Cybersecurity

January 13, 2022

Community Emergency Response Team

City of Novi, Michigan

Cybersecurity?

COMMUNITY EMERGENCY RESPONSE TEAM

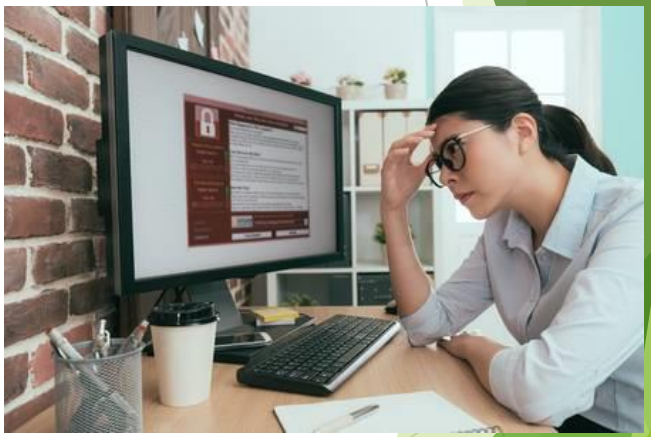
Goals of this presentation

- Why are you at risk?
- Real world examples
- Understanding Ransomware/Phishing
- How to protect yourself, your family and your business

CERT
COMMUNITY EMERGENCY RESPONSE TEAM

Are you worried?

- Antivirus software only catches 5% of new threats targeting your computer.
- Data brokers collect more than 50 trillion unique data transactions per year.
- 82% of Android apps track your other online activities.
- An American is the victim of identify theft every 2 seconds.
- Over 600,000 Facebook accounts are hacked every day.
- 80% of cybercriminals are now working with organized crime.



CERT
COMMUNITY EMERGENCY RESPONSE TEAM

Why are YOU at greater risk?

- Fewer resources to prevent data disaster
- Limited resources to then combat disaster
- Can't afford to lose valuable data
- Negative impact on reputation

Why are SMALL BUSINESSES at greater risk?

- Can't afford to not produce revenue
- Loss of competitive edge
- Negative impact with customers
- Potential regulation non-compliance

