Fraud Advisory for **Businesses**: Corporate Account Take Over
Updated April 2012

This advisory 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:
Employees and businesses of all sizes are being targeted by cyber thieves though phishing and other social engineering[1] attacks to entice them to download and spread malware through their company's networks. This then allows the cyber thieves unauthorized access to financial accounts and other sensitive information, resulting in significant business disruption and substantial monetary losses due to fraudulent transfers from these accounts. Often these funds may not be recovered[2].

N.Y. Firm Faces Bankruptcy from $164,000 E-Banking Loss

European Cyber-Gangs Target Small U.S. Firms, Group Says

e-Banking Bandits Stole $465,000 From Calif. Escrow Firm

La. firm sues [bank] after losing thousands in online bank fraud

Cyber attackers empty business accounts in minutes

Zeus hackers could steal corporate secrets too

TEXAS FIRM BLAMES BANK FOR $50,000 CYBER HEIST

Computer Crooks Steal $100,000 from Ill. Town

FBI Investigating Theft of $500,000 from NY School District

Zeus Botnet Thriving Despite Arrests in the US, UK

[1] Social engineering is the use of manipulation and deceit to obtain personal of confidential information or convince someone to perform an action they might not normally perform.
[2] 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.

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

Cyber thieves target employees– often senior executives or accounting and HR personnel[3]- and business partners[4] and cause the targeted individual to spread malicious software (or "malware") which in turn steals their personal information and log-in credentials. Once the account is compromised, the cyber thief is able to electronically steal money from business accounts.

Cyber thieves 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; and/or
- initiate other changes to the account.

In addition to targeting account information, cyber thieves 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 the types of companies targeted and the technologies and techniques employed by cyber thieves. Where cyber thieves 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.[5] 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.

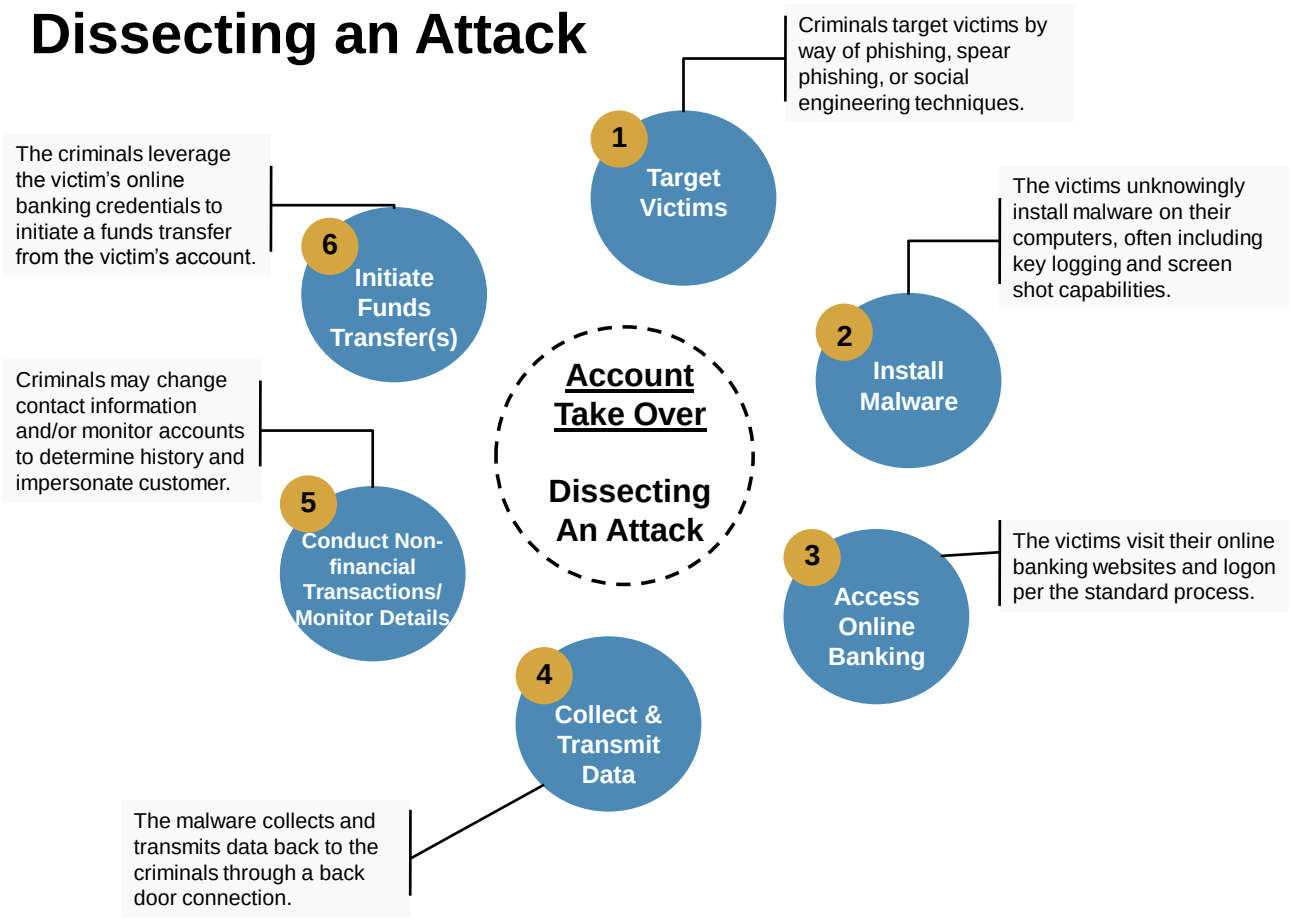
It is very important to note that as the cyber thieves change their techniques, businesses must continue to improve their knowledge of and security posture against these attacks. In addition, the tips and recommendations contained in this advisory may help reduce the likelihood of fraud, but they should not be expected to provide complete protection against these attacks.

