MITIGATING THE RISK OF CORPORATE ACCOUNT TAKEOVER, BUSINESS EMAIL COMPROMISE & RANSOMWARE

A Presentation of Federal Law Enforcement Agency Guidance

Presentation Description

This presentation focuses on several widespread forms of targeted on-line fraud impacting businesses, non-profits, schools and public sector entities. Perpetrators of these crimes attempt to transfer money out of bank accounts using wire transfers and ACH transactions, or may attempt to encrypt the contents of computer disk drives and then demand ransom payments in exchange for access. FBI & US Secret Service recommended risk mitigation techniques will be presented, as described in several related FBI & US Secret Service publications.

Topic Outline

This presentation and the related federal fraud advisories are directed to audiences comprised of commercial bank customers, law enforcement and security personnel, and covers:

1. Characteristics: how the frauds work, victim selection, perpetration methods
2. Protection: education; technical & business process enhancements; fraud loss liability
3. Detection: account monitoring, warning signs, anti-virus software
4. Response: compromised computer handling and reporting suspicious activity

Fraud Advisory for **Businesses**: Corporate Account Take Over

This product was created as part of a joint effort between the United States Secret Service, the Federal Bureau of Investigation, the Internet Crime Complaint Center (IC3) and the Financial Services Information Sharing and Analysis Center (FS-ISAC).

Problem:
Cyber criminals are targeting the financial accounts of owners and employees of small and medium sized businesses, resulting in significant business disruption and substantial monetary losses due to fraudulent transfers from these accounts. Often these funds may not be recovered[1].

Figure 1: Recent news headlines from *The New York Times*, *The Washington Post*, *Computer World*, and *Krebs on Security*.

To obtain access to financial accounts, cyber criminals target employees– often senior executives or accounting and HR personnel[2]- and business partners[3] and cause the targeted individual to spread

[1] Consumer accounts are subject to Federal Reserve Regulations E (12C.F.R. Part 205) which requires banks to provide reimbursement for certain losses. Regulation E does not apply to business accounts. Therefore, banks are not required to provide reimbursement for certain losses.
[2] *Any* employee is vulnerable to being targeted.

malicious software (or "malware") which in turn steals their personal information and log-in credentials. Once the account is compromised, the cyber criminal is able to electronically steal money from business accounts. Cyber criminals also use various attack methods to exploit check archiving and verification services that enable them to issue counterfeit checks, impersonate the customer over the phone to arrange funds transfers, mimic legitimate communication from the financial institution to verify transactions, create unauthorized wire transfers and ACH payments, or initiate other changes to the account. In addition to targeting account information, cyber criminals also seek to gain customer lists and/or proprietary information - often through the spread of malware - that can also cause indirect losses and reputational damage to a business.

First identified in 2006, this fraud, known as "corporate account take over," has morphed in terms of the types of companies targeted and the technologies and techniques employed by cyber criminals. Where cyber criminals once attacked mostly large corporations, they have now begun to target municipalities, smaller businesses, and non-profit organizations. Thousands of businesses, small and large, have reportedly fallen victim to this type of fraud. Educating all stakeholders (financial institutions, businesses and consumers) on how to identify and protect themselves against this activity is the first step to combating cyber criminal activity.

This advisory was created by financial institutions, industry trade associations, Federal law enforcement and regulatory agencies.[4] It is intended to make businesses aware of this issue, identify some examples of how the fraud may occur, and provide updated recommendations to businesses to protect themselves against it. The information contained in this advisory is intended to provide basic guidance and resources for businesses to learn about the evolving threats and to establish security processes specific to their needs. However, it is very important to note that as the cyber criminals change their techniques, businesses must continue to improve their knowledge of and security posture against these attacks. In addition, the tips and recommendations contained in this advisory may help reduce the likelihood of fraud, but they should not be expected to provide complete protection against these attacks.

How it's Done:

Cyber criminals employ various technological and non-technological methods to manipulate or trick victims into divulging personal or account information. Such techniques may include performing an action such as opening an email attachment, accepting a fake friend request on a social networking site, or visiting a legitimate, yet compromised, website that installs malware on their computer(s).

---

[3] Business partners can include, among other third parties, contractors and accountants.

[4] This advisory was created through a collaborative cross-industry effort to develop and distribute recommended practices to prevent, detect and respond to corporate and consumer account takeovers. Led by the Financial Services Information Sharing and Analysis Center (FS-ISAC), contributors include more than 30 of the largest financial institutions in the U.S., industry associations including the American Bankers Association (ABA), NACHA - The Electronic Payments Association, BITS/The Financial Services Roundtable; and federal regulatory and law enforcement agencies. This advisory is an update to recommendations previously released in August 2009 by the FS-ISAC, FBI and NACHA and NACHA (Operations Bulletin) in December 2009.

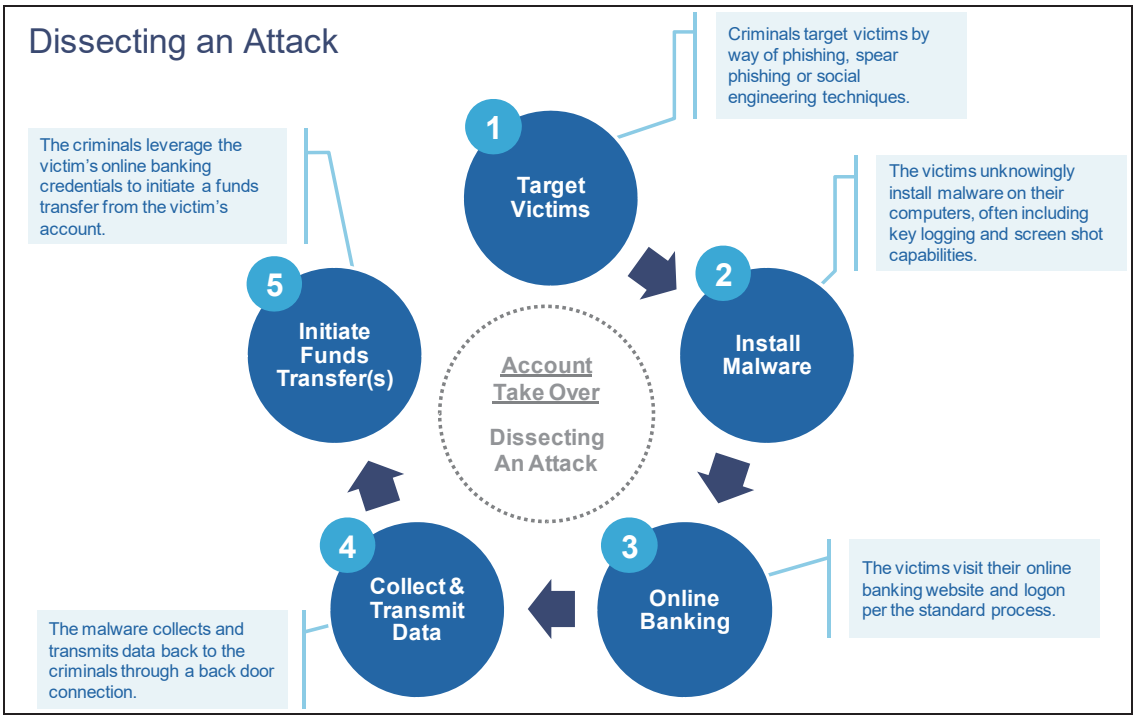


Figure 2: Dissecting An Account Take Over Attack

Cyber criminals will often "phish" for victims using mass emails, pop-up messages that appear on their computers, and/or the use of social networking and internet career sites[5]. For example, cyber criminals often send employees unsolicited emails that:

- Ask for personal or account information;
- Direct the employee to click on a malicious link provided in the email; and/or
- Contain attachments that are infected with malware.

Cyber criminals use various methods to trick employees into opening the attachment or clicking on the link, including:

- Disguising the email to look as though it's from a legitimate business. Often, these criminals will employ some type of scare tactic to entice the employee to open the email and/or provide account information. For example, cyber criminals have sent emails claiming to be from:
  1. UPS (e.g., "There has been a problem with your shipment.")
  2. Financial institutions (e.g., "There is a problem with your banking account.")
  3. Better Business Bureaus (e.g., "A complaint has been filed against you.")
  4. Court systems (e.g., "You have been served a subpoena.")

- Making the email appear to provide information regarding current events such as natural disasters, major sporting events, and celebrity news to entice people to open emails and click on links.

[5] Cyber criminals also use "vishing", which is soliciting victims over the phone or Voice over IP (VoIP).

- Using email addresses or other credentials stolen from company websites or victims, such as relatives, co-workers, friends, or executives and designing an email to look like it is from a trusted source to entice people to open emails and click on links.

The cyber criminal's goal is to get the employee to open the infected attachments or click on the link contained in the email and visit the nefarious website where hidden malware is often downloaded to the employee's computer. This malware allows the fraudster to "see" and track employee's activities across the business' internal network and on the Internet. This tracking may include visits to your financial institution and use of your online banking credentials used to access accounts (account information, log in, and passwords). Using this information, the fraudster can conduct unauthorized transactions that appear to be a legitimate transaction conducted by the company or employee.

How to Protect, Detect, and Respond

Protect

1. **Educate everyone on this type of fraud scheme**
    - Don't respond to or open attachments or click on links in unsolicited e-mails. If a message appears to be from your financial institution and requests account information, do not use any of the links provided. Contact the financial institution using the information provided upon account opening to determine if any action is needed. Financial institutions do not send customers e-mails asking for passwords, credit card numbers, or other sensitive information. Similarly, if you receive an email from an apparent legitimate source (such as the IRS, Better Business Bureau, Federal courts, UPS, etc.) contact the sender directly through other means to verify the authenticity. Be very wary of unsolicited or undesired email messages (also known as "spam") and the links contained in them.
    - Be wary of pop-up messages claiming your machine is infected and offering software to scan and fix the problem, as it could actually be malicious software that allows the fraudster to remotely access and control your computer.
    - Teach and require best practices for IT security. See #2, "Enhance the security of your computer and networks".

