

# Cybersecurity

January 13, 2022



## Community Emergency Response Team

City of Novi, Michigan



**Cybersecurity?**



# Goals of this presentation

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

# 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.



# 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.



# 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.



Oops, 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](mailto:wowsmith123456@posteo.net). Your personal installation key:

o7XeBG-Y9iP5D-MwGgYJ-8UV7FP-DH49Se-BRKSsP-iSHDba-G9TBXm-t474gP-bSUJhU

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





CryptoLocker

# Your Personal files are encrypted!



Private key will be destroyed on

1/6/2015 1:11:17 PM

Time left

71:55:27

Checking wallet..

Received: 0.00 BTC

Your personal files **encryption** produced on this computer: photos, videos, documents, etc. Encryption was produced using a **unique** public key RSA-2048 generated for this computer.

To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow to decrypt on a secret server on the Internet; the server will **destroy** the specified in this window. After that, **nobody and never will be** files...

To **obtain** the private key for this computer, which will autom files, you need to pay **1.00 bitcoin** (~291 USD).

You can easily delete this software, but know that without it, be able to get your original files back.

Disable your antivirus to prevent the removal of this software

For more information on how to buy and send bitcoins, click "To open a list of encoded files, click "Show files"

Do not delete this list, it will be used for decryption. And do not

Show files



Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)

Wana Decrypt0r 2.0

## Ooops, your files have been encrypted!

English

### What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

### Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

### How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

GMT from Monday to Friday

Send \$300 worth of bitcoin to this address:



12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Check Payment

Decrypt



Unauthorized or pirated software has been detected. Your system has been blocked.



**Willful copyright infringement is a federal crime that carries penalties of up to five years in federal prison, a \$250,000 fine, forfeiture and restitution (17 U.S.C s.506, 18 U.S.C s.2319)**

As a first-time offender you are required by law to pay a fine of 250 USD

If the fine is not paid within three days, a warrant will be issued for your arrest, which will be forwarded to your local authorities.

You will be charged, fined, convicted for up to 5 years.

There are two ways to pay a fine:

1. You can pay your fine online through BitCoin. BitCoin is available nationwide.

Click the tabs below to find the nearest ATM or exchange.

Your computer will be unlocked after you make your payment.

2. (Offline Option) You can come to your local courthouse and pay your fine at the 'Cashiers' window.

Your computer will be unlocked within 4-5 working days.

To regain access now, transfer BitCoin to the following address (click to copy):

17Zuq1SV7g2ooyPTKp1h1mws4neduoNgGU

After the payment is finalized enter Transfer ID below.

Amount: Transfer ID:

BTC 0.378

NOTE: Files on this computer, including network files, have been encrypted. Do not attempt to remove this message. This will damage your files, hard

[Payment](#) [How to pay a fine](#) [Find nearest ATM](#)

Office of Criminal Investigation  
Cybercrime

## YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:

Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.



For you are obliged to pay a fine of \$200.

If you do not pay the fine, otherwise you will be arrested.

Enter the digits resulting code, which is displayed in the payment form and press the OK button. If you have any questions, enter them one after the other and press the OK button.

For more information, please contact our support team via email at [line@fbi.gov](mailto:line@fbi.gov).

### Payment for private key



Private key will be destroyed on  
**10/13/2013**  
1:21 PM

Time left  
**71 : 33 : 17**

Choose a convenient payment method and click «Next»:

**Bitcoin (most cheap option)**

 **bitcoin**

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send **2 BTC** to Bitcoin address  and specify the Transaction ID on the next page, which will be verified and confirmed.

[Home Page](#)  
[Getting started with Bitcoin](#)

<< Back
Next >>







# REAL WORLD Story Time

# 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.



# 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.



# 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



# 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.





## 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.



## 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.



# 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.



# 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.



# 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.



# The UPDATE Protocol

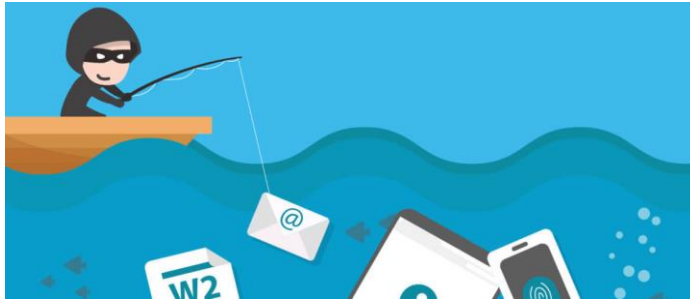
## Encrypt

- ▶ 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.



# 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 Billion 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>



# 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".





# Types of Phishing Attacks



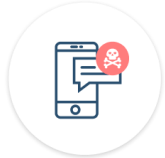
## Clone Phishing

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.



## 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



# 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.



# How BEC Impacts You

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

## The most common CEO fraud scenarios



Invoices sent from contractors, suppliers or other external parties that seem to have a legitimate relationship with the company.



