We've added speaker notes! The speaker notes are not meant to be read line-by-line!!! Similarly, don't read everything on the slides word-for-word. Instead, engage with your audience. Tell stories to help back up the material. Watch your attendees to determine if you are losing them or if you need to spend more time on a topic. Ask questions or randomly poll them about various material. Even something as simple as using audience members names in theoretical examples is a great way to pull them back in. Most importantly, have fun!

whoami

- 25+ years of IT & Cybersecurity Experience
- Consulted for companies all over the world
- Multiple computer-related bachelor degrees from FHSU
- Master's degree in Information Security Engineering from SANS Technology Institute
- Alphabet soup of security-related certifications: GSE #231, CISSP, SANS/GIAC (x10)
- Co-Organizer of BSidesKC Annual Cybersecurity Conference (Kansas City)
- Founded IT Provider (MSP) in 2003, acquired in 2016
- Founded TreeTop Security in 2016, lead design on Peak Platform
- Founded 501(c)(3) STEM Harvest in 2021 - stemharvest.org
- 2024 SBA Kansas Small Business Person of the Year
- 2025 Hays Chamber Entrepreneur of the Year

My background. This is a chance for you to tell the audience a little bit about yourself. Include information about how you relate to the subject such as why you enjoy helping people avoid scams, why you're qualified to talk about cybersecurity, etc. Maybe it's because you were scammed yourself so you have some additional insight. Personal stories can go a long way to helping attendees better understand the material and make it more relatable.

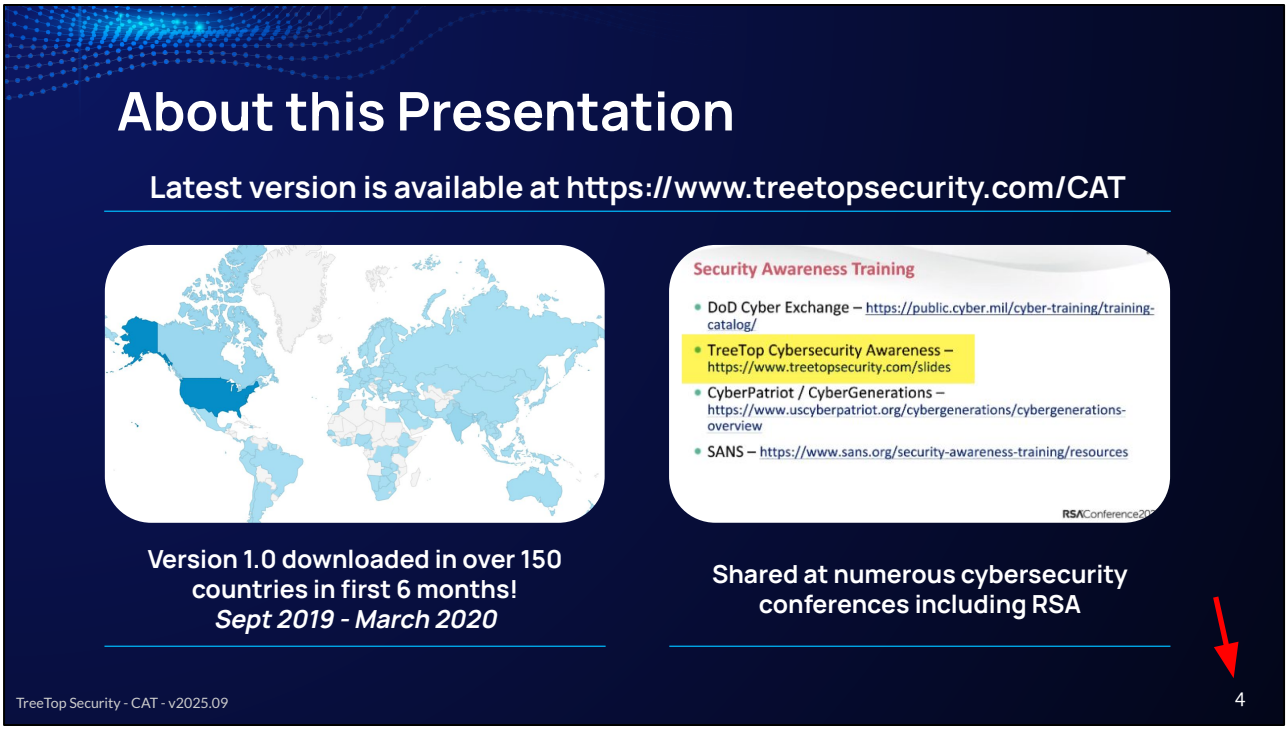
This content is free! If you feel the need to compensate us for our time, please instead send a donation to STEM Harvest, which is a 501(c)(3) non-profit to help teach kids in rural Kansas about technology. There are numerous ways to donate via the https://stemharvest.org website.

Legal Disclaimer

While we'd love to boast that our cybersecurity awareness training is foolproof, the reality is no training can safeguard you from all cyber threats and that includes cyber criminal's relentless attempts to send you malware laced cat memes. It is, however, the best single hour you can use to learn ways to better protect yourself from the evil lurking on the digital interwebs. Your best defense against cyber-foolery is your own cyber-wisdom. Remain vigilant, keep your passwords as complex as the plot twist in Fight Club, and learn to embrace your inner cybersecurity awareness ninja!

Note: We were told we needed a disclaimer. Many thanks to ChatGPT for adding some flair.

We were told this training needed a legal disclaimer because someone might think this 1 hour training would make them immune from cyberattacks. So we added a disclaimer that states this, but also makes it funny so people will actually read it. A little ChatGPT, a little extra flair, and this is the result! To all of my lawyer friends, sorry not sorry.



In the first 6 months after it was released, version 1.0 of this slide deck was downloaded in over 150 countries. Since then, it has been downloaded hundreds of thousands of times. It is downloaded or viewed over 10,000 per month and those are just the views we can reliably count! This presentation is consistently receiving feedback from people all over the world so it can continue improving. Many organizations use the slides as part of their new employee training or as a part of their ongoing employee training. This deck has been recommended by numerous IT and security experts. In February 2020, it was shared alongside some other fantastic resources at the RSA security conference, which is one of the largest security conferences in the world.

Note: The red arrow pointing at the slide number is a reminder for presenters to mention this material is available for download from the TreeTop Security website, https://treetopsecurity.com/CAT, i.e. there's no need to hurriedly write down everything from every slide. The slide number also makes it easy to reference with attendee notes.

