



# Cybersecurity Awareness

Protecting You And Your Data

Roadhaven  
Edition

PRESENTED BY

Brent Wissbrod  
[bwissbrod@gmail.com](mailto:bwissbrod@gmail.com)

# # whoami

- About Me
  - Based in Lakeville, MN
  - Currently at NC SECU (2nd largest credit union)
  - Formerly CyberSecurity at Accenture & PWC
  - Background
    - Computer Science and Software Engineering Degrees
    - 10 years Application Development
    - 20 years Security - IAM (Identity & Access Management)
  - Why am I here?





**LIVE  
LAUGH  
GET HACKED  
STOP LAUGHING**

# Overview

- Why security awareness?
- Backup, backup, backup
- Patching ALL of your devices
- Passwords
- Multi-factor authentication
- Internet safety & email
- Phone scams
- Privacy concerns

*What to do when things go wrong*



**Why is  
cybersecurity  
awareness  
important?**



# 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
  - Parents
  - Seniors
  - Business owners
  - Kids
  - Everyone!



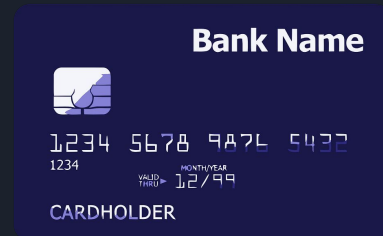
Reminder: Many tips that keep you safe at work will also keep you safe at home!



But an attacker isn't interested in me...

**Wrong!!! You are exactly what an attacker wants!**

- Credit card and financial data
- Medical data
  - Prescription, insurance, or identity fraud
  - Far more valuable than financial data
- Computer resources
  - Cryptomining
  - Ransomware
  - Advertising
  - Jump point
- User or email credentials
  - Sending spam
  - "More" access
  - Recovery/reset other accounts





# HELP!!!

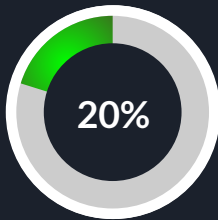


Ways to protect  
yourself!

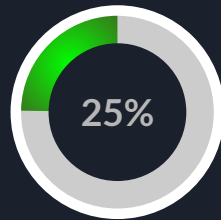


# Backups

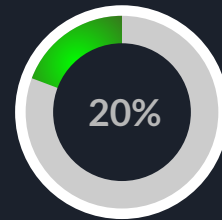
- Backups protect when all else fails
  - NO level of protection is perfect
  - Only “guaranteed” protection against ransomware
- Backup media should \*not\* be connected at all times
- Test your backups! Restore, restore, restore...



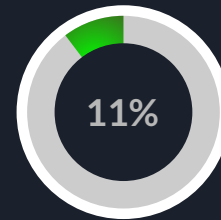
Users that have never backed up



Users that backup yearly



Users that backup monthly



Users that backup daily



# 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”



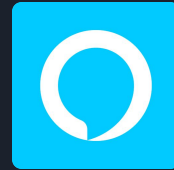
# Keeping your system up-to-date

- Operating Systems
  - Microsoft Windows, Apple MacOS, Linux
  - Windows 7 end of life was January 2020
- Anti-virus
  - Update to the latest definitions to ensure protection against the latest threats
  - Symantec/Norton, McAfee, Windows Defender, Avast, and many others!



# 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 could keep going forever!



A dark blue, 3D-rendered padlock is centered on the page. The padlock is closed, and its body features a folder icon. The text 'All About Passwords' is overlaid on the padlock in a large, white, sans-serif font.

# All About Passwords

A close-up photograph of a small, fluffy puppy with white fur and brown patches on its ears and face. The puppy is sitting in a bed of green grass and has its right front paw raised towards the camera. The puppy's eyes are dark and looking directly at the viewer.

