 Moderated by
Daniel Eliot, Director
Small Business Programs
National Cyber Security Alliance

Myla Pilao, Director
Technical Marketing
Trend Micro

NATIONAL CYBER SECURITY ALLIANCE
New Year’s Resolution: Protect Your Sensitive Business Information in 2019
Be a Part of Something Big

Get involved and promote a safer, more secure internet.

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 and prepare.

Thanks to our National Sponsors MediaPRO, Trend Micro, and Initiative for Education.
New Orleans CyberSecure My Business™ Workshop

**When:** February 7, 2019

**Where:** Ernest M. Morial Convention Center, Rivergate Room, 900 Convention Center Boulevard, New Orleans, LA

**Two Events--**

**SMB Advisors:**
[cybersecuremybizadvisorsnola.eventbrite.com](https://cybersecuremybizadvisorsnola.eventbrite.com)

**SMB Workshop:**
[https://cybersecuremybizneworleans.eventbrite.com](https://cybersecuremybizneworleans.eventbrite.com)

**Presented By:**

**National Signature Sponsor**

**National Contributing Sponsor**

**Local Event Sponsors:**
NATIONAL CYBER SECURITY ALLIANCE

New Year’s Resolution: Protect Your Sensitive Business Information in 2019

Myla Pilao, Director
Technical Marketing

TREND MICRO
Initiative for Education
DIGITAL SAFETY OUTREACH
Make Protecting Your Small Business Assets Against Cyber Threats a Goal This New Year

Myla V. Pilao
Director Technology Marketing
SECURITY IS COMPLICATED
KEEP YOUR BUSINESS RUNNING
MAPPING THE FUTURE
Dealing With Pervasive and Persistent Threats

TREND MICRO SECURITY PREDICTIONS FOR 2019
Gone are the days of one-platform computing. As the world becomes more diverse and social via chat, video, and increased online transactions, cybercriminals will pull the ultimate throwback: good old social engineering.
Social Engineering via Phishing Will Replace Exploit Kits as Attack Vector

- As the state of “monoculture” declines, exploit kit attacks will decline, and cybercriminals will use social engineering even more.
- There will be more cases of phishing not only in email but also in SMS and chat; SIM-jacking.
- Sporting events, upcoming elections, and sociopolitical developments will be used as premise for social engineering attacks.
Chatbots Will Be Abused

- In the same way that telephone attacks evolved to take advantage of prerecorded messages and interactive voice response (IVR) systems, attackers will design chatbots that can hold an initial conversation with a target to create a convincing pretext for eventually sending over a phishing link or obtaining personal information.
- Impact: manipulation of orders, installation of RAT, extortion
Actual Mass Real-World Use of Breached Credentials Will Be Seen

- Credential stuffing has become more rampant
- Users recycle passwords across various sites
- Applications: for rewards, mileage, benefits, troll accounts
Getting Ready for the Year Ahead

- Users must stay on top of threat news via blogs like *Simply Security* and *Security Intelligence* to avoid falling for new social engineering attacks.
- Protect all devices and data from malware, malicious email and URLs
- Enforce good security practices (password maintenance)
Risks related to the WFH trend, GDPR compliance difficulties, social engineering, BEC, automation, and extortion will become causes for concern.
Home Networks in Work-From-Home Scenarios Will Open Enterprises to BYOD-like Security Risks

- Intersection of rise of remote-working/WFH arrangements and presence of more smart devices in the home
- Printers, network storage devices, etc. in the home double as employee devices
- Every unsecure home device is an entry point into the enterprise network
Real-World Events Will Be Used in Social Engineering Attacks

- Tokyo Olympics 2020, Brexit, Italian budget issues, and other sociopolitical developments will be used as social engineering lures.
► Business Email Compromise Will Go 2 Levels Down the Org Chart

- Cybercriminals will target the CxO’s secretary or executive assistant, or a high-ranking director or manager in the finance department, etc.
Automation Will Be a New Wrinkle in Business Process Compromise

- More aspects of monitoring and function are conducted through software or online applications
- Will also be used in supply chain attacks
More unknowns require intelligent, multilayered security. The IT security skill set shortage will thus become more pronounced, and augmenting existing expertise will become more critical.

