Securing Your Home Office or Home-Based Business

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

Presented By:
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:

- Trend Micro
- education
- INFOSEC

---

The "CyberSecure My Business" was a 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.
Upcoming Events

• **August 13:** What are Phishing, vishing and smishing and how can I protect my business from these threats?

• **September 24:** CyberSecure My Business workshop in Madison, WI

• **October:** National Cybersecurity Awareness Month!

Register and view all events at: https://staysafeonline.org/events/
How to Get Involved

• Become a NCSAM Champion (starting mid to late July) – sign up, take action and make a difference in online safety and security. It’s free and simple to register.
• Post on social media using #CyberAware
• Promote NCSAM and link to staysafeonline.org/ncsam on your company website
• Submit your events to NCSA’s community calendar by emailing info@staysafeonline.org

Sneak Peak of Topics:
• Weekly cyber safe habits related to top threats - phishing, public WIFI, updates, etc.
• Personal accountability and proactive behavior
• Consumer connected devices
• Privacy
• Ecommerce security

For more information: https://staysafeonline.org/ncsam/
Michael Palmer
Product Manager
Consumer division, Trend Micro

Cyber-Securing Your Home Office or Home-Based Business

July 9, 2019
Introduction

Today, the home network has become a fertile target for hackers looking to commit financial fraud, steal data or compromise devices for use in large-scale attacks. Home offices and remote workers face steep challenges when it comes to staying secure.

• Agenda
  – Threats for Home Offices and Remote Workers
  – How Home Offices and Remote Workers are Vulnerable
  – How Home Offices and Remote Workers Can Secure Themselves
Threats for Home Offices and Remote Workers
Threats for Home Offices and Remote Workers

• Credential Theft
• Ransomware
• Tech Support Scams
• Breach Entry Point
Credential Theft

- Phishing 🔄
  - Clicking on links
  - DNS Changer
Credential Theft

• Credential Stuffing
  – Steal credentials
  – Try in other services

Almost 60% of login attempts at consumer online banking are credential stuffing
- Threatpost (July 2018)
Ransomware

• Hackers encrypt your files and ask for ransom to decrypt them

• WannaCry (2017)
Tech Support Scams

• “Microsoft Tech Support”
Breach Entry Point

• Remote Workers: Don’t be that guy!
• Beware of:
  – Social engineering
  – Phishing
  – Credential stuffing

“74% of IT decision makers surveyed whose organizations have been breached in the past, say it involved privileged access credential abuse”
- Forbes (Feb 2019)
How Home Offices and Remote Workers are Vulnerable
How Home Offices and Remote Workers are Vulnerable

• Insecure practices
• Insecure networks
• Insecure devices
Insecure Practices

• Clicking on links
• Default or weak passwords
• Using the same password for everything
• Out-of-date OS
• No data backups
• No security software installed
Insecure Networks

- Default admin login and password
- Remote management enabled
- Open ports
- Out-of-date firmware
Insecure Devices

- Default admin login and password
- Insecure security settings
- Out-of-date firmware
How Home Offices and Remote Workers Can Secure Themselves
Lockdown your Router

• Set a password on your SSID
• Change the admin password
• Turn off remote administration
Lockdown your PCs

• Turn off WiFi sharing
• Update OS regularly
• Install antivirus
Lockdown your Smart Devices

• Change the admin password
• Update the devices regularly
• Move to the guest network
Use a password manager

• Saves passwords
• Encourages use of different passwords
• Generates strong passwords
Protect Your Data

• Backups
• More Backups
  – Cloud
  – Physical
• Automate
American Airlines Support <cinziawolfgang@tiscali.it>

Michael Palmer (PM-TW)
Tuesday, July 2, 2019 at 3:30 AM
Show Details

Unsubscribe

View in browser

American Airlines

Dear valued customer,

Thank you for booking with American Airlines. We have received your booking under reference 6777-783 and are reviewing your payment.

Yours sincerely,
American Airlines Support

You can also view the details of this request by following this link:
https://www.aa.com/?clientrequest=6777-783

http://essemengineers.com/blog/wp-content/guessnw.html
For Remote Workers

• Follow company IT security guidelines
• Don’t connect to untrusted networks
• Use company VPN
• Don’t use work equipment for personal use
THE ART OF CYBERSECURITY

Threats detected and blocked globally by Trend Micro in 2018. Created with real data by artist Daniel Beauchamp.
Whitney Moore
Attorney,
Division of Privacy and Identity Protection,
Federal Trade Commission

https://www.ftc.gov/smallbusiness
SECURING YOUR HOME BUSINESS

Whitney Moore
July 9, 2019
Federal Trade Commission
DISCLAIMER

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 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.