**SOMEONE FIGURED  
OUT MY PASSWORD,**

**NOW I HAVE TO RENAME MY DOG**

# Managing Passwords

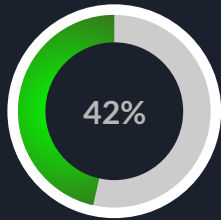
- Keep your passwords in a secure location
  - Do NOT use paper or sticky notes
  - Do NOT store passwords in clear-text on your computer - Word, Excel, etc.
  - Do NOT use the same password everywhere!
- Utilize a password manager (aka vault)
  - **Bitwarden** ○ KeePass ○ 1Password
  - Chrome? ○ ~~LastPass~~
- 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



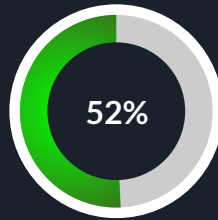
# Password Tips

- 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

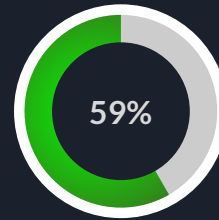
Easy with a password manager



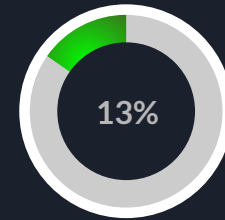
Rely on sticky notes for password mgmt



Re-use password for multiple accounts



Use name or birthdate in password



Reuse same password for all accounts





# 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@ssw0rd
  - Great password (25): MysonwasbornNovember1995!

Why are most passwords exactly 8 characters?

# Top 20 passwords by rank & year

Rank	2020	2021	2022	Rank	2020	2021	2022
1	123456	123456	password	11	1234567	qwerty123	1234567
2	123456789	123456789	123456	12	qwerty	000000	1234
3	picture1	12345	123456789	13	abc123	1q2w3e	1234567890
4	password	qwerty	guest	14	Million2	aa12345678	000000
5	12345678	password	qwerty	15	000000	abc123	555555
6	111111	12345678	12345678	16	1234	password1	666666
7	123123	111111	111111	17	iloveyou	1234	123321
8	12345	123123	12345	18	aaron431	qwertyuiop	654321
9	1234567890	1234567890	col123456	19	password1	123321	7777777
10	senha	1234567	123123	20	qqww1122	password123	123

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

# 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	Instantly	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 passwords.

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

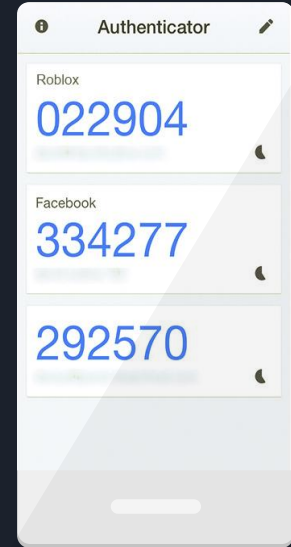
# MFA - Multi-Factor Auth

- What is MFA?
  - “Beyond” a username and password
  - Second form to prove it is you
  - Typically out-of-band

- “Your one-time code is...”

- SMS
- Phone call
- Email
- Phone pop-up
- Authenticators
  - Microsoft
  - Google
  - ForgeRock, Okta, Ping, etc.

Not as  
secure



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



# Just A Little Click



# Is the link safe in 4 steps

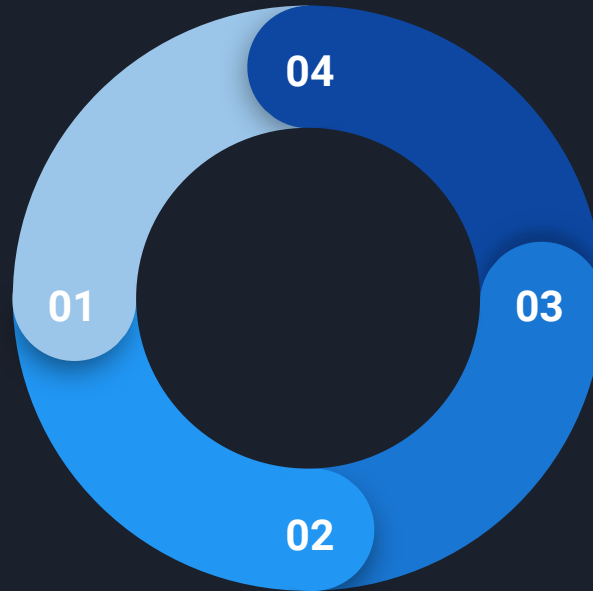
## 1. Verify

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

# Easy to recognize scam

Everything is allowed! Just don't forget Viagra.