Enterprises must be protected using endpoint, network and gateway solutions like:

- User Protection
- Hybrid Cloud Security Solution
- Network Defense
- Connected Threat Defense
InfoSec and IT teams will see more cases of threat actors using “normal” objects to blend in the network, successful n-day exploit attacks, and more reasons to invest in AI for cybersecurity.
Cybercriminals Will Use More Techniques to Blend In

- New ways of using normal computing objects for purposes other than their intended uses or designs — a practice known as “living off the land” — will continue to be discovered, documented, and shared:
  - Unconventional file extensions
  - Less reliance on actual executables, as in the use of “fileless” components, **Powershell**, scripts, and macros
  - **Digitally signed malware**
  - **New activation methods**
  - Abuse of email accounts or online storage services and apps
  - Minimally modifying or infecting legitimate system files
Highly Targeted Attacks Will Begin Using AI-Powered Techniques

- AI to predict the movements of executives or other persons of interest (hotels, routes, flights, other preferences, etc.)
Fileless malware is designed to make detection by security solutions more difficult. Organizations, therefore, need to implement multilayered solutions that can help detect threats in gateways, networks, servers, and endpoints.

Likewise, a proactive, multilayered approach to security is key to thwarting threats that exploit vulnerabilities. This includes network traffic solutions and vulnerability protections.
Smart home administrators will find their routers caught in an IoT worm war, and the elderly will become easy victims to cybercriminals through health trackers.
Cybercriminals Will Compete for Dominance in an Emerging IoT ‘Worm War’

- Recent router-based/IoT attacks are mostly based on the same leaked source code from Mirai
- They use the same handful of exploits and mostly bad login credentials, which means they are auto-scanning and discovering the same devices
- Since one malware needs to be in control of a single device, cybercriminals will add code to lock out “competitors”
The First Case of Senior Citizens Falling Easy Victims to Smart Health Device Attacks Will Emerge

- Companies are exploring the senior citizen customer base as potential users of smart trackers or other internet-connected health devices.
- Senior citizens have been targets of phone scams because of their relative wealth, given their retirement savings.
- Elderly users of health trackers will not be computer-savvy enough to check the privacy settings of these devices or to keep their accounts secure.
Getting Ready for the Year Ahead

- For home users **Network Security** solutions that blocks threats at the router level, so the devices are protected as well as IoT scanning tool.

- For enterprises monitors **all ports and protocols** for advanced threats and defends the network in real time using machine learning.
2019 Take Aways

1. Patch and backup – no excuses.
2. It’s still all about vulnerabilities and exploits.
3. Data is the new currency.
5. Security embedded into non-traditional initiatives.
6. Don’t use people as the solution for everything new.
7. Increase security awareness – non negotiable.
TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.
• 12 Modules
  • Fact Sheet
  • Quiz
  • Video
• Discussion Guide
Ftc.gov/cybersecurity

- Cybersecurity Basics
- 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
Cybersecurity and Your Small Business
Topic: Online Safety & Security
Language: English
Format: Booklet
Information on 12 different cybersecurity topics to help small business owners and staff understand common cyber threats and how they can protect their business.

Topic: Online Safety & Security
Language: English
Format: Booklet
What can companies learn from the FTC's >50 data security cases? Lesson #1: Start with security.

Careful Connections: Building Security in the Internet of Things
Topic: Online Safety & Security, Privacy & Identity
Language: English
Format: Booklet
Advice for innovators about keeping security at the forefront when developing connected products for the Internet of Things.
SMB Quick Wins for 2019

NEW YEAR’S RESOLUTION? STOP HITTING “PAWS” ON THAT SYSTEM UPDATE.

#UPDATEMEOW

Disclaimer: No component or product can be absolutely secure.
SMB Quick Wins for 2019

• Set up 2-Factor Authentication
• Think Before You Connect
• Keep a Clean Machine for Desktop and Mobile Devices
• Socialize online with security in mind
• Back up your data
• Establish and maintain strong passphrases
• Make training available to your staff and colleagues
• Awareness is not action...so go act now
Webinar Series
Second Tuesdays
2:00 p.m. EST

Up-Coming Webinars:

- **February 12th** “Hackers love tax time! Learn how to secure your W-2s and other sensitive business and customer information this tax season”
- **March 19th** Cybersecurity for Small Agricultural Businesses: Cyber threats to precision agriculture

To Register: www.staysafeonline.org
New Year’s Resolution: Protect Your Sensitive Business Information in 2019

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

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

**Contributing Sponsor**
MediaPRO  
https://www.mediapro.com/SMB

**National Institute of Standards & Technology**
www.nist.gov/cyberframework

**Federal Trade Commission**
www.FTC.gov/smallbusiness

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