2. **Enhance the security of your computer and networks to protect against this fraud**[6]
    - Minimize the number of, and restrict the functions for, computer workstations and laptops that are used for online banking and payments. A workstation used for online banking should not be used for general web browsing, e-mailing, and social networking. Conduct online banking and payments activity from at least one dedicated computer that is not used for other online activity.
    - Do not leave computers with administrative privileges and/or computers with monetary functions unattended. Log/turn off and lock up computers when not in use.
    - Use/install and maintain spam filters.

[6] See the "Resources" section for links to helpful and detailed tips on how to enhance your information technology (IT) security.

- Install and maintain real-time anti-virus and anti-spyware desktop firewall and malware detection and removal software.
  - Use these tools regularly to scan your computer. Allow for automatic updates and scheduled scans.
- Install routers and firewalls to prevent unauthorized access to your computer or network.
  - Change the default passwords on all network devices.
- Install security updates to operating systems and all applications, as they become available. These updates may appear as weekly, monthly, or even daily for zero-day attacks.
- Block pop-ups.
- As recommended by Microsoft for users more concerned about security, many variants of malware can be defeated by using simple configuration settings like enabling Microsoft Windows XP[7], Vista[8], and 7 Data Execution Prevention (DEP)[9] and disabling auto run commands[10]. You may also consider disabling JavaScript in Adobe Reader[11]. If these settings do not interfere with your normal business functions, it is recommended that these and other product settings be considered to protect against current and new malware for which security patches may not be available.
- Keep operating systems, browsers, and all other software and hardware up-to-date.
- Make regular backup copies of system files and work files.
- Encrypt sensitive folders with the operating system's native encryption capabilities. Preferably, use a whole disk encryption solution.
- Do not use public Internet access points (e.g., Internet cafes, public wi-fi hotspots (airports), etc.) to access accounts or personal information. If using such an access point, employ a Virtual Private Network (VPN)[12].
- Keep abreast of the continuous cyber threats that occur. See the Additional Resources section for recommendations on sites to bookmark.

3. Enhance the security of your corporate banking processes and protocols

- Initiate ACH and wire transfer payments under dual control using two separate computers. For example: one person authorizes the creation of the payment file and a second person authorizes the release of the file from a different computer system. This helps ensure that one person does not have the access authority to perform both functions, add additional authority, or create a new user ID.

---

[7] How to configure memory protection in Windows XP SP2; http://technet.microsoft.com/en-us/library/cc700810.aspx
[8] Change Data Execution Prevention Settings; http://windows.microsoft.com/en-US/windows-vista/Change-Data-Execution-Prevention-settings
[9] Change Data Execution Prevention Settings; http://windows.microsoft.com/en-US/windows7/Change-Data-Execution-Prevention-settings
[10] How to disable the Autorun functionality in Windows: http://support.microsoft.com/kb/967715/
[11] Disabling JavaScript in Adobe Reader and Acrobat; http://blogs.adobe.com/psirt/2009/04/update_on_adobe_reader_issue.html
[12] A VPN uses the public telecommunication infrastructure and the Internet to provide remote and secure access to an organization's network.

- Talk to your financial institution about Positive Pay and other services such as SMS texting, call backs, and batch limits which help to protect companies against altered checks, counterfeit check fraud and unauthorized ACH transactions.
- If, when logging into your account, you encounter a message that the system is unavailable, contact your financial institution immediately.

4. **Understand your responsibilities and liabilities**
   - Familiarize yourself with your institution's account agreement**.** Also be aware of your liability for fraud under the agreement and the Uniform Commercial Code (UCC), as adopted in the jurisdiction, as well as for your responsibilities set forth by the Payment Card Industry Data Security Standard (PCI DSS), should you accept credit cards. For more information, see https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

Detect

5. **Monitor and reconcile accounts at least once a day**
   - Reviewing accounts regularly enhances the ability to quickly detect unauthorized activity and allows the business and the financial institution to take action to prevent or minimize losses.

6. **Discuss the options offered by your financial institution to help detect or prevent out-of-pattern activity (including both routine and red flag reporting for transaction activity).**

7. **Note any changes in the performance of your computer such as:**
   - A dramatic loss of speed.
   - Changes in the way things appear.
   - Computer locks up so the user is unable to perform any functions.
   - Unexpected rebooting or restarting of your computer.
   - An unexpected request for a one time password (or token) in the middle of an online session.
   - Unusual pop-up messages.
   - New or unexpected toolbars and/or icons.
   - Inability to shut down or restart.

8. **Pay attention to warnings**
   - Your anti-virus software should alert you to potential viruses. If you receive a warning message, contact your IT professional immediately.

9. **Be on the alert for rogue emails**
   - If someone says they received an email from you that you did not send, you probably have malware on your computer.
   - You can also check your email "outbox" to look for email that you did not send.

10. **Run regular virus and malware scans of your computer's hard drive**
    - This can usually be set to run automatically during non-peak hours.

Respond

11. **If you detect suspicious activity, immediately cease all online activity and remove any computer systems that may be compromised from the network.**
    - Disconnect the Ethernet cable and/or any other network connections (including wireless connections) to isolate the system from the network and prevent any unauthorized access.

12. **Make sure your employees know how and to whom to report suspicious activity to within your company and at your financial institution**

13. **Immediately contact your financial institution so that the following actions may be taken:**
    - Disable online access to accounts.
    - Change online banking passwords.
    - Open new account(s) as appropriate.
    - Request that the financial institution's agent review all recent transactions and electronic authorizations on the account. If suspicious active transactions are identified, cancel them immediately.
    - Ensure that no one has added any new payees, requested an address or phone number change, created any new user accounts, changed access to any existing user accounts, changed existing wire/ACH template profiles, changed PIN numbers or ordered new cards, checks or other account documents be sent to another address.

14. **Maintain a written chronology of what happened, what was lost, and the steps taken to report the incident to the various agencies, financial institutions, and firms impacted**
    - Be sure to record the date, time, contact telephone number, person spoken to, instructions, and any relevant report or reference number.

15. **File a police report and provide the facts and circumstances surrounding the loss**
    - Obtain a police report number with the date, time, department, location and officer's name taking the report or involved in the subsequent investigation. Having a police report on file will often help facilitate the filing of claims with insurance companies, financial institutions, and other establishments that may be the recipient of fraudulent activity.
    - The police report may result in a law enforcement investigation into the loss with the goal of identifying, arresting and prosecuting the offender, and possibly recovering losses.
    - Depending on the incident and the circumstance surrounding the loss, investigating officials may request specific data be recorded and some or all of the system's data may need to be preserved as potential evidence.
    - In addition, you may choose to file a complaint online at www.ic3.gov. For substantial losses, contact your local FBI field office (http://www.fbi.gov/contact-us/field/field-offices), your local United States Secret Service field office

(http://www.secretservice.gov/field_offices.shtml), or the Secret Service's local Electronic Crimes Task Force (http://www.secretservice.gov/ectf.shtml).

16. **Have a contingency plan to recover systems suspected of compromise**
    - The contingency plan should cover resolutions for a system infected by malware, data corruption, and catastrophic system/hardware failure. A recommended malware removal option is to reformat the hard drive, then reinstall the operating system and other software on the infected computer(s). There is no preservation of data using this method – all your data will be permanently erased. Do not take this step until you determine if a forensic analysis of the computer is needed. For additional recommendations on steps to take following a compromise, see the section "What if I am Compromised" on page 6 of the US CERT document, *Malware Threats and Mitigation Strategies* available at http://www.us-cert.gov/reading_room/malware-threats-mitigation.pdf

17. **Consider whether other company or personal data may have been compromised**

18. **Report exposures to PCI DSS.**
    - If your business accepts credit cards, you are subject to compliance with the Payment Card Industry Data Security Standard (PCI DSS) and you may be required to report and investigate the incident, limit the exposure of the cardholder data, and report the incident to your card company. For more information, see https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