Live, laugh, get hacked, stop laughing. It's meant to bring a little bit of light to the subject but keep in mind that cybersecurity is affecting a lot of people in very adverse ways after their data gets hacked, their company gets breached, a product or service they use gets hacked, etc.

Overview

- Why security awareness?
- Backup, backup, backup
- Patching ALL of your devices
- Passwords
- 2-Factor Authentication (MFA)
- Internet Safety & Email
- Phone Scams
- Privacy Concerns

What to do when things go wrong?

We have a lot of ground to cover. Generally, why is security awareness important. From there, some ways to protect yourself including privacy concerns. And last but not least, what should you do if you or someone you know *thinks* they may be the victim of a scam.

Let’s get started...

Awareness training is a must!

Technology alone ***cannot*** protect you from everything

Attackers go where security is weakest

People → a link in the chain & the ~~last~~ first line of defense

A must to reduce cybersecurity risk

Cybersecurity awareness is for…

- Employees
- Business Owners
- Parents
- Kids
- Seniors
- **Everyone!**

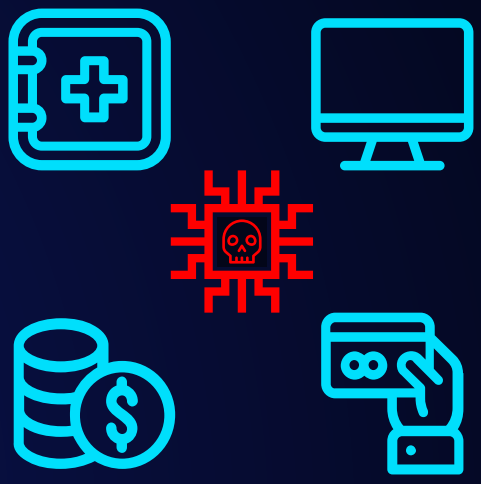
Reminder: Many tips that keep you safe at work will also keep you safe at home!

Cybersecurity awareness training is to vital to security. This is a key topic because many people assume if they have the best security technologies, it will provide them with 100% coverage. Example: Large corporations and governments spend millions of dollars (or more) and still aren't immune from cyberattacks. Another common belief is that our IT department will take care of it or they assume a firewall and anti-virus will protect them against anything. Cybersecurity awareness is a must for everyone! Also hit on the fact that they tips work at home too. That tends to help keep the interest of audience because they know this could save them money or time if they get malware, scammed, etc.

But an attacker isn't interesting in me…

⊗Wrong!!! - You are exactly what an attacker wants!

- Credit Card & Financial Data
- Medical Data
  - Prescription, insurance, or identity fraud
  - Far more valuable than financial data
- Computer Resources
  - Cryptomining
  - Advertising
  - Ransomware
  - "Jump Point"
- User or email credentials
  - Sending spam
  - "More" access
  - Recovery/Reset other accounts



The bottom line is that everyone has something that an attacker wants. With data, it could be financial, personal, or even medical related. Even if someone claims they don't have anything on their computer worth stealing, an attacker can still use their computer resources for cryptomining. Cryptomining uses your computer resources for financial gain. Attackers have also injected ads into users' browsers to provide them advertising revenue. Or they could use your computer as a jump point to attack someone else. This is also a good time to ask if everyone knows what ransomware is. A go-to analogy is comparing it to a Hollywood kidnapping movie where the criminals ask for a ransom to get the person back. Ransomware is similar, except it is keeping you from accessing your data unless you pay the ransom.
Something we frequently hear is that we only do email on this computer. Ok, but what other accounts might be tied to that email. For example, if I'm a bad guy and I have access to your email, do I need your bank password? Why not just go to your bank website, say "forgot password" and then have the new password sent to me? That last comment is typically a light bulb moment for a lot of attendees.

02

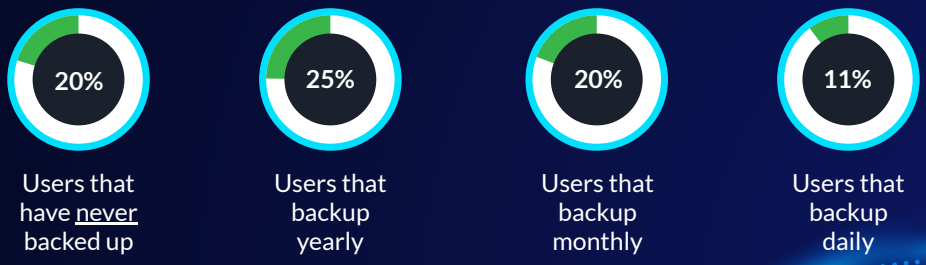
HELP!!!

Ways to protect yourself!

Enough of the doom and gloom, let’s get into ways to protect yourself.

Backups

- Backups protect when all else fails
  - NO level of protection is perfect
  - Only "guaranteed" protection against ransomware
- Backup media should *not* be connected at all times
- Test your backups! Restore, restore, restore!



Backups are absolutely necessary for security. Backup media (such as a USB drive) cannot stay connected all the time because if you are hit with ransomware, it will almost certainly encrypt the USB backup files as well. Also, don't forget to test your backups! As any person in IT can attest, there are an endless number of companies who thought they were backing up their data every day only to found out differently when they go to recover data. Pro tip: Tell them to add testing restore processes to their calendar every quarter. We never dive into all of the statistics at the bottom because that can get tedious, but we do often highlight the statistic at the bottom that is in white (instead of gray). In this case, 20% of users have never backed up their data.
Source: https://www.backblaze.com/blog/the-state-of-backups-whos-most-at-risk/

Worksheet #1

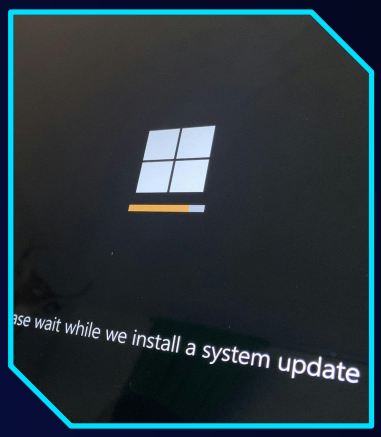
Your data, your backups

https://www.treetopsecurity.com/CAT

This page refers back to the worksheet on backups.
https://www.treetopsecurity.com/CAT

Updates are essential to security.

