



# US Secret Service Cyber Protection

Tim Benitez – Resident Agent in Charge

New Hampshire & Vermont



# Cyber Protection

## How to prevent, detect and mitigate your exposure to cyber enabled financial fraud.

- Learn your organizations vulnerabilities and be prepared to persevere during an incident
- Understand the roles of entities that may be involved during an incident
  - Executive suite
  - Communications
  - Legal
  - Insurance
  - Information Technology
  - Incident Response Firm – External counsel
  - Law Enforcement
- How to mitigate the situation through a collaborative approach (LEO, Bank, Private Sector)



# What is Cybersecurity?

- The ability to protect or defend the use of cyberspace from cyber attacks.
  - (National Institute of Standards and Technology – NIST)
- Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.
  - (US Government - Cybersecurity and Infrastructure Security Agency – CISA)
- Cyber Security is the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber-attacks. It aims to reduce the risk of cyber attacks and protect against the unauthorized exploitation of systems, networks and technologies.



# THE UNITED STATES SECRET SERVICE

of show that, hey, I can  
get into these networks.



WORTHY OF TRUST AND CONFIDENCE

# Malware

- Malware, or “**MAL**icious soft**WARE**”, is a catch-all term used to describe software that attempts to harm computers in different ways. Depending on what the malware does, different terms are used in relation to it. For example:

- Ransomware
- Bots & Botnets
- Viruses
- Worms
- Trojans
- Adware
- Spyware
- Scareware
- Rootkits
- Exploits
- Cryptominers
- Keyloggers



# Ransomware

- Ransomware is a type of malware that **prevents or limits users from accessing** their system by encrypting the users' files until a ransom is paid.
- **How does it get on your computers?**
  - Remote Desktop Protocol (RDP)
  - Phishing Emails
  - Software Vulnerabilities
  - Malware, Viruses, USBs, etc.
    - Clicking on something you shouldn't, or plugging something into your computer you shouldn't.
  - Social Engineering





# Ransomware

- No guarantee that you will be able to recover your files even after the ransom is paid.
- Law Enforcement does not support paying a ransom in response to a ransomware attack. It encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity.
  - Possible funding for additional illegal activities, terrorism, etc.



# Ransomware Statistics

- The total ransomware costs are projected to exceed \$20 billion in 2021. ([Cybercrime Magazine](#), 2019)
- In 2021, the largest ransomware payout was made by an insurance company at \$40 million, setting a world record. ([Business Insider](#), 2021)
- The average ransom fee requested has increased from \$5,000 in 2018 to around \$200,000 in 2020. ([National Security Institute](#), 2021)
- The average downtime a company experiences after a ransomware attack is 21 days. ([Coveware](#), 2021)
- From a survey conducted with 1,263 companies, 80% of victims who submitted a ransom payment experienced another attack soon after, and 46% got access to their data but most of it was corrupted. ([Cybereason](#), 2021)
- Additionally, 60% of survey respondents experienced revenue loss and 53% stated their brands were damaged as a result. ([Cybereason](#), 2021)