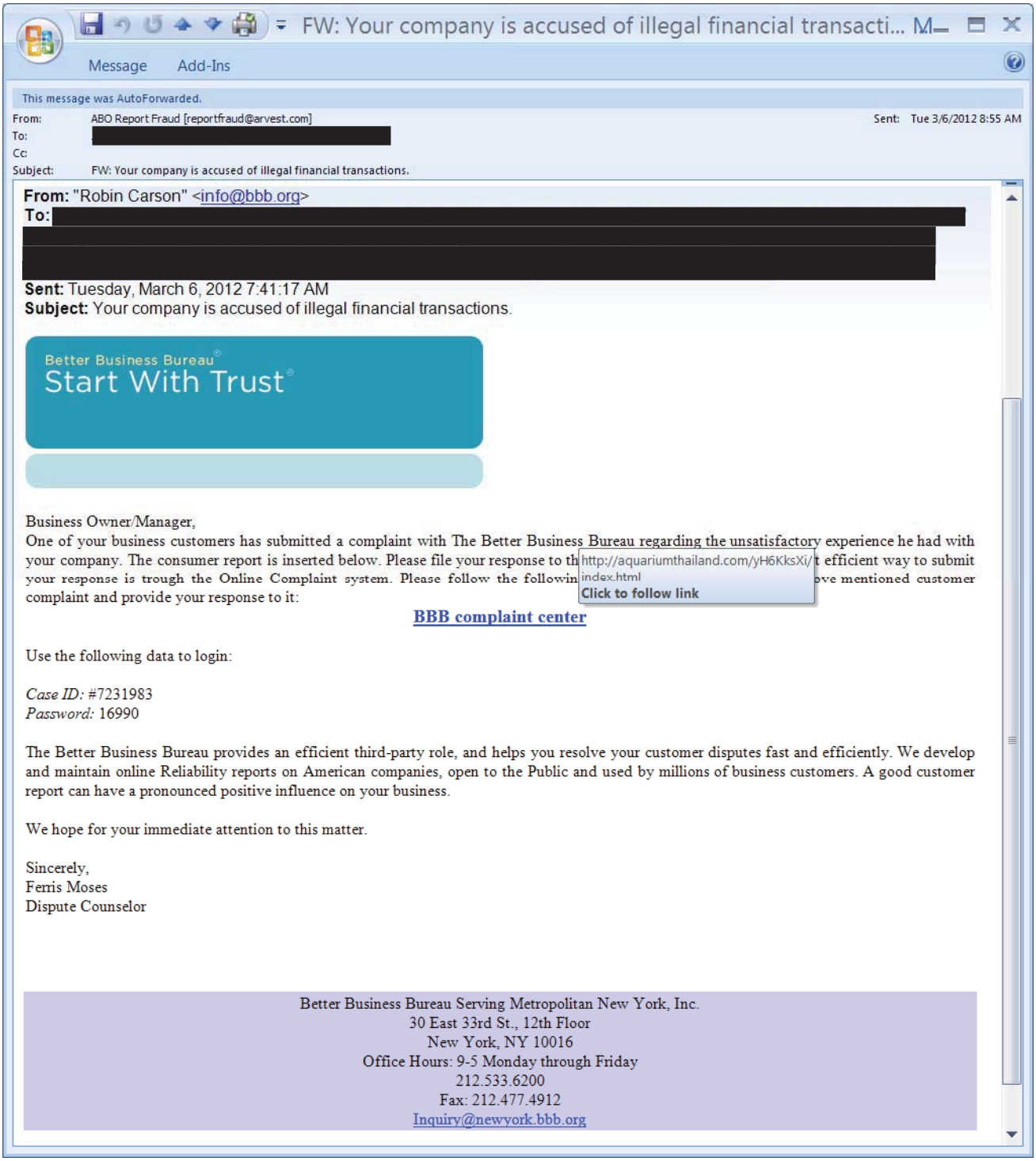
Contact your financial institution for more information.

Additional Resources:

- Federal Trade Commission (FTC) website, "Computers& the Internet: Privacy and Security"[13] (includes OnGuard Online),
- Internet Crime Complaint Center (IC3)[14],
- Department of Homeland Security Cyber Report[15],
- National Cyber Security Alliance Stay Safe Online[16].
- Better Business Bureau- "Data Security Made Simple"[17]
- Microsoft Security Page[18]
- U.S. Chamber of Commerce's "Internet Security Essentials for Small Business"[19]

[13] http://www.ftc.gov/bcp/menus/consumer/tech/privacy.shtm
[14] The IC3 is a partnership between the Federal Bureau of Investigation (FBI), the National White Collar Crime Center (NW3C), and the Bureau of Justice Assistance (BJA). For more information, see http://www.ic3.gov/default.aspx.
[15] http://www.cyber.st.dhs.gov/
[16] http://www.staysafeonline.org/
[17] http://www.bbb.org/data-security/
[18] http://www.microsoft.com/security/default.aspx
[19] This document is scheduled for release on October 26, 2010. Visit www.uschamber.com/cybersecurity for more information.

Corporate Account Takeover E-Mail Message Examples



FW: Your company is accused of illegal financial transacti... M

Message Add-Ins

This message was AutoForwarded.

From: ABO Report Fraud [reportfraud@arvest.com] Sent: Tue 3/6/2012 8:55 AM
To: [redacted]
Cc:
Subject: FW: Your company is accused of illegal financial transactions.

From: "Robin Carson" <info@bbb.org>
To: [redacted]
Sent: Tuesday, March 6, 2012 7:41:17 AM
Subject: Your company is accused of illegal financial transactions.

Better Business Bureau®
Start With Trust®

Business Owner/Manager,
One of your business customers has submitted a complaint with The Better Business Bureau regarding the unsatisfactory experience he had with your company. The consumer report is inserted below. Please file your response to th http://aquariumthailand.com/yH6KksXi/ t efficient way to submit your response is trough the Online Complaint system. Please follow the followin index.html ove mentioned customer complaint and provide your response to it:
Click to follow link

BBB complaint center

Use the following data to login:

Case ID: #7231983
Password: 16990

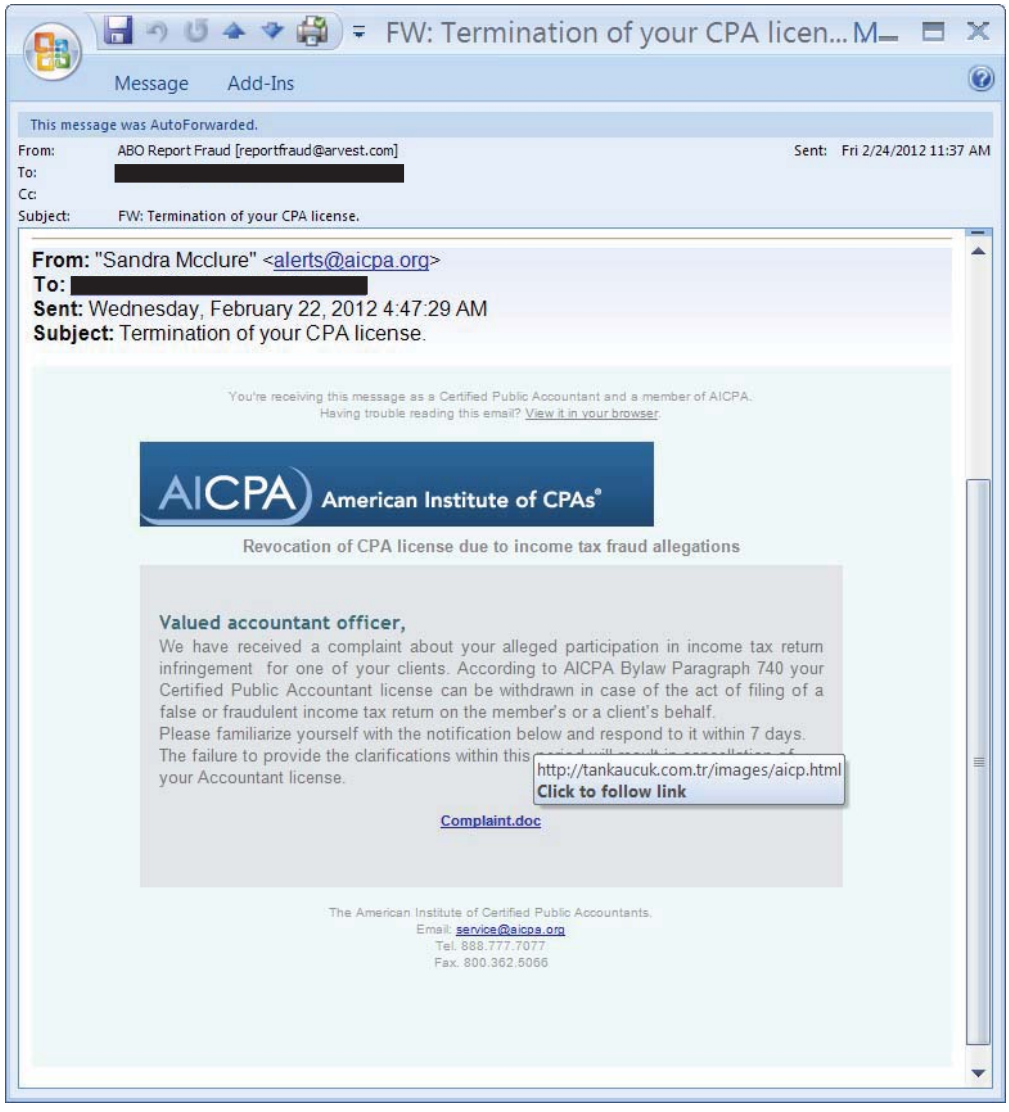
The Better Business Bureau provides an efficient third-party role, and helps you resolve your customer disputes fast and efficiently. We develop and maintain online Reliability reports on American companies, open to the Public and used by millions of business customers. A good customer report can have a pronounced positive influence on your business.

We hope for your immediate attention to this matter.

