Creating A Cyber Aware Culture in Your Small Business

Webinar will begin promptly at 2pm Eastern
*All speakers will remain muted until that time

Presented By:
CyberSecure
MY BUSINESS
PLAN. PROTECT. RESPOND.

Moderator
Kelvin Coleman, Executive Director

Speaker
Lisa Plaggemier, Chief Evangelist

Speaker
Zara Smith, Strategic Programs Manager

Speaker
Sarah Choi, Attorney

National Cyber Security Alliance
INFOSEC
America's SBDC Michigan
Happy National Small Business Week!
May 5-11, 2019 | sba.gov/nsbw

National Cyber Security Alliance’s
Small Business Week Initiatives and Resources: www.staysafeonline.org
Goal of 5-Step Approach Is Resilience

- **Know the threats and Identify** and **Protect** your assets
- **Detect** problems and **respond** quickly and appropriately
- **Know what recovery looks like** & prepare

Thanks to our National Sponsors

The "CyberSecure My Business" was great event hosted by the National Cyber Security Alliance. If you are an owner or manager of a small business I highly recommend you visit their website and attend one of these workshops. Excellent presentations and panel discussion! Thanks Daniel Elliot (NCSA) and the sponsors for organizing this event.
$17 Trillion
58% of malware victims are small business

$2.2M ave. cost of cyber attack to SMB

$6T global cost of cybercrime by 2021

Ponemon Institute's 2017 State of Cybersecurity in Small & Medium-Sized Businesses
DOH!

“95% of all security incidents involved some form of human error.”

Source: IBM Security Services 2016 Cyber Security Intelligence Index
UGH!

91% of all breaches started with a spear phishing email

Source: Trend Micro
Stores swindled by hacker battle over blame

Judge orders 1 to pay again for vehicles
People

- Background Checks
- Onboarding
- Offboarding
- Phishing Simulations
- Training
- Culture
Process

- Password Policy
- BYOD
- Access Controls
- Verification
- Virtual Private Networking (VPN)
- Patching/Updates
- Email Encryption/File Transfer
Technology

- Firewalls
- Anti-virus
- Internet Proxy/Content Filter
- Email Filtering
- Virtual Private Networking (VPN)
- Backups
- Data Encryption
- BYOD
Speaker
Zara Smith,
Strategic Programs Manager

https://smallbusinessbigthreat.com/
The Michigan SBDC

Funded through a cooperative agreement with the:

- U.S. Small Business Administration (SBA)
- Michigan Economic Development Corporation (MEDC)
- Matching funds from Local Network partners in each region.
Organizational culture encompasses values and behaviors that contribute to the unique social and psychological environment of a business. The organizational culture influences the way people interact, the context within which knowledge is created, the resistance they will have towards certain changes, and ultimately the way they share (or the way they do not share) knowledge.

-Wikipedia

The team members needs to understand:
• What is it that we are doing?
• Why are we doing what we are doing?
• How do I personally fit into it?
What is phishing?

• A type of social engineering attack
  • Other forms of phishing
    • Spear Phishing
    • Whaling
    • Vishing
• Other forms of social engineering
  • Tailgating
  • Pretexting
What can you do about phishing?

• Educate your employees:
  • Think before you click
  • Pick up the phone
  • Do not give out their passwords and usernames to others
  • Report a visitor or guest who is acting suspicious, provide great customer service
  • Trust but verify
What is malware?

• Malware
  • Virus
  • Trojan Horse
  • Rootkit
  • Bots
  • Worms
  • Spyware
What can you do about malware?

• Implement an anti-virus and an anti-malware program on all your devices
• Verify software before downloading and installing
• Think before you click
• Backup your critical data
What is ransomware?

• Ransomware
  • A type of malware that typically encrypts data on your computers, storage devices, network devices, etc.
  • Once encrypted, the attacker asks for a “ransom” usually bitcoin to unlock the data.
What can you do about ransomware?

• Employee awareness and training
• Think before you click
• Minimize opening files in emails
• Deploy security tools to analyze incoming emails for dangerous links and files
• Have regular (daily) backups of data that are separated from infected files
What is VPN?

• VPN (Virtual Private Network)
  • Not just for off-site accessing in site resources… but critical for employee ability to connect to your network off-site.
  • Encrypts communication between your device and your data
What is a firewall?

• Firewalls
  • What does it actually do?
    • Helps prevent unauthorized access to your network or computers
  • Hardware vs Software
    • Hardware firewalls are physical appliances installed on your network
    • Software firewalls are installed on your computer
What can firewalls do?

• Block unauthorized access to your computer or to your network
• Assist in preventing hackers from infiltrating your network
• Properly configured firewalls are vital assets, while improperly configured firewalls are a disaster waiting to happen
What is a password manager?