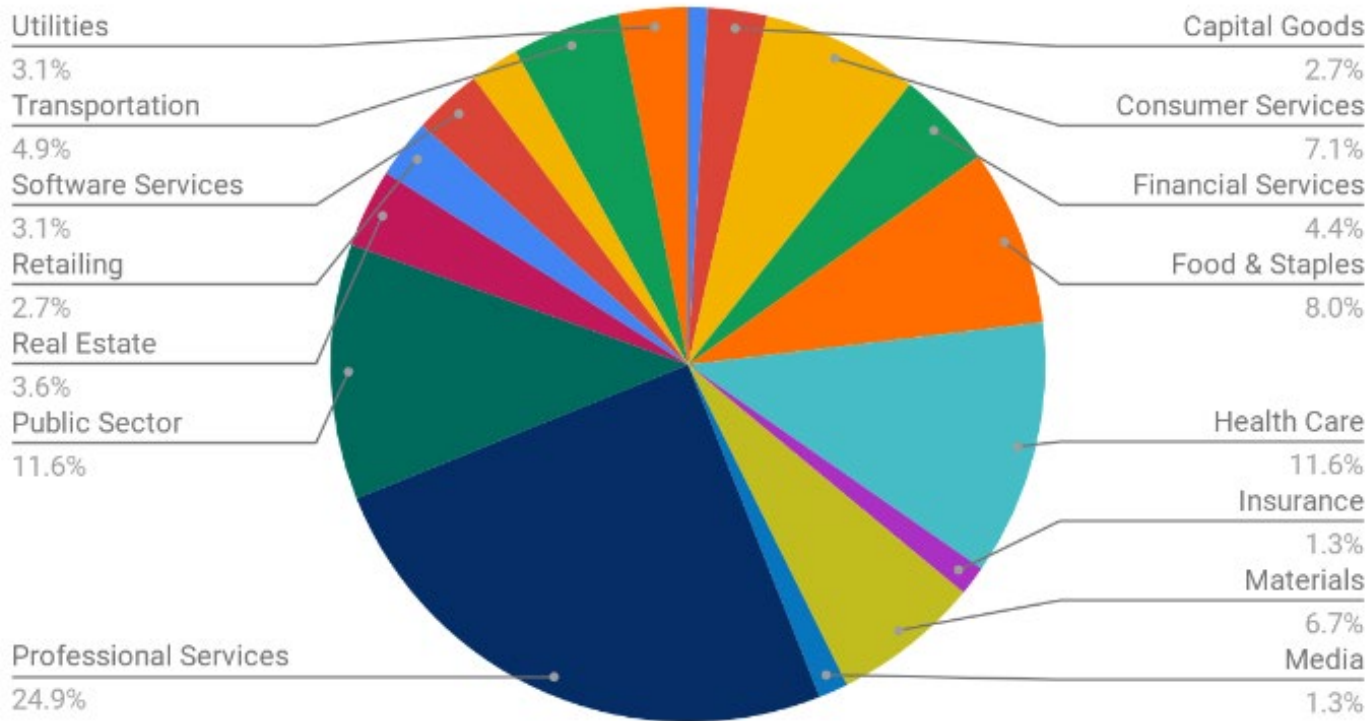


# Ransomware Statistics

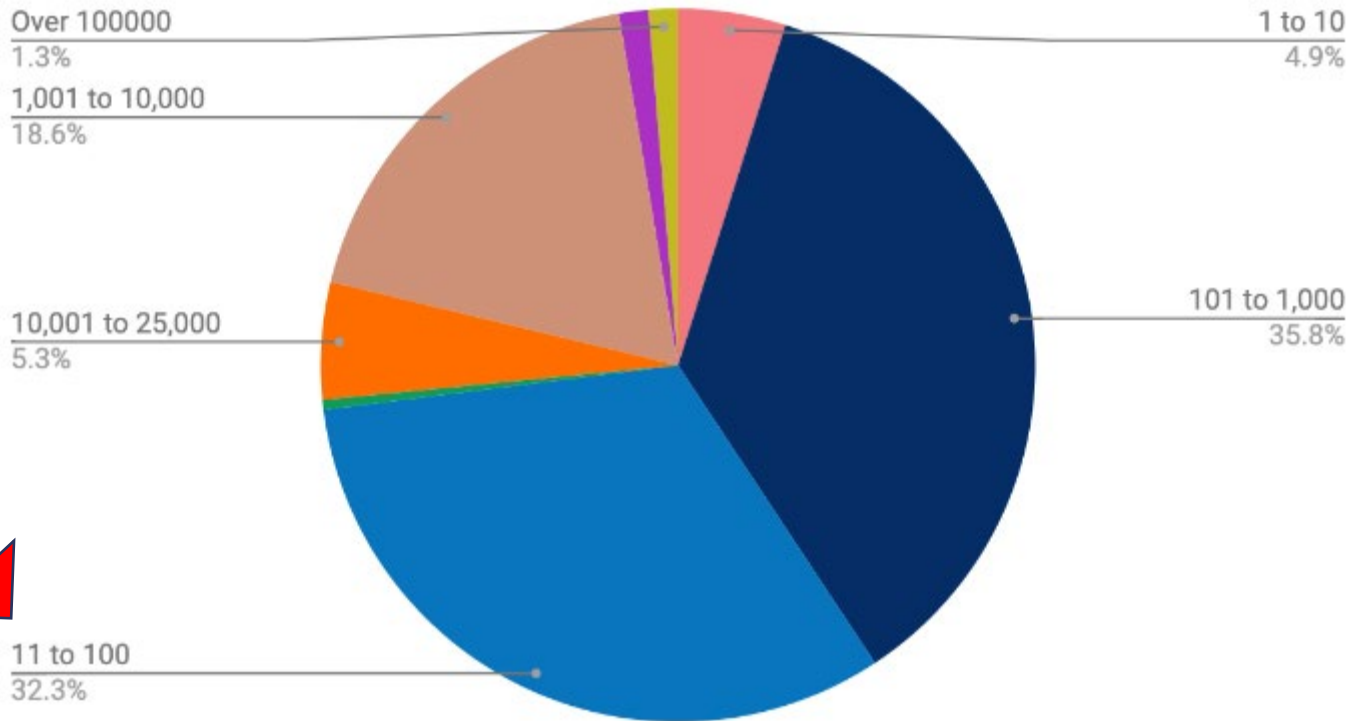
- Malicious emails are up 600% due to COVID-19. ([ABC News](#), 2021)
- Remote workers will be the main target of cybercriminals throughout 2021. ([Security Magazine](#), 2020)
- 84% of organizations will keep remote work as the norm even after COVID-19 restrictions are lifted, resulting in an increase of internet users and a greater risk of data exposure. ([Bitglass](#), 2020)
- Future hackers will target stay-at-home workers since personal devices are easier to hack than office hardware. ([Security Magazine](#), 2020)



## Common Industries Targeted by Ransomware Q1 2021



## Distribution by Company Size (Employee Count)



# Small Businesses are a Target of Ransomware!

- Ransomware attacks still disproportionately affect small businesses. These small companies rarely end up in the headlines and often don't have the financial or technical expertise to properly handle the incident OR perform the proper remediation required to prevent a repeat attack.
- Most notable change in Q1 2001 was the Professional Services industry as the #1 target, specifically small and medium law firms.

<https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound>



# Some of the Many Ransomware Variants..

- Sodinokibi
- Conti
- Lockbit
- Clop
- Egreggor
- Avaddon
- Ryuk
- Darkside
- Suncrypt
- Netwalker
- Phobos
- Mespinoza
- Hello Kitty
- THT v2
- LV
- Zeppelin
- Bad Rabbit
- Cryptolocker
- GoldenEye
- Jigsaw
- Locky
- Maze
- NotPetya
- Petya
- Wannacry



# Ransomware Ransom Letter Examples



**Wana Decrypt0r 2.0**

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.

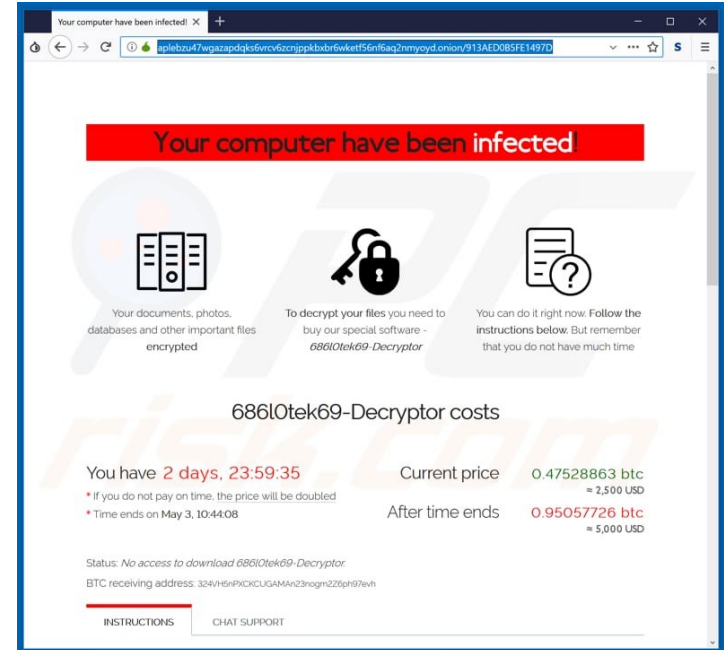
**How Do I Pay?**  
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.  
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.  
And send the correct amount to the address specified in this window.  
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

**Payment will be raised on**  
5/15/2017 16:32:52  
Time Left  
02:23:59:49


**Your files will be lost on**  
5/19/2017 16:32:52  
Time Left  
06:23:59:49


[About bitcoin](#)  
[How to buy bitcoins?](#)  
[Contact Us](#)


 **Send \$300 worth of bitcoin to this address:**  
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw



Your computer have been infected!

 Your documents, photos, databases and other important files encrypted

 To decrypt your files you need to buy our special software - 686l0tek69- Decryptor

 You can do it right now. Follow the instructions below. But remember that you do not have much time

**686l0tek69-Decryptor costs**

You have **2 days, 23:59:35** Current price **0.47528863 btc**  
\* If you do not pay on time, the price will be doubled ≈ 2,500 USD  
\* Time ends on May 3, 10:44:08 After time ends **0.95057726 btc**  
≈ 5,000 USD

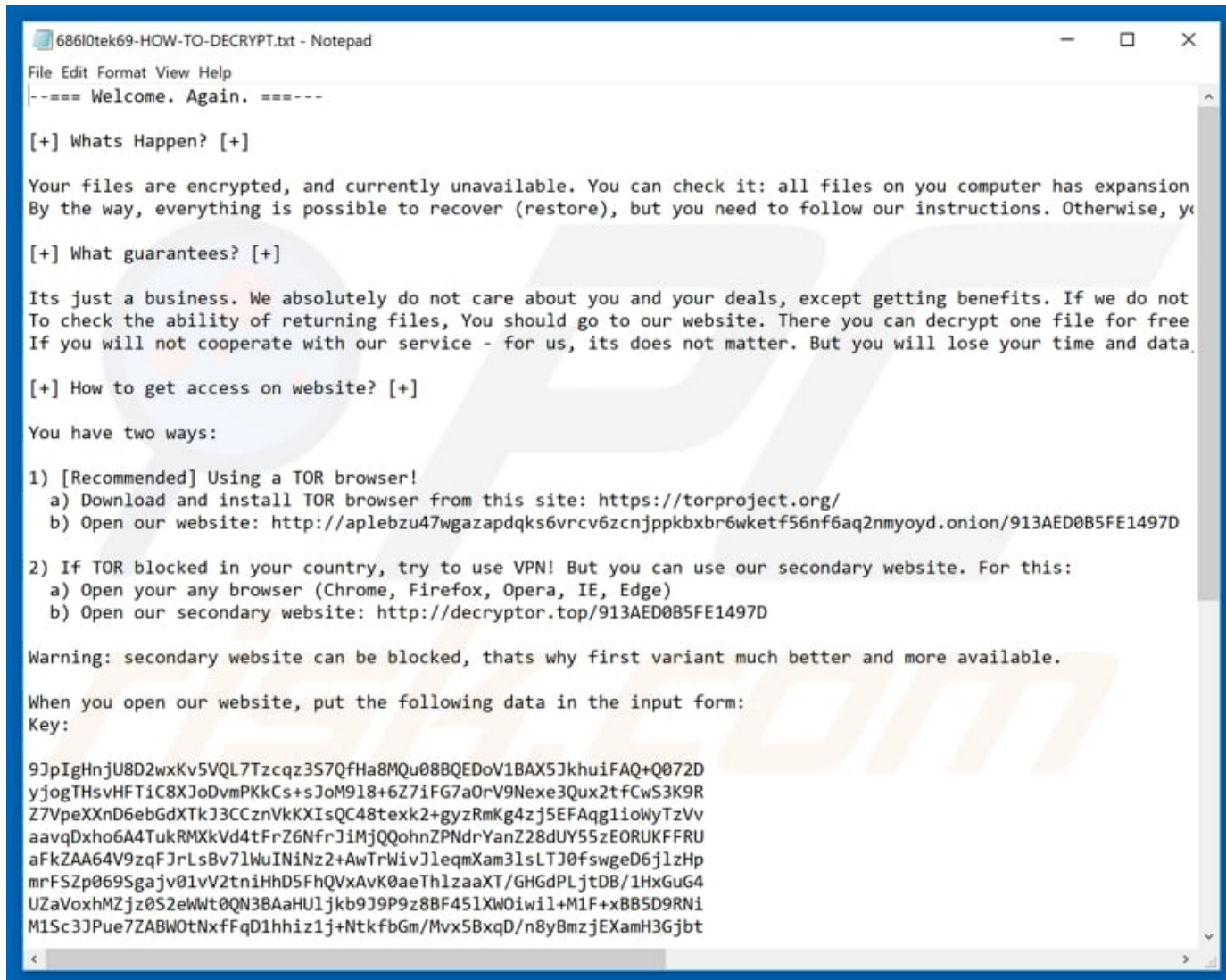
Status: No access to download 686l0tek69- Decryptor.  
BTC receiving address: 324vHsrPICKUCUGAMAn23nognZ26ph97evh

[INSTRUCTIONS](#) [CHAT SUPPORT](#)





# Ransomware Ransom Letter Examples



The image shows a screenshot of a Notepad window titled "686I0tek69-HOW-TO-DECRYPT.txt - Notepad". The text inside is a ransom letter. It starts with a welcome message, followed by a section titled "[+] Whats Happen? [+]" which explains that files are encrypted and provides instructions on how to recover them. Another section titled "[+] What guarantees? [+]" states that the ransomware is just a business and offers a free decryption of one file as a guarantee. A third section titled "[+] How to get access on website? [+]" provides two methods to access the decryption website: using a TOR browser or a VPN. It includes specific URLs for both. A warning is given that the secondary website can be blocked. Finally, it provides a long alphanumeric key to be entered in the input form on the website.

```
File Edit Format View Help
|----- Welcome. Again. -----

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on you computer has expansion
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, y

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not
To check the ability of returning files, You should go to our website. There you can decrypt one file for free
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data.

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
a) Download and install TOR browser from this site: https://torproject.org/
b) Open our website: http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbxbr6wketf56nf6aq2nmyoyd.onion/913AED0B5FE1497D

2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
b) Open our secondary website: http://decryptor.top/913AED0B5FE1497D

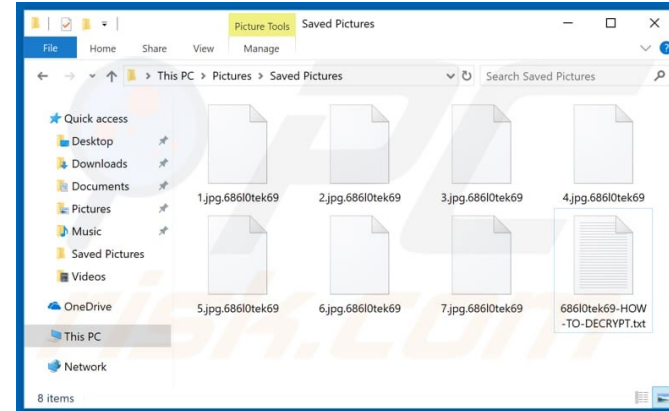
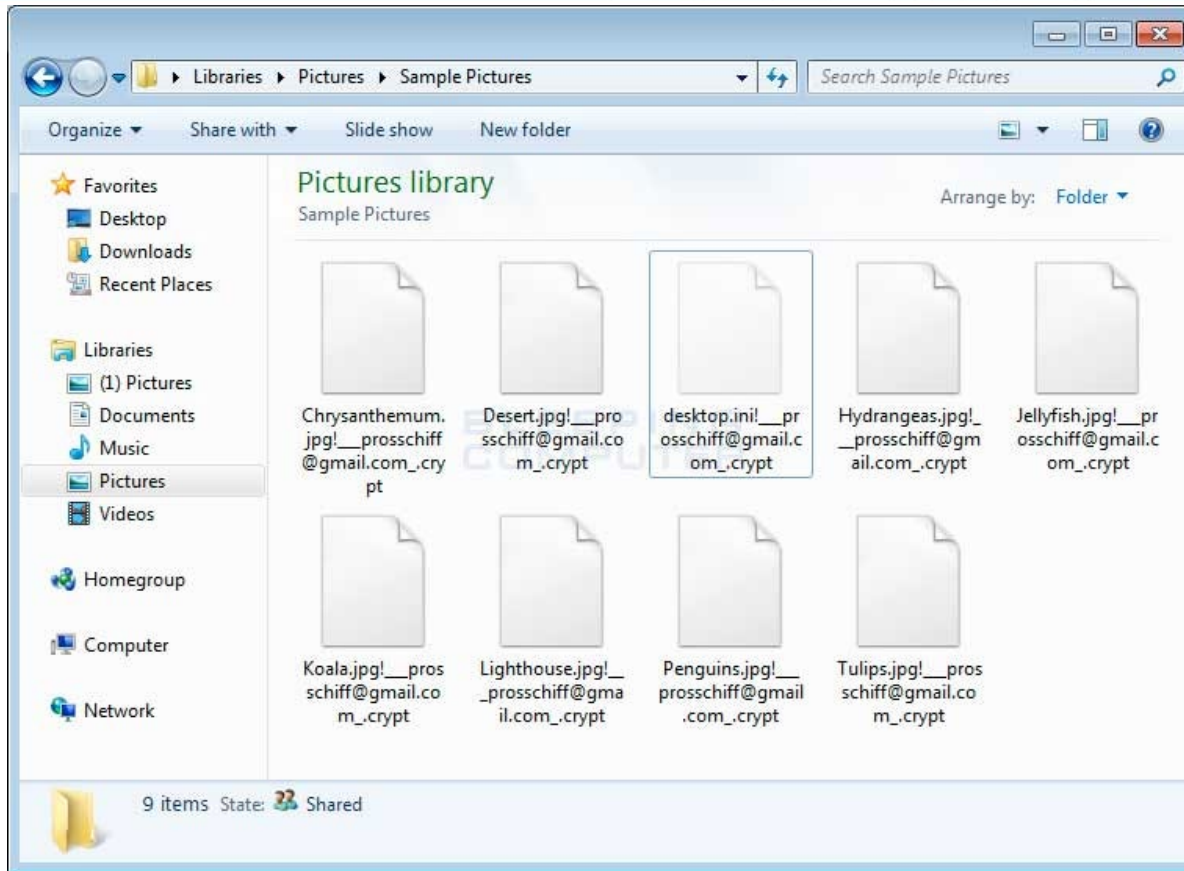
Warning: secondary website can be blocked, thats why first variant much better and more available.

When you open our website, put the following data in the input form:
Key:

9JpIgHnjU8D2wxKv5VQL7Tzcqz3S7QfHa8MQu08BQEDoV1BAX5JkhuiFAQ+Q072D
yjogTHsvHFTiC8XJoDvmPKkCs+sJoM9l8+6Z7iFG7aOrV9Nexe3QuX2tfCwS3K9R
Z7VpeXXnD6ebGdXTkJ3CCznVkkXIsQC48texk2+gyzRmKg4zj5EFAqg1ioWyTzVv
aavqDxho6A4TukRMXkVd4tFrZ6NfrJ1MjQQohnZPNdrYanZ28dUY55zEORUKFFRU
aFkZAA64V9zqFJrLsBv7lWuINiNz2+AwTrWivJleqmXam3lsLTJ0fswgeD6jLzHp
mrFSZp069SgaJv0lvV2tniHhD5FhQVxAvK0aeThlzaaXT/GHGdPLjtDB/1HxGuG4
UZAvoXhMzjz0S2eWt0QN38AaHULjkb9J9P9z8BF451XWOiwi1+M1F+xBB5D9RNI
M1Sc3JPue7ZABW0TnxFFQd1hhiz1j+NtkfbGm/Mvx5BxqD/n8y8mzjEXamH3Gjbt
```



# Files Encrypted by Ransomware...



# Ransomware

## Prevention

- **Back up your computer.** Perform frequent backups of your system and other important files, and verify your backups regularly. If your computer becomes infected with ransomware, you can restore your system to its previous state using your backups.
- **Store your backups separately.** Best practice is to store your backups on a separate device that cannot be accessed from a network, such as on an external hard drive. Once the backup is completed, make sure to disconnect the external hard drive, or separate device from the network or computer. AirGap
- **Train your organization.** Organizations should ensure that they provide cybersecurity awareness training to their personnel. Ideally, organizations will have regular, mandatory cybersecurity awareness training sessions to ensure their personnel are informed about current cybersecurity threats and threat actor techniques.

*<https://us-cert.cisa.gov/>*



# Ransomware

## Prevention

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks.
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g. search the internet for the sender organization's website or the topic mentioned in the email). Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net).
- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files (or word/excel documents that ask you to Enable Macros).
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

<https://us-cert.cisa.gov/>



# Ransomware

## Prevention

- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques.
  - Anti-Phishing Working Group
    - <https://apwg.org>
  - Cybersecurity & Infrastructure Security Agency (CISA)
    - <https://us-cert.cisa.gov/ncas/alerts>
- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.

<https://us-cert.cisa.gov/>



# Ransomware

## Incident response

- **Communicate**

- Employees
- Report to Law Enforcement immediately (USSS, FBI, DHS-CISA, Local LEO)

- **Isolate**

- Disconnect PCs from network – stop using them.
- Do not turn off computer if possible (more evidence)– but when in doubt, shut it all down.

- **Document**

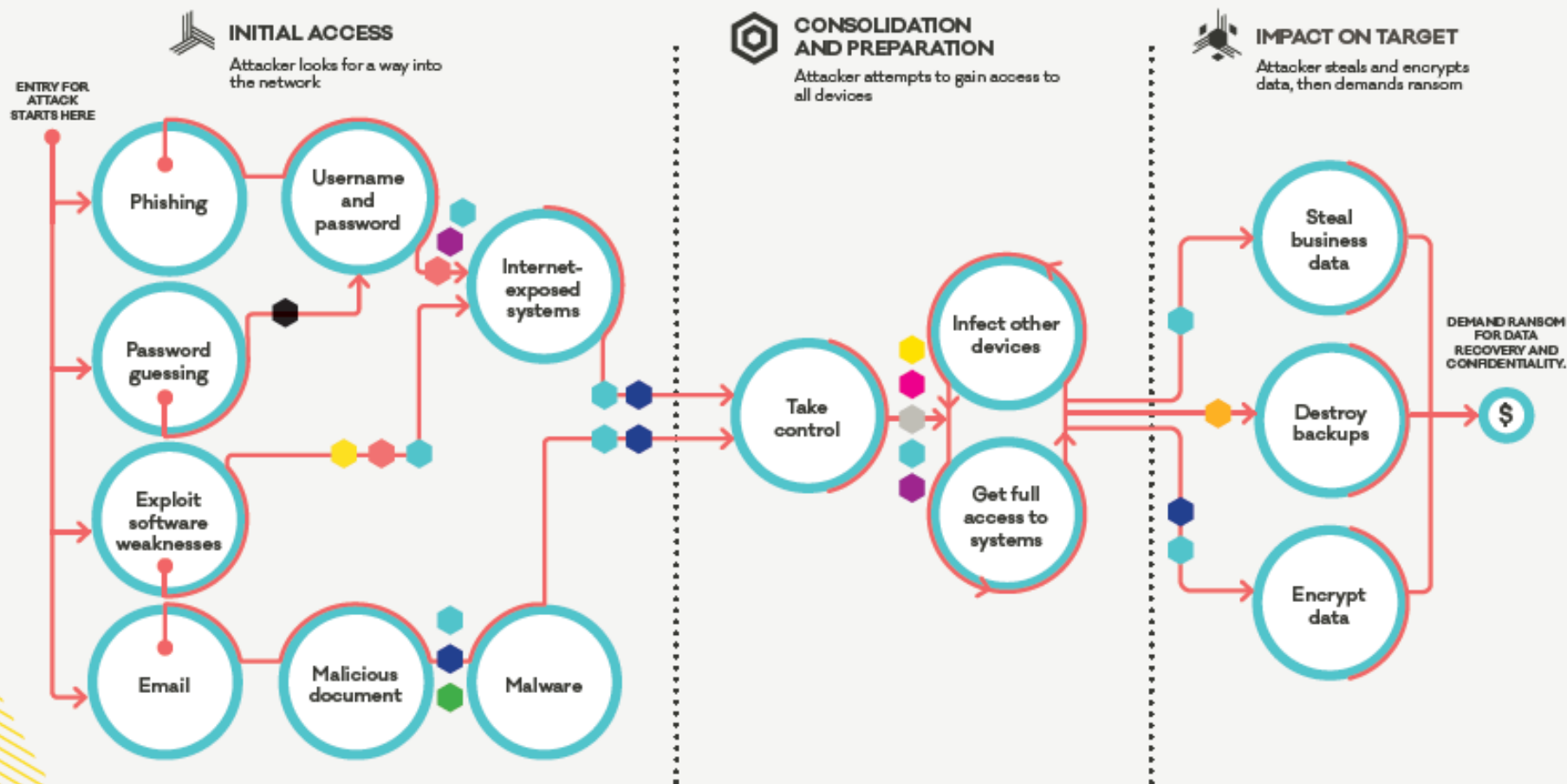
- Pictures & Notes (dates, times, actions)
- Names and positions of people using computer systems
- People allowed to have access to various systems
- Company IT contacts - layout of network, computer systems, logs, etc.





# HOW RANSOMWARE WORKS

How you can protect your business against a ransomware attack.



Talk to your IT provider about the relevant CERT NZ Critical Controls for your business.