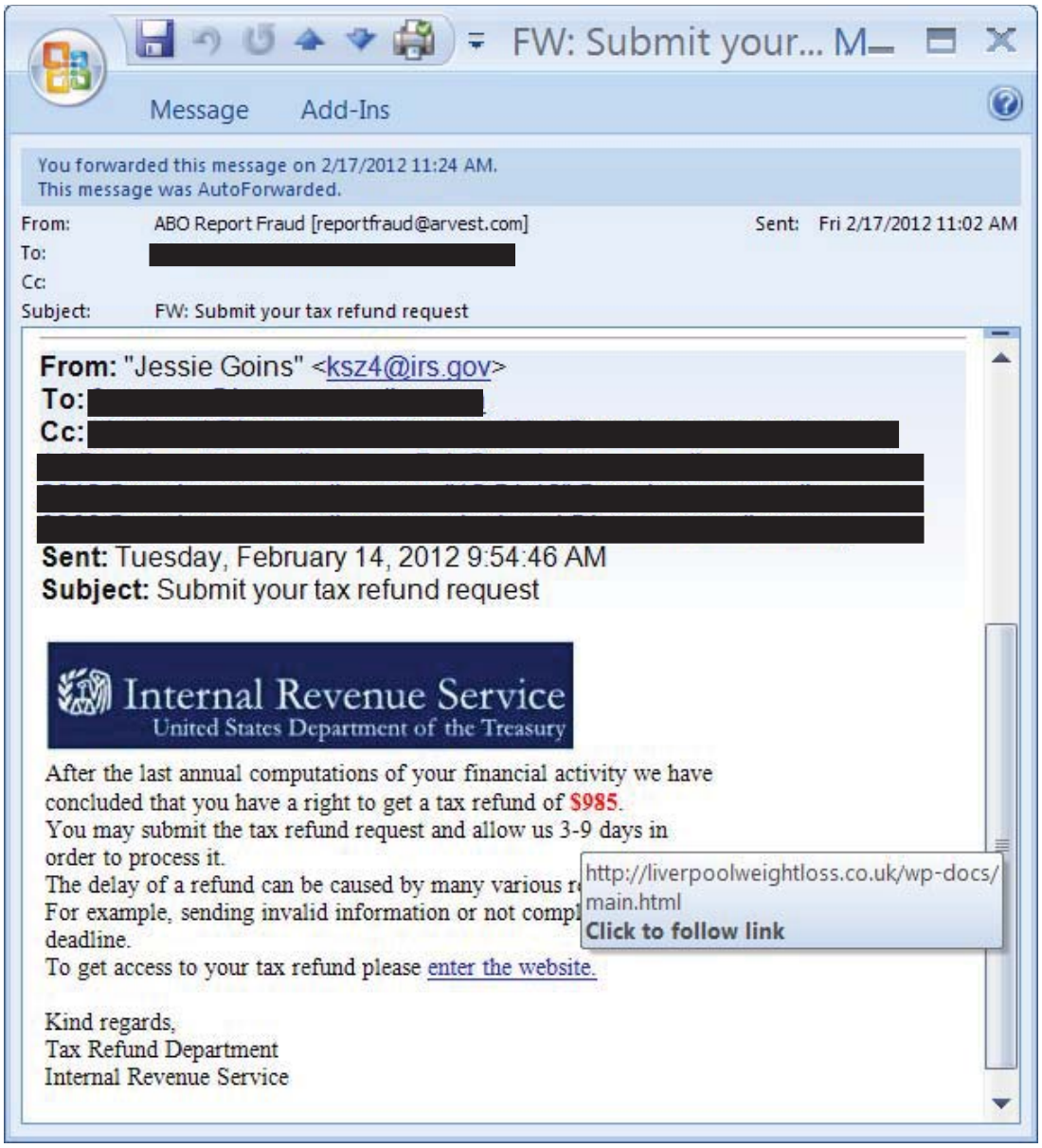
Sincerely,
Ferris Moses
Dispute Counselor

Better Business Bureau Serving Metropolitan New York, Inc.
30 East 33rd St., 12th Floor
New York, NY 10016
Office Hours: 9-5 Monday through Friday
212.533.6200
Fax: 212.477.4912
Inquiry@newyork.bbb.org

Corporate Account Takeover E-Mail Message Examples



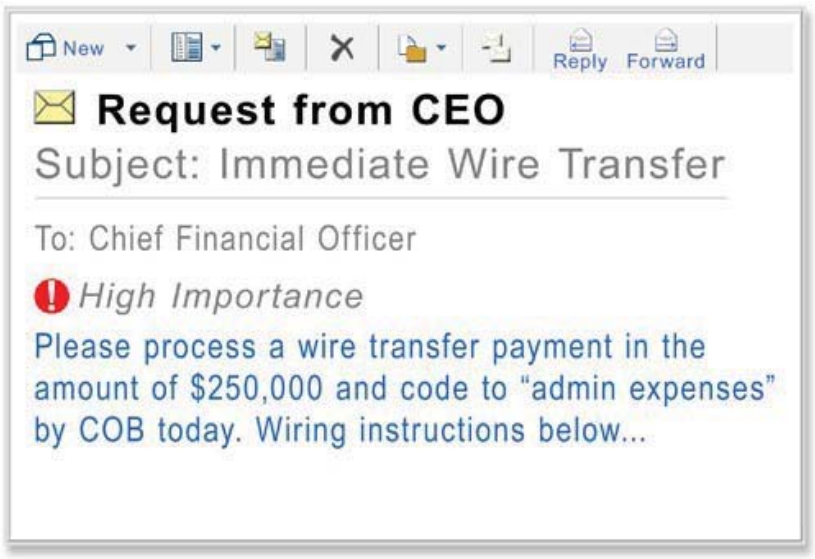
Corporate Account Takeover E-Mail Message Examples



Business E-mail Compromise (BEC) Message Examples

In these examples, the perpetrator impersonates a company executive and sends an email to an individual at the executive's company who is authorized to initiate a wire transfer:

Example 1:



Example 2:

[redacted]

From: [redacted]@[redacted]com] <--- Typically the CEO or president.
Sent: Wednesday, December 10, 2014 9:55 AM
To: [redacted] <--- Typically the controller, office manager, treasurer or equivalent.
Subject: Fwd: Wire Payment
Attachments: Universal Wiring Instructions.pdf

[redacted]

Process a wire of $137,818.43 to the attached account information and code this to Admin Expense. Send me the confirmation as soon as the wire has been processed.

Thanks,
[redacted]

Corporate Account Takeover

ARVEST

Frequently Asked Questions (FAQ)

1) **What is Corporate Account Take Over Fraud (CAT)?**
   a) CAT results in fraudulent transfers of funds from the accounts of business banking customers. In general, the victim is tricked into installing malicious "Banking Trojan" software on their computer by clicking on a link to a virus infected Web page in a spoofed email. Through this malicious software, the perpetrator steals the victim's logon credentials and gains access to the customer's account through the business web banking site.
2) **Where does the money go?**
   a) Stolen funds are generally sent via ACH or wire transfer to foreign accounts or to "money mules" in the United States who then transfer the money overseas via popular money transfer services.
3) **Who is perpetrating CAT fraud?**
   a) According to Federal law enforcement agencies, Eastern European organized crime groups are believed to be predominantly responsible.
4) **What types of companies are targeted?**
   a) Cyber criminals once attacked mostly large corporations, but have now begun to target municipalities, smaller businesses and non-profit organizations such as schools and hospitals.
5) **How are businesses tricked into installing the malicious "Banking Trojan" software?**
   a) Perpetrators use various techniques, but generally send targeted emails which appear to be sent by official entities such as the FDIC, the Federal Reserve Bank, the American Bankers Association (ABA) or NACHA which falsely suggest that there is a problem with a transaction, wire transfer, ACH batch or bank account. These spoofed messages contain links to web sites which host malicious software often called "Banking Trojans" which are automatically installed on victim's computers when they visit the web site.
6) **Does anti-virus software protect against this type of threat?**
   a) Banking Trojan software is often customized by the fraudster for each attack and is rarely detected or removed by current anti-virus software.
7) **Who would be responsible for losses resulting from CAT fraud?**
   a) While Federal Reserve Board Regulation E (12 CFR 205) affords certain protections to consumer bank accounts against fraudulent losses, business accounts, including small business "DBA" accounts, are not afforded these same protections. Liability for a fraudulent loss in a business account would be dependent upon the specific circumstances of the incident and the terms and conditions of the account agreement and related contracts between the customer and the bank.
   b) NACHA rules govern ACH transactions and related dispute resolutions, while Federal Reserve Board rules and procedures may affect wire transfer activity. In addition, UCC provisions for the applicable states may also apply.
8) **What should a business do if they believe they may be a victim of CAT fraud?**
   a) Cease all online activity, disconnect the computer from the network (leaving it turned on), and contact the bank immediately.
9) **What is the source of this information and where can I learn more about CAT fraud?**
   a) This information was taken from an FBI publication titled "Fraud Advisory for Business: Corporate Account Take Over," which also contains more information about this type of fraud.

Corporate Account Takeover

ARVEST

Glossary of Terms

Banking Trojan – Malicious software that may allow a hacker remote access to a targeted computer system. Once a Banking Trojan has been installed, the hacker may gain remote access to the computer and may be able to perform various operations such as stealing web banking credentials or initiating unauthorized funds transfers.

Credentials – Information needed to log into a secure computer system which may include a user name, password or token code.

Dual Control – A security procedure requiring two people (or possibly processes or devices) to cooperate in gaining authorized access to a system resource (data, files, devices.)

Keystroke logger – Malicious software used to monitor a user's activities by recording every keystroke the user makes with the intent to steal passwords and confidential information. (source: zdnet.com)

Malware – (Short for MALicious softWARE) Software designed to compromise computers or computer information. Examples include viruses, worms, spyware and Trojan horse applications such as "banking Trojans."

Money mule – A person who transfers stolen money as a part of a fraudulent scam, either in person, through a courier service or electronically. Money mules may or may not be aware that the money they are transferring is stolen. The stolen funds are generally transferred from the victim's country to the scam operator's country. (source: Wikipedia.org)

Phishing – The fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. (Phishing is a form of social engineering using spoofed email.)

Security Token – A small hardware device that the owner carries to authorize access to a network service. Sometimes called an authorization token. The devices may be in the form of a smart card or key fob.

Spear phishing – A method of Phishing whereby individuals or businesses are specifically targeted.

Social engineering – Manipulating people into performing actions or divulging confidential information by trickery, rather than by physically breaking in or by using technical techniques.

Spoofed email – E-mail sent so that the sender's address and other parts of the message are altered to appear as though the e-mail originated from a different source. The message may incorporate graphics taken from a legitimate entity's web site to give the appearance of authenticity.

Vishing – Refers to phishing attacks that involve the use of voice calls, using either conventional phone systems or Voice over Internet Protocol (VoIP) systems.

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

04 May 2017

Alert Number
I-050417-PSA

BUSINESS E-MAIL COMPROMISE
E-MAIL ACCOUNT COMPROMISE
THE 5 BILLION DOLLAR SCAM

This Public Service Announcement (PSA) is an update to Business E-mail Compromise (BEC) PSAs 1-012215-PSA, 1-082715a-PSA and I-061416-PSA, all of which are posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data as of December 31, 2016.

DEFINITION
Business E-mail Compromise (BEC) is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The E-mail Account Compromise (EAC) component of BEC targets individuals that perform wire transfer payments.