BEST CAN DRUGS <online\_pillsshop5hfal@pharmacy.canada>

To:

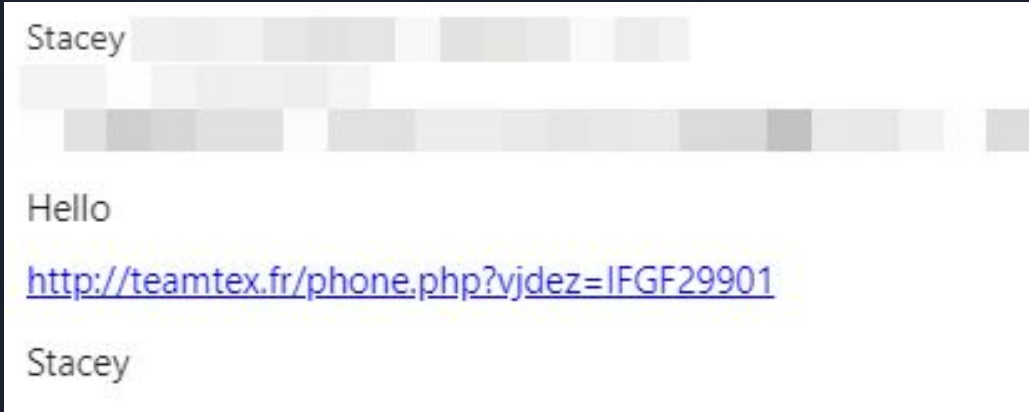
[SHIP NOW \[RX-COMPANY\]](#)

Red flags?

- Viagra <- !?!?!>
- Strange wording
- Email address

Domain name  
Expected email?  
Interesting link

# From known email account



Hacked or spoofed  
email from  
someone you know

*Similar attacks via  
Facebook & social media*

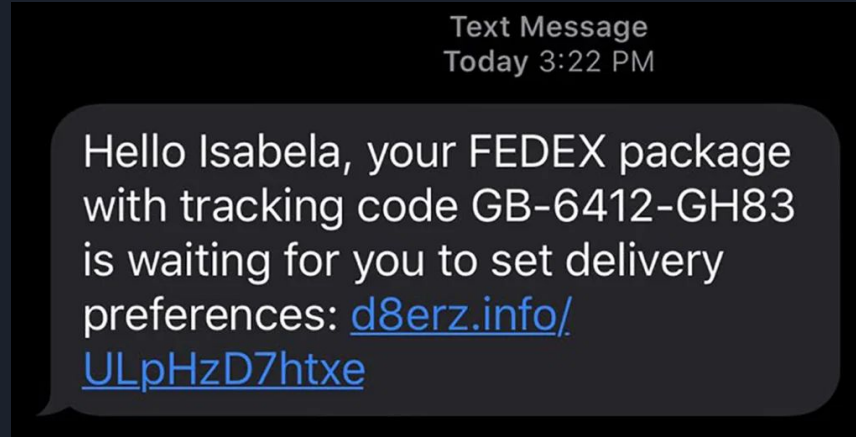
Red flags?

- Email address ok
- Name ok
- Odd "signature"

Expected email?  
Link - .fr is France



# Text messaging example



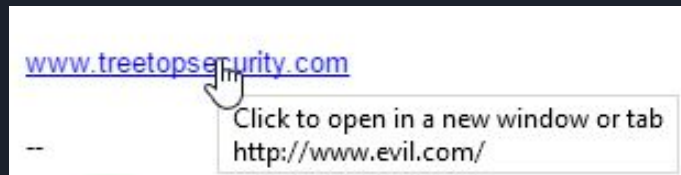
Red flags?

- Name in SMS ok
- Number ok?
- Expected text?
- Received a text regarding a package before?
- Recognized domain?

# 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!!!

Desktop - Hover



Mobile - Long Press

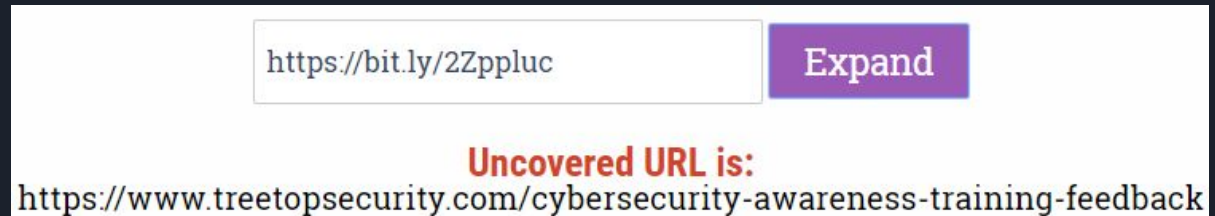




# Shortened or obfuscated links?

- Instead of 300 characters, the link is reduced to 15 characters
  - Bit.ly
  - TinyURL
- Extremely common and helpful, but...
- Abused by criminals to hide malicious websites

