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

- Malware, or “MALicious softWARE”, 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](https://www.cybercrimenews.com), 2019)

- In 2021, the largest ransomware payout was made by an insurance company at $40 million, setting a world record. ([Business Insider](https://www.businessinsider.com), 2021)

- The average ransom fee requested has increased from $5,000 in 2018 to around $200,000 in 2020. ([National Security Institute](https://www.nsii.org), 2021)

- The average downtime a company experiences after a ransomware attack is 21 days. ([Coveware](https://www.coveware.com), 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](https://www.cybereason.com), 2021)

- Additionally, 60% of survey respondents experienced revenue loss and 53% stated their brands were damaged as a result. ([Cybereason](https://www.cybereason.com), 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

- Utilities: 11.6%
- Transportation: 3.1%
- Software Services: 4.9%
- Retailing: 3.1%
- Real Estate: 2.7%
- Public Sector: 3.6%
- Professional Services: 24.9%
- Health Care: 11.6%
- Insurance: 1.3%
- Materials: 6.7%
- Media: 1.3%
- Capital Goods: 2.7%
- Consumer Services: 7.1%
- Financial Services: 4.4%
- Food & Staples: 8.0%
Distribution by Company Size (Employee Count)

- Over 100,000: 1.3%
- 1,001 to 10,000: 18.6%
- 10,001 to 25,000: 5.3%
- 11 to 100: 32.3%
- 101 to 1,000: 35.8%
- 1 to 10: 4.9%
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

--- Welcome. Again. ---

[+] What happens? [+]  
Your files are encrypted, and currently unavailable. You can check it: all files on your computer have expansion. By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you...

[+] What guarantees? [+]  
It’s just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not comply with your demands, we will not cooperate with our service. For this, it 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://applebzu47wzgazapdqs6vrcv6zcnpkxbxbrgwkeff56nf6aq2nmyod.onion/913AED0B5FE1497D

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

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

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

Key:  
9JpoIgHnJU8D2wxKv5VQL7Zcqz357QFHabQNu08BQEDoV1BAX5jkhuIFAQmQ872D  
yjogTHsvHFTiC8X0DvmPKCs+sJoM918+6Z71FGa7aOrV9Nex30x2tfcWw3K9R  
Z7VpcXxnD6ebGdXTk3C3C3nVXX1sQC48textk2gyzRmkg4Fj5EFAng11oWyt2yv  
avqXh06A4TukRXXkVd4tFrZ6nfrJ1MjQyqohnZPNdY28duY55SROUKFRU  
aFkZAA649v2qFJrLsBv7LwUINnz2+4wTrWivJlqemXam3tlsLT69swggeD6j1zHp  
mrsF5po69Sgaj0v1V2tnjth50fHQvAk0aThlzaaTH/GHgdPljtDB/1hx6u4  
uazXvkhMzj0S2ewWbQ0N3BAAhUijk9J999P88BFA51Xw0i1+4M1fxB5D9RN1  
M15s3Jpue72ABWoTnxFfqD1hhiz1j+NtkebGm/Mvxs5BxqD/n8yBmzjEXamh36jbt
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/
• **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](https://apwg.org)
  • Cybersecurity & Infrastructure Security Agency (CISA)
    • [https://us-cert.cisa.gov/ncas/alerts](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/](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.

INITIAL ACCESS
Attacker looks for a way into the network

- Phishing
- Password guessing
- Exploit software weaknesses
- Email
- Malicious document
- Malware
- Username and password
- Internet-exposed systems

CONSOLIDATION AND PREPARATION
Attacker attempts to gain access to all devices

- Take control
- Infect other devices
- Get full access to systems

IMPACT ON TARGET
Attacker steals and encrypts data, then demands ransom

- Steal business data
- Destroy backups
- Encrypt data
- Demand ransom for data recovery and confidentiality.

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

CRITICAL CONTROLS KEY
- Internet-exposed services
- Patching
- Multi-factor authentication
- Network segmentation
- Principle of least privilege
- Backups
- Application hardening
- Logging and alerting
- Enable access
- Password manager

New Zealand Government

WORTHY OF TRUST AND CONFIDENCE
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
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
Phishing

Attn: Your Credit Scores Just Changed on: 8/15/2018. View/Confirm Changes. Msg#: 153441

Dear Customer,

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

To start the Verification process click on [Click Here](#).