- What was secure yesterday may not be secure today
- New software vulnerabilities are found every day
- Over **450,000** new malware (viruses & ransomware) released every day
- Nothing is “Set & Forget”



Most people think of updates and think of Windows, Mac, or phone updates and the handful of new features they receive. Many are not aware that those updates also include fixes to better protect them. Statistic source: https://www.av-test.org/en/statistics/malware/

Keeping your system up-to-date

Operating Systems

- Microsoft Windows, Apple MacOS, Linux
- Windows 7 end of life? January 2020
- Windows 10 end of life? October 2025

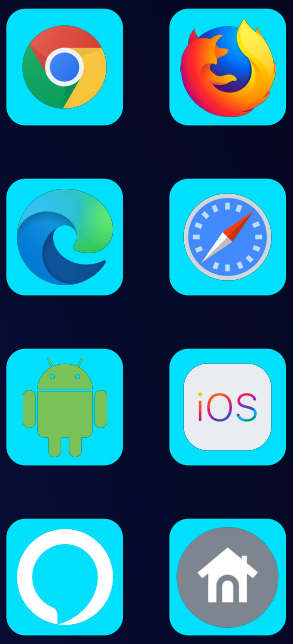
Anti-Virus

- Update to the latest definitions to ensure protection against the latest threats
- Symantec/Norton, McAfee, Windows Defender, Avast, and many others!

Keep your systems up-to-date. Don't just ignore updates until the system forces you to update.
Most people don't understand how traditional anti-virus works so this might be an opportunity to explain why receiving virus definitions on a regular basis is a must. A great analogy tends to be an entry/patron list for a high-end restaurant, i.e. that list operates by ONLY allowing people in whose name are on the list. Traditional anti-virus is the opposite, i.e. it operates by preventing someone when their name is on the list. What that means is if your list isn't up-to-date, you're not blocking everything you should be. This "deny" approach is why traditional anti-virus largely doesn't work in today's internet. As a reminder, the previous slide highlighted the insane number of new pieces of malware released every day.

Don't forget to update…

- Browser - your portal to the internet
  - Chrome, Firefox, Edge, Safari, Brave, etc.
  - ~~Internet Explorer~~ (Not recommended)
- Mobile devices - cell phones & tablets
- Internet of Things (IoT) - Alexa, Google Home, light bulbs, thermostats, doorbells, surveillance system, smart locks, pet feeder, vacuums, health monitors…
  This list could keep going forever!



Tons of other applications/apps on your computers and phones also need updating. An up-to-date browser is vital. At this point, Microsoft no longer recommends using Internet Explorer to browse the web. Inevitably, there will be a hand or two raise stating they must use Internet Explorer for certain websites, often government related. The standard response is if that is the case, then those websites should be the ONLY ones you use IE on.
"Internet of things" devices also need updates and a majority of these devices will be problematic for years to come. Why? Because most do *not* receive automatic updates, i.e. that wifi-enabled dog feeder you had to have may cause security issues down the road if you're not careful.
You might get asked about how to handle those types of devices. Either a) don't buy them or b) segment them onto their own network. Let them know you can chat after the training if they have additional questions about that.

Worksheet #2

What's on your network?

https://www.treetopsecurity.com/CAT

This page refers back to the worksheet that guides an attendee through scanning a network. https://www.treetopsecurity.com/CAT

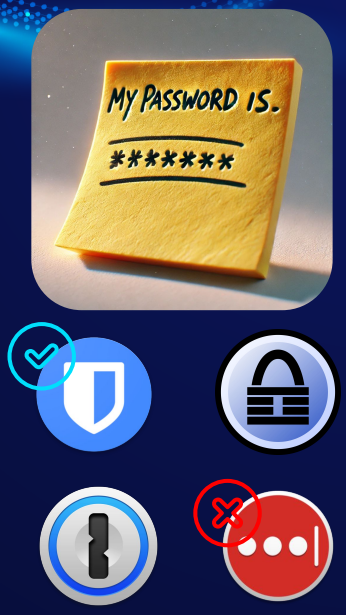
03 All About Passwords

These transition slides are a great place to pause and ask if anyone has questions. It is also a great way for someone consuming a lot of new information to reset their thoughts.

Give everyone a chance to read it and then explain the joke, i.e. it's easier for some people to rename their dog than for them to change their password. And he's such a cute little puppy! ;-)

Managing Passwords

- Keep your passwords in a secure location
  - Do NOT use paper or sticky notes
  - Do NOT store passwords in clear-text on your computer - Word, Excel, etc.
- Utilize a password manager (aka vault)
  - **Bitwarden** ○ KeePass ○ ~~LastPass~~
  - Chrome? ○ Apple Keychain?
- Benefits of a password manager
  - One strong password to access them all
  - Passwords are stored securely
  - Auto-fill username/password on websites
  - Sync between desktop, laptop, and mobile

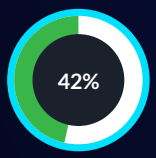


This slide often generates a LOT of discussion. It's extremely common for people to come back and tell us about how they implemented a password manager at some point after the training.
It's never a bad idea to explain that the first thing an attacker or malware does after gaining access to a system is to look for way to gain access to OTHER systems. What better way to do that then by looking for usernames/passwords the user might have laying around?
Inevitably, someone will ask about built-in password managers such as Google Chrome or Apple Keychain. Long story short, they are better than not using a password manager, although they are not quite as secure. They also have some drawbacks including locking you into a particular ecosystem, browser, etc.

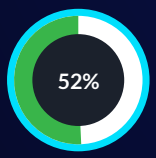
Password Tips

- Avoid using items that can be associated with you
  - Address
  - Phone numbers
  - Pet names
  - Child names
  - Birthdays
  - Sports teams
- Separate passwords for every account
- Auto-generated, near impossible to guess

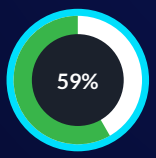
Much easier with a password manager!



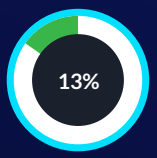
Rely on sticky notes for password mgmt



Re-use password for multiple accounts



Use name or birthdate in password



Reuse same password for all accounts

This is pretty self-explanatory. We often have to explain that it is ok to *not* know or remember a password. That is exactly what your password manager is for. Don't forget the highlighted stat below that 52% of all people re-use passwords for multiple accounts. One question you can ask here is why using a different password is important, i.e. if one website gets breached, an attacker will attempt to use that same username and password on other sites. Source: https://www.comparitech.com/blog/information-security/password-statistics/

Passphrases, not passwords

- Useful when passwords must be typed in
  - Computer login
  - Wireless <- no phone numbers!
- Should not be easy to guess
  - At least 12 characters, but 15 or more is far better
  - Length better than "complexity" - upper, lower, number, & special characters (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
  - Bad password (8): P@ssword
  - Great password (25): MysonwasbornNovember1995!

