Hosted by SCORE | Bucks County

Cyber Security for Small Business

RICHARD S. ZWEIG – CMIT SOLUTIONS

About SCORE

As a resource partner of the SBA, we help small businesses by:

Providing free business advice and mentoring

Offering low or no-cost business training

Sharing free business templates and resources

Request a SCORE mentor at www.score.org/find-mentor

Your Presenter

Richard Zweig

Owner of CMIT Solutions of Central Bucks

25+ Years of Information Technology experience

Managing the technology needs of small businesses for over 8-years.

Cyber Security Threat Landscape

- In 2024, small businesses face increasing cybersecurity threats, prompting a focus on advanced technologies and updated strategies.
- Key trends include the adoption of Zero Trust Security, the integration of AI and Machine Learning for threat detection, and enhanced cloud and supply chain security measures. Also, small business are adoption new regulations such as PCI DSS 4.0
- Small businesses are now the focus of hackers due to lack of security in place, using small businesses to test for bigger “phish”
- 60% of small to medium businesses are forced to suspend operations, and in many cases, never reopen for business after a security incident.

Topics that we will cover

- The definition of Cyber Security
- Security concerns for Small Businesses
- What do you need to protect?
- Passwords
- Advanced Technologies
- Steps that you can take Right Now to improve your security!

What is Cyber Security?

Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices, and data from cyber attacks.

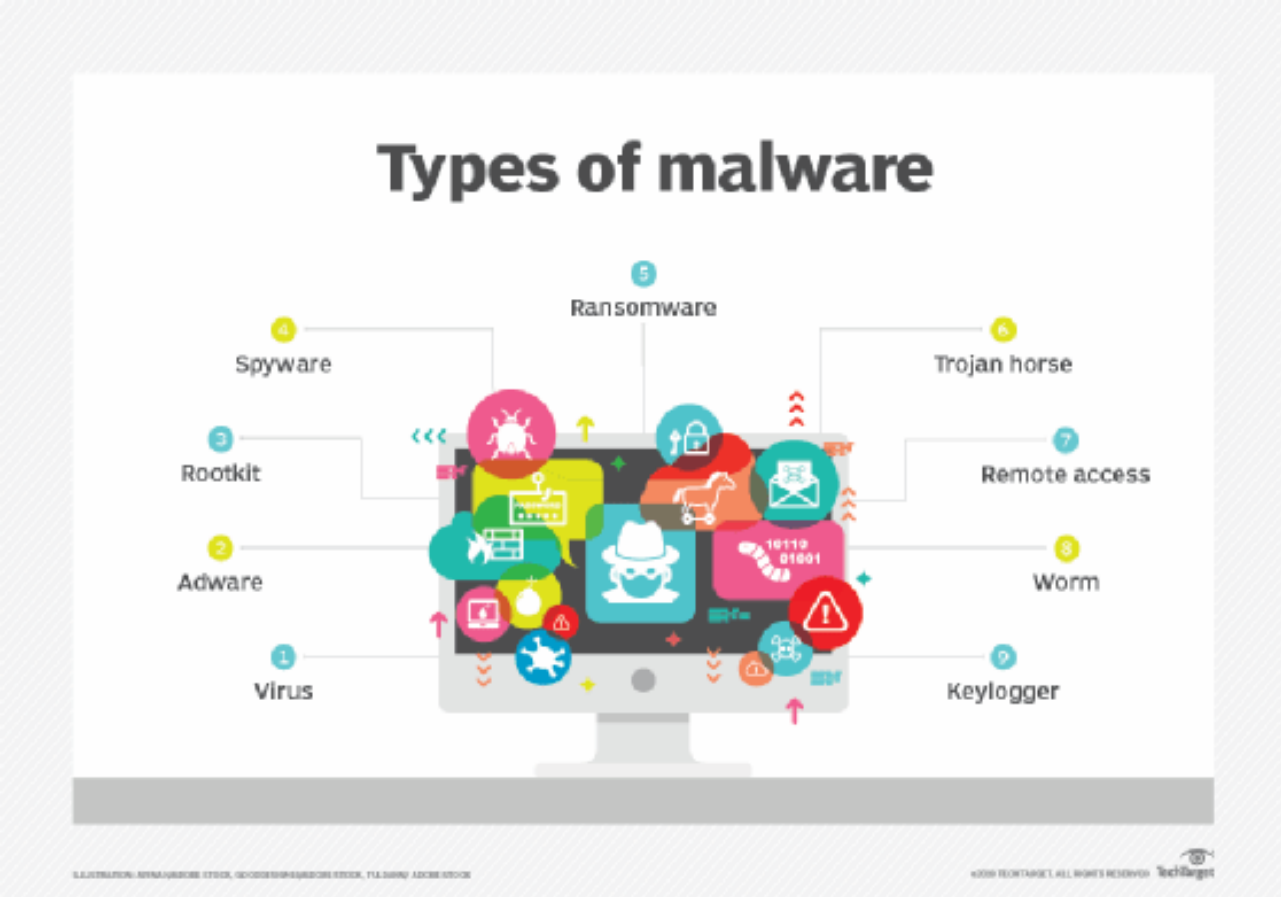
A multi-layered approach aims to reduce the risk of cyber attacks and protect against unauthorized exploitation of systems, networks, and technologies.