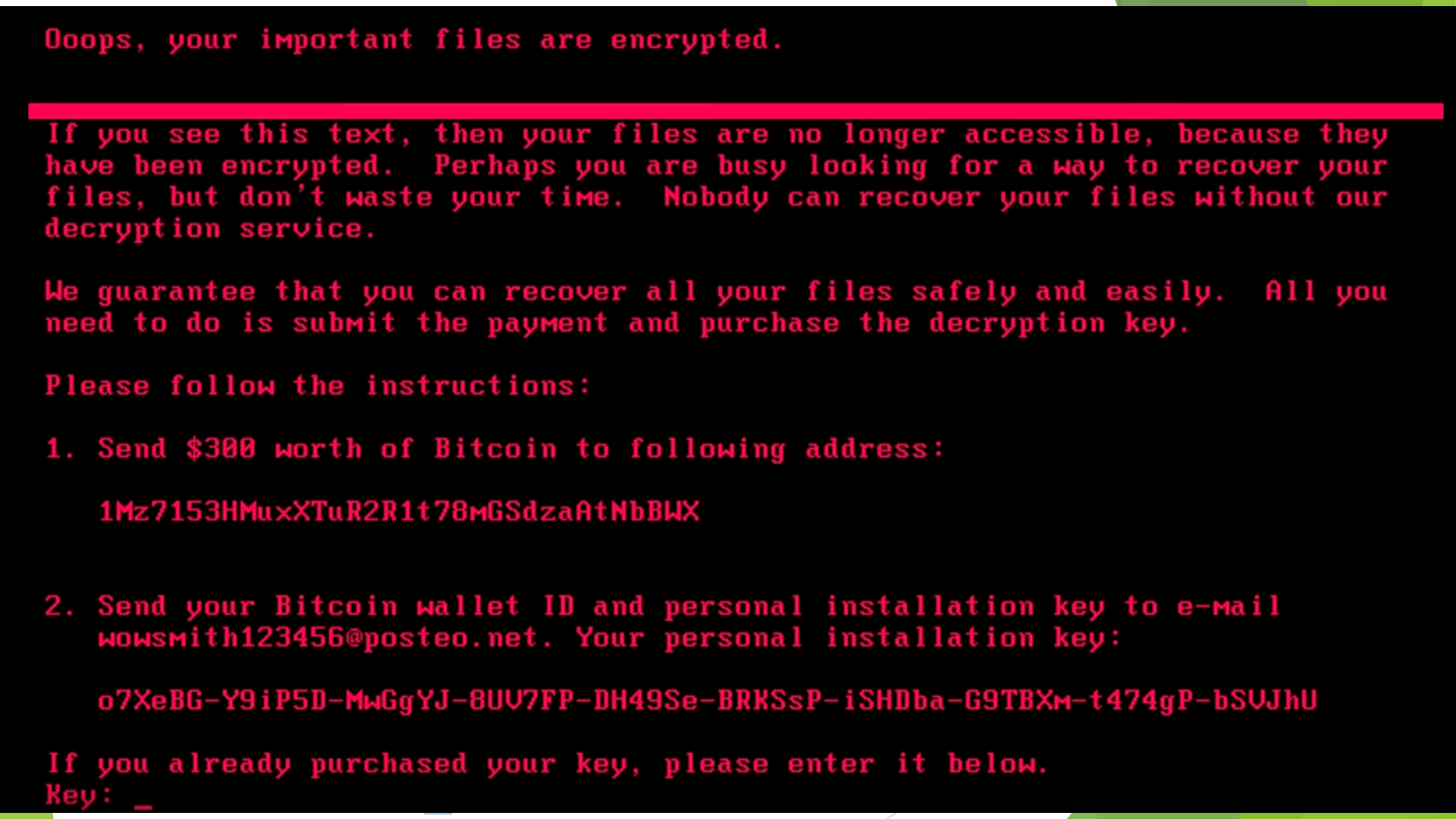
Cybersecurity is EVERYONE's job, including yours.

CERT COMMUNITY EMERGENCY RESPONSE TEAM

How is Ransomware changing things?

- Ransomware attacks have been on the rise and getting more dangerous in recent years, with cyber criminals aiming to encrypt as much of a corporate network as possible in order to extort a bitcoin ransom in return for restoring it.
- **A single attack can result in cyber criminals making hundreds of thousands or even millions of dollars.**
- Despite the changing working circumstances with more people working remotely during 2020/2021, with Bitdefender's *Mid-Year Threat Landscape Report 2020* claiming a **715% year-on-year increase** in detected – and blocked – ransomware attacks.
- Ransomware and Email based threats pose a significant challenges to you, your family and your business, let's dive in about how Ransomware works.