Why are most passwords exactly 8 characters?

The important takeaway is that length matters far more than complexity. We also like to point out the "great" password and how no one probably would have thought they could remember a 25 character password. However, it's pretty easy to remember that particular one and better yet, it even meets all password complexity requirements for systems that still require them.

A quick side note about why you should *not* use phone numbers for wireless passwords. I personally first became aware of ISPs setting up customer wireless passwords as their phone number back in 2015. I quickly discovered it wasn't limited to my community based on internet feedback. I blogged about my own experience many years ago after several ISPs were STILL following this bad practice despite me providing evidence years earlier showing them the dangers. The worst part is that it's STILL a common practice for numerous ISPs and users today. :-(Aside from the obvious that it doesn't take much to find someone's phone number, an all number password with a known length can be cracked in well under a minute. Here's the original story from my blog with technical details of how it works.
https://linuxincluded.com/why-phone-numbers-make-horrible-wifi-passwords/

The question at the bottom is to get the attendees to think about why. The answer is because almost every system and website on the planet has 8 characters as the minimum length… And given the choice, most will choose the minimum because they don't fully understand the security implications.

Top 20 passwords by rank & year

Rank	2022	2023	2024	Rank	2022	2023	2024
1	password	123456	123456	11	1234567	1234567	1234567890
2	123456	admin	123456789	12	1234	123123	1234567
3	123456789	12345678	12345678	13	1234567890	111111	000000
4	guest	123456789	password	14	000000	Password	qwerty
5	qwerty	1234	qwerty123	15	555555	12345678910	abc123
6	12345678	12345	qwerty1	16	666666	000000	password1
7	111111	password	111111	17	123321	admin123	iloveyou
8	12345	123	12345	18	654321	1111	11111111
9	col123456	Aa123456	secret	19	7777777	P@ssw0rd	dragon
10	123123	123457890	123123	20	123	root	monkey

If you use any of these, change them NOW!!!

Source: Nordpass

Pick out a few passwords and discuss them. The takeaway is that these “terrible” passwords don’t change much. The other point you might make is “how do we know what passwords people use?” These passwords are from hacked databases *after* a breach occurs. Security researchers then analyze those hacked accounts to search for similarities. Remember our discussion on why you should have a different password for each website? Source: https://nordpass.com/most-common-passwords-list/

Password Length ‹ › Time to Crack

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instant	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

Time for an attacker to brute force your passwords.

Are you in the **yellow** or **green**?

Source: Hive Systems

This table/data is slightly nuanced. What it does well is provide the average user an easily way to visually understand how longer passwords are exponentially better than shorter passwords. Source: https://www.hivesystems.io/blog/are-your-passwords-in-the-green

MFA - Multi-Factor Authentication

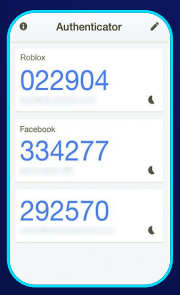
What is MFA?

- "Beyond" a username and password
- Another form to prove it is you
- Typically out-of-band
- Can be biometric - fingerprint, facial, etc.

"Your one-time code is…"

- SMS (Not as secure)
- Phone Call (Not as secure)
- Authenticator applications
  - ➔ Google Authenticator
  - ➔ Microsoft Authenticator
  - ➔ Built into a password manager?
- Email
- Phone Pop-Up

Biometric - fingerprint or facial recognition



Authenticator apps

99.9% **LESS** likely to be compromised if you use MFA

Source: Microsoft Tech Community

People's eyes tend to glaze over when talking about multi-factor authentication. I usually explain that if you have logged into your bank account and it sent you a text message stating "your passcode is…" then congratulations, you've used multi-factor authentication. It's also worth mentioning to not get confused when talking about two-factor authentication (2FA) versus multi-factor authentication (MFA). 2FA is simply a subset of MFA as it defines the number of authentication mechanisms. A short discussion on how the phone-based authentication applications work never hurts either.

While any form of MFA is substantially better than a username/password by itself, it's important to recognize that SMS and phone call-based verifications have some security concerns. Aside from SIM-jacking (or SIM-swapping), which is where an attacker coerces a cell phone carrier to issue a new SIM card, there are other attacks that allow an attacker to re-direct SMS and phone calls to a new device.

Unfortunately, it can happen for as little as $16, although there are some caveats.

Source:
https://www.vice.com/en/article/y3g8wb/hacker-got-my-texts-16-dollars-sakari-netnumber

Don't miss the opportunity to briefly discuss the quote from Microsoft stating their research showed that 99.9% accounts are LESS likely to be compromised if you use MFA. <- Wow!

Source:
https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/your-pa-word-doesn-t-matter/ba-p/731984

MFA Under Attack

MFA Fatigue

- Attacker targets the end user rather than jump through technical hoops
- Users overwhelmed by frequent authentication requests causing:
  - Frustration
  - Carelessness in approving prompts
  - Potential security risks
- Users may unknowingly approve malicious requests just to stop the prompts
- Your phone becomes unusable due to an MFA pop-up every 5 seconds. Would you click approve?

MFA Fatigue occurs when users become overwhelmed by frequent authentication requests. Attackers exploit MFA fatigue by

- Constant MFA prompts: Attackers bombard users with repeated authentication requests.
- User Behavior: Users may unknowingly approve malicious requests just to stop the prompts.

This is a great time to explain this through an example. There are a lot of write-ups about this concept used in the real-world, but it's just as easy to discuss it from a theoretical perspective. Basically, if you were to receive 15 pop-ups in 5 minutes, would you eventually just click "ok" to make them go away?

This page refers back to the worksheet that guides through the initial setup of a password manager and some discussion on 2FA.
https://www.treetopsecurity.com/CAT

Another opportunity to ask if anyone has questions and let them do a mental reset as we move onto some different concepts.

Is the link safe in 4 steps

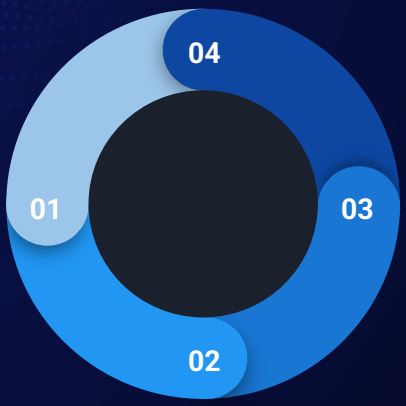
1. Verify

Were you expecting a link?