[3] *Any* employee is vulnerable to being targeted.
[4] Business partners can include, among other third parties, contractors and accountants.
[5] 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.

How it's Done:
The cyber thief's goal is to get an employee to download malware onto their 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.

Figure 2: Dissecting An Account Take Over Attack

Cyber thieves 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).



They 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[6]. For example, cyber thieves often send employees unsolicited emails that:

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

- 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 thieves 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 thieves will employ some type of scare tactic to entice the employee to open the email and/or provide account information. For example, cyber thieves 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.")

- Claiming the emails contain information about money transfers or remittances received.

- 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.

- 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.

Other ways that an employee may unknowingly infect their business computers with malware, can include:

- Visiting legitimate websites – especially social networking sites – and clicking on infected documents, videos or photos posted there;
- Accepting fake friend requests;
- Using a flash drive that was infected by another computer;
- Moving a cursor over an infected page or pop-up, launching a drive by download; and/or
- Downloading infected "scareware"[7]

How to Protect, Detect, and Respond to Corporate Account Take Over Fraud

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.

[7] Scareware is malicious software that poses as legitimate computer security software and purports to detect a variety of threats on the affected computer that do not actually exist. Users are then informed they must purchase what they are told is anti-virus software in order to repair their computers. The users are then barraged with aggressive and disruptive notifications until they supply their credit card number and pay for the worthless "anti-virus" product. The product is, in fact, fake. (Source: Feb. 2011 FBI Advisory, "Scareware Distributors Targeted"

- 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.
- Educate your employees about the dangers of providing and sharing personal and sensitive information among social and business networking sites. Providing details of their position could make them a target of a spear-phishing attack by cybercriminals hoping to gain access to the systems they support or the functions they perform.
- 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[8]

- 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[9].
- 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.
- 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[10], Vista[11], and 7 Data Execution Prevention (DEP)[12] and disabling auto run commands[13]. You may also consider disabling JavaScript in Adobe Reader[14]. 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.

[8] See the "Resources" section for links to helpful and detailed tips on how to enhance your information technology (IT) security.
[9] A dedicated computer is a single computer, either within a network, or a standalone that is uniquely and specifically reserved for a single source of transaction, function or communication with the bank. The isolation can be achieved through operational or technical means. An example of operational means is restricting the computer's communications from the time of initial set-up to only the services/functions for receiving software security updates and communicating with the bank. Examples of technical means are secure web browsers, bootable CDs or jump drives, and other techniques that effectively sandbox the bank communication(s), or do not rely on the native operating system and software for bank communication(s), functions or transactions.
[10] How to configure memory protection in Windows XP SP2; http://technet.microsoft.com/en-us/library/cc700810.aspx
[11] Change Data Execution Prevention Settings; http://windows.microsoft.com/en-US/windows-vista/Change-Data-Execution-Prevention-settings
[12] Change Data Execution Prevention Settings; http://windows.microsoft.com/en-US/windows7/Change-Data-Execution-Prevention-settings
[13] How to disable the Autorun functionality in Windows: http://support.microsoft.com/kb/967715/
[14] Disabling JavaScript in Adobe Reader and Acrobat; http://blogs.adobe.com/psirt/2009/04/update_on_adobe_reader_issue.html

- 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)[15].
- 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.
   - 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**
   - There may be different protections offered for business accounts versus consumer accounts. Familiarize yourself with your institution's account agreement and understand the protections offered to your business account**.** 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), if your business accepts credit or debit 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.

[15] A VPN uses the public telecommunication infrastructure and the Internet to provide remote and secure access to an organization's network.

8. **Pay attention to warnings**
    - Your anti-malware 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.
    - 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[16]
- OnGuardOnline.gov
- Internet Crime Complaint Center (IC3)[17]
- Department of Homeland Security Cyber Report[18]
- National Cyber Security Alliance Stay Safe Online[19]
- Better Business Bureau- Data Security Made Simpler[20]
- Microsoft Security Page[21]
- U.S. Chamber of Commerce's Internet Security Essentials for Small Business[22]
- Federal Communications Commission's (FCC) Small Biz Cyber Planner[23] and 10 Cybersecurity Strategies for Small Business tip sheet[24]

[16] http://www.ftc.gov/bcp/menus/consumer/tech/privacy.shtm
[17] 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.
[18] http://www.cyber.st.dhs.gov/
[19] http://www.staysafeonline.org/
[20] http://www.bbb.org/data-security/
[21] http://www.microsoft.com/security/default.aspx
[22] http://www.uschamber.com/issues/technology/internet-security-essentials-business
[23] http://www.fcc.gov/cyberplanner
[24] http://www.uschamber.com/sites/default/files/issues/defense/files/10_CYBER_Strategies_for_Small_Biz.pdf