The techniques used in the BEC/EAC scam have become increasingly similar, prompting the IC3 to begin tracking these scams as a single crime type[1] in 2017.

The scam is carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

Most victims report using wire transfers as a common method of transferring funds for business purposes; however, some victims report using checks as a common method of payment. The fraudsters will use the method most commonly associated with their victim's normal business practices.

The scam has evolved to include the compromising of legitimate business e-mail accounts and requesting Personally Identifiable Information (PII) or Wage and Tax Statement (W-2) forms for employees, and may not always be associated with a request for transfer of funds.

BACKGROUND
The victims of the BEC/EAC scam range from small businesses to large corporations. The victims continue to deal in a wide variety of goods and services, indicating that no specific sector is targeted more than another.

[1] The IC3 uses descriptions of crime types for categorization purposes.

It is largely unknown how victims are selected; however, the subjects monitor and study their selected victims using social engineering techniques prior to initiating the BEC scam. The subjects are able to accurately identify the individuals and protocols necessary to perform wire transfers within a specific business environment. Victims may also first receive "phishing" e-mails requesting additional details regarding the business or individual being targeted (name, travel dates, etc.).

Some individuals reported being a victim of various Scareware or Ransomware cyber intrusions immediately preceding a BEC incident. These intrusions can initially be facilitated through a phishing scam in which a victim receives an e-mail from a seemingly legitimate source that contains a malicious link. The victim clicks on the link, and it downloads malware, allowing the subject(s) unfettered access to the victim's data, including passwords or financial account information.

The BEC/EAC scam is linked to other forms of fraud, including but not limited to: romance, lottery, employment, and rental scams. The victims of these scams are usually U.S. based and may be recruited as unwitting money mules[2]. The mules receive the fraudulent funds in their personal accounts and are then directed by the subject to quickly transfer the funds to another bank account, usually outside the U.S., upon direction, mules may open bank accounts and/or shell corporations to further the fraud scheme.

STATISTICAL DATA

The BEC/EAC scam continues to grow, evolve, and target small, medium, and large businesses. Between January 2015 and December 2016, there was a 2,370% increase in identified exposed losses[3]. The scam has been reported in all 50 states and in 131 countries. Victim complaints filed with the IC3 and financial sources indicate fraudulent transfers have been sent to 103 countries.

Based on the financial data, Asian banks located in China and Hong Kong remain the primary destinations of fraudulent funds; however, financial institutions in the United Kingdom have also been identified as prominent destinations.

The following BEC/EAC statistics were reported to the IC3 and are derived from multiple sources, including IC3 and international law enforcement complaint data and filings from financial institutions between **October 2013 and December 2016**:

Domestic and international incidents:	40,203
Domestic and international exposed dollar loss:	$5,302,890,448

The following BEC/EAC statistics were reported in victim complaints to the IC3 from **October 2013 to December 2016:**

Total U.S. victims:	22,292
Total U.S. exposed dollar loss:	$1,594,503,669
Total non-U.S. victims:	2,053
Total non-U.S. exposed dollar loss:	$626,915,475

[2] Money mules are defined as persons who transfer money illegally on behalf of others.
[3] Exposed dollar loss includes actual and attempted loss in United States dollars.

UNCLASSIFIED

Federal Bureau of Investigation
Public Service Announcement

The following BEC/EAC statistics were reported by victims via the financial transaction component of the new IC3 complaint form, which became available in June 2016[4]. The following statistics were reported in victim complaints to the IC3 from **June 2016 to December 2016:**

Total U.S. financial recipients:	3,044
Total U.S. financial recipient exposed dollar loss:	$346,160,957
Total non-U.S. financial recipients:	774
Total non-U.S. financial recipient exposed dollar loss:	$448,464,415

SCENARIOS OF BEC/EAC
Based on IC3 complaints and other complaint data, there are five main scenarios by which this scam is perpetrated.

Scenario 1: Business Working with a Foreign Supplier
A business that typically has a longstanding relationship with a supplier is requested to wire funds for an invoice payment to an alternate, fraudulent account. The request may be made via telephone, facsimile, or e-mail. If an e-mail is received, the subject will spoof the e-mail request so it appears similar to a legitimate request. Likewise, requests made via facsimile or telephone call will closely mimic a legitimate request. This particular scenario has also been referred to as the "Bogus Invoice Scheme," "Supplier Swindle," and "Invoice Modification Scheme."

Scenario 2: Business Executive Receiving or Initiating a Request for a Wire Transfer
The e-mail accounts of high-level business executives (Chief Financial Officer, Chief Technology Officer, etc.) are compromised. The account may be spoofed or hacked. A request for a wire transfer from the compromised account is made to a second employee within the company who is typically responsible for processing these requests. In some instances, a request for a wire transfer from the compromised account is sent directly to the financial institution with instructions to urgently send funds to bank "X" for reason "Y." This particular scenario has been referred to as "CEO Fraud," "Business Executive Scam," "Masquerading," and "Financial Industry Wire Frauds."

Scenario 3: Business Contacts Receiving Fraudulent Correspondence through Compromised E-mail
An employee of a business has his or her personal e-mail hacked. This personal e-mail may be used for both personal and business communications. Requests for invoice payments to fraudster-controlled bank accounts are sent from this employee's personal e-mail to multiple vendors identified from this employee's contact list. The business may not become aware of the fraudulent requests until that business is contacted by a vendor to follow up on the status of an invoice payment.

Scenario 4: Business Executive and Attorney Impersonation
Victims report being contacted by fraudsters who typically identify themselves as lawyers or representatives of law firms and claim to be handling confidential or time-sensitive matters. This contact may be made via either phone or e-mail. Victims may be pressured by the fraudster to act quickly or secretly in handling the transfer of funds. This type of BEC scam may occur at the end of the business day or work week and be timed to coincide with the close of business of international financial institutions.

[4] "Financial Recipient" is defined as an account holder who receives the fraudulent funds.

Scenario 5: Data Theft
Fraudulent requests are sent utilizing a business executive's compromised e-mail. The entities in the business organization responsible for W-2s or maintaining PII, such as the human resources department, bookkeeping, or auditing section, have frequently been identified as the targeted recipients of the fraudulent request for W-2 and/or PII. Some of these incidents are isolated and some occur prior to a fraudulent wire transfer request. Victims report they have fallen for this new BEC scenario even if they were able to successfully identify and avoid the traditional BEC scam. This data theft scenario of the BEC scam first appeared just prior to the 2016 tax season.

TRENDS
W-2/PII Data Theft
This scenario of BEC/EAC was identified in 2016 in which a human resource department or counterpart was targeted with a spoofed e-mail seemingly on behalf of a business executive requesting all employee PII or W-2 forms for tax or audit purposes. The request appeared to coincide with the 2016 U.S. tax season, which runs from January through April. The number of complaints and reported losses peaked in April 2016, although complaints were still submitted by victims throughout 2016. Victims appeared to be both the businesses responsible for maintaining PII data and the employees whose PII was compromised. In several instances, thousands of employees were compromised. Employees filed identity theft–related complaints with IC3 that included reported incidents of fraudulent tax return filings, credit card applications, and loan applications.

Resurgence of Original Scheme
The IC3 saw a 50% increase in the number of complaints in 2016 filed by businesses working with dedicated international suppliers. This scenario was described in the earliest BEC/EAC complaints and quickly evolved into more sophisticated scenarios[5]. In some instances, instead of requesting a change in a single remittance or invoice payment, BEC/EAC perpetrators changed the remittance location to redirect all incoming invoice payments. The fraudulent request appeared to be facilitated through a spoofed e-mail or domain.

Real Estate Transactions
The BEC/EAC scam targets all participants in real estate transactions, including buyers, sellers, agents, and lawyers. The IC3 saw a 480% increase in the number of complaints in 2016 filed by title companies that were the primary target of the BEC/EAC scam. The BEC/EAC perpetrators were able to monitor the real estate proceeding and time the fraudulent request for a change in payment type (frequently from check to wire transfer) or a change from one account to a different account under their control.

SUGGESTIONS FOR PROTECTION
Businesses with an increased awareness and understanding of the BEC/EAC scam are more likely to recognize when they have been targeted by BEC/EAC fraudsters, and are therefore more likely to avoid falling victim and sending fraudulent payments.

Businesses that deploy robust internal prevention techniques at all levels (especially for front line employees who may be the recipients of initial phishing attempts) have proven highly successful in recognizing and deflecting BEC/EAC attempts.

UNCLASSIFIED

Federal Bureau of Investigation
Public Service Announcement

Some financial institutions reported holding their customer requests for international wire transfers for an additional period of time to verify the legitimacy of the request.

The following list includes self-protection strategies:

- Avoid free web-based e-mail accounts: Establish a company domain name and use it to establish company e-mail accounts in lieu of free, web-based accounts.
- Be careful what you post to social media and company websites, especially job duties and descriptions, hierarchal information, and out-of-office details.
- Be suspicious of requests for secrecy or pressure to take action quickly.
- Consider additional IT and financial security procedures, including the implementation of a two-step verification process. For example:
  - Out-of-Band Communication: Establish other communication channels, such as telephone calls, to verify significant transactions. Arrange this two-factor authentication early in the relationship and outside the e-mail environment to avoid interception by a hacker.
  - Digital Signatures: Both entities on each side of a transaction should utilize digital signatures. This will not work with web-based e-mail accounts. Additionally, some countries ban or limit the use of encryption.
- Immediately report and delete unsolicited e-mail (spam) from unknown parties. DO NOT open spam e-mail, click on links in the e-mail, or open attachments. These often contain malware that will give subjects access to your computer system.
- Do not use the "Reply" option to respond to any business e-mails. Instead, use the "Forward" option and either type in the correct e-mail address or select it from the e-mail address book to ensure the intended recipient's correct e-mail address is used.
- Consider implementing two-factor authentication for corporate e-mail accounts. Two-factor authentication mitigates the threat of a subject gaining access to an employee's e-mail account through a compromised password by requiring two pieces of information to log in: (1) something you know (a password) and (2) something you have (such as a dynamic PIN or code).
- Beware of sudden changes in business practices. For example, if a current business contact suddenly asks to be contacted via their personal e-mail address when all previous official correspondence has been through company e-mail, the request could be fraudulent. Always verify via other channels that you are still communicating with your legitimate business partner.
- Create intrusion detection system rules that flag e-mails with extensions that are similar to company e-mail. For example, a detection system for legitimate e-mail of *abc_company.com* would flag fraudulent e-mail from *abc-company.com*.
- Register all company domains that are slightly different than the actual company domain.
- Verify changes in vendor payment location by adding additional two-factor authentication such as having a secondary sign-off by company personnel.
- Confirm requests for transfers of funds. When using phone verification as part of two-factor authentication, use previously known numbers, not the numbers provided in the e-mail request.
- Know the habits of your customers, including the details of, reasons behind, and amount of payments.
- Carefully scrutinize all e-mail requests for transfers of funds to determine if the requests are out of the ordinary.