- Not just email!
- Social Media
- SMS/iMessage
- Zoom, Teams, Slack, etc.

2. Hover

Hover over the link to ensure that it leads to where it says it does



4. Click

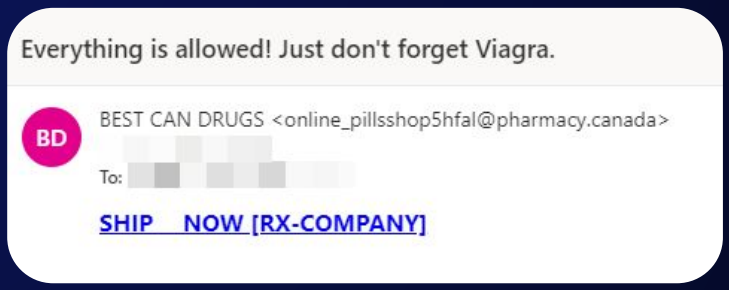
Does it pass all 3 tests?
Still use caution
"When in doubt, throw it out"

3. Sniff test

Is it a site you recognize?
Does it feel "familiar" to you?
Be skeptical

Go around the circle with a brief explanation on each. Go quick because we go into many of these more in-depth so simply help attendees understand that these 4 simple steps can help prevent link-based attacks. The big one is to point out that links aren't just email.

Easy to Recognize Scam



Red flags? →

- Viagra ← ?!?!?!
- Strange Wording
- Email Address
- Domain Name
- Expected email?
- Interesting link

This should hopefully be an easy to spot scam (spam) for most everyone. Go through each of the red flags and talk about how you can use this same, systematic approach to all emails and even some non-email scenarios.

From a Known Email Account

Hacked or spoofed email from someone you know. Includes signature line!

Similar attacks via Facebook & Social Media

Red flags? →

Email address = OK

Name = OK

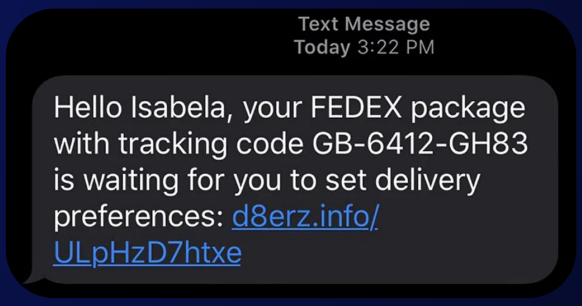
Odd "Signature"

Expected email?

Link → .fr is France

This might be more difficult to spot because it is from someone you know, but their account was hacked. You may ask if anyone has experienced this or if they know of someone this happened to. Remember to get the audience involved! Although not email related, everyone with a Facebook account has likely experienced this situation where a friend gets their account hacked and you get a odd message like "Is this you in this video" or something similar.

Text Messaging Example



Red flags? →

- Name in SMS = OK
- Number OK?
- Expected Text?
- Received a text regarding a package before?
- Recognized domain?

Image Source: CNN

Reminder: links aren't just for email! This is an SMS text message claiming to be FedEx. Were you expecting a package? Have you ever received a package notification via text message before? Also, note the odd domain name.

Hover before you click

- Why hover?
  - Blue text can be deceiving
  - Underlying URL may be different
  - “Foreign” domains - .uk, .cn, or .ru
- Numbers instead of letters
  - Example: 192.168.1.1
  - Don’t trust it!
- Hover on mobile/tablet?
  - Long press (hold)
- Any doubts? Don’t click it!!!

Hovering is your friend. Hovering shows where the link will take you *before* you click on it. If you see numbers, then there is a really good chance it isn’t legit. Also, if you are on a mobile device or table you can still hover by performing a long press. Be careful though because if you don’t hold down the long press long enough, you will unintentionally click the link!

Shortened or Obfuscated Links?

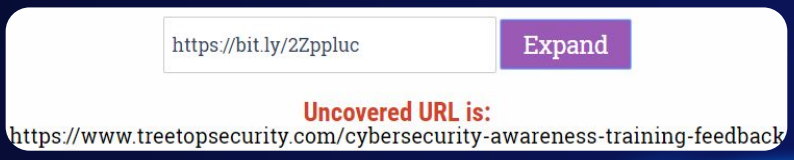
Instead of 300 characters, the link is reduced to 15 characters.

- Bit.ly
- TinyURL
- Cutt.ly
- Many more!

Extremely Common and helpful, but…

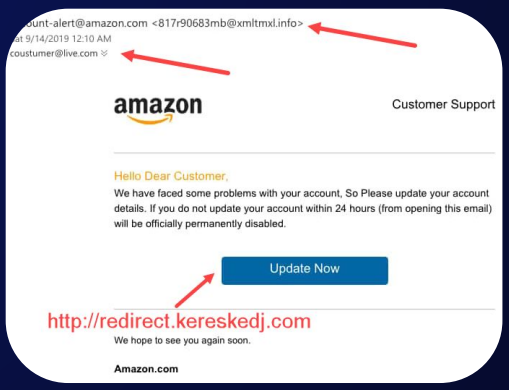
Abused by criminals to hide malicious websites.

Link Expander
www.linkexpander.com



Don’t spend a ton of time here other than to explain how link shortening services work. If they come across this, you can use a number of services including Link Expander to show the *actual* URL, e.g. if you expand the bit.ly link in the picture it expands to the fairly long URL for our TreeTop cybersecurity awareness feedback.

Hovering is your Friend



Red flags? →

Email address OK?

Sense of Urgency

Expected Email?

HOVER!!!

Image Source: Malware Traffic Analysis

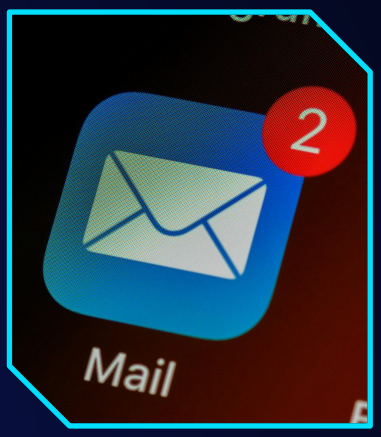
Hovering in action. But first, do you use Amazon? If this is a business account, have you ever received Amazon (or vendor) email before? Note the sense of urgency the attacker is trying to use to their advantage. We'll see that time and time again in numerous attacks including phishing schemes. Take a look at the email address. Is that really Amazon? Last but certainly not least, if you were to hover over the "update now" button, it revealed another extremely odd website.