Alarming Statistics

- It takes about 6-months to detect a data breach
- 43% of all cyber attacks are aimed at small businesses
- 91% of attacks launch with a phishing email
- A business falls victim to a ransomware attack every 14 seconds
- 38% of malicious attachments are masked as one Microsoft Office type of file or another

Types of Threats

Cybersecurity Threats	Likely to Affect	Need to Understand Better
Virus	64%	41%
Spyware	62%	42%
Phishing	52%	32%
Firmware Hacking	34%	29%
IP Spoofing	32%	29%
Ransomware	31%	30%
Attacks on Virtualization	30%	30%
Social Engineering	26%	26%
Hardware-Based Attacks	26%	25%
DDoS	24%	22%
IoT-Based Attacks	23%	22%
Botnets	22%	23%
Rootkits	21%	21%
Man in the Middle Attacks	20%	23%
SQL Injection	18%	20%



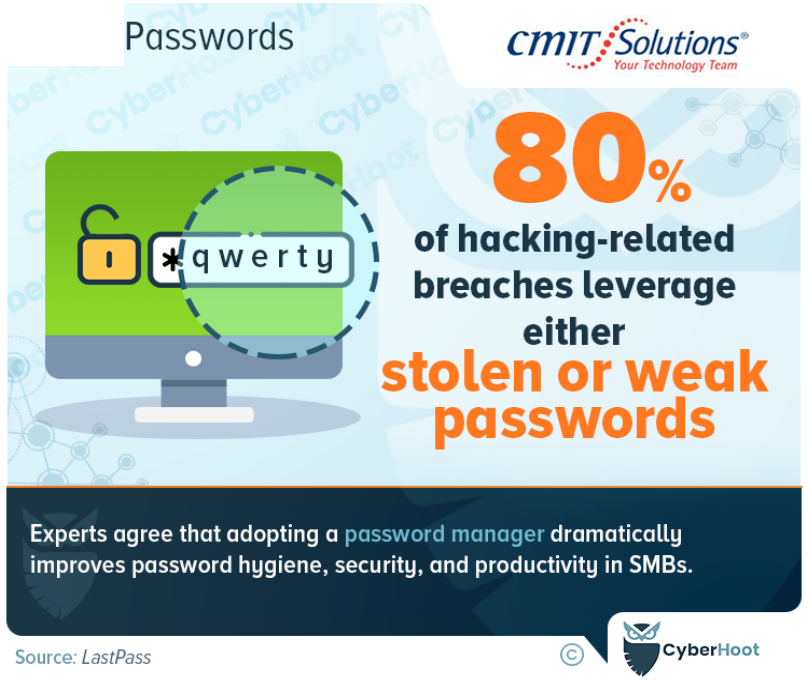
What are the risks of poor cybersecurity?

There are many risks, some more serious than others.