CERT
COMMUNITY EMERGENCY RESPONSE TEAM

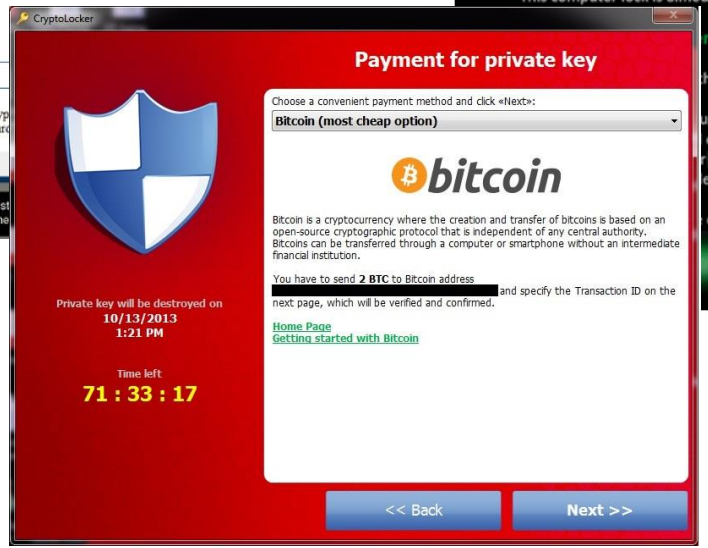

Ooops, your important files are encrypted.
If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.
We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.
Please follow the instructions:
1. Send $300 worth of Bitcoin to following address:
1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:
o7XeBG-Y9iP5D-MwGgYJ-8UV7FP-DH49Se-BRKSsP-iSHDba-G9TBXm-t474gP-bSVJhU
If you already purchased your key, please enter it below.
Key: _

What exactly is Ransomware?

- Malicious software that is installed on your computers and servers by way of email or infected websites
- Files are then encrypted and can only be opened (UNLOCKED) with a key that only the cybercriminals retain
- You have two options:
    1. Restore from backups (if you have them!)
    2. Pay the ransom and hope the criminals send the key

COMMUNITY EMERGENCY RESPONSE TEAM

COMMUNITY EMERGENCY RESPONSE TEAM



COMMUNITY EMERGENCY RESPONSE TEAM

CERT
COMMUNITY EMERGENCY RESPONSE TEAM

REAL WORLD
Story Time

CERT
COMMUNITY EMERGENCY RESPONSE TEAM

Day 1 – Medical Office Ransomware Attack

- 12 PM: Staff member clicks on a link on their personal email account from an office computer while eating their lunch
- 1 PM: Lunch ends – Front desk staff can't access the patient management system to check in patients.
- 1:05 PM: Doctor can't access patients digital x-ray information
- 1:15 PM: Call to Huntington Technology (HT) Support Line - HELP!
- 1:20 PM: HT determines they were hit with Crypto-locker ransomware.
- 1:30 PM: HT determines that all files on the server have been encrypted and finds text file with instructions from the cybercriminals on what to do to get their data back.
- 1:35 PM: HT determines that the local external backup drive was also encrypted, and all the backup files are encrypted.
- 1:40 PM: HT asks client if the spare external backup drive is up to date – Client informs the tech that they haven't been swapping drives for several years.
- **No other backup device exists.** - Dr. sends staff home and cancels all appointments for the rest of the day.

CERT COMMUNITY EMERGENCY RESPONSE TEAM

Days 2 through 15
REACTING TO THE ATTACK

- OVER 2 WEEKS OF DOWNTIME
- With no other recovery options available paying the ransom was only choice...
- There was no guarantee of getting the data!
- Ransom of 5 Bitcoin requested – negotiated down to 2 over the next few days.
- Finally, 10 days later we received the decoding software from the criminals.
- Systems are fully restored.

CERT
COMMUNITY EMERGENCY RESPONSE TEAM

The fallout and Impact on the business

The Client spent $2,500 in Bitcoin.

Plus the added 20-30 hours of IT support.

Unable to see patients for several days.

Unable to send out billing or make payments.

Total cost of downtime & remediation?

$18,000

The average payment for a ransomware decryption key

Q3 2019	41,198	
Q4 2019	84,116	+ 104%

- Veeam Jan 2020

CERT COMMUNITY EMERGENCY RESPONSE TEAM

What could they have done better?

- The UPDATE Protocol
- Follow these simple steps and you can avoid 85% of the most common digital threats out there.
- This is the digital equivalent of locking your front door.

CERT
COMMUNITY EMERGENCY RESPONSE TEAM

The UPDATE Protocol

Update Frequently

- Modern software are riddled with bugs – security vulnerabilities which cybercriminals use to break into your computer, cell phone and other devices.
- Plug these holes by setting your software to automatically update from trusted parties.