More Email Attacks

94% of malware is delivered by Email

1.2% of all emails sent are malicious

Over three billion phishing emails every day!



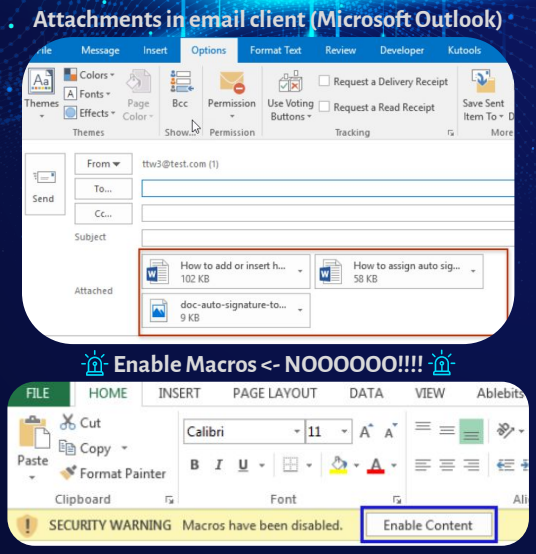
Another chance to reset, but also point out that you're continuing on with other email attacks. Why more email attacks? Because 92% of malware is delivered by email.

Email Attachments

- Stop & Think before you click!
- Recognized Sender?
- Expecting Attachments?
- Is it normal for that contact to send attachments?

Macros

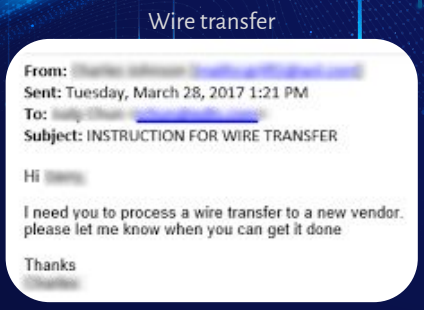
- Step 1: Don't do it!!!
- Step 2: Please See "Step 1"
- Found in downloaded files also



Email attachments can appear in Microsoft Outlook or any other email client including your browser. The best defense is to stop and think. Do you recognize the sender and do they normally email you attachments? A frequent example to use here might be someone's parents or grandparents. Sure, they might email but would it be weird to get a PDF document from them out of the blue? Macros are worth mentioning because they are still used. Basically, if someone knows what macros are then they should use caution when opening documents with them (and enabling content). If you don't know what macros are, don't ever click enable content. Why? Because by clicking on that, a Word document or Excel spreadsheet can infect your computer.

Business Email Compromise (BEC)

- FBI: BEC cost businesses $1.8B every year
- Moving funds -> more susceptible
  - Policy requiring phone call?
- "Trusted" senders (Partner, Vendor, or Executive)
  - Research using publicly available data
    - Published organization chart
    - Spear phishing (CEO <-> CFO)
  - Spoofed domain
    - microsoft.com - microsoft.com
  - Compromise account of 3rd parties
    - Employee, vendor, or customer
    - Thread hijacking <- lookout



Often requires very little technical skill

Image Source: Dark Reading

Many organizations have published organization charts (or even board of directors) because it lets others get familiar with them. Unfortunately, attackers can use them to gain a better understanding of an organization or decide who they would like to target. In this example, no technical control can help because this could just as easily be a legitimate request. Often times, something as simple as implementing a company policy for a follow-up phone call would thwart many of these attacks.

This might be a good time to use a story from your area or depending on your audience, you could also talk about Barbara Corcoran from Shark Tank and how she almost lost $400,000 from a phishing email. In Barbara's example, her assistant was sent an email asking for renovation funds, which is a common ask in her line of business. Fortunately, the reply included her and she was able to put a stop to the wire transfer (and scam). For most of these, it requires almost zero technical skill because it looked like it was coming from a trusted source.

We've seen a HUGE uptick in thread hijacking. Thread hijacking is when someone else that you know (and trust) gets their email account compromised; the attacker then utilizes previous conversations on new emails to make it seem more plausible. This can occur from an currently compromised account or MONTHS later after the attacker no longer has access, i.e. the attacker will send an email from an external system posing as that person so you simply assume they are replying to your conversation from a different email address.

Source:
https://www.darkreading.com/attacks-breaches/fbi-business-email-compromise-cost-1-8b-in-2020

Source:

https://www.cnbc.com/2020/05/06/how-barbara-corcoran-almost-lost-400000-dollars-to-an-email-scam.html

QR Code & Mobile-Based Threats

- Malicious QR codes can bypass email filters
  - Fake Parking Meters, Restaurant Menus, or even Mailed QR Codes
- Defending against these threats
  - Train users to be wary of scanning QR codes, especially from unknown sources
  - Train users to verify URLs after scanning by analyzing the link first

Analyze link before visiting website

Avoid QR codes

Would you go to *evil.com*? Then why would you go to a QR code that could be doing the exact same thing!

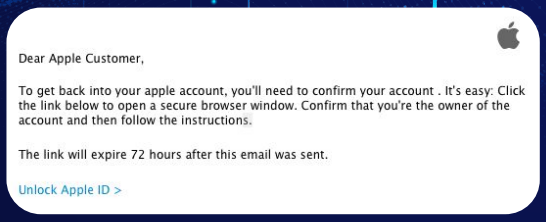
QR codes have become part of everyday life from restaurant menus to parking meters, they're everywhere. Unfortunately, attackers know this too. Malicious QR codes can bypass email filters and other defenses because they rely on human behavior, not technology, to trigger the attack. Once scanned, these codes can redirect users to phishing sites, malware downloads, or fake login portals. The real danger is that many people don't think twice about scanning a QR code, especially when it appears in a familiar context. Just like you wouldn't willingly type in "evil.com," you shouldn't blindly trust where a QR code sends you. The most effective defense here isn't technical, it's training users to pause, verify the URL after scanning, and treat QR codes with the same suspicion as unexpected email links.

