Corporate Account Takeover

Corporate Account Takeover is a type of business identity theft in which a criminal entity steals a business's valid online banking credentials. Small to mid-sized businesses remain the primary target of criminals, but any business can fall victim to these crimes.

Attacks today are typically perpetrated quietly by the introduction of malware through a simple email or infected website. For a business that has low resistance to such methods of attack, the malware introduced onto its system may remain undetected for weeks or even months.

Introducing layered security processes and procedures, technological and otherwise, and other tightened security efforts, can help protect businesses from criminals seeking to drain accounts and steal confidential information. These increased security procedures may help reduce the number of incidents, and mitigate financial losses, business risks and reputational damage that can result from such attacks.

The sound business practices outlined in this web page are not meant to be adopted as exclusive approaches businesses should implement to address risks associated with Corporate Account Takeover, nor are they meant to be considered mandatory. Implementing some or all of the items in this web page are not a guarantee that a business will not fall victim to a Corporate Account Takeover, but they will aid in making such a criminal effort much more difficult and less appealing to the criminal. No single security measure alone is likely to be effective in preventing or mitigating all risks associated with Corporate Account Takeover. Similarly, some of these sound business practices may not be appropriate for or applicable to all businesses. Accordingly, each business must identify its own risks and design and implement appropriate security measures to prevent and mitigate risks associated with Corporate Account Takeover.

The sound business practices for entities outlined in this web page include:

Computer Security

- Layered System Security
- Online Banking Safety
- Education
- Websites
- User Accounts
- Staying Informed

Account Security

- Dual Control
- Reconcilement
- Account Services
- Reporting Suspicious Activity
- Credentials

Sound Business Practices

Each business should evaluate its risk profile with regard to Corporate Account Takeover and develop and implement a Risk Assessment, including sound business practices to prevent and mitigate risk. Such a plan should consider the unique circumstances of the business. However, in developing the plan each business should consider the following sound business practices, which are recommended in most cases, and any other sound business practices identified in the business' environment.

Computer Security

Layered System Security

It is recommended that a business:

- Use appropriate tools to prevent and deter unauthorized access to its network and periodically review such tools to ensure they are up to date. These tools include:
    - ✓ Firewall
    - ✓ Security suite
    - ✓ Anti-botnet, anti-malware, and anti-spyware programs
    - ✓ Encryption of laptops, hard drives, VPNs and/or other communication channels
    - ✓ Education of all computer users regarding appropriate internet usage
- Install robust anti-virus and security software for all computer workstations and laptops and ensure that such software is automatically patched regularly and remains current.
- Implement multi-layered system security technology. Anti-virus software alone will not protect a business from most threats. Layering security software constructs a multi-level barrier between businesses' networks and criminals attempting to access such networks.
- Implement security suites so all security options (i.e., firewall, anti-virus, anti-spyware, anti-malware, etc.) work harmoniously to provide superior protection.

Online Banking Safety

It is recommended that a business:

- Create a secure financial environment by dedicating one computer exclusively for online banking and cash management activity. This computer should not be connected to the business network, have email capability, or connect to the Internet for any purpose other than online banking.
- Disallow a workstation used for online banking to be used for general Web browsing and social networking.
- Verify use of a secure session ("https") in the browser for all online banking activity.
- Disallow online banking activities from free Wi-Fi hot spots, like airports and Internet cafes.
- Cease all online banking activity if the online banking application appears different or questionable. Do not continue and contact the appropriate financial institution immediately.

Education

