Digital Spring Cleaning

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

Presented By:

CyberSecure
MY BUSINESS
PLAN. PROTECT. RESPOND.

NATIONAL CYBERSECURITY ALLIANCE
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**

Enterprise Projects Mgr at Hancock Whitney... 36m

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.

StaySafeOnline
Powered by: National Cyber Security Alliance

I am loving the "CyberSecure My Business" webinars. Nice work @StaySafeOnline!
National Small Business Week

In-Person Workshops

--May 7 in Atlanta Georgia
--May 9 in Chicago, Illinois

Webinar

--May 7, 2-3EDT Creating a Cyber Aware Culture in Your Small Business

Contact Daniel Eliot for more information: daniel@staysafeonline.org
Secure Your ID Day

Better Business Bureau
Secure Your ID Day *to prevent identity theft*

• First Secure Your ID Day event in May 2008
• Work together as a system, coast-to-coast, under the BBB brand name to:
  – Keep identity protection as a top-of-mind issue;
  – Deliver needed identity protection education to the public and
  – Perform community service while also providing best practices for securing personal information.
Benefits to Participating

• Exposure/visibility for BBB and its brand  
• Reinforces BBB as an identity protection champion  
• Opportunity for partnerships with ABs and others  
• Great community service  
• Fun for staff to interact with community  
• Sets example for best practices  
• Reinforces the BBB’s mission of Trust in the Marketplace
History of Success

Since 2008, BBBs have collected and shred nearly 6,000 tons of paper

Since 2012, BBBs have shred and safely disposed of more than 216 tons of computers, phones, and office equipment
2019 Secure Your ID Day Events

• Nearly 50 events in 18 states
• BBBs partnering with Accredited Businesses, community organizations, media outlets and others to host and promote shred day events
• Most have electronics disposal added by the shredding company
• Digital Spring Cleaning campaigns across the U.S. and Canada
2019 Digital Spring Cleaning Campaign

• National article on BBB.org to be shared on local BBB websites
• Social media messaging on Facebook, LinkedIn, Twitter, Instagram, etc.
• Podcast featuring NCSA executive director Kelvin Coleman
• Media interviews using joint NCSA/BBB tips
• Special emphasis on small-to-mid-sized businesses
• Sharing tips in newsletters for BBB Accredited Business
DIGITAL SPRING CLEANING CHECKLIST FOR SMBs

Available At: https://staysafeonline.org/resource/digital-spring-cleaning-smb-checklist/
**Keep a Clean Machine**

- **Update the software** on all of your company’s devices – including point of sale systems and IoT (Internet of Things) devices.

- **Establish or update BYOD** (Bring Your Own Device) **policies**

- **Delete software and apps** you are no longer using.

- **Teach employees good habits** when it comes to maintaining clean and secure devices
CLEAN UP YOUR ONLINE PRESENCE

• **Own your online presence** by reviewing the privacy and security settings on accounts you use.

• **Control your role** by reviewing and limiting who has administrative access to your online accounts.

• **Clean up your social media presence** by deleting old or unnecessary photos and by deleting accounts no longer in use.

• **Take care with what you share** by updating or creating policies and procedures for what content should be/can be shared on your business social media accounts.

• **Web browsers should be updated** to the most current versions for all internet-connected devices.
Cybersecurity should be part of any organization’s continuity planning, and the plan should be reviewed annually at a minimum.
DIGITAL SPRING CLEANING CHECKLIST FOR SMBs

Available At: https://staysafeonline.org/resource/digital-spring-cleaning-smb-checklist/
Whitney Moore, Attorney
Digital Spring Cleaning for Your Small Business

Federal Trade Commission
April 9, 2019
The views expressed in this presentation are those of the speaker and do not necessarily reflect the views of the Commission or any individual Commissioner.
PROTECT
YOUR FILES & DEVICES

Update your software
This includes your apps, web browsers, and operating systems. Set updates to happen automatically.

Secure your files
Back up important files offline, on an external hard drive, or in the cloud. Make sure you store your paper files securely, too.

Encrypt devices
Encrypt devices and other media that contain sensitive personal information. This includes laptops, tablets, smartphones, removable drives, backup tapes, and cloud storage solutions.

Require passwords
Use passwords for all laptops, tablets, and smartphones. Don’t leave these devices unattended in public places.