Article:
https://www.zdnet.com/article/these-phishing-emails-use-qr-codes-to-bypass-defences-and-steal-microsoft-365-usernames-and-passwords/

Other Email Scams

- Mostly “non-technical”
- What the attackers want
  - Money
    - Gift cards
    - Wire transfers
  - Access to email & accounts
- Possible signs
  - Sense of urgency
  - Never happened before
  - No limit on what they say/do

Account credential phishing attack

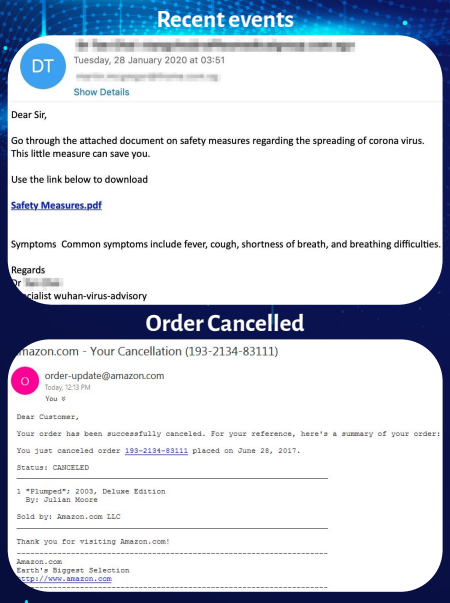


Technology alone <u>cannot</u> solve this

Yes these are still over email. The non-technical statement is meant to point out that just because there might not be any links or attachments, doesn’t mean it isn’t malicious. You can easily ask for someone to send gift card numbers via email and unfortunately, a lot of people fall for this scam. Likewise, an attacker introducing themselves as tech support and then asking someone for their password isn’t a technical attack per se, however, it is still widely used because it works! Similar to prior examples, point out some of the tell tale signs such as the sense of urgency, recognizing something as “off” because it’s never happened before, etc. It’s also important to recognize that attackers have NO limits on what they can say or do. There have been several examples of attackers claiming there was an active shooter situation at a school, they want money to get someone out of jail, etc.

Scammer Favorites

- Mimic recent, breaking news
  - Worldwide
    - Health scares (COVID, outbreaks)
    - Protests
    - Elections
  - Local and regional
- Seasonal/holidays
  - Order & delivery issues
  - Tax issues



Keep your guard up!

Scammers always have and always will use news headlines in their attacks so you put your guard down. During the last few years, scammers used coronavirus themed attacks for phishing campaigns. Around the holidays, they will use cancelled orders or delayed deliveries because people are ordering gifts for loved ones. These tactics will *never* change.

Worksheet #4

Have you been part of a breach?

https://www.treetopsecurity.com/CAT

This page refers back to the worksheet that guides a user through looking up whether their data was part of a previous breach using the awesome resource, https://haveibeenpwned.com. https://www.treetopsecurity.com/CAT

05 Reach Out & Scam Someone

A great chance to reset and ask if anyone has questions before moving onto the next topic.
A US phone company once said “reach out and touch someone” so this is a little play on that.

Phone Scams

Social Engineering, what is it?

- Banks, Credit Card Companies, or Any Past Due Balance
- Medical & Insurance
- Government - IRS, Police, Jury Duty or even Tolls
- Objective: Access your sensitive info

Phone Numbers can be easily spoofed

- Make the caller provide verification
- Hang up & call back a published number

Other common phone scams

- Grandparent Scam or Family Emergencies
- Tech Support - Microsoft, Apple, Dell, etc. will NEVER contact the average user "out of the blue"

A quick chat on social engineering and how attackers use it to gain information, gain access, etc. Sometimes attackers will pose as banks, energy companies, or someone else to get your payment information. A social engineering tactic may include calling you from a "recognizable" phone number. Most people don't realize how easy it is to spoof a phone number, which makes it trivial to make their phone call look like it is coming from the local electricity company, phone company, hospital, etc. This is done in an effort to get people to let their guard down. If someone calls and their phone number matches someone you are familiar with, be skeptical. It's usually easiest to simply tell them you are busy, hang up and call them back at a published phone number that you have in your possession.

We always highlight the tech support scam because we saw it so many times over the years. As callous as it may sound, Microsoft, Apple, Dell, etc. will never call you out of the blue to tell you about a problem on your computer or device.

Phone Scam Example - Old School

Hi! This is Kathleen from Microsoft. We have been trying to get in touch with you. However, we will be disconnecting your license within 48 hours because your IP address has been compromised from several countries. So we need to change your IP address and license key. So please press 1 to get connected...

Red flags? →

- Sense of Urgency
- Purposefully Confusing
- Expected a call from Microsoft?

This is a audio recording pulled from a neighbor's old school, wood-grained answering machine, i.e. it's about as low tech as you get these days. If you have audio, let the audio play. Either of the "links" in the lower right hand corner will play the audio if speakers are setup. If it doesn't work or you're not sure on the volume/quality, let the audience know the white text is the same as what is stated in the audio clip. Highlight the red flags because several of them are the same tactics we used to spot phishing email, which are obviously text-based. Also highlight that there is very little we can do from a technical perspective to block this attack.

Phone Scam Example - AI Remake

Hello, this is Kathleen and I'm reaching out on behalf of the Microsoft Security Team. We've noticed some unusual activity involving your account. Your IP address has been accessed from multiple countries indicating a potential security breach. To ensure the safety and integrity of your account and personal information, it's critical that we update your IP address and license key. Without this update, we will suspend your license within the next 48 hours to prevent further unauthorized access. We're here to help you through this process and address any concerns you may have. For immediate assistance, please press 1 to connect with our support team.

ChatGPT

This is a message from a spam caller, we're using it in a cybersecurity awareness presentation - can you make the context of it sound more natural and more realistic but don't change the meaning behind it?

Everyone has heard or even used artificial intelligence at this point. Well, the bad guys can use AI as well! We used the text prompt at the bottom of the page to have ChatGPT (from OpenAI) re-write the previous slide text. We then used an AI voice program to speak the text in a more conversational, more realistic tone. Once again, if you have audio, let the audio play. Either of the “links” in the lower right hand corner will play the audio if speakers are setup. If it doesn’t work or you’re not sure on the volume/quality, let the audience know the white text is the same as what is stated in the audio clip.

AI Powered Scam

- AI makes scams harder to spot
  - Don't rely on misspelled words or bad grammar
  - AI writes flawless emails and texts
- Deepfake technology in play (voice or video)
  - Voices cloned from public recordings or voicemail samples
  - Example: "CEO" voice clone calls accounting: "We need an urgent wire transfer today."
- Defenses
  - Always verify financial or sensitive requests out-of-band (phone call, known contact, secondary channel)
  - Train staff to be aware of deepfake risks and slow down under urgency pressure
  - Implement policies requiring multi-person approval for wire transfers or major changes

AI has completely changed the landscape of scams. In the past, we told people to look for misspellings, bad grammar, or awkward phrasing as a way to spot phishing emails, but that advice no longer holds. Today, attackers are using AI to generate flawless, personalized emails and even clone voices or create deepfake videos. Imagine receiving a call from your "CEO," whose voice sounds identical, asking you to urgently approve a wire transfer. It feels real, but it may not be. The best defense isn't spotting grammar mistakes anymore, it's having strong verification procedures, slowing down when urgency is being forced, and making sure sensitive actions require confirmation through trusted out-of-band channels.