• Password Mangers
  • Save passwords in a secure encrypted “vault”
  • Easily manage usernames & passwords
What can password managers do?

• Help you create complex passwords
• Remember what logins the passwords are for
• Allow you to only have to remember one complex password, which is used to login to your password manager
• Some password managers let you save to the cloud allowing you to access your passwords from multiple devices, while others save a file to a specific device that can only be accessed with that device
What is multi-factor authentication?

- Adds additional layers of security
  - Something you have
    - USB Dongle
    - Card Swipe
  - Something you know
    - Username
    - Password
  - Something you are
    - Fingerprint
    - Facial Recognition
What can multi-factor authentication do?

• Help prevent unauthorized access
• Send alerts if someone is trying to login to one of your accounts

• Accounts to use Multifactor on
  • Banking % financial Accounts
  • Health/medical accounts
  • Insurance accounts
  • Social media
  • Email
  • Business accounts
  • Network and system accounts
Resources

• Small Business, Big Threat (Michigan SBDC)
  • https://smallbusinessbigthreat.com

• Small Business Administration (SBA)
  • https://www.sba.gov/managing-business/cybersecurity

• United States Computer Emergency Readiness Team (US-CERT)
  • https://www.us-cert.gov/security-publications
  • https://www.us-cert.gov/ncas/tips

• SANS Institute
  • https://www.sans.org/security-resources/policies

• Federal Trade Commission (FTC)
  • https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity

• National Cyber Security Alliance
  • https://staysafeonline.org/
CyberSecure
MY BUSINESS
PLAN. PROTECT. RESPOND.

Speaker
Sara Choi, Attorney

https://ftc.gov/smallbusiness
Creating A Cyber Aware Culture In Your Small Business

Sarah Choi
Federal Trade Commission
May 7, 2019

The views expressed are those of the speaker, and do not necessarily represent the views of the Commission or any individual Commissioner.
Protecting Small Businesses

As a small business owner, you have a lot on your mind. You can’t afford to lose time or money to scammers or a compromised network. We can help you avoid scams, protect your computers and networks, keep your customers’ data safe – and protect your bottom line. You also can find out what the FTC is doing to protect small businesses.

Stay connected by subscribing to the FTC’s Business Blog.

FEATURED

Cybersecurity

Scams and Your Small Business
Small Business Discussion Guide for Employers

Cybersecurity for Small Business

Talking Cybersecurity With Your Employees

Cyber criminals target companies of all sizes. Knowing about cybersecurity and putting some best practices in place will help you protect your business and reduce the risk of a cyber attack.

Here are some ideas to help you and your staff learn about cybersecurity and make it part of your business routine:

- Learn about cybersecurity
  Read the cybersecurity fact sheets at FTC.gov/SmallBusiness. Consider how the information applies to your business.

- Talk about cybersecurity
  Talk about cybersecurity with your employees, vendors, and others involved in your business. Share with them the information at FTC.gov/SmallBusiness.

- Use online videos and quizzes
  Ask your employees to watch the videos at FTC.gov/SmallBusiness. Use online quizzes to test their understanding of the cybersecurity topics.

Make cybersecurity part of your next staff meeting
Assign a staff member to guide a discussion on one of the cybersecurity topics at FTC.gov/SmallBusiness. Show a video and then discuss how the information can be applied to your business.

Create policies
Create business policies covering basic cybersecurity practices and give a copy to your employees. Explain the importance of following these policies. Include tips for spotting and protecting against cyber threats like phishing emails and ransomware.

Stay in the know
Sign up for the FTC’s Business Blog at Business.FTC.gov/Blog. Suggest that your employees do the same.

This information is part of the Federal Trade Commission’s efforts to help improve cybersecurity for small business. The information was developed in collaboration with the U.S. Department of Commerce’s National Institute of Standards and Technology (NIST), the U.S. Small Business Administration (SBA), and the Department of Homeland Security (DHS). Learn more at FTC.gov/SmallBusiness.
Cybersecurity and Your Small Business

October 2018

Topic: Online Safety & Security
Language: English
Format: Booklet
8.5” x 11”, 28 pages

Information on 12 different cybersecurity topics to help small business owners and staff understand common cyber threats and how they can protect their business. Topics include ransomware, phishing, vendor security, and email authentication. Includes a discussion guide for employers on how to use the materials.

Select Quantity 25
Need more copies?
Add to cart

All publications and shipping are free.
Small Business Cybersecurity’s Twelve Modules

- Cybersecurity Basics
- Understanding the NIST Cybersecurity Framework
- Physical Security
- Ransomware
- Phishing
- Business Email Imposters
- Tech Support Scams
- Vendor Security
- Cyber Insurance
- Email Authentication
- Hiring a Web Host
- Secure Remote Access
Phishing Fact Sheet

You get an email that looks like it’s from someone you know. It seems to be from one of your company’s vendors and asks you to click on a link to update your business account. Should you click? Maybe it looks like it’s from your boss and asks for your network password. Should you reply? In either case, probably not. These may be phishing attempts.

