Are you ready to get hacked?  
Cybersecurity: Top 5 things you can do to protect your office (and personal)

Objectives

- Review basic cybersecurity terms and frameworks to suggest Top 5 small business cybersecurity issues
  - Password protection
  - Social engineering – Phishing, SM/Smhing, Vishing
  - Wi-Fi security
  - Response and Incident Plan
  - Don’t delay

Basic Cybersecurity Terms
Cyber History

- ‘Cyber’ is from the Greek word for navigator
- Norbert Wiener coined ‘cybernetics’ around 1948
- Cybernetics - the science of communications and automatic control systems in both machines and living things

Norbert Wiener

Cybersecurity - CIA

The Right Mindset

Cybersecurity is about much more than IT
Computer security, physical security, information security

- Hardware
- Software
- Policies / procedures
- Plans
- Training
- Physical security (controlled access, locked equipment)
- Personnel security (screening process, background checks)
- 3rd Party Access security - Pivoting

Cybersecurity Frameworks you can use for your business

1. CIS Controls (Center for Internet Security)
2. NIST 800 (National Institute of Standards and Technology)
Why should you care about online security?

Understand what is at stake when you create an account online:

- Think about the data you are giving them?
- How and where do they share data?
- Places like: Facebook, Instagram, etc.

Your email is a VALUABLE asset.

Top 5 Small Business Issues
1. Password Protection

Forget Tough Passwords: New guidelines Make It Simple!
- Keep passwords long and memorable
- Experts no longer suggest special characters
- No mix of lower and uppercase letters
- Passwords never need to expire

Here’s what we’ve been told about passwords:
- Make them complicated.
- Use numbers, question marks and hash marks.
- Change them regularly.
- Use different passwords for each app and website.

Paul Grassi, senior standards and technology adviser at NIST, led the new revision of guidelines.

Source: https://www.npr.org/sections/alltechconsidered/2017/08/14/543434808/forget-tough-passwords-new-guidelines-make-it-simple

2. Social Engineering
- Phishing
- SMSishing
- Vishing
Phishing...

Fake Virtual Private Network
- Man in the middle
- Young people at school
Spear Phishing

SMSishing ...

Vishing ...
Vishing ...
Voice solicitation in order to get information
- Never give out personal information over a call
- Use a VPN – it spoofs your IP

DEF CON – Hacker Convention, Las Vegas
- Jessica Clark, Social Engineer Competitor
- Super Intelligent
- Uses “giddy” tactic
- Uses special tool in order to persuade...

Post Video Breakdown
DEF CON – Hacker Convention, Las Vegas
- Jessica Clark, Social Engineer Competitor
- Super Intelligent
- Uses “giddy” tactic
- Uses CRYING BABY in order to persuade...

For small / medium business...
- Do you have Customer Service checks?
- Do you have security procedures?
- Have you discussed this with your employees?
- Would your company have fallen victim?
3. Secure your Wi-Fi

Have you taken a “set it and forget it” approach with your Wi-Fi network?

- Change your admin username and password upon setup
- Activate encryption
- Disable guest networks
- Check your router for firmware updates once a month
- Turn down the transmit power control (if able)

These steps are easy to take. They can also go a long way in keeping your Wi-Fi network secure.

Internet of Things (IoT)

- NEST or other Thermostats
- Alexa, Google Home, Apple Home
- Television, Xbox (gaming consoles)
- Ring (doorbells)
- Cameras

Griefer hacks baby monitor, terrifies toddler with spooky voices
Dangers of Public Wi-Fi
4. Have a Response Plan (Incident Plan)

- Preparation
- Detection & Response
- Containment & Eradication
- Post-Incident Handling

NIST SP 800-61, Computer Security Incident Handling Guide

Do have plans...
- Ransomware
- Social Media
- Network Breach
- Data Breach

Turn your Plans into procedures...

5. Don’t delay if you spot a security concern
- “It’s better to be safe than sorry” absolutely holds true in regard to security for your small business.
- If you have any reason to believe something has gone wrong, no matter how big or small the issue, it’s imperative to pinpoint the problem and implement an immediate solution.
Implement a cybersecurity program

- Train employees on cybersecurity issues
- Inventory / count your IT assets
- Patch all software and OS’s
- Refresh networking gear software (routers, etc.)

**Have great backups**

- Get a cybersecurity audit and heed its findings
- Use Access Control
- Revisit or create cybersecurity policies
- Have procedures for a cyber incident

**Utilize a Cybersecurity Framework!!!**

Thanks and remember....

1. Password protection
2. Social engineering awareness
3. Wi-Fi security
4. Response and Incident Plan
5. Don’t delay

John M. Romero
john.romero@tamu.edu