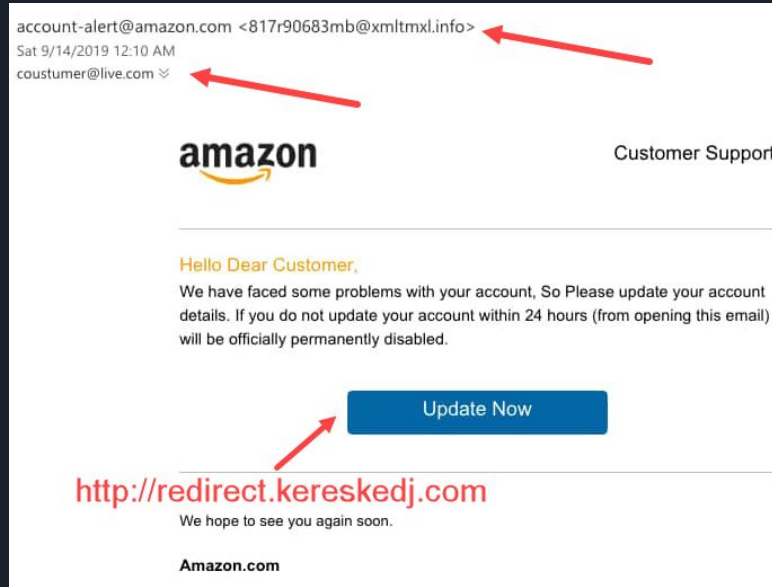
Link expander  
www.linkexpander.com



https://bit.ly/2Zppluc [Expand](#)

**Uncovered URL is:**  
<https://www.treetopsecurity.com/cybersecurity-awareness-training-feedback>

# Hover is your friend



Red flags?

- Email address ok?
- Expected email?
- Sense of urgency
- **HOVER!!!**



# 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*

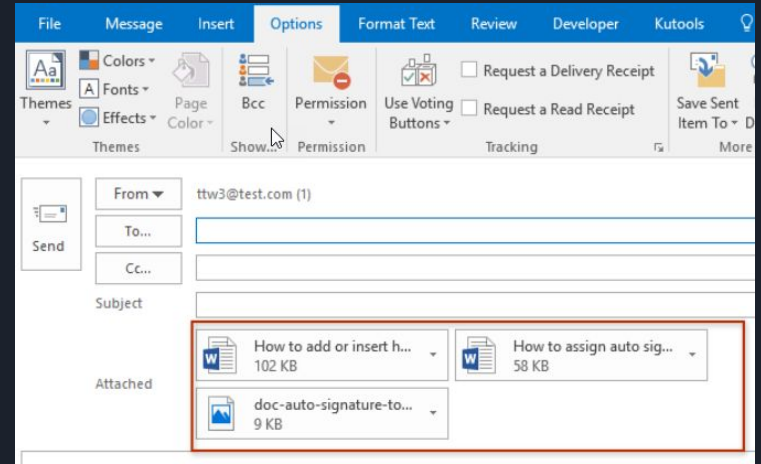
# Email Attachments

- Stop & think before you click!
- Recognized sender?
- Expecting attachment?
- Is it normal for that contact to send attachments?