Source: FutureCrimes.com

CERT COMMUNITY EMERGENCY RESPONSE TEAM

The UPDATE Protocol

Passwords

- Do not use the same password across multiple sites.
- Use a password management program to generate long unique passwords without the need to memorize them all.
- Take advantage of two-factor authentication whenever possible.

Source: FutureCrimes.com

CERT COMMUNITY EMERGENCY RESPONSE TEAM

The UPDATE Protocol

Download

- Download software only from trusted parties, such as Apple's App Store or directly from a company's own verified website.
- Be highly skeptical of third-party sites offering "free" software.
- Pay attention to apps and their permissions. They are "free" for a reason and you're paying with your privacy.

Source: FutureCrimes.com

CERT COMMUNITY EMERGENCY RESPONSE TEAM

The UPDATE Protocol

Admin

- Administrator login accounts have the highest level of privilege to make changes on your computer.
- Create a separate standard “user” account to perform your work and online browsing.

Source: FutureCrimes.com

CERT COMMUNITY EMERGENCY RESPONSE TEAM

The UPDATE Protocol

Turn-Off

- Turn-off your computer or at least your Wi-Fi connection when not in use.
- Turn off services and connections on your smartphone when you are not using them. Keeping Bluetooth, Wi-Fi, NFC and cellular hotspots active at all times provides additional avenues for attack.

Source: FutureCrimes.com

CERT COMMUNITY EMERGENCY RESPONSE TEAM

The UPDATE Protocol

Encrypt

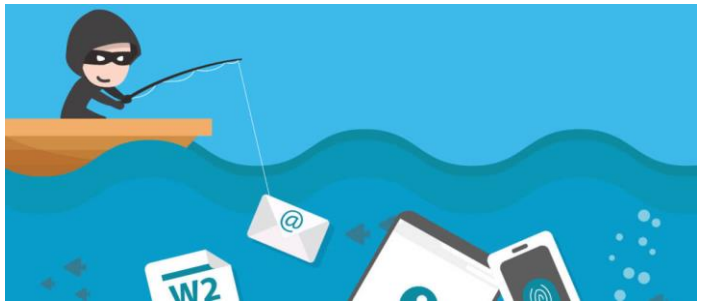
- Windows and Mac both include free programs for full hard disk encryption
- Use Virtual Private Network (VPN) software, especially when on public Wi-Fi networks.
- Setting a password on your smartphone not only limits access to the device but encrypts your data.

Source: FutureCrimes.com

CERT COMMUNITY EMERGENCY RESPONSE TEAM

Story 2 - Phishing: Business Email Compromise

- Cybercriminals spoof email accounts and impersonate company Executives.
- Goal is to fool employees in accounting or HR into sending wire transfers or sending out confidential information (tax information).
- According to FBI statistics, Business Email Compromise is now a $26 **B**illion scam.
- Between May 2018 and July 2019, there was a 100% increase in identified losses.
- The scam has been reported in all 50 states and in 150+ countries.



Source: https://www.ic3.gov/Media/Y2019/PSA190910

COMMUNITY EMERGENCY RESPONSE TEAM

What is Phishing?

Phishing is a type of online scam where criminals send out fraudulent email messages that appear to come from a legitimate source.

The emails are designed to trick the recipient into entering confidential information (ex: account numbers, passwords, pin, birthday) into a fake website by clicking on a link.

The email includes a link or attachment that, when clicked, will steal sensitive information or infect a computer with malware.

Phishing involves tricking people into giving out sensitive information or passwords. It's called PHishing due to a long-time hacker tradition of using "PH" in place of "F".

CERT COMMUNITY EMERGENCY RESPONSE TEAM

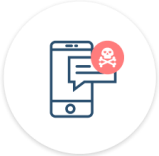
Types of Phishing Attacks

Clone Phishing

Clone Phishing is where a legitimate and previously delivered email is used to create an identical email with malicious content. The cloned email will appear to come from the original sender but will be an updated version that contains malicious links or attachments. Think emails from banks/service providers that you would normally see in your mailbox.