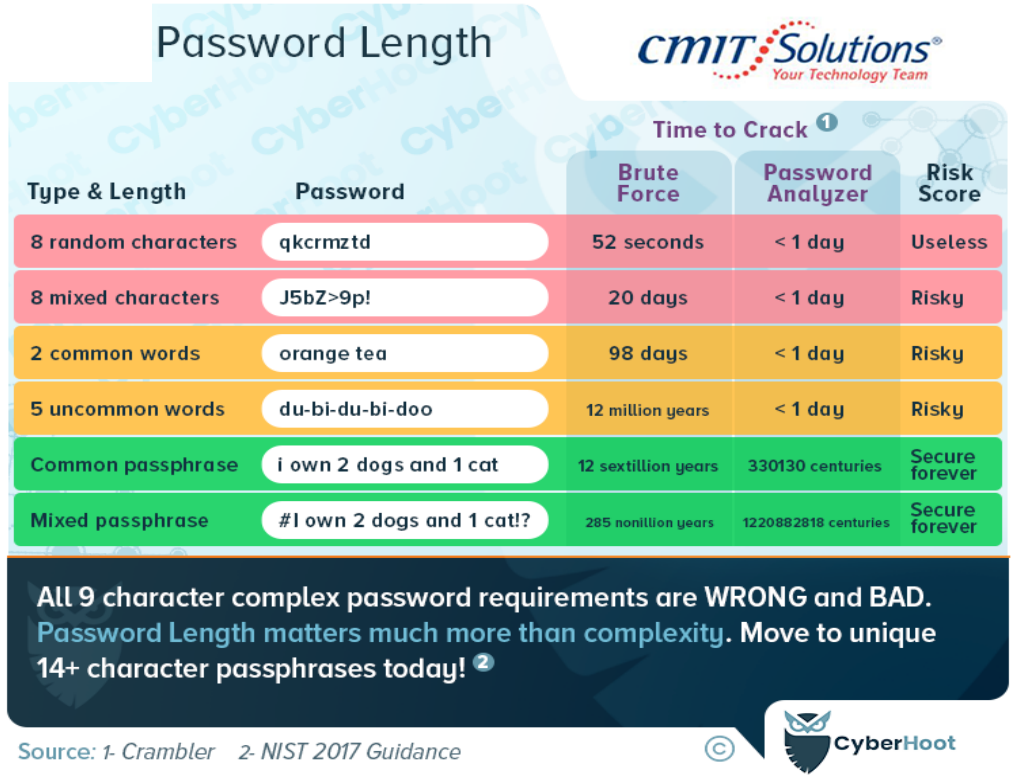
How about:

- Malware erasing your entire system
- Hacker breaking in and altering files
- Attacker using your computer to attack others
- Attacker stealing your credit card information, or your customers, and making unauthorized purchases

Passwords



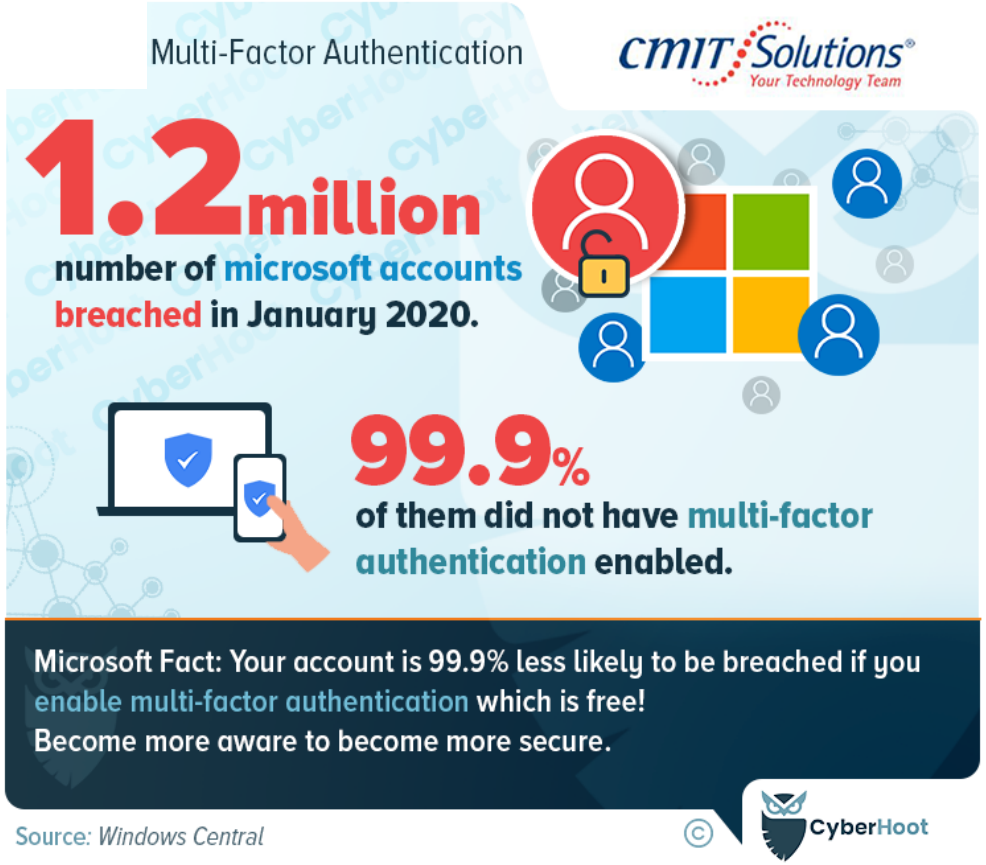
Source: *LastPass*



Source: *1- Crambler 2- NIST 2017 Guidance*

CMIT Solutions Your Technology Team

What is MFA/2FA? Why is it so important?