For more information:
https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network
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.
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.
How the Scam Works

The scammers may pretend to be from a well-known tech company, such as Microsoft. They use lots of technical terms to convince you that the problems with your computer are real. They may ask you to open some files or run a scan on your computer — and then tell you those files or the scan results show a problem...but there isn't one.

The scammers may then:

- Ask you to give them remote access to your computer — which lets them access all information stored on it, and on any network connected to it
- Install malware that gives them access to your computer and sensitive data, like user names and passwords
- Try to sell you software or repair services that are worthless or available elsewhere for free
- Try to enroll you in a worthless computer maintenance or warranty program
- Ask for credit card information so they can bill you for phony services or services available elsewhere for free
- Direct you to websites and ask you to enter credit card, bank account, and other personal information
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
TEMAS DESTACADOS

Ciberseguridad

Las estafas y su pequeño negocio

Aprenda conceptos de ciberseguridad e incorpórelos a la rutina de su negocio.

Desarrolle un plan para proteger la información personal de sus clientes.

Entérese de lo que tiene que hacer si se produce un incidente de seguridad de datos. (en inglés)

Suscríbase para recibir los artículos del Blog para negocios en business.ftc.gov/blog. (en inglés)

Infórmese sobre las estafas dirigidas contra su pequeño negocio

Encargue publicaciones gratuitas y compartálas con sus colegas.

Mire este video y aprenda más sobre las estafas dirigidas contra los pequeños negocios.

Reporte las estafas contra los pequeños negocios en ftc.gov/queja.

https://www.ftc.gov/es/tips-advice/business-center/small-businesses/espanol
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

**Title:** Stick with Security: A Business Blog Series

**Date:** November 2017

---

## Stick with Security: A Business Blog Series

The 2017 Stick with Security series focuses on the issues of cybersecurity and information security. The series is designed to provide practical solutions to common cybersecurity challenges and to help businesses, organizations, and individuals stay ahead of the curve in their cybersecurity efforts.

## Table of Contents

<table>
<thead>
<tr>
<th>#</th>
<th>Stick with Security: A Business Blog Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Stick with Security: A Business Blog Series</td>
</tr>
<tr>
<td>2</td>
<td>Stick with Security: A Business Blog Series</td>
</tr>
<tr>
<td>3</td>
<td>Stick with Security: A Business Blog Series</td>
</tr>
<tr>
<td>4</td>
<td>Stick with Security: A Business Blog Series</td>
</tr>
<tr>
<td>6</td>
<td>Stick with Security: A Business Blog Series</td>
</tr>
<tr>
<td>7</td>
<td>Stick with Security: A Business Blog Series</td>
</tr>
<tr>
<td>8</td>
<td>Stick with Security: A Business Blog Series</td>
</tr>
<tr>
<td>9</td>
<td>Stick with Security: A Business Blog Series</td>
</tr>
<tr>
<td>10</td>
<td>Stick with Security: A Business Blog Series</td>
</tr>
<tr>
<td>11</td>
<td>Stick with Security: A Business Blog Series</td>
</tr>
<tr>
<td>12</td>
<td>Stick with Security: A Business Blog Series</td>
</tr>
</tbody>
</table>

---

**Notes:**

- The Stick with Security series is a collaborative effort between various experts in the field of cybersecurity.
- The series aims to provide businesses with practical tips and strategies to improve their cybersecurity practices.
- For more information, visit the Stick with Security website or contact the series' lead editor.

---

**Acknowledgments:**

This series was made possible with the support of our sponsors, who provided valuable insights and resources to help businesses stay ahead of the curve in their cybersecurity efforts.

---

**About the Series:**

The Stick with Security series is the result of a partnership between cybersecurity experts, businesses, and organizations. The series is designed to provide practical solutions to common cybersecurity challenges and to help businesses, organizations, and individuals stay ahead of the curve in their cybersecurity efforts.

---

**Contact Information:**

For more information, contact the series' lead editor at stickwithsecurity@ cybersecurity.com or visit the Stick with Security website at stickwithsecurity.com.
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