## CRITICAL CONTROLS KEY



New Zealand Government



# Phishing

The fraudulent practice of sending emails purporting to be from reputable individuals or companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers and/or to click on something malicious.

- Phishing Email
- Spear Phishing
- Link Manipulation
- Fake Websites
- CEO Fraud
- Content Injection
- Session Hijacking
- Malware
- Mobile SMS Phishing (Smishing)
- Voice Phishing (Vishing)
- Man-In-The-Middle
- Malvertising



# Phishing



Dear Customer,

The following information for your Apple ID was updated on March 11, 2019.

**This message is to inform you that your Apple ID has been locked for security reasons.**

Someone has tried to sign in to your Apple account from a different IP address. Please verify your identity today or your account will be disabled due to concerns we have for the security and integrity of the Apple Community.

For your security, a trusted identity is removed from your account. You can verify your identity again one in the Security section of your [Apple ID account page](#).

Sincerely,

Apple Support

[Apple ID](#) | [Support](#) | [Privacy Policy](#)

Copyright © 2019 Apple Distribution International, Hollyhill Industrial Estate, Hollyhill, Cork, Ireland.  
All Rights Reserved.

## ITunes Order Details 4 February 2019

Confirmation Order "Harry Potter : Hogwarts Mystery" Confirmed, on App-Store Monday, February 4, 2019  
To: undisclosed-recipients;; Bcc: [REDACTED]

Dear Customer,



Confirmation about your order of item "Harry Potter : Hogwarts Mystery" accepted

Order successfully placed, for more information we send attached on this email

Open and read the attached

ThankYou For Always Trusting Us.

### App Store

Invoice Confirmation		BILLED WITH:		TOTAL
DATE Sunday, February 4, 2019		CREDIT CARD		\$ 29.98
ORDER ID: 19C11201802262	DOCUMENT ID: 101884807174679			
App Store	Type	Purchased From	Price	
	Harry Potter : Hogwarts Mystery <a href="#">Report Problem</a>	In-App Purchases	iPhone : 6 Plus	\$ 19.99
	Harry Potter : Cursed Child <a href="#">Report Problem</a>	In-App Purchases	iPhone : 6 Plus	\$ 9.99
TOTAL				\$ 29.98

Having problem with this transaction ?

If you haven't authorized this transaction click the link below to cancel your order and get full refund

[Report a problem, manage payment or cancel your orders](#)

Copyright © 2019 Apple Pay Ltd. One Apple Park Way, Cupertino, CA 95014, United States All rights reserved.



# Phishing

Attn:Your Credit-Scores\_Just Changed on: 8/15/2018. View/Confirm Changes. Msg#:153443

 **Score Alert** <tammy@pacconsultingfirm.net>  
To: [redacted]

Experian Transunion Equifax

Hello  
Membership ID #9211351

## A Key Change Has Been Posted to

You're receiving this alert to inform you that a key change that has been posted to your national credit reports. Several scoring updates likely had an impact on your score.

>> Confirm or dispute the recent change

>> Review Accuracy

>> [Click Here Now to See How Your Score](#)

[Access Your Account](#)

Compose    
< Back 1

Verification Required-ID: 53339

 **PNC Alerts** <tefwire@cox.net>  
To: undisclosed-recipients;



Dear Member ,  
Your account security is our priority,so our smart security system established a new secure system.  
For your protection, you must verify this activity before you can continue using your account.  
[Click here to complete verification process](#)  
Your account will work as normal after the verification processed  
Sincerely,  
Online Customer Service

Compose    
< Back 2

Action Required ID:619

 **Chase Alerts** <chshaver1@cox.net>  
To: undisclosed-recipients;



Dear Member ,  
This to notify you that we detected irregular activity on your online Bank.  
For your protection, you must verify this activity before you can continue using your account.  
[Click here to complete verification process](#)  
Your account will work as normal after the verification processed  
Sincerely,  
Online Customer Service

## Verification Required

 **Capital One** <capitalone@notification.capitalone.com>  
To: [redacted]  
 Follow up.



Dear Customer,

Please be informed that your account has been restricted, as a result of multiple logon attempt on your capital one, Please complete an account verification process.

To start the Verification process click on [Click Here](#)<sup>SM</sup>

Note: To protect your account, we've shredded and securely disposed of any returned documents with your information that was send back to us.

Thank You

Capital One Services Team



WORTHY OF TRUST AND CONFIDENCE

# Phishing for Email Credentials

## Example 4

**From:** Microsoft office365 Team [<mailto:cyh11241@lausd.net>]  
**Sent:** Monday, September 25, 2017 1:39 PM  
**To:**  
**Subject:** Your Mailbox Will Shutdown Verify Your Account



Detected spam messages from your <EMAIL APPEARED HERE> account will be blocked.

If you do not verify your mailbox, we will be force to block your account. If you want to continue using your email account please [verify](#).

[Verify Now](#)

Microsoft Security Assistant  
Microsoft office365 Team! ©2017 All Rights Reserved



To You

Wednesday, April 24, 1:09 PM

Attention: A user account was created or modified. Retrieve your user's temporary password. | [View this email in your browser.](#)



## Your account password has expired.

The following contains password security guidelines.

Please note:

- A strong password consists of at least three of the following: uppercase letters, lowercase letters, numbers, symbols.
- For your protection and security, passwords are valid for 120 days.
- When distributing IDs and passwords, be sure to do so in a safe and secure manner.

To avoid service interruption, please change your password now.

Go to the sign-in page, <https://portal.office.com> and sign in with your User ID:

User Name: [\[redacted\]](#) A red arrow points to the redacted user name.

Once you have successfully signed in, you can create a new password by following the instructions on the si

We appreciate your prompt attention to this matter, and look forward to continuing to meet your business nee

Thank you for choosing to host your IT solutions with Microsoft.

Sincerely,  
The Microsoft Online Services Team

This is an important account related service notification. To set your contact preferences for other communications, [Promotional Communications Manager](#).

This message was sent from an unmonitored e-mail address. Please do not reply to this message.  
[Contact Us](#) | [Privacy](#) | [Legal](#)

Microsoft Office



WORTHY OF TRUST AND CONFIDENCE

# BEC – Business Email Compromise

## DEFINITION OF BUSINESS E-MAIL COMPROMISE

- Business e-mail compromise (BEC) is when a scammer impersonates a company employee or other trusted party, and tries to trick an employee into sending money, usually by sending the victim email from fake or compromised email accounts (a “spear phishing” attack).
- BEC is also known as a “man-in-the-email” attack. This is derived from the “man-in-the-middle” attack where two parties think that they are talking to each other directly, but in reality, an attacker is listening in and possibly altering the communication.
- BECs don’t use malware or malicious links that can be analyzed with standard cyber defenses. Instead, BEC attacks rely instead on impersonation and other social engineering techniques to trick people interacting on the attacker’s behalf.

<https://digitalguardian.com/>





# Business Email Compromise

## HOW BUSINESS E-MAIL COMPROMISE WORKS

- A BEC scam starts with research. An attacker will sift through publicly available information about your company from your website, press releases, and even social media posts. He/she might look for the names and official titles of company executives, your corporate hierarchy, and even travel plans from email auto-replies.
- The attacker will then try to gain access to an executive's e-mail account. To remain undetected, he/she might use inbox rules or change the reply-to address so that when the scam is executed, the executive will not be alerted.
- Attacker can also gain access to a company email account through phishing.
- The attacker can monitor emails in the company and wait until an opportune time to inject themselves and their scam into the conversation.

*<https://digitalguardian.com/>*



# IC3 2020 Data (ic3.gov)

## By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	\$1,866,642,107	Overpayment	\$51,039,922
Confidence Fraud/Romance	\$600,249,821	Ransomware	**\$29,157,405
Investment	\$336,469,000	Health Care Related	\$29,042,515
Non-Payment/Non-Delivery	\$265,011,249	Civil Matter	\$24,915,958
Identity Theft	\$219,484,699	Misrepresentation	\$19,707,242
Spoofing	\$216,513,728	Malware/Scareware/Virus	\$6,904,054
Real Estate/Rental	\$213,196,082	Harassment/Threats Violence	\$6,547,449
Personal Data Breach	\$194,473,055	IPR/Copyright/Counterfeit	\$5,910,617
Tech Support	\$146,477,709	Charity	\$4,428,766
Credit Card Fraud	\$129,820,792	Gambling	\$3,961,508
Corporate Data Breach	\$128,916,648	Re-shipping	\$3,095,265
Government Impersonation	\$109,938,030	Crimes Against Children	\$660,044
Other	\$101,523,082	Denial of Service/TDos	\$512,127
Advanced Fee	\$83,215,405	Hacktivist	\$50
Extortion	\$70,935,939	Terrorism	\$0
Employment	\$62,314,015		
Lottery/Sweepstakes/Inheritance	\$61,111,319		
Phishing/Vishing/Smishing/Pharming	\$54,241,075		



# Business Email Compromise

## EXAMPLES OF BUSINESS E-MAIL COMPROMISE

- **Fraudulent Invoice Scam** is when a cybercriminal uses an employee's e-mail to send notifications to customers and suppliers asking for payment to the cybercriminal's account.
- **Fake Boss Scam** is when a fraudulent email is sent from a business executive's account to employees instructing them to urgently transfer money from the corporate account to the criminal's account.
- **Fake Attorney Scam** is when a lawyer's e-mail address is used to contact clients, asking that they pay money immediately to keep things confidential.
- **Data Theft Scams** typically target HR employees in an attempt to obtain personal or sensitive information about individuals within the company such as CEOs and executives. This data can then be leveraged for future attacks such as CEO Fraud.



# Business Email Compromise

## WARNINGS SIGNS

- You receive an email from a higher-up ordering you to quickly process an invoice, change the recipient of a payment or provide sensitive documents.
- The message is brief, urgent and presses you to bypass normal policies and procedures.
- The email uses strange phrases and/or poor English – may stand out from prior emails from the whom you thought was the same person.
- The email comes from a Gmail, Hotmail or other personal account rather than an organizational account.
- Someone you've become close to online asks you to open a bank account for the purpose of receiving or sending them money.



# Business Email Compromise

- Another trick is to create an e-mail with a spoofed domain. For example, instead of [john.smith@company.com](mailto:john.smith@company.com), the attacker might use:

john.smith@c0mpany.com

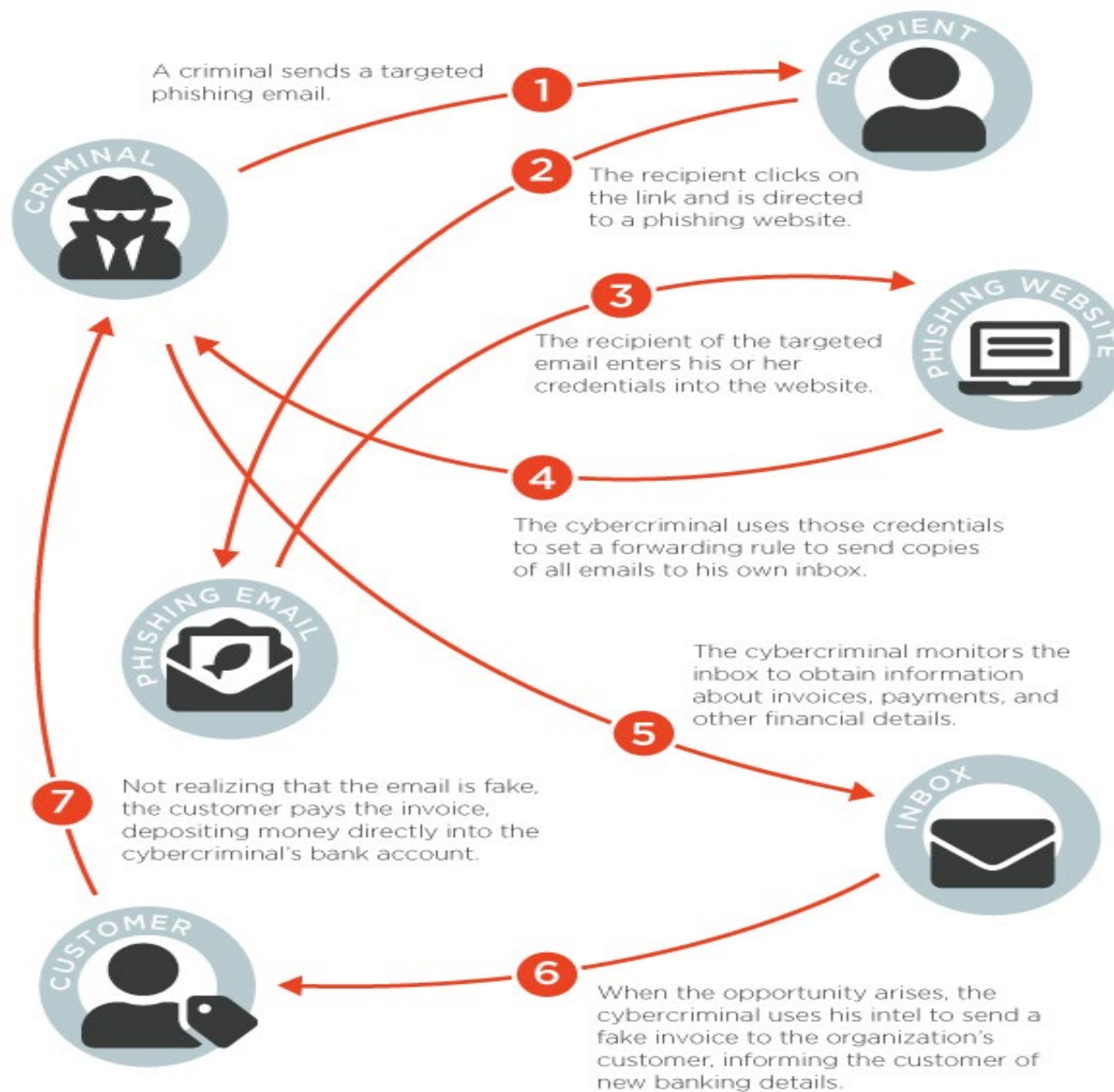
john.smith@cornpany.com

john.smith@gmail.com

john.smith@company.com

- If you do not pay close attention, it is easy to get fooled by these slight differences!





<https://www.agari.com/email-security-blog/silent-stalling-vendor-email-compromise/>





# Business Email Compromise

## DON'TS

- **Don't** act on a request to send money or sensitive employee information without confirming that it's authentic.
- **Don't** reply to a suspicious email. Speak directly to the person the sender claims to be, or forward it to a known email address for that person.
- **Don't** call a phone number listed in the suspicious email. Contact the actual person on a number you know to be legitimate.
- **Don't** click on links or open attachments in a suspicious business email. It could unleash malware.
- **Don't** open a new bank account at the behest of someone you've forged a relationship with online or as part of a supposed work-at-home opportunity.

*<https://www.aarp.org/money/scams-fraud/info-2019/business-email-compromise.html>*



# Business Email Compromise

## DO'S

- **Do** check with an executive by phone or in person to verify a request to send money or provide personnel records.
- **Do** verbally confirm emailed instructions from a vendor or supplier to change payment methods or bank information. Call them on a known contact number.
- **Do** carefully check the sender's email address. Scammers may slightly vary a genuine address, adding a letter or changing punctuation, to make it seem legit on first glance.
- **Do** train staff on the BEC threat and how to spot spoofed and spear-phishing emails.
- **Do** verify a request from someone involved in a property transaction to change a payment type (for example, from check to wire transfer) or bank data. Do so in person or by phone, not by email.

*<https://www.aarp.org/money/scams-fraud/info-2019/business-email-compromise.html>*



# Business Email Compromise

## DO'S (continued)

- **Do immediately** contact your financial institution if you discover a fraudulent transfer. It may be able to recall the funds.
- **Do** save all emails and other evidence of a BEC attack to provide to authorities.
- **Do** immediately change passwords on compromised accounts.
- **Do** alert other businesses/clients that may be included in scam.
- **Do** contact law enforcement **immediately**. The ability to stop transactions/recall funds is time sensitive!

*<https://www.aarp.org/money/scams-fraud/info-2019/business-email-compromise.html>*



# Business Email Compromise

## BEST PRACTICES FOR PROTECTING AGAINST BUSINESS EMAIL COMPROMISE

- Business e-mail compromise attacks are successful for three main reasons:
  - Insufficient security protocols
  - Social engineering
  - Lack of employee awareness
- **Multi-factor authentication** should be implemented as an IT security policy. This will help prevent unauthorized access of e-mails, especially if an attacker attempts to login from a new location.



# **New England Cyber Fraud Task Force -** **NECFTF**

The NECFTF's mission is to prevent, detect, and mitigate complex cyber-enabled financial crimes against payment systems and critical infrastructure as well as develop Digital Forensic capabilities at the local level. The regional based task force allows us to share expertise and resources related to digital forensic training and cyber investigations received at our National Computer Forensic Institute - NCFI, [www.ncfi.usss.gov](http://www.ncfi.usss.gov), in Hoover, AL.



# RESOURCES

## **Secret Service Cyber slick sheet**

<https://www.secretservice.gov/investigation/Preparing-for-a-Cyber-Incident>

## **DHS-CISA, CSA Rick Rossi NH, Ron Ford MA**

**Alerts** <https://us-cert.cisa.gov/ncas/alerts>

**Home Page** <https://us-cert.cisa.gov/>

**Stop Ransomware** <https://www.cisa.gov/stopransomware>

**Third Party IR Firms**

**Security blogs (Twitter, Youtube)**

**DOJ Press Release**

**Google alerts for incidents**



**QUESTIONS?**  
**Tim Benitez**  
**(603) 626-7026 - office**  
**(202) 355-3037 - cell**  
**timothy.benitez@usss.dhs.gov**  
**http://linkedin.com/in/tim-benitez-603**