Why Use a Password Manager?

Biggest Password Problem and Risk Today

- The average person has to logon to over 170+ sites/services and only has 3 to 19 passwords
- Lots of weak, shared passwords (or password patterns)
- Lots of passwords that are easy for adversaries to guess
- One compromise more easily leads to other compromises

Advanced Technologies

- AI and Machine Learning – These technologies are being used to analyzed vast amounts of data, identify patterns, and predict potential threats. This improves the speed and accuracy of threat detection and response.
- Zero Trust Security – This model assumes no user or device is inherently trustworthy, requiring strict verification and authentication for all access attempts, minimizing the risk of unauthorized access
- Cloud Security – With the increasing reliance on cloud services, businesses are focusing on securing their data in the cloud the encryption, access controls, and regular audits.

Additional Security Measures

- Supply chain security
- Cryptography
- Data Loss Prevention (DLP)

Regulations and Compliance

PCI DSS 4.0 – Latest version for the credit card industry is now mandatory.

Proactive Strategies such as incident response planning, regular security assessments, secure configuration, monitoring and detection

Protecting your business

Planning and assessment

- The main focus is to protect your business
- Use an IT Security Professional to help you determine what is critical to your business operations, or use a cybersecurity planning tool provided by the FCC, SBA, or other reputable organization.
- Every business is different. Focus your assessment to your specific type of business

Serious about Cybersecurity!

- All businesses need to get serious about Security
- Warnings by FBI that cyber attacks will increase, especially for small businesses
- Businesses that don't get serious, and are attacked, will no longer be in business

What do you need to keep your business secure?

- All devices (Computers, phones, etc.) must have security software
- Implementation of Technology (minimum have a firewall)
- Must implement Data Backup (Backup, Backup, Backup and Backup…….)
- Password Management Program with MFA
- Security Awareness Training

What should be done RIGHT NOW!

- Perform a Cyber Security Assessment
  - What you don't know, you don't know
  - An assessment can identify the vulnerabilities that you need to address
  - Either hire an IT security professional, or access online resources from reputable agencies (i.e., SBA, FCC, NIST, etc.)
- Implement Technology
  - Install a Firewall
  - Install security software on all endpoints
  - Keep all software up-to-date
  - Email security

What should be done RIGHT NOW!

- Backup all data
  - Implement a data protection and backup program. Test backups often.
  - Secure ALL information, whether onsite or in the cloud
  - Encrypt all endpoints
- Password Management with MFA
  - Strong Passwords! (Don't use the same or a reiteration of a previous password)
  - Enable MFA or 2FA
  - Do not write down passwords or keep in a file (Excel, Note, Sticky Note, etc.)
  - Strongly suggest use a Password Manager

What should be done RIGHT NOW!

- Conduct Security Awareness Training for all employees.
- Teach them how to identify phishing emails
- Teach them how to identify bogus links
- Teach them what to be aware of in all aspects while using company equipment (Remote or in the office)
- Create IT use policies!

Additional Security Topics

- We used to protect by locking down the perimeter, think walls around a castle. However, the cloud and a remote working environment has changed that! Need to protect data, information, etc. in that space as well
- Cloud companies not responsible for your information. You are!
- Make sure you have solid remote working policies and that your employees know and understand them!
- AI is and will play a crucial role in cybersecurity

Summary

- We defined cyber security
- We discussed the concerns of security on small business and poor cyber security presents inherent risks
- We discussed the importance of each business protecting themselves based on the business industry
- Perform a security risk assessment to identify your vulnerabilities
- Use an IT Professional or utilize resources for small businesses to perform a cybersecurity assessment.

Identified the following to do RIGHT NOW!

- Implement technology such as Firewalls, security software, encryption, etc. Use a Layered Security Approach!
- Backup all data!
- Strong Password Management. Use MFA or 2FA
- Train your employees (Security Awareness Training)

Check online resources for more information on Cybersecurity for Small Business (FCC, SBS, NIST, FBI, etc.)

Questions?

Helpful Links

- Find SCORE resources for small businesses at www.score.org/templates-resources
- Find more SCORE live and recorded workshops and courses at www.score.org/get-business-training
- Book an appointment with a SCORE mentor at www.score.org/find-mentor

THANK YOU FOR YOUR PARTICIPATION

Funded in part through a cooperative agreement with the U.S. Small Business Administration.

All opinions, conclusions, and/or recommendations expressed herein are those of the author(s) and do not necessarily reflect the views of the SBA.