06

General Tips & Privacy

Once again, a great time to take a breather and ask if anyone has any questions? Moving onto the last section!

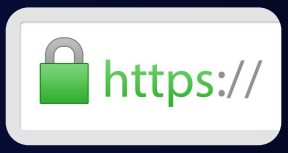
USB Drives & More

- Do NOT connect unknown or unauthorized media (or devices)
- Programs can run when plugged in without you doing anything
- Examples
  - USB/flash drives
  - SD or micro SD cards
  - CDs or DVDs
  - External hard drives
  - Cell phones <- Often forgotten

I often use the example of how attackers have mailed USB drives or even left them in parking lots knowing someone would plug them in. Most people don't realize these devices can infect your computer simply by plugging it in.

Encryption

- Can help protect your data
- Can also "help" an attacker, e.g. ransomware
- Protecting data sent or received
  - HTTP vs. HTTPS
  - Wireless -> WPA2 (AES) recommended
- Protecting devices
  - Helpful if device is lost/stolen
  - Often associated with phone PIN/passcode
  - Microsoft Windows - BitLocker
  - Apple MacOS - FileVault



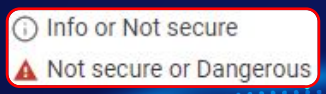
Here's another topic that eyes often glaze over. Use the HTTP versus HTTPS as an example. Explain how encryption helps protect all of us including shopping on the internet, when using wireless communications, etc. If you have anyone from the medical field in attendance, then I would also point out that lost and stolen devices such as laptops are the #1 reason for patient data breaches of more than 500 records. (Source: https://www.texmed.org/HIPAALostLaptop/)

Internet Safety Quick Tips

- Never click or install anything based on a pop-up from a website
- "Trusted" websites can & have hosted malware, aka malvertising
  - Local news, local schools?
  - WSJ, Forbes, ESPN, Yahoo, etc.
  - Limit browsing to business relevant sites?
- Avoid public: Wi-Fi, computers (hotels, libraries), charging, etc.

Do NOT assume a site is legitimate simply because of the "padlock"

No more padlock?



A few tips that didn't fit in well elsewhere. Any website can unwillingly be used to distribute malware. We also recommend avoiding public wi-fi and public computers because they are perfect places for attackers to lurk. Also, after discussing HTTP and HTTPS from the previous slide, this is a great opportunity to point out that HTTPS (and the padlock) doesn't necessarily mean a site is legit. It simply means your communications with that website are encrypted and it is up to the user to make sure they are at the correct site. To make matters more confusing, some browsers are now showing nothing (no padlock even) for secure websites. Instead, they only show "not secure" or something similar if the website is just HTTP, i.e. *not* HTTPS.

Internet Privacy

- Data is the new gold -> your data is valuable!
- If you're not paying for it, are you the product?
  - Data analytics & predictive results
  - Examples: advertising & insurance rates
- Are you oversharing?
  - "Fun" online surveys => data harvesting
  - Default privacy settings on social media
  - Vacation photos & checking-in (location sharing)
    - Thieves see that information also
    - Would you be comfortable telling people on the street?

A short discussion on privacy and not oversharing. The "fun" surveys to figure out your IQ, which cartoon character you are most like, etc. are all ways to get access to your social media profile and harvest data from you! Everyone knows someone who posted their vacation pictures while they were on vacation and their house was broken in as a result. I tell people to wait until they come home to post their pictures; that will make the following week of work go faster when they are reminiscing about their recent vacation. ;-)

Uh oh! You've been scammed!

- It happens! Don't be ashamed!
- Don't panic, but don't wait around
  - Unplug computer!
  - Contact your technical support
  - Write down details - event timeline, financial accounts, credentials used, phone numbers, etc.
- Ransomware or scam
  - Report the incident to law enforcement?
  - In the US
    - BBB - https://www.bbb.org/scamtracker
    - FBI - Ransomware keys may be available
    - FTC - https://reportfraud.ftc.gov/
  - https://www.nomoreransom.org/

Last but not least, what do you do when you or a loved one falls victim to a scam. Ask for help! Time is of the essence so act fast! Maybe that includes unplugging the power to your computer or the network cable to avoid the possibility of infecting other machines? Write down any details you think might be helpful such as dates/times, which accounts or credentials might be in question, as well as any other relevant info. If it's ransomware or a scam, do you report it? Who do you report it to? If it's ransomware, ransomware keys may be available. The folks at nomoreransom.org have an awesome site that is setup for just that purpose.

More Resources

- When in doubt, ask questions
  - Your IT dept/provider?
- Don't stop here! Attacks change, so should you
- Additional Resources
  - SANS Ouch! - free monthly newsletter
  - StaySafeOnline.org - numerous free resources
  - Stop. Think. Connect. - free, little bit of everything
  - TreeTop Security - Cybersecurity Awareness Training (free)
    These slides, video presentation of this material, value-add worksheets, post-training quizzes, feedback form, newsletter sign-up, certificate of completion & more! - https://www.treetopsecurity.com/CAT
- Worksheet #5 - Share this with others

Encourage attendees to ask questions if they are unsure if something is legit. Typically if their gut tells them it's not quite right, there's a reason for it! Encourage them to ask someone more tech savvy or if it's at a business, have them ask their IT department. A 30 second question is far better than weeks (or more) of agony.
Encourage the audience to continue learning, i.e. attacks evolve so they should too. The SANS Ouch newsletter is a fantastic, free monthly newsletter that anyone can sign up for; they frequently cover scams in the news as well as ways to protect yourself online and they are aimed at the average user, not IT people. Staysafeonline.org has tons of free resources and DHS has the Stop.Think.Connect. program to help educate business and end users alike.
Finally, our website has these slides and a video of us presenting these slides. There are also worksheets for attendees to take home or back to the office, a feedback form on how we can improve this presentation, a sign-up for our monthly newsletter, along with a cybersecurity quiz to test what users learned. We even have a certificate of completion so they can others (and their boss) that they are more cyber aware!
Finally, encourage attendees to help others in the process by sharing this information/presentation.

My contact info. Place your information here for others to get in contact with you. Remember, you're the expert!
Don't forget to recognize the original content was provided free of charge from TreeTop Security.