Cybersecurity Considerations for Small Business

SABDOC - April 18, 2019
“Cyber theft is the fastest growing crime in the United States.”

- More than six in ten Americans own a smartphone
- Nearly one in five Americans has been the victim of a cybercrime
- The weakest link continues to be the “most valuable asset” of an organization, the people who sit between the seat and the keyboard
  - $2.4 million average cost of malware attack
  - 50 days to resolve insider attack
  - 23 days to resolve a ransomware attack

With Permission from Geoff Jenista, CISSP
Department of Homeland Security
Today we’ll cover . . .

Tips
7(j) Training
The Easy 6
What? Me Worry?

- 58 percent of malware attack victims are categorized as small businesses.
- 60 percent of small businesses say attacks are becoming more severe and more sophisticated.
- (Ponemon Institute's 2017 State of Cybersecurity in Small & Medium-Sized Businesses report)

- The average amount demanded from ransomware was $1,077
- The average cost to businesses per attack was $133,000. (includes downtime, lost opportunities and recovery)
- (SCORE - at Booth 13 today at SADBOC Procurement Fair)
The single biggest risk?

- **Email** is responsible for spreading 92% of all malware. CSO Online estimates that email is the primary method of malware delivery (www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html)

- Office files constitute 48% of malicious email attachments. Forty-eight percent of malicious email attachments were Microsoft Office files in 2018, according to Symantec’s ISTR 2019 report. “.Doc” or “.dot” files represented 37% of malicious email attachments.

This pops up on your email . . . what do you do?
Do **NOT** click any of the choices!!

Hold down the CONTROL (Ctrl) and at the same time, press the F4 key.
1. Have security software and keep it ‘current’
2. Automate software updates
3. Protect all devices that connect to the internet (along with computers, smartphones, gaming systems and other web-enabled devices also need protection)
4. Plug & Scan - USBs and other external devices can be infected by viruses and malware - use your security software to scan them.
5. Lock Down your Login (LockDownYourLogin.Org)
6. Back up your business date using 3-2-1; 3 backup copies, 2 different media, 1 offline and in a separate location
What is the 7(j) program?

The 7(j) Program Management & Technical Training is funded by the U.S. Small Business Administration (SBA) with a network of partners to help firms successfully compete for federal, state and local contracting opportunities as a prime contractor or subcontractor.

For cybersecurity, Synergy Solutions facilities online training for the 7(j) program;

Link to registration page: https://synergysolutions.talentlms.com/

Flier at the US SBA - - - table 14 (back corner) for more information.
7(j) - Cybersecurity Training

To be eligible for FREE training, your firm must meet one of the following criteria:

- Certified 8(a) participant or HUBZone small business; or economically disadvantaged women-owned small business;
- A small business that is owned and controlled by an economically and socially disadvantaged individual;
- A small business located in an area of high unemployment or low-income; or
- A small business that is owned by a low-income individual.
7(j) - Cybersecurity Training

- NIST Cybersecurity Framework
  (https://www.nist.gov/cyberframework)
NIST has a special section for small business - guides and other resources here
Tips

- Do a Security ‘check-up’ on yourself (handout)
- Use a Password Manager - (Who can remember all those passwords?)
- 2-Factor Verification
- Put a ‘space’ in the PW, especially at the END.
- Data Breach Notification in MN Minn. Stat. §§ 325E.61, 325E.64
Have I been pwned.com

(https://haveibeenpwned.com/)
Tools available - Handouts

1. FTC/Homeland Security/NIST/SBA - “Cybersecurity for Small Business” booklet
Questions?
Thank You!

Lyle Wright, Associate State Director
651-259-7419
Lyle.Wright@state.mn.us