S. Small Business Administration, U.S. Department of Labor/Bureau of Labor Statistics, U.S. Census Bureau

Sponsored by:

