Commercial Appraisal
Practice Security
Cyber security:

It’s life or death for your business!
43% of cyber attacks target small business
75% of SMB reported an attack in 2018
34% of hacked businesses suspend operations for more than a week
75% of hacked businesses permanently lose data
The average time to detect a breach is six months
60% of small businesses die within six months of a cyber breach (Small Biz Trends)
Agenda

- Avoid threats
- Manage your passwords
- Surf safely
- Prevent as much as possible
- When all else fails, know what to do
Avoid cyber threats
Your office faces three data loss threats:

- Social Engineering: 18%
- Hacking: 23%
- Malware: 59%
By far, the most dangerous security threat in your office is...

PEOPLE!

• 95% of successful cyber attacks take advantage of people
Most human error is lost or stolen devices

- Work Area: 39%
- Vehicle: 34%
Types of cyber attacks

MALWARE

PHISHING

SOCIAL ENGINEERING
What is Malware?

• Definition:
  • Software designed to disrupt, damage, or breach computer systems
Malware has seen explosive growth
Malware types

- Ransomware
- Botnet
- Crypto jack
Ransomware

• Locks computers
• Encrypts data
• Demands payment to restore access
Botnet

• Takes control of computers
• Uses them in illegal activity
Crypto Jack

• Takes control of computers
• Uses them to create crypto currency, e.g. Bitcoin
Malware is a business

- There are products and frameworks to build it
- You can buy the tools and parts on the “dark web”
- Our own NSA leaked sophisticated cyber technology
- Small businesses are sometimes collateral damage
How does malware spread?

- Malicious links in email
- “Lost” memory sticks
- Programs masquerading as something useful
- 40% of Malware is transmitted through Microsoft Office documents
Does Malware only exist for Windows?

- Nope...
  - Windows machines are the most common, so they get more attention from the bad actors
  - Macs are also vulnerable
  - iPhones too
  - And especially Android
How to avoid computer Malware

- Distrust email that contains attachments or links
- Verify email with attachments
- Treat email links as highly suspect
- Never, ever put an unverified USB device in your computer
- Don’t install free software
- Use anti-virus protection

Get security training!!!
What about mobile malware?

- Same as for computers
- And don’t install software outside your phone’s app store
- Apple does a good job keeping malware out of its store
- Android, not so well, but still better than nothing
Anti-Malware tip!!

Reduce dependence on email

• Consider a closed messaging platform such as:
  • Slack
  • Microsoft Teams
  • HipChat
What is “Phishing”? 

• Definition: 
  • Email designed to infect a company with malware
Phishing attacks

• Email posing as a legitimate company
• Requests some kind of action that requires the target to divulge information
• The victim will click the link and then hand over the info
Spam and phishing go hand in hand

- 91% of cyber attacks come through phishing email
- More than half of inbound email is spam
- 1 in 20 spam messages is malicious
People still fall for phishing

30% of people open phishing messages...

12% of people click on the link!
Spam topics change with the times

- Attackers use topics that are top of mind
- Money topics are hot around tax time
- Health topics show up with the New Year
- The hottest topic of 2019 is CBD
“Spear Phishing” targets a specific individual

- It is precise and purposeful
- The attacker knows some details about the company
- It’s the hardest type of phishing to recognize
How to recognize phishing

- Ask: Ask yourself if the sender would email with you in this way
- Look: Look at the sender email address
- Check: Check for spelling and grammar errors
- Watch: Watch for terms or expressions that seem out of place
- Hover: Hover your mouse pointer over the link to see if it’s legit
- Don’t: When in doubt, don’t!
Here’s a phishing example

--- Forwarded Message ----
From: PayPal <paypal@notice-access.273.com>
To: 
Sent: Wednesday, January 25, 2017 10:13 AM
Subject: Your Account Has Been Limited (Case ID Number PP-003-153-352-657)

PayPal

Dear Customer,
We need your help resolving an issue with your account. To give us time to work together on this, we’ve temporarily limited what you can do with your account until the issue is resolved.

We understand it may be frustrating not to have full access to PayPal account. We want to work with you to get your account back to normal as quickly as possible.

What the problem’s?
We noticed some unusual activity on your PayPal account.
As a security precaution to protect your account until we have more details from you, we’ve placed a limitation on your account.

How you can help?
It’s usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account.
To help us with this and to find out what you can and can’t do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

Log In

Help | Contact | Security
This email was sent to you, please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking Help at the bottom of any PayPal page.

Hover here. It won’t be paypal.com!
Don’t click, but if you did...
Here’s a really tricky technique

Good Morning.
Please see attached and confirm.

Hi,
I didn’t get any feedback

Thanks

Malicious email

Real email thread
What is “Social Engineering”?  

• Definition:  
• The art of manipulating people to divulge confidential information or perform harmful action
How Social Engineering fools us

- USB devices like memory sticks planted as if lost or misplaced
- Walk-ins from people who look like service professionals
- People deceiving security or cleaning staff
- Phone calls from official-sounding people
Phishing has a cousin called “Vishing”

- "Vishing" is Phishing but by phone instead of email
- Vishing also leverages targeting information
- Vishing is the most common form of Social Engineering
Social engineering attacks are often slow

Could be an occasional call spread over hours or days

Each question answered is a piece of the puzzle

Eventually, the attacker has enough info to act
The in-person attack

An attacker poses as a service worker
Their uniform makes them seem legitimate and trustworthy

They stroll through your premises and scout the place
If they see anything of value, they either take it or plan the theft
How to protect against social engineering

- Never use an unverified memory stick
- Never divulge personal or privileged information to a stranger
- Be suspicious of any requests for contact information
- Verify service personnel and ensure they are escorted
What about Exploits?

• Definition:
  • A flaw in software or hardware that exposes it to misuse by hackers or malicious software
Software Exploits

Microsoft Office

Adobe Acrobat

Microsoft Windows Operating System

- Microsoft Remote Desktop Protocol (RDP)
- Windows Mount manager
- Microsoft SMB
- Edge browser
- Internet Explorer browser
Hardware Exploits

Consumer Wi-Fi access points
• Asus, Belkin, Buffalo, D-Link, Edimax, EnGenius, Linksys, Netgear and TP-Link

Commercial Wi-Fi access points
• Cisco, Huawei

Intel microprocessors
Exploit breaches are rare

It’s harder for the criminals to pull it off

The technology and techniques are extremely sophisticated

This is often a collateral damage situation

There’s only so much you can do, but a little goes a long way
How to protect against exploits

• Keep computer operating systems up to date and patched
• Keep all software up to date and patched
• Use commercial grade network equipment
• Regularly update firmware on network equipment
• When in doubt, hire a pro
Summary

• A data breach can kill your business
• All breaches are preventable
• Ransomware is the most deadly
• People are the biggest threat in your office
• 95% of breaches involve human error
Break (10 minutes)
Manage your passwords
Password protection is paramount

Of all the personal information that can be stolen, passwords are the most vital.

We place a lot of faith in passwords to keep things secure.

We have to treat passwords with great care.
This is not good password management
This is not good password management!
This is not good password management
The wrong way to pick passwords

- Family names
- Pet names
- Addresses, phone numbers
- Common words
- Social media information

- And definitely avoid the famous ones
  - Password, Password1
  - qwerty
  - 123456
The most common, still not great way

- It has to be eight characters, right?
- And a capital and a digit and a symbol
- So,
  - Choose a word (aardvark)
  - Capitalize it (Aardvark)
  - Add a number (Aardvark1)
  - Add a symbol (Aardvark1!)
  - And tah dah! It passes!
- But you’ve got a really weak password
A good way to pick passwords

- At least eight characters
- Mix uppercase, lowercase, numbers, and symbols

- For instance, choose letters from a phrase you know
  - F s a s y a
- Swap some numbers for letters
  - Fs4sy4
- Add some symbols, and voila!
  - #Fs4sy4?!

- But, that’s not so easy to remember
A better way to pick a password

- Use a “pass-phrase”
- Choose three or four words that have no clear relationship
- Base the words on a mental image or silly sentence
- For instance,
  - Cukes zukes overflow
- Dress it up to meet the rules
  - 4CukesZukes0verflow
How to protect passwords

- Don’t write
  - Don’t write them down. Seriously!
- Remember
  - Make them memorable, but not predictable
- Do not reuse
  - Do not reuse them. Ever!
- Change
  - Change them regularly
- Manage
  - Strongly consider a Password Manager
What is a password manager?

