Security - Understanding Corporate Takeovers

An Important Security Notice

Corporate account takeover is the business equivalent of personal identity theft. Hackers, backed by professional criminal organizations are targeting small and medium businesses to obtain access to their web banking credentials or remove controls of their computers. These backers will then drain the deposit and credit lines of the compromised bank accounts, funneling the funds through mules that quickly redirect the monies overseas into backer accounts. A computer can be infected very easily by visiting an infected website or by simply opening an email. There has been a steady increase in account takeovers lately. resulting in billions of dollars in damage. We encourage all businesses to learn about this cybercrime and how to prevent it.

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).

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. 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. Federal Reserve (e.g., “The outgoing wire transaction was cancelled...")
2. UPS (e.g., "There has been a problem with your shipment.")
3. Financial institutions (e.g., "There is a problem with your banking account.")
4. Better Business Bureaus (e.g., "A complaint has been filed against you.")
5. Court systems (e.g., "You have been served a subpoena.")
6. IRS (e.g., "Federal Tax transaction canceled.")
7. Federal Trade Commission (FTC) (e.g., "...to inform you of an existing complaint against your company")
8. NACHA (e.g., "ACH payment rejected")

Other known tactics include:

- Making emails 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.

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

- 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.
- Install online protection created specifically to protect log in credentials and bank account information.
- Install and maintain real-time anti-virus and anti-spyware desktop firewall and malware detection and removal software. Use these tools to 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 XP7, Vista, and Data Execution Prevention (DEP)9 and disabling auto run commands. You may also consider disabling JavaScript in Adobe Reader. 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).
- Keep abreast of the continuous cyber threats that occur.

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.
- Periodically, or as new information becomes available, perform a risk assessment and controls evaluation for activities with a higher risk profile such as wire transfer or ACH transactions. The risk assessment should lead to appropriate changes where necessary.

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 stop 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 and 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

The tips included here are designed to reduce the risk of Corporate Account Takeover. No amount of risk mitigation can eliminate it completely. For additional resources related to Corporate Account Takeover Prevention, contact the Federal Trade Commission (FTC), the Better Business Bureau or the Small Business Administration (SBA) website on Protecting and Securing Customer Information. Other resources may be available online.