Spear Phishing/Whaling

Spear Phishing is a more targeted attempt to steal sensitive information. It typically focuses on a specific individual or organization. These types of attack use personal information that is specific to the individual in order to appear legitimate.



Vishing/Smishing

Vishing refers to phishing scams that take place over a phone call/voicemail. This type of attack involves the most human interaction, but it follows the same pattern of deception as other types of phishing attacks.

Smishing is a type of phishing that uses SMS (text) messages as opposed to emails to target individuals.

CERT
COMMUNITY EMERGENCY RESPONSE TEAM

Step 1:
Identify a Target

Organized crime groups target U.S. and European businesses, exploiting information available online to develop a profile on the company and its executives.

Step 2:
Grooming

Spear phishing e-mails and/or telephone calls target victim company officials (typically an individual identified in the finance department).

Perpetrators use persuasion and pressure to manipulate and exploit human nature.

Grooming may occur over a few days or weeks.

Step 3:
Exchange of Information

The victim is convinced he/she is conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

Step 4:
Wire Transfer

Upon transfer, the funds are steered to a bank account controlled by the organized crime group.*

*Note: Perpetrators may continue to groom the victim into transferring more funds.

Business E-Mail Compromise Timeline

An outline of how the business e-mail compromise is executed by some organized crime groups

CERT
COMMUNITY EMERGENCY RESPONSE TEAM

How Business Email Compromise (BEC) Impacts You

- The Start:

Cybercriminals see if they can ‘spoof’ your domain or impersonate the CEO or other important employees.

COMMUNITY EMERGENCY RESPONSE TEAM

How BEC Impacts You

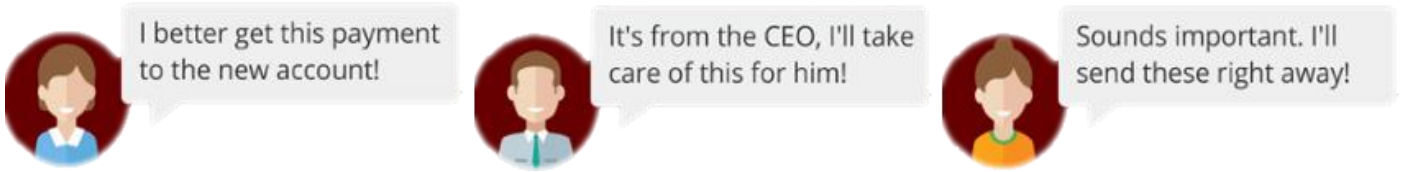
The Phish: Spoofed emails are sent to high-risk employees in the organization. Finance, HR, Purchasing…

To: Finance Department	To: CFO	To: Human Resources
Urgent wire transfer request! Please send $100,000 to new acct #987654-3210	Please pay this time-sensitive invoice. I'm on vacation and will be unavailable, no need to respond. - Your CEO	I need a PDF copy of ALL employee W-2s for the IRS ASAP!

CERT COMMUNITY EMERGENCY RESPONSE TEAM

How BEC Impacts You

The Response: End user receives an email and acts without reflection or questioning the source.



How BEC Impacts You

The Damage: Phishing was successful, giving cybercriminals what they were after. This causes fraudulent wire transfers and massive data breaches.

CERT
COMMUNITY EMERGENCY RESPONSE TEAM

How BEC Impacts You

The Result: The fallout after a successful attack can be highly damaging for both company and its employees.

- Money is gone forever. In most cases only 4% can be recovered.
- Employees are often fired.
- Lawsuits are filed.
- Intangibles – tarnished reputation, loss of trust, etc.

Please Think Before You Click!