• One product that holds all your passwords securely
• Much safer than a notepad or the bottom of your keyboard
• Many permit secure password sharing
Benefits of a Password Manager

• Only one password to remember!
• Lets you use extra-strong, generated passwords everywhere else
  • Like this 1j2!*0RMaZj8
  • Or this o82fIrQ@nu5S
• No need to reuse passwords
• Works across all your devices, browsers, and even outside the browser
• Every site/product can have a different password! Yes!!
Dangers of a password manager

• All your eggs are in one basket

• If the vendor is breached, or your master password is compromised, you’re in big trouble

• Beware, some products won’t help you if you forget your master password
Lots of products to choose from

My company uses LastPass

- Works on Google Chrome and Firefox browsers
- Works on iPhone
- Works on Mac/PC
- Permits secure password sharing
- Warns about password reuse

Do some research to find your favorite

- Google “top 10 password managers for…”
- Try a few and see what works best

Require that the whole company use it
You can check to see if you’ve been compromised

• Lots of big web companies have been breached
• Many of them are holding your credentials

• Check here to see if your information is in the wild
  • https://haveibeenpwned.com/

• If the answer is yes, change your passwords!
Be Careful With Your Security Questions

• To keep you safe, many vendors use security challenge questions
  • What’s your spouse’s name?
  • What’s the name of your elementary school?
  • What’s your favorite food?

• They seem smart, but are they really safe?
How much of this is on Facebook, Twitter, LinkedIn, etc?

Security Questions.
Select three security questions below. These questions will help us verify your identity should you forget your password.

Security Question: What was the name of your first pet?
Answer:

Security Question: What is your dream job?
Answer:

Security Question: In what city did your parents meet?
Answer:
Security questions are vulnerable

- If you’re social online, your answers are out there
- Bad actors will get your answers in short order
- Best practice is to answer incorrectly but memorably
- Use fake answers that you can recall
  - Spouse=Anakin
  - School=Hogwarts
  - Food=Unicorn
What is Multi-factor Authentication (MFA)?

• More than just the password

• The factors include
  • Something you know (password, passcode)
  • Something you have (USB fob, phone)
  • Something you are (fingerprint, iris, face)
2-Factor Authentication (2FA)

• Reduce the “multi” to just two
• Adds one more thing to the password you know
• Common factors include
  • Text message
  • Phone call
  • Email
• A little inconvenient, but worth it
Surf safely
Don’t click the clickbait

- Most of those ads are harmless enough
- They may tag you with a bunch of tracking cookies, but not a huge problem
- The deeper you go down the rabbit hole, the sketchier it gets
If your browser says a site is suspect

It’s probably a malicious site

Unless you know what you’re doing, don’t continue
Beware Public Wi-Fi

• Even secured public Wi-Fi isn’t truly secure
• Bad actors can masquerade as free Wi-Fi
• A “man in the middle” can see all your transmissions
If you use public Wi-Fi, use a VPN

• A Virtual Private Network (VPN)
  • Keeps your traffic encrypted
  • Prevents prying eyes in the middle
  • Also blocks some ad networks

• I use SurfEasy
  • It’s inexpensive
  • It works on Mac and iPhone

• There are many
  • Google “top 10 vpn products”
Tips and techniques to stay safe online

• Beware search results
  • Web search
  • Social search
• Check the context
• Hover, hover, hover
Prevent as Much as Possible
Protect Your Workplace

- Stop visitors at the door
- Control access in off hours
- Protect your network
- Use high-quality components
- Use a professional installer
Lock Down Your Devices

- Put anti-virus software on both Windows and Apple machines
- Mobile phones are not immune
- Put locks on your laptops and desktops
- Use a safer browser
Don’t Ignore “Smart” Products

CAMERAS  PRINTERS  THERMOSTATS  ACCESS POINTS  ANYTHING ON YOUR NETWORK
Train your folks

STATIC COURSES

AUTOMATED TESTING

REGULAR CHECKUPS
Our company uses a training and testing service.

- Lots of fresh content
- Schedulable, configurable tests
- Automated, simulated phishing attacks

We use KnowBe4, and it helped. A lot.

There are many others

- Google “security awareness training”
Keep Current Backups

• Use an online service
• On site backups can be compromised
• Our company uses several interlocking products
  • Apple TimeMachine
  • Microsoft OneDrive
  • Microsoft SharePoint
  • Box
  • Other cloud software
• Use as much cloud software as possible
Regularly test your backups

• Backups can fail silently for months
• And backups might not restore properly
• If you don’t test it, you don’t know it’s working
When you get hacked, know what to do.
Have a plan

Even if you create the plan yourself, get a professional involved

Start with legal requirements

Consider your personnel

Consider your clients

Have a professional partner at the ready

For starters, Google “data breach response plan”
Know your first steps

- **Own it**: Stuff happens. Don’t try to hide it. It won’t go away.
- **Communicate**: Tell all of your staff immediately.
- **Turn off**: Turn off computers, routers, everything.
- **Stay close**: Don’t let computers leave the facility to “work from home”.
- **Call**: Call your pro partner.
- **Execute**: Execute the rest of your plan.
Remember

- Avoid threats
- Manage your passwords
- Surf safely
- Prevent as much as possible
- When all else fails, know what to do