National Cyber Security Awareness Month

3 REASONS HACKERS LOVE YOUR SMALL BUSINESS

1. HACKERS PREY ON THE WEAK

Small businesses are often less equipped *to protect against an attack and dedicate fewer resources to fighting cybercrime*

Nearly half of all small businesses *have been a victim of cyber-attacks* [1]

71% of security breaches *target small businesses* [2]

2. HACKERS LOVE INTERNAL ACCESS

77% of all employees *leave their computers unattended* [2]

Stealing credentials *from key employees allows hackers to send email that looks legitimate to other companies they want to attack by disguising the email to look like it's coming from a business partner*

Disgruntled former employees *pose internal threats, stealing trade secrets and data, and increasingly use Internet cloud services to hack companies by gaining remote access to corporate networks* [3]

One of the country's large scale breaches was hacked by gaining entry through a HVAC technician who had access

3. HACKERS LOVE WHAT SMALL BUSINESSES HAVE TO OFFER

95% of credit card breaches *that Visa Inc. discovers are from its smallest business customers*

Intellectual property

Personally identifiable information *(PII)*

AMONG SMALL AND MEDIUM BUSINESS OWNERS THAT SUFFER A BREACH, A STAGGERING 60% GO OUT OF BUSINESS AFTER SIX MONTHS[4]

THE MOST IMPORTANT LESSONS ARE STILL THE MOST BASIC

Talk to your employees about cybersecurity. They need to know the policies and practices you expect them to follow in the workplace regarding Internet safety.

FOCUS ON WHAT NEEDS TO BE PROTECTED
Create a risk management plan that identifies both critical company and customer information that must be secured.

FORECAST THE CONSEQUENCES OF A SUCCESSFUL ATTACK
Quantify the risk and what could happen as a result a successful cyber-attack against your company.

CREATE A CULTURE OF CYBERSECURITY
Teach your employees to STOP.THINK.CONNECT. and to understand the value of protecting company and customer information and the importance of security to the business. Establish Internet security policies.

STOP | THINK | CONNECT™

TALK TO YOUR EMPLOYEES ABOUT VULNERABILITIES
Links in email, social media posts and online can lead to malware. When in doubt, throw it out! And encourage your employees to speak up if they notice strange happenings on their computer.

HAVE A PLAN
Hacks, data breaches and other cybercrime happen every day, and so do fires, floods and burglary. Have a plan in place to grow your cybersecurity protections that also addresses how you would respond if an attack occurs.

NEED HELP IMPLEMENTING A CYBERSECURITY PLAN?

RE: Cyber: cybersecurity guidance for small business CEOs
staysafeonline.org/re-cyber/about/

Data privacy/security plans, and other small business tools
go.bbb.org/biz-toolkits

Implementing a cyber plan:
staysafeonline.org/business-safe-online/implement-a-cybersecurity-plan/

FCC Small Biz Cyber Planner 2.0: ***fcc.gov/cyberplanner***

National Institute of Standards and Technology: ***nist.gov/***

Cybersecurity education information and tools: ***stopthinkconnect.org***

Small business STOP.THINK.CONNECT. resource guide: ***stcguide.com/explore/small-business***

CREATED FOR NATIONAL CYBER SECURITY AWARENESS MONTH: EVERY OCTOBER SINCE 2004.
Cosponsored by the Department of Homeland security and the National Cyber Security Alliance, the nation's leading nonprofit public private partnership promoting the safe and secure use of the internet.

1 National Small Business Association
2 US Small and Medium-Sized Business 2014-2018 forecast by IDC
3 Federal Bureau of Investigation and Department of Homeland Security
4 http://www.experian.com/blogs/business-credit/2013/11/26/experian-data-breach-resolution-advises-small-businesses-to-be-prepared-for-a-data-breach/
5 IDC US Mobile Security Survey, 2013