Requests for confidential or personal information, often from either a person of authority or the company's legal counsel.

Urgent request for a transfer of funds from a person of authority within the organisation, usually sent as a plain text email without email signatures and other corporate branding.



Checking to see if a person is available or on location. Often this type of fraudulent email is for reconnaissance purposes and precedes the actual attack.



To: Finance Department

Urgent wire transfer request!  
Please send \$100,000 to new acct #987654-3210

To: CFO

Please pay this time-sensitive invoice. I'm on vacation and will be unavailable, no need to respond. - Your CEO

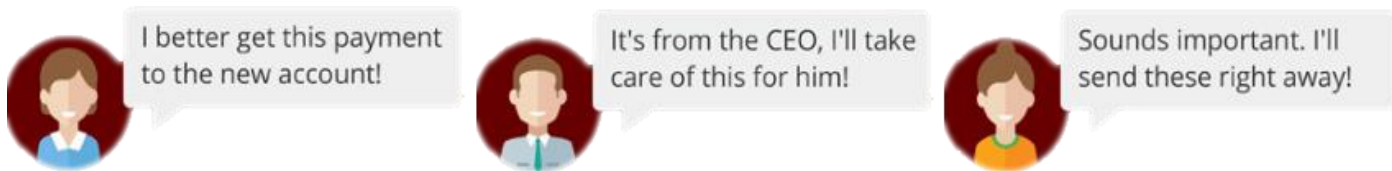
To: Human Resources

I need a PDF copy of ALL employee W-2s for the IRS ASAP!



## 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.



## 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!**



# 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





# What to Look For?

Please pa..

**Please pay overdue toll**

EP **EasyPay Support** — **Sender Name and Domain Spoof Known Brand**  
to AP@yourcompany.com

**Notice to Appear,** — **Impersonalized Messages**

You have not **paied** for driving on a toll road and the **fee is past due.** — **Grammatical Errors**

The copy of the invoice is attached to this email. — **Scare Tactics**

Best Regards,  
John Doe  
**EasyPass Agent** — **Imitating a Known Brand**

**E-ZPass\_0000300019.zip** — **Compressed Attachments**

FILE MESSAGE ADOBE PDF

Delete Respond Quick Steps Move Tags Editing Zoom

Fri 1/29/2016 9:08 AM

**ITServiceDesk**  
Admin Server Portal.

To

Your mailbox size has reached of your 2000MB quota. and you or receive new mail until you re-re-validate your mailbox **CLICK HERE**.

<http://www.electro-univers.ro/wp-content/wp/>  
**Click to follow link**

Thanks  
Admin Server Portal.

IT Service Desk IT Service Desk

Messages may appear to come from a trusted source but the reply goes to a fraudulent site.

Phishing emails often include a generic greeting or no greeting at all.

Many phishing emails include a link that either leads to a malicious download or directs you to a forged website asking you to provide credentials.

Note that in Outlook when you place your mouse pointer over the link it shows the actual destination web site.  
**Always check before you click.**

There is often a sense of urgency created by presenting consequences to encourage you to act quickly



# 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





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



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

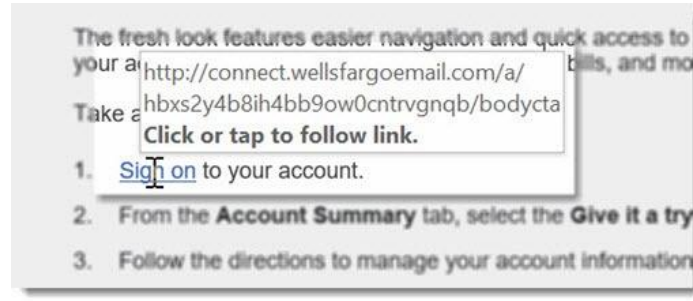
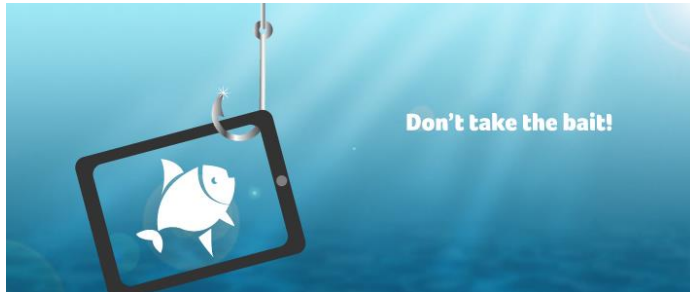
## A PERFECT SPEAR PHISHING ATTACK

- ❖ 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.



# Educational Reminders!

- ❖ Check the domain name.
  - *Do you know the difference between whitehouse.gov and vwhitehouse.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!



**CYBERSECURITY IS  
EVERYONE'S JOB.**

**INCLUDING YOURS.**