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
Phishing for Email Credentials

Example 4

From: Microsoft 365 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 forced to block your account. If you want to continue using your email account please verify.

Verify Now

Microsoft Security Assistant
Microsoft 365 Team! ©2017 All Rights Reserved
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

<table>
<thead>
<tr>
<th>Crime Type</th>
<th>Loss</th>
<th>Crime Type</th>
<th>Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>BEC/EAC</td>
<td>$1,866,642,107</td>
<td>Overpayment</td>
<td>$51,039,922</td>
</tr>
<tr>
<td>Confidence Fraud/Romance</td>
<td>$600,249,821</td>
<td>Ransomware</td>
<td>**$29,157,405</td>
</tr>
<tr>
<td>Investment</td>
<td>$336,469,000</td>
<td>Health Care Related</td>
<td>$29,042,515</td>
</tr>
<tr>
<td>Non-Payment/Non-Delivery</td>
<td>$265,011,249</td>
<td>Civil Matter</td>
<td>$24,915,958</td>
</tr>
<tr>
<td>Identity Theft</td>
<td>$219,484,699</td>
<td>Misrepresentation</td>
<td>$19,707,242</td>
</tr>
<tr>
<td>Spoofing</td>
<td>$216,513,728</td>
<td>Malware/Scareware/Virus</td>
<td>$6,904,054</td>
</tr>
<tr>
<td>Real Estate/Rental</td>
<td>$213,196,082</td>
<td>Harassment/Threats Violence</td>
<td>$6,547,449</td>
</tr>
<tr>
<td>Personal Data Breach</td>
<td>$194,473,055</td>
<td>IPR/Copyright/Counterfeit</td>
<td>$5,910,617</td>
</tr>
<tr>
<td>Tech Support</td>
<td>$146,477,709</td>
<td>Charity</td>
<td>$4,428,766</td>
</tr>
<tr>
<td>Credit Card Fraud</td>
<td>$129,820,792</td>
<td>Gambling</td>
<td>$3,961,508</td>
</tr>
<tr>
<td>Corporate Data Breach</td>
<td>$128,916,648</td>
<td>Re-shipping</td>
<td>$3,095,265</td>
</tr>
<tr>
<td>Government Impersonation</td>
<td>$109,938,030</td>
<td>Crimes Against Children</td>
<td>$660,044</td>
</tr>
<tr>
<td>Other</td>
<td>$101,523,082</td>
<td>Denial of Service/TDos</td>
<td>$512,127</td>
</tr>
<tr>
<td>Advanced Fee</td>
<td>$83,215,405</td>
<td>Hacktivist</td>
<td>$50</td>
</tr>
<tr>
<td>Extortion</td>
<td>$70,935,939</td>
<td>Terrorism</td>
<td>$0</td>
</tr>
<tr>
<td>Employment</td>
<td>$62,314,015</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lottery/Sweepstakes/Inheritance</td>
<td>$61,111,319</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phishing/Vishing/Smishing/Pharming</td>
<td>$54,241,075</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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, the attacker might use:
  - john.smith@c0mpany.com
  - john.smith@cornpany.com
  - john.smith@gmail.com
  - john.smithe@company.com

• If you do not pay close attention, it is easy to get fooled by these slight differences!
A criminal sends a targeted phishing email.

1. The recipient clicks on the link and is directed to a phishing website.

2. The recipient of the targeted email enters his or her credentials into the website.

3. The cybercriminal uses those credentials to set a forwarding rule to send copies of all emails to his own inbox.

4. Not realizing that the email is fake, the customer pays the invoice, depositing money directly into the cybercriminal’s bank account.

5. The cybercriminal monitors the inbox to obtain information about invoices, payments, and other financial details.

6. When the opportunity arises, the cybercriminal uses his intel to send a fake invoice to the organization’s customer, informing the customer of new banking details.

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.

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.

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!

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, 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@ussss.dhs.gov
http://linkedin.com/in/tim-benitez-603