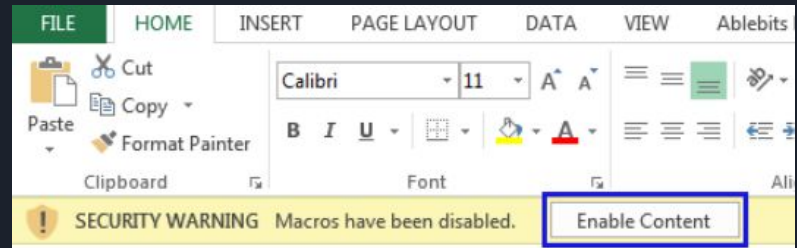
## Macros

- Step 1: Don't do it!!!
- Step 2: See step 1
- Found in downloaded files too

## Attachments in email client (Microsoft Outlook)



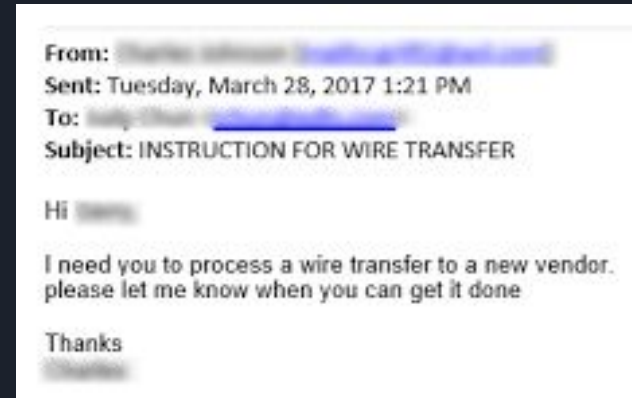
Enable Macros <- NOOOOOO!!!!



# Business email compromise (BEC)

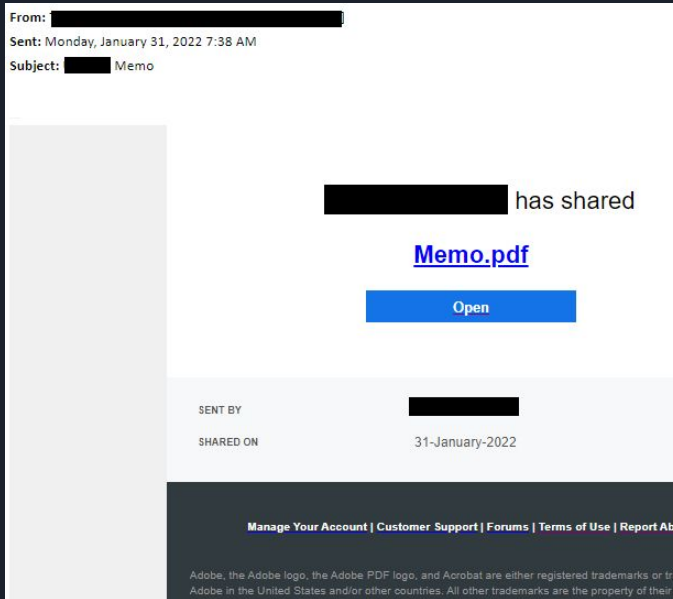
- FBI: BEC cost businesses \$1.8B every year
- Moving funds -> more susceptible
  - Policy requiring phone call?
- “Trusted” senders
  - Research using publicly available data
    - Published organization chart
    - Spear phishing (CEO <-> CFO)
  - Spoofed domain
    - microsoft.com - micros0ft.com
  - Compromise account of 3rd parties
    - Employee, vendor, or customer
    - Thread hijacking <- lookout

## Wire transfer



*Often requires very little technical skill*

# Customer BEC example

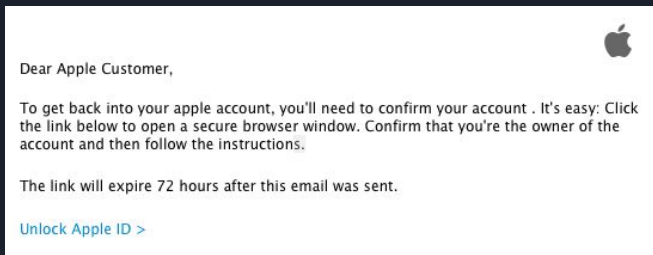


- Small business < 100 employees
- CEO received email
  - From school district (their customer)
  - Bid proposal
  - Busy CEO blocked, certain it was legit
  - Asked us to “bypass” blocks/alerts
- Give us 5 minutes
  - Contacted school IT
  - “You’re the 2nd call”
  - All within 30 mins of 1st alert



# Other Email Scams

## Account credentials



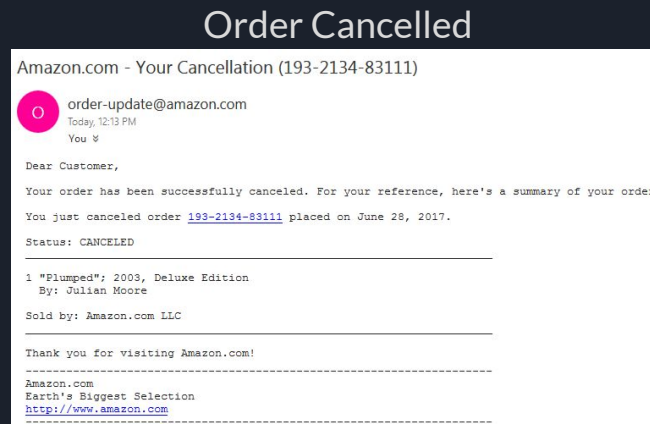
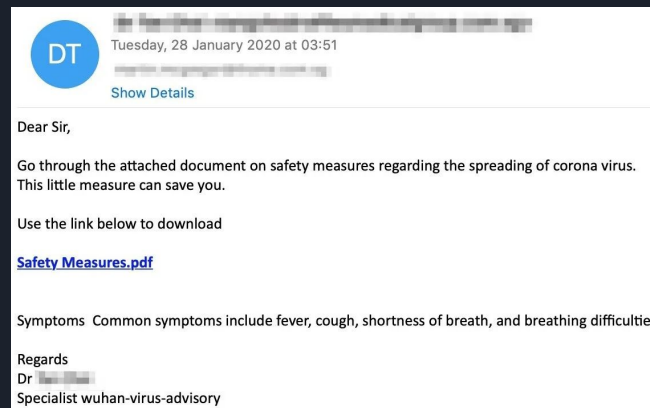
*Technology alone  
cannot solve this*

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

# Scammer favorites

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

*Keep your guard up!*





# Reach Out & Scam Someone

# Phone Scams

- Social engineering, what is it?
  - Banks & credit card companies
  - Medical & insurance
  - IRS or any past due account balance
  - 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
  - Tech support - Microsoft, Apple, Dell, etc.
- Artificial Intelligence (AI) will make this exponentially worse!!!



will

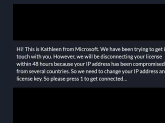


# Phone scam example



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 call from Microsoft?

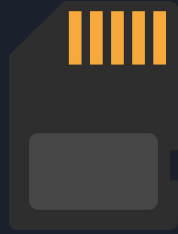


*Technical safeguards can only do so much...  
That's why security awareness is a must!*



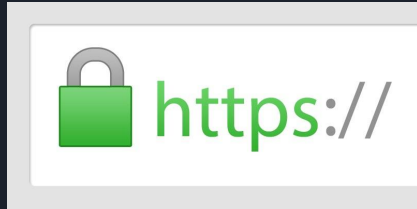
# General Tips & Privacy

# 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

# 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



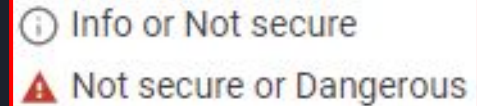
# Internet Safety Quick Tips

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

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



*No more padlock?*



# 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?



# Social Media Privacy

- If you use the any social media please review your settings!
  - Facebook, Twitter, TikTok, Instagram, Snapchat, etc.
- Is your profile private vs. public?
  - Do you care?
- USSOCOM Recommendations
  - A wealth of information on how to secure various services and devices:
  - <https://www.soc.mil/IdM/publications/IdMpubs.html>





# Identity Theft Protection



- Services that will help you recover from Identity theft:
  - Norton LifeLock
  - EverSafe
  - IDShield
- A good option for people that do not want to deal with the aftermath of identity theft (aka spending hours on the phone with your bank(s), credit card(s), and other financial institutions)
- Overview of identity theft insurance and restoration:
  - <https://www.nerdwallet.com/article/insurance/identity-theft-insurance>

# 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
    - <https://www.identitytheft.gov/>
  - <https://www.nomoreransom.org/>



# 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
    - <https://www.sans.org/newsletters/ouch/>
  - StaySafeOnline.org - numerous free resources
  - Stop. Think. Connect. - free, little bit of everything
    - <https://www.stopthinkconnect.org/>
  - 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>



# Even More Resources

- Additional Resources
  - Cybersecurity & Infrastructure Security Agency (CISA)
    - <https://www.cisa.gov/>
  - Canadian Centre for Cyber Security
    - <https://www.cyber.gc.ca/en>
  - USSOCOM Recommendations
    - <https://www.soc.mil/IdM/publications/IdMpubs.html>
  - Bruce Schneier - Crypto-Gram Newsletter
    - <https://www.schneier.com>
  - CyberInsureOne
    - <https://cyberinsureone.com/online-safety-seniors/>





# Questions?

Brent Wissbrod

[bwissbrod@gmail.com](mailto:bwissbrod@gmail.com)



<https://www.linkedin.com/in/brent-wissbrod/>