CERT COMMUNITY EMERGENCY RESPONSE TEAM

Reviewing the Possible Risks of Phishing

In Your Personal Life

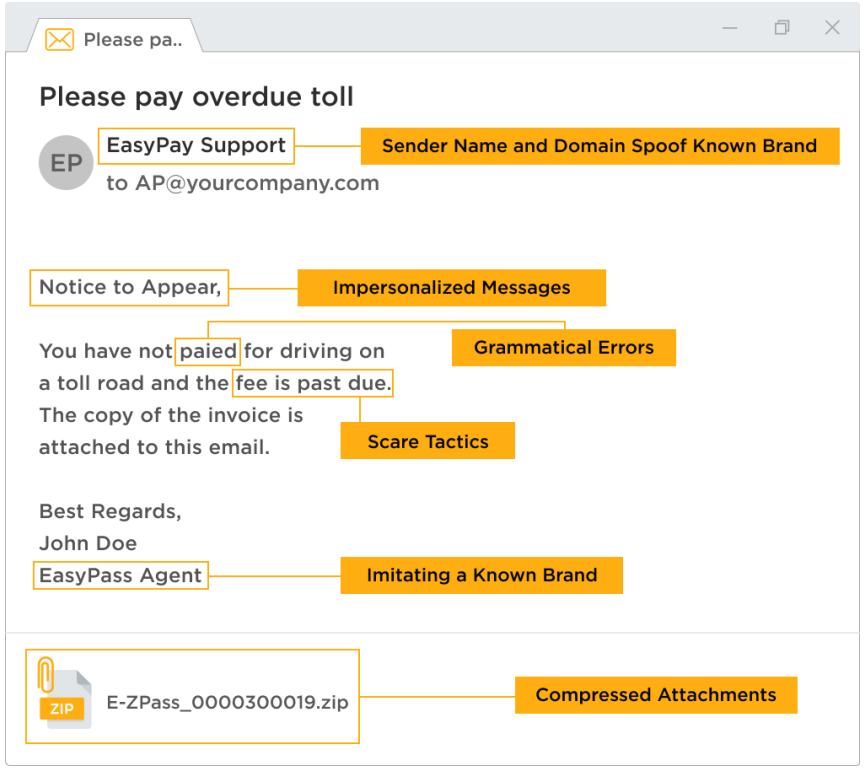
- Money stolen from bank accounts
- Fraudulent charges on credit cards
- Tax returns filed in a person's name
- Loans and mortgages opened in a person's name
- Loss of access to photos, videos, files, and other important documents
- Fake social media posts made in a person's accounts