UNCLASSIFIED

Federal Bureau of Investigation
Public Service Announcement

A complete list of self-protection strategies is available on the United States Department of Justice website www.justice.gov in the publication titled "Best Practices for Victim Response and Reporting of Cyber Incidents."

WHAT TO DO IF YOU ARE A VICTIM

If funds are transferred to a fraudulent account, it is important to act quickly:

- Contact your financial institution immediately upon discovering the fraudulent transfer.
- Request that your financial institution contact the corresponding financial institution where the fraudulent transfer was sent.
- Contact your local Federal Bureau of Investigation (FBI) office if the wire is recent. The FBI, working with the United States Department of Treasury Financial Crimes Enforcement Network, might be able to help return or freeze the funds.
- File a complaint, regardless of dollar loss, with www.ic3.gov or, for BEC/EAC victims, BEC.IC3.gov

When contacting law enforcement or filing a complaint with IC3, it is important to identify your incident as "BEC/EAC"; also consider providing the following information:

- Originating business name
- Originating financial institution name and address
- Originating account number
- Beneficiary name
- Beneficiary financial institution name and address
- Beneficiary account number
- Correspondent bank if known or applicable
- Dates and amounts transferred
- IP and/or e-mail address of fraudulent e-mail

Detailed descriptions of BEC/EAC incidents should include but not be limited to the following when contacting law enforcement:

- Date and time of incidents
- Incorrectly formatted invoices or letterheads
- Requests for secrecy or immediate action
- Unusual timing, requests, or wording of the fraudulent phone calls or e-mails
- Phone numbers of the fraudulent phone calls
- Description of any phone contact, including frequency and timing of calls
- Foreign accents of the callers
- Poorly worded or grammatically incorrect e-mails
- Reports of any previous e-mail phishing activity

Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

September 10, 2019

Alert Number

I-091019-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

Business Email Compromise The $26 Billion Scam

This Public Service Announcement is an update and companion piece to Business Email Compromise PSA 1-071218-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center complaint information and updated statistics from October 2013 to July 2019.

DEFINITION

Business Email Compromise/Email Account Compromise (BEC/EAC) is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests.

The scam is frequently carried out when a subject compromises legitimate business or personal email accounts through social engineering or computer intrusion to conduct unauthorized transfers of funds.

The scam is not always associated with a transfer-of-funds request. One variation involves compromising legitimate business email accounts and requesting employees' Personally Identifiable Information or Wage and Tax Statement (W-2) forms.[1]

STATISTICAL DATA

The BEC/EAC scam continues to grow and evolve, targeting small, medium, and large business and personal transactions. Between May 2018 and July 2019, there was a 100 percent increase in identified global exposed losses[2]. The increase is also due in part to greater awareness of the scam, which encourages reporting to the IC3 and international and financial partners. The scam has been reported in all 50 states and 177 countries. Fraudulent transfers have been sent to at least 140 countries.

Based on the financial data, banks located in China and Hong Kong remain the primary destinations of fraudulent funds. However, the Federal Bureau of Investigation has seen an increase of fraudulent transfers sent to the United Kingdom, Mexico, and Turkey.

The following BEC/EAC statistics were reported to the IC3 and are derived from multiple sources, including IC3 and international law enforcement complaint data and filings from financial institutions between October 2013 and July 2019:

The following statistics were reported in victim complaints to the IC3 between **June 2016 and July 2019:**

Domestic and international incidents:	166,349
Domestic and international exposed dollar loss:	$26,201,775,589

The following BEC/EAC statistics were reported in victim complaints to the IC3 between **October 2013 and July 2019:**

Total U.S. victims:	69,384
Total U.S. exposed dollar loss:	$10,135,319,091
Total non-U.S. victims:	3,624
Total non-U.S. exposed dollar loss:	$1,053,331,166

The following statistics were reported in victim complaints to the IC3 between **June 2016 and July 2019:**

Total U.S. financial recipients:	32,367
Total U.S. financial recipient exposed dollar loss:	$3,543,308,220
Total non-U.S. financial recipients:	14,719
Total non-U.S. financial recipient exposed dollar loss:	$4,843,767,489

BEC AND PAYROLL DIVERSION

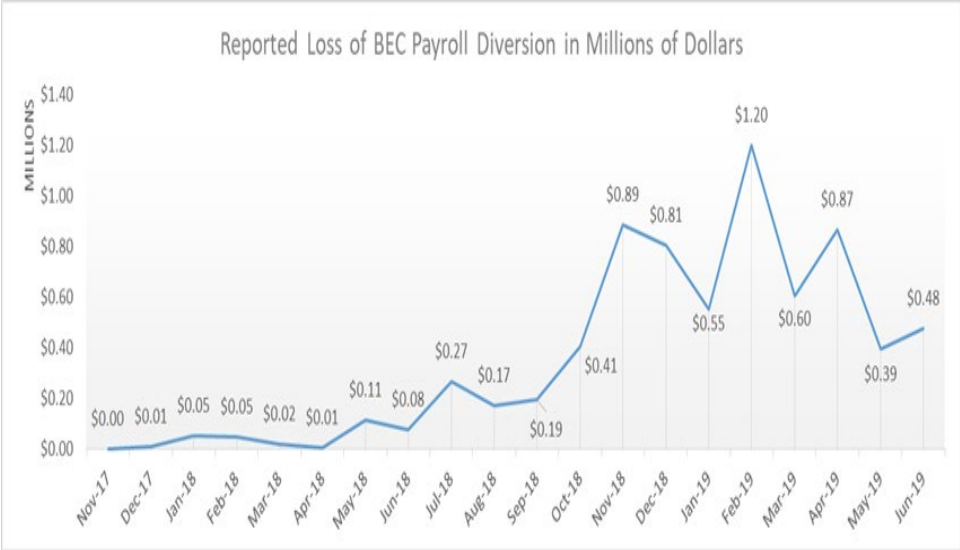
The IC3 has received an increased number of BEC complaints concerning the diversion of payroll funds. Complaints indicate that a company's human resources or payroll department receives spoofed emails appearing to be from employees requesting a change to their direct deposit account. This is different from the payroll diversion scheme in which the subject gains access to an employee's direct deposit account and alters the routing to another account.[3]

In a typical example, HR or payroll representatives received emails appearing to be from employees requesting to update their direct deposit information for the current pay period. The new direct deposit information provided to HR or payroll representatives generally leads to a pre-paid card account.

Some companies reported receiving phishing emails prior to receiving requests for changes to direct deposit accounts. In these cases, multiple employees may receive the same email that contains a spoofed log-in page for an email host. Employees enter their usernames and passwords on the spoofed log-in page, which allows the subject to gather and use employee credentials to access the employees' personal information. This makes the direct deposit requests appear legitimate.

Payroll diversion schemes that include an intrusion event have been reported to the IC3 for several years. Only recently, however, have these schemes been directly connected to BEC actors through IC3 complaints.

A total of 1,053 complaints reporting this BEC evolution of the payroll diversion scheme were filed with the IC3 between Jan. 1, 2018, and June 30, 2019, with a total reported loss of $8,323,354. The average dollar loss reported in a complaint was $7,904. The dollar loss of direct deposit change requests increased more than 815 percent between Jan. 1, 2018, and June 30, 2019 as there was minimal reporting of this scheme in IC3 complaints prior to January 2018.



SUGGESTIONS FOR PROTECTION

Employees should be educated about and alert to this scheme. Training should include preventative strategies and reactive measures in case they are victimized. Among other steps, employees should be told to:

- Use secondary channels or two-factor authentication to verify requests for changes in account information.
- Ensure the URL in emails is associated with the business it claims to be from.
- Be alert to hyperlinks that may contain misspellings of the actual domain name.
- Refrain from supplying login credentials or PII in response to any emails.
- Monitor their personal financial accounts on a regular basis for irregularities, such as missing deposits.
- Keep all software patches on and all systems updated.
- Verify the email address used to send emails, especially when using a mobile or handheld device by ensuring the senders address email address appears to match who it is coming from.
- Ensure the settings the employees' computer are enabled to allow full email extensions to be viewed.

If you discover you are the victim of a fraudulent incident, immediately contact your financial institution to request a recall of funds and your employer to report irregularities with payroll deposits

As soon as possible, file a complaint regardless of the amount with www.ic3.gov or, for BEC/EAC victims, BEC.IC3.gov.