**HOW PHISHING WORKS**

You get an email or text.

It seems to be from someone you know, and it asks you to click a link or give your password, business bank account, or other sensitive information.

It looks real.

It’s easy to spoof logos and make up fake email addresses. Scammers use familiar company names or pretend to be someone you know.

It’s urgent.

The message pressures you to act now — or something bad will happen.

What happens next.

If you click on a link, scammers can install ransomware or other programs that can lock you out of your data and spread to the entire company network. If you share passwords, scammers now have access to all those accounts.

**WHAT YOU CAN DO**

Before you click on a link or share any of your sensitive business information:

- **Check it out.**
  - Look up the website or phone number for the company or person behind the link or email. Make sure that you’re getting the real company and not about to download malware or talk to a scammer.

- **Talk to someone.**
  - Talking to a colleague might help you figure out if the request is real or a phishing attempt.

- **Make a call if you’re not sure.**
  - Pick up the phone and call that vendor, colleague, or client who sent the email. Confirm that they really need information from you. Use a number you know to be correct, not the number in the email or text.

**HOW TO PROTECT YOUR BUSINESS**

Back up your data.

Regularly back up your data and make sure those backups are not connected to the network. That way, if a phishing attack happens and hackers get to your network, you can restore your data. Make data backup part of your routine business operations.

Keep your security up to date.

Always install the latest patches and updates. Look for additional means of protection, like email authentication and intrusion prevention software, and set them to update automatically on your computer. On mobile devices, you may have to do it manually.

Alert your staff.

Share this information. Keep in mind that phishing scammers change their tactics often, so make sure you include tips for spotting the latest phishing schemes in your regular training.

Deploy a safety net.

Use email authentication technology to help prevent phishing emails from reaching your company’s inboxes in the first place.

**WHAT IF YOU FALL FOR A PHISHING SCHEME**

Alert others.

Talk to your colleagues and share your experience. Phishing attacks happen to more than one person in a company.

Limit the damage.

Immediately change any compromised passwords and disconnect from the network any computer or device that’s infected with malware.

Follow your company’s procedures.

These may include notifying specific people in your organization or contractors that help you with IT.

Notify customers.

If your data or personal information was compromised, make sure you notify the affected parties — they could be at risk of identity theft. Find information on how to do that in Data Breach Response: A Guide for Business (FTC.gov/DataBreach).

Report it.

Forward phishing emails to spam@ abuse.gov (an address used by the FTC) and to reportphishing@usao-wdpa.gov (an address used by the Anti-Phishing Working Group, which includes ISPs, security vendors, financial institutions, and law enforcement agencies). Let the company or person that was impersonated know about the phishing scheme. And report it to the FTC at FTC.gov/Complaint.
Phishing Quiz

You get an email or text that seems to be from one of your company's vendors. It asks you to click on a link to update your business account. Should you click? Probably not. This could be a phishing attempt.

To find out how much you know about phishing, choose the best response for each question or statement.

1. Which one of these statements is correct?

   A. If you get an email that looks like it's from someone you know, you can click on any links as long as you have a spam blocker and anti-virus protection.

   B. You can trust an email really comes from a client if it uses the client's logo and contains at least one fact about the client that you know to be true.

   C. If you get a message from a colleague who needs your network password, you should never give it out unless the colleague says it's an emergency.

   D. If you get an email from Human Resources asking you to provide personal information right away, you should check it out first to make sure they are who they say are.

This is correct! This email could be a phishing scam, where you get a message that looks like it's from someone you know, asking you urgently for sensitive information. Before responding, call Human Resources and confirm they sent the message.
Cybersecurity for Small Business

Made in USA

Safeguard your network and customer credentials: Tips from the latest FTC data security case

Business Center

Your link to consumer protection law.

EXPLORE THE BUSINESS CENTER
Scams and Your Small Business
May 2018

This booklet explains common scams such as fake invoices, directory listings scams, and utility company imposter scams that target small businesses and non-profit organizations. It also describes scammers' tactics to help people spot scams, and provides steps business owners can take to protect their company from scams.
ftc.gov/startwithsecurity

• Lessons learned from FTC data security cases

• 10 actionable steps that companies can take for better data security
11 Videos Covering the Start with Security Principles
1. Take Stock.
2. Scale Down.
3. Lock It.
4. Pitch It.
5. Plan Ahead.
Data Breach Response: A Guide for Business

- Guidance for businesses if you discover a data breach
- Explains steps to take and who to notify