Cyber Security for Small Business

Hello there.

We're CMIT Solutions.

Cyber Security Threat Landscape

- Cyber incidents have surged among small businesses
- 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
- Cybersecurity Myths
- What do you need to protect?
- Passwords
- 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

CMIT Solutions
Your Technology Team

10 Cybersecurity Myths Debunked

Solutions®
Your Technology Team

Security Concerns

Types of Threats

Staying ahead of cybersecurity threats is not an easy task! There is a long list of threats, and the problem keeps growing.

Cybersecurity Threats

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

Types of malware

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 and MFA

Day 03 Passwords

cmit Solutions® Your Technology Team

80%

of hacking-related breaches leverage either

stolen or weak passwords

Experts agree that adopting a password manager dramatically improves password hygiene, security, and productivity in SMBs.

Source: *LastPass*

Day 17 Password Length

cmit Solutions® Your Technology Team

Type & Length	Password	Time to Crack [1] Brute Force	Password Analyzer	Risk Score
8 random characters	qkcrmztd	52 seconds	< 1 day	Useless
8 mixed characters	J5bZ>9p!	20 days	< 1 day	Risky
2 common words	orange tea	98 days	< 1 day	Risky
5 uncommon words	du-bi-du-bi-doo	12 million years	< 1 day	Risky
Common passphrase	i own 2 dogs and 1 cat	12 sextillion years	330130 centuries	Secure forever
Mixed passphrase	#I own 2 dogs and 1 cat!?	285 nonillion years	1220882818 centuries	Secure forever

All 9 character complex password requirements are WRONG and BAD. Password Length matters much more than complexity. Move to unique 14+ character passphrases today! [2]

Source: 1- Crambler 2- NIST 2017 Guidance

CyberHoot

Day 26 Multi-Factor Authentication

cmit Solutions® Your Technology Team

1.2 million

number of microsoft accounts breached in January 2020.

99.9%

of them did not have multi-factor authentication enabled.

Microsoft Fact: Your account is 99.9% less likely to be breached if you enable multi-factor authentication which is free!
Become more aware to become more secure.

Source: *Windows Central*

CyberHoot

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

What do you need to protect?

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 (FCC, SBA, etc.)
- Every businesses is different, so the focus is specific to your business

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

What do you need to do to keep your business secure?

- All devices 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 can you do 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 a professional IT professional, or access online resources from reputable agencies (i.e., SBA, FCC, NIST, etc.

Implement technology

- At a minimum, install and configure a Firewall
- All end-points should have security software (Anti-Virus, Anti-Malware, Anti-Spyware)
- Implement a maintenance program to keep up-to-date on software and firmware patches.
- Email security to prevent phishing, etc.
- Internet Content Filtering

Backup, Backup, Backup!

- Implement a data protection and backup program
- You must secure all information. Whether on premise, or in the cloud.
- Encrypt all end-points.
- Test backups often

Password Management with MFA

- A strong password management program is vital to the security. 50% of passwords are reiterations of previous passwords (ex. Gre8tBoss1, Gre8tBoss2!, Imagreatboss123!) – Now it is recommended that you use a password phrase 14+ characters, not a password (i.e., I like to eat 2 pickles!)
- Enable MFA (Multifactor Authentication)
- Do not write down passwords, excel, note, sticknotes, etc.

Security Awareness Training

- 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!

Summary

- We defined cyber security as the application of technologies, processes, and controls to protect systems, networks, programs, devices, and data from cyber attacks, and this was to reduce risk and protect your business.
- Cybersecurity Myths
- We discussed the concerns of security on small business and poor cyber security presents inherent risks

Summary

- We discussed that each business should plan to protect their environment based on their needs. Cyber security is implemented differently by industry and business need
- Perform a security risk assessment to identify your specific vulnerably and how to address it.
- Use an IT professional, or utilize online resources from reputable sources (SBA, FCC, NIST, etc.) to perform a cyber security assessment.

Summary

- 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 with MFA
  - Train your employees (Security Awareness Training)

Questions?

Thanks!

Richard Zweig
CMIT Solutions of Central Bucks
(267) 895-1785
rzweig@cmitsolutions.com
www.cmitcentralbucks.com