---

1. Reference PSA 1-022118-PSA Increase in W-2 Phishing Campaigns
2. Exposed dollar loss includes actual and attempted loss in United States dollars
3. Reference PSA I-091818-PSA Cybercriminals Utilize Social Engineering Techniques to Obtain Employee Credentials to Conduct Payroll Diversion

April 06, 2020

Alert Number
I-040620-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

Cyber Criminals Conduct Business Email Compromise through Exploitation of Cloud-Based Email Services, Costing US Businesses More Than $2 Billion

Cyber criminals are targeting organizations that use popular cloud-based email services to conduct Business Email Compromise (BEC) scams. The scams are initiated through specifically developed phish kits designed to mimic the cloud-based email services in order to compromise business email accounts and request or misdirect transfers of funds. Between January 2014 and October 2019, the Internet Crime Complaint Center (IC3) received complaints totaling more than $2.1 billion in actual losses from BEC scams using two popular cloud-based email services. While most cloud-based email services have security features that can help prevent BEC, many of these features must be manually configured and enabled. Users can better protect themselves from BEC by taking advantage of the full spectrum of protections that are available.

DEFINITIONS

Cloud-based email services are hosted subscription services that enable users to conduct business via tools such as email, shared calendars, online file storage, and instant messaging.

Business Email Compromise is a sophisticated scam targeting businesses that perform electronic payments such as wire or automated clearing house transfers. The scam is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques resulting in an unauthorized transfer of funds.

BACKGROUND

Over the last decade, organizations have increasingly moved from on-site email systems to cloud-based email services. Losses from BEC scams overall have increased every year since IC3 began tracking the scam in 2013. BEC scams have been reported in all 50 states and in 177 countries. Small and medium-size organizations, or those with limited IT resources, are most vulnerable to BEC scams because of the costs of robust cyber defense.

THREAT

There are a number of BEC scam variants. One of the most effective types is initiated through phishing emails designed to steal email account credentials. Cyber criminals use phishing kits that impersonate

popular cloud-based email services. Many phishing kits identify the email service associated with each set of compromised credentials, allowing the cyber criminal to target victims using cloud-based services. Upon compromising victim email accounts, cyber criminals analyze the content of compromised email accounts for evidence of financial transactions. Often, the actors configure mailbox rules of a compromised account to delete key messages. They may also enable automatic forwarding to an outside email account.

Using the information gathered from compromised accounts, cyber criminals impersonate email communications between compromised businesses and third parties, such as vendors or customers, to request pending or future payments be redirected to fraudulent bank accounts. Cyber criminals frequently access the address books of compromised accounts as a means to identify new targets to send phishing emails. As a result, a successful email account compromise at one business can pivot to multiple victims within an industry.

Depending upon the provider, cloud-based email services may provide security features such as advanced phishing protection and multi-factor authentication that are either not enabled by default or are only available at additional cost.

RECOMMENDATIONS FOR END USERS

- Enable multi-factor authentication for all email accounts.
- Verify all payment changes and transactions in person or via a known telephone number.
- Educate employees about BEC scams, including preventative strategies such as how to identify phishing emails and how to respond to suspected compromises.

RECOMMENDATIONS FOR IT ADMINISTRATORS

- Prohibit automatic forwarding of email to external addresses.
- Add an email banner to messages coming from outside your organization.
- Prohibit legacy email protocols, such as POP, IMAP, and SMTP[1], that can be used to circumvent multi-factor authentication.
- Ensure changes to mailbox login and settings are logged and retained for at least 90 days.
- Enable alerts for suspicious activity, such as foreign logins.
- Enable security features that block malicious email, such as anti-phishing and anti-spoofing policies.
- Configure Sender Policy Framework, DomainKeys Identified Mail, and Domain-based Message Authentication Reporting and Conformance to prevent spoofing and validate email.
- Disable legacy account authentication.

WHAT TO DO IF YOU ARE A VICTIM

If you discover unauthorized payments, contact your financial institution immediately to request recall of the funds. Report attempted or actual fraudulent financial transfers to the Internet Crime Complaint Center at www.ic3.gov or to your local FBI field office, which can be found at www.fbi.gov/contact-us/field. The FBI may be able to assist financial institutions in the recovery of lost funds.

---

1. POP, IMAP and SMTP are the most commonly used email protocols that standardize the method for proper message transmittance.

Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

September 15, 2016

Alert Number
I-091516-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field

RANSOMWARE VICTIMS URGED TO REPORT INFECTIONS TO FEDERAL LAW ENFORCEMENT

The FBI urges victims to report ransomware incidents to federal law enforcement to help us gain a more comprehensive view of the current threat and its impact on U.S. victims.

What Is Ransomware?

Ransomware is a type of malware installed on a computer or server that encrypts the files, making them inaccessible until a specified ransom is paid. Ransomware is typically installed when a user clicks on a malicious link, opens a file in an e-mail that installs the malware, or through drive-by downloads (which does not require user-initiation) from a compromised Web site.

Why We Need Your Help

New ransomware variants are emerging regularly. Cyber security companies reported that in the first several months of 2016, global ransomware infections were at an all-time high. Within the first weeks of its release, one particular ransomware variant compromised an estimated 100,000 computers a day.

Ransomware infections impact individual users and businesses regardless of size or industry by causing service disruptions, financial loss, and in some cases, permanent loss of valuable data. While ransomware infection statistics are often highlighted in the media and by computer security companies, it has been challenging for the FBI to ascertain the true number of ransomware victims as many infections go unreported to law enforcement.

Victims may not report to law enforcement for a number of reasons, including concerns over not knowing where and to whom to report; not feeling their loss warrants law enforcement attention; concerns over privacy, business reputation, or regulatory data breach reporting requirements; or embarrassment. Additionally, those who resolve the issue internally either by paying the ransom or by restoring their files from back-ups may not feel a need to contact law enforcement.

The FBI is urging victims to report ransomware incidents regardless of the outcome. Victim reporting provides law enforcement with a greater understanding of the threat, provides justification for ransomware investigations, and contributes relevant information to ongoing ransomware cases. Knowing more about victims and their experiences with ransomware will help the FBI to determine who is behind the attacks and how they are identifying or targeting victims.

Threats to Users

All ransomware variants pose a threat to individual users and businesses. Recent variants have targeted and compromised vulnerable business servers (rather than individual users) to identify and target hosts, thereby multiplying the number of potential infected servers and devices on a network. Actors engaging in this targeting strategy are also charging ransoms based on the number of host (or servers) infected. Additionally, recent victims who have been infected with these types of ransomware variants have not been provided the decryption keys for all their files after paying the ransom, and some have been extorted for even more money after payment.

This recent technique of targeting host servers and systems could translate into victims paying more to get their decryption keys, a prolonged recovery time, and the possibility that victims will not obtain full decryption of their files.

What to Report to Law Enforcement

The FBI is requesting victims reach out to their local FBI office and/or file a complaint with the Internet Crime Complaint Center, at www.IC3.gov, with the following ransomware infection details (as applicable):

1. **Date of Infection**
2. **Ransomware Variant** (identified on the ransom page or by the encrypted file extension)
3. **Victim Company Information** (industry type, business size, etc.)
4. **How the Infection Occurred** (link in e-mail, browsing the Internet, etc.)
5. **Requested Ransom Amount**
6. **Actor's Bitcoin Wallet Address** (may be listed on the ransom page)
7. **Ransom Amount Paid** (if any)
8. **Overall Losses Associated with a Ransomware Infection** (including the ransom amount)
9. **Victim Impact Statement**

The Ransom

The FBI does not support paying a ransom to the adversary. Paying a ransom does not guarantee the victim will regain access to their data; in fact, some individuals or organizations are never provided with decryption keys after paying a ransom. Paying a ransom emboldens the adversary to target other victims for profit, and could provide incentive for other criminals to engage in similar illicit activities for financial gain. While the FBI does not support paying a ransom, it recognizes executives, when faced with inoperability issues, will evaluate all options to protect their shareholders, employees, and customers.

Defense

The FBI recommends users consider implementing the following prevention and continuity measures to lessen the risk of a successful ransomware attack.

- Regularly back up data and verify the integrity of those backups. Backups are critical in ransomware incidents; if you are infected, backups may be the best way to recover your critical data.
- Secure your backups. Ensure backups are not connected to the computers and networks they are backing up. Examples might include securing backups in the cloud or physically storing them offline. It should be noted, some instances of ransomware have the capability to lock cloud-based backups when systems continuously back up in real-time, also known as persistent synchronization.
- Scrutinize links contained in e-mails and do not open attachments included in unsolicited e-mails.
- Only download software – especially free software – from sites you know and trust. When possible, verify the integrity of the software through a digital signature prior to execution.
- Ensure application patches for the operating system, software, and firmware are up to date, including Adobe Flash, Java, Web browsers, etc.
- Ensure anti-virus and anti-malware solutions are set to automatically update and regular scans are conducted.
- Disable macro scripts from files transmitted via e-mail. Consider using Office Viewer software to open Microsoft Office files transmitted via e-mail instead of full Office Suite applications.
- Implement software restrictions or other controls to prevent the execution of programs in common ransomware locations, such as temporary folders supporting popular Internet browsers, or compression/decompression programs, including those located in the AppData/LocalAppData folder.

Additional considerations for businesses include the following:

- Focus on awareness and training. Because end users are often targeted, employees should be made aware of the threat of ransomware, how it is delivered, and trained on information security principles and techniques.
- Patch all endpoint device operating systems, software, and firmware as vulnerabilities are discovered. This precaution can be made easier through a centralized patch management system.
- Manage the use of privileged accounts by implementing the principle of least privilege. No users should be assigned administrative access unless absolutely needed. Those with a need for administrator accounts should

only use them when necessary; they should operate with standard user accounts at all other times.

- Configure access controls with least privilege in mind. If a user only needs to read specific files, he or she should not have write access to those files, directories, or shares.
- Use virtualized environments to execute operating system environments or specific programs.
- Categorize data based on organizational value, and implement physical/logical separation of networks and data for different organizational units. For example, sensitive research or business data should not reside on the same server and/or network segment as an organization's e-mail environment.
- Require user interaction for end user applications communicating with Web sites uncategorized by the network proxy or firewall. Examples include requiring users to type in information or enter a password when the system communicates with an uncategorized Web site.
- Implement application whitelisting. Only allow systems to execute programs known and permitted by security policy.

Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

October 02, 2019

Alert Number
I-100219-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

High-Impact Ransomware Attacks Threaten U.S. Businesses And Organizations

This Public Service Announcement (PSA) is an update and companion to Ransomware PSA I-091516-PSA posted on www.ic3.gov. This PSA contains updated information about the ransomware threat.

WHAT IS RANSOMWARE?

Ransomware is a form of malware that encrypts files on a victim's computer or server, making them unusable. Cyber criminals demand a ransom in exchange for providing a key to decrypt the victim's files.

Ransomware attacks are becoming more targeted, sophisticated, and costly, even as the overall frequency of attacks remains consistent. Since early 2018, the incidence of broad, indiscriminant ransomware campaigns has sharply declined, but the losses from ransomware attacks have increased significantly, according to complaints received by IC3 and FBI case information.

Although state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector.

HOW DOES RANSOMWARE INFECT ITS VICTIMS?

Cyber criminals use a variety of techniques to infect victim systems with ransomware. Cyber criminals upgrade and change their techniques to make their attacks more effective and to prevent detection.

The FBI has observed cyber criminals using the following techniques to infect victims with ransomware:

- Email phishing campaigns: The cyber criminal sends an email containing a malicious file or link, which deploys malware when clicked by a recipient. Cyber criminals historically used generic, broad-based spamming strategies to deploy their malware, while recent ransomware campaigns have been more targeted. Criminals may also compromise a victim's email account by using precursor malware, which enables the cyber criminal to use a victim's email account to further spread the infection.
- Remote Desktop Protocol vulnerabilities: RDP is a proprietary network protocol that allows individuals to control the resources and data of a computer over the internet. Cyber criminals have used both brute-force methods, a technique using trial-and-error to obtain user credentials, and credentials purchased on darknet marketplaces to gain unauthorized RDP access to victim systems. Once they have RDP access, criminals can deploy a range of malware—including ransomware—to victim systems.
- Software vulnerabilities: Cyber criminals can take advantage of security weaknesses in widely used software programs to gain control of victim systems and deploy ransomware. For example, cyber criminals recently exploited vulnerabilities in two remote management tools used by managed service providers (MSPs) to deploy ransomware on the networks of customers of at least three MSPs.

IF MY SYSTEM IS INFECTED, SHOULD I PAY THE RANSOM? SHOULD I CONTACT THE FBI?

The FBI does not advocate paying a ransom, in part because it does not guarantee an organization will regain access to its data. In some cases, victims who paid a ransom were never provided with decryption keys. In addition, due to flaws in the encryption algorithms of certain malware variants, victims may not be able to recover some or all of their data even with a valid decryption key.

Paying ransoms emboldens criminals to target other organizations and provides an alluring and lucrative enterprise to other criminals. However, the FBI understands that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers.

Regardless of whether you or your organization have decided to pay the ransom, the FBI urges you to report ransomware incidents to law enforcement. Doing so provides investigators with the critical information

they need to track ransomware attackers, hold them accountable under U.S. law, and prevent future attacks.

HOW CAN I PROTECT MYSELF AGAINST RANSOMWARE?

The most important defense for any organization against ransomware is a robust system of backups. Having a recent backup to restore from could prevent a ransomware attack from crippling your organization. The time to invest in backups and other cyber defenses is *before* an attacker strikes, not afterward when it may be too late.

As ransomware techniques and malware continue to evolve and become more sophisticated, even the most robust prevention controls are no guarantee against exploitation. This makes contingency and remediation planning crucial to business recovery and continuity. Those plans should be tested regularly to ensure the integrity of sensitive data in the event of a compromise.

CYBER DEFENSE BEST PRACTICES

- Regularly back up data and verify its integrity. Ensure backups are not connected to the computers and networks they are backing up. For example, physically store them offline. Backups are critical in ransomware; if you are infected, backups may be the best way to recover your critical data.
- Focus on awareness and training. Since end users are targeted, employees should be made aware of the threat of ransomware and how it is delivered, and trained on information security principles and techniques.
- Patch the operating system, software, and firmware on devices. All endpoints should be patched as vulnerabilities are discovered. This can be made easier through a centralized patch management system.
- Ensure anti-virus and anti-malware solutions are set to automatically update and that regular scans are conducted.
- Implement the least privilege for file, directory, and network share permissions. If a user only needs to read specific files, they should not have write-access to those files, directories, or shares. Configure access controls with least privilege in mind.
- Disable macro scripts from Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Office Suite applications.
- Implement software restriction policies or other controls to prevent the execution of programs in common ransomware locations, such as temporary folders supporting popular internet browsers, and compression/decompression programs, including those located in the AppData/LocalAppData folder.
- Employ best practices for use of RDP, including auditing your network for systems using RDP, closing unused RDP ports, applying two-factor authentication wherever possible, and logging RDP login attempts.
- Implement application whitelisting. Only allow systems to execute programs known and permitted by security policy.
- Use virtualized environments to execute operating system environments or specific programs.
- Categorize data based on organizational value, and implement physical and logical separation of networks and data for different organizational units. For example, sensitive research or business data should not reside on the same server and network segment as an organization’s email environment.
- Require user interaction for end-user applications communicating with websites uncategorized by the network proxy or firewall. For example, require users to type information or enter a password when their system communicates with a website uncategorized by the proxy or firewall.

RANSOMWARE

What It Is & What To Do About It

What is Ransomware?

Ransomware is a type of malicious software, or malware, that encrypts data on a computer making it unusable. A malicious cyber criminal holds the data hostage until the ransom is paid. If the ransom is not paid, the victim's data remains unavailable. Cyber criminals may also pressure victims to pay the ransom by threatening to destroy the victim's data or to release it to the public.

Government Efforts to Combat Ransomware

While ransomware attacks impact all sectors, the federal government is particularly concerned about the impact of ransomware on the networks of state, local, tribal, and territorial governments, municipalities, police and fire departments, hospitals, and other critical infrastructure. These types of attacks can delay a police or fire department's response to an emergency or prevent a hospital from accessing lifesaving equipment. To combat this threat, the NCIJTF has convened an interagency group of subject matter experts to educate the public on ways to prevent ransomware attacks, to improve law enforcement coordination and response, and to enable and sequence whole-of-government actions that impose consequences against the criminals engaged in this malicious activity. The Cybersecurity and Infrastructure Security Agency (CISA) leads a number of efforts including —CISA Cyber Essentials—and—CISA Insights— to assist entities in protecting themselves from cyber incidents like ransomware. More about these efforts and the tools CISA offers can be found at https://www.cisa.gov/ransomware. The FBI's IC3.gov website has additional ransomware focused resources that can be found at https://ic3.gov/Home/Ransomware.

Common Infection Vectors

Although cyber criminals use a variety of techniques to infect victims with ransomware, the most common means of infection are:

- Email phishing campaigns: The cyber criminal sends an email containing a malicious file or link, which deploys malware when clicked by a recipient. Cyber criminals historically have used generic, broad-based spamming strategies to deploy their malware, though recent ransomware campaigns have been more targeted and sophisticated. Criminals may also compromise a victim's email account by using precursor malware, which enables the cyber criminal to use a victim's email account to further spread the infection.

- Remote Desktop Protocol (RDP) vulnerabilities: RDP is a proprietary network protocol that allows individuals to control the resources and data of a computer over the internet. Cyber criminals have used both brute-force methods, a technique using trial-and-error to obtain user credentials, and credentials purchased on dark web market - places to gain unauthorized RDP access to victim systems. Once they have RDP access, criminals can deploy a range of malware—including ransomware—to victim systems.

- Software vulnerabilities: Cyber criminals can take advantage of security weaknesses in widely used software programs to gain control of victim systems and deploy ransomware.

RANSOMWARE

What It Is & What To Do About It

Best Practices To Minimize Ransomware Risks

1. Backup your data, system images, and configurations, test your backups, and keep the backups offline
2. Utilize multi-factor authentication
3. Update and patch systems
4. Make sure your security solutions are up to date
5. Review and exercise your incident response plan

How Ransomware Has Impacted The Public Sector

The examples below may show the impacts in terms of ransom paid or service restoration cost, but it is difficult to calculate the total impact/costs of a ransomware infection. In addition, paying a ransom does not guarantee that stolen sensitive data will not be sold on the dark web.

- A U.S. county was infected by Ryuk, taking almost all of the county's systems offline. The county had backup servers, but they were not isolated from the network, allowing them to be infected as well. The county paid a $132,000 ransom.

- A U.S. city's systems were infected by Robbinhood with a ransom demand of 13 Bitcoins ($76,000). The attackers entered the network through old, out-of-date hardware and software. The ransom was not paid, but service restoration was estimated to cost over $9 million.

- A U.S. county's computer systems were infected by Ryuk. The attackers demanded over $1.2 million in Bitcoin for a decryption key. Officials decided to rebuild their systems rather than pay the ransom and spent $1 million in new equipment and technical assistance. A user allegedly opened a malicious link or attachment which caused the infection.

Reporting Information

- The FBI does not encourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Paying the ransom also does not guarantee that a victim's files will be recovered. Regardless of whether you or your organization have decided to pay the ransom, the FBI urges you to report ransomware incidents to your local field office or the FBI's Internet Crime Complaint Center (IC3). Doing so provides investigators with the critical information they need to track ransomware attackers, hold them accountable under U.S. law, and prevent future attacks.

Victims of ransomware can file a complaint with law enforcement or report incidents by:

- **Contacting your local federal law enforcement field office**
- **Filing a complaint with the Internet Crime Complaint Center (IC3)** https://ic3.gov/Home/Ransomware
- **Contacting NCIJTF CyWatch 24/7 support at 1-855-292-3937**
- **Reporting incidents, phishing, malware or vulnerabilities with CISA** https://us-cert.cisa.gov/report