Use multi-factor authentication
Require multi-factor authentication to access areas of your network with sensitive information. This requires additional steps beyond logging in with a password — like a temporary code on a smartphone or a key that’s inserted into a computer.
PROTECT YOUR WIRELESS NETWORK

Secure your router
Change the default name and password, turn off remote management, and log out as the administrator once the router is set up.

Use at least WPA2 encryption
Make sure your router offers WPA2 or WPA3 encryption, and that it’s turned on. Encryption protects information sent over your network so it can’t be read by outsiders.
CYBERSECURITY FOR SMALL BUSINESS

PHYSICAL SECURITY
HOW TO PROTECT EQUIPMENT & PAPER FILES

Here are some tips for protecting information in paper files and on hard drives, flash drives, laptops, point-of-sale devices, and other equipment.

**Store securely**
When paper files or electronic devices contain sensitive information, store them in a locked cabinet or room.

**Limit physical access**
When records or devices contain sensitive data, allow access only to those who need it.

**Send reminders**
Remind employees to put paper files in locked file cabinets, log out of your network and applications, and never leave files or devices with sensitive data unattended.

**Keep stock**
Keep track of and secure any devices that collect sensitive customer information. Only keep files and data you need and know who has access to them.
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 text 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.
CYBERSECURITY FOR SMALL BUSINESS EDUCATION CAMPAIGN

12 modules:

1. Cybersecurity Basics
2. NIST Cybersecurity Framework
3. Physical Security
4. Ransomware
5. Phishing
6. Business Email Imposters
7. Tech Support Scams
8. Vendor Security
9. Cyber Insurance
10. Email Authentication
11. Hiring a Web Host
12. Secure Remote Access
MORE TOOLS FOR BUSINESS
ftc.gov/startwithsecurity

• Lessons learned from FTC data security cases
• 10 actionable steps that companies can take for better data security
• 11 videos
Stick with Security: A Business Blog Series

The 2017 Stick with Security series on the Bureau of Consumer Protection business blog shares insights into the ten Stick with Security principles. Based on the Bureau’s recent law enforcement actions, media investigations, and experiences compiled, these stories share about dealing with security in their business.

For businesses, the key to keeping sensitive information is to stick with security. The Stick with Security blog was released in 2015 offering guidelines to data from the FTC’s 2014 data security cases. From security information collection policies and product design through training, implementation, strategy, monitoring, and disposition, Stick with Security makes data security guidance in ten actionable principles suited for companies of any size and in any sector.

Looking for a deeper look? The Stick with Security series on the Bureau of Consumer Protection Business Blog offers additional insights into these ten principles, based on the actions of recent law enforcement actions, media investigations, and experiences compiled, these stories share about dealing with security in their business.

<table>
<thead>
<tr>
<th>Stick with Security: Insights into FTC investigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1 Stick with security — and stick with it.</td>
</tr>
<tr>
<td>#2 Stick with security: Control access to data sensitivity</td>
</tr>
<tr>
<td>#3 Stick with security: Require encryption and authentication</td>
</tr>
<tr>
<td>#4 Stick with security: Store sensitive personal information securely and protect it during transmission</td>
</tr>
<tr>
<td>#5 Stick with security: Segment your network and monitor who’s trying to get in and out</td>
</tr>
<tr>
<td>#6 Stick with security: Ensure remote access to your network</td>
</tr>
<tr>
<td>#7 Stick with security: Apply sound security practices when developing new products</td>
</tr>
<tr>
<td>#8 Stick with security: Make sure your service providers implement reasonable security measures</td>
</tr>
<tr>
<td>#9 Stick with security: Put procedures in place to keep your security current and address vulnerabilities that may arise</td>
</tr>
<tr>
<td>#10 Stick with security: Use paper, physical media, and devices</td>
</tr>
<tr>
<td>Stick with security: FTC resources for your business</td>
</tr>
</tbody>
</table>
Protecting Personal Information: A Guide for Business

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
Digital Spring Cleaning

**Founding Sponsor**
FedEx  
smallbusiness.fedex.com

**Signature Sponsor**
Trend Micro  
www.trendmicro.com

**Contributing Sponsor**
Infosec  
www.infosecinstitute.com

**Council of BBB’s**
https://www.bbb.org/council/for-businesses/cybersecurity/

**Federal Trade Commission**
https://ftc.gov/smallbusiness

**National Cyber Security Alliance**
www.staysafeonline.org/cybersecure-business