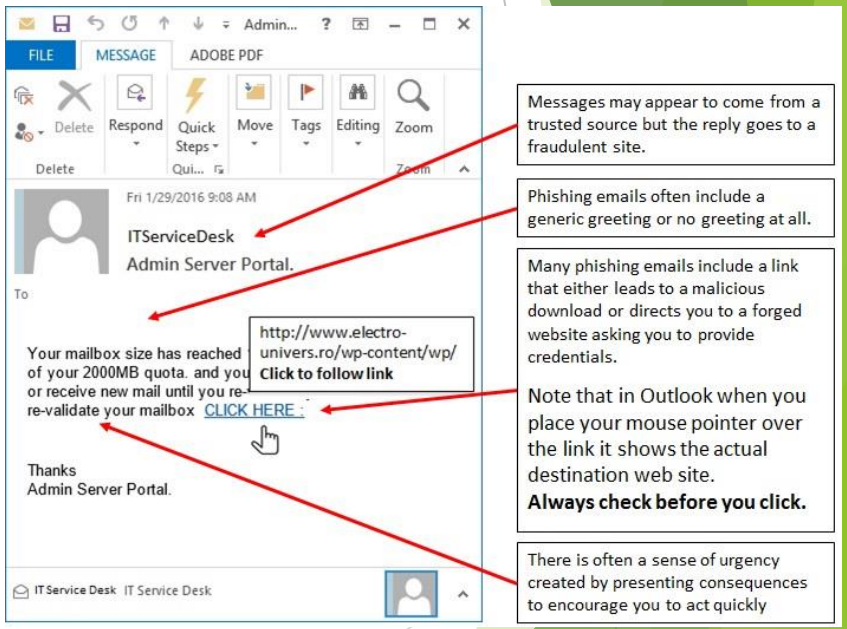
At Work

- Loss of corporate funds
- Exposed personal information of customers and co-workers
- Outsiders gain access to confidential communications, files, and systems
- Files become locked and inaccessible
- Damage to employer's reputation

CERT COMMUNITY EMERGENCY RESPONSE TEAM

What to Look For?





CERT
COMMUNITY EMERGENCY RESPONSE TEAM

How to Protect Yourself Against a Phishing Attack

- Never click on suspicious links
- Do not reply to suspicious emails
- Be careful what you post online
- Verify the security of websites
- Be vigilant while downloading email attachments to your computer - If in doubt, do not download!
- Always call and get verbal confirmation before making any financial transactions

CERT
COMMUNITY EMERGENCY RESPONSE TEAM

If you think you've received or engaged in a phishing email, PLEASE report it

Story 3 - Do you have a spare $150k?

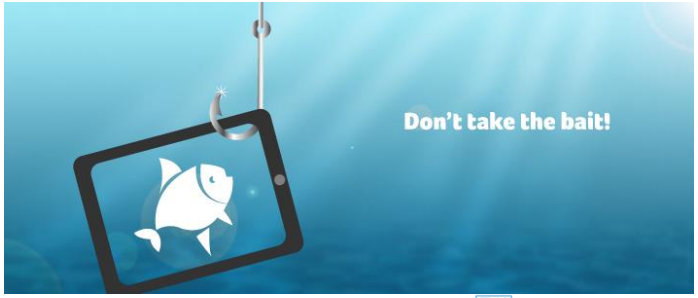
A PERFECT SPEAR PHISHING ATTACK

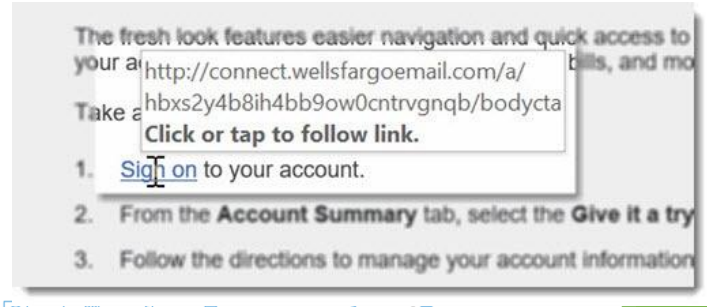
- **Business owner** clicks targeted malicious link and proceeds to enter email login information, and **never tells anyone**.
- Employee in the Finance Department, over the course of 10 days, sends multiple wire transfers believing they are approved by the business owner. *(The owner is on vacation.)*
- Owner returns from vacation to discover $150,000 has been sent to cybercriminals.
- Client then contacts Huntington Technology after all of this occurs to request help.
- Damage had been done, only 20% was able to be recovered by the bank.

CERT COMMUNITY EMERGENCY RESPONSE TEAM

Educational Reminders!

- Check the domain name.
  - *Do you know the difference between whitehouse.gov and vvhitehouse.gov, whitehouses.gov?*
- Hover over any links in emails or on websites. *Does the URL reveal a legitimate website address?*
- Be skeptical of emails asking to reset passwords or open/download/view documents. *Did you request this email?*
- Never initiate a wire transfer (or send sensitive data) without getting **verbal** approval!





COMMUNITY EMERGENCY RESPONSE TEAM

CYBERSECURITY IS EVERYONE'S JOB.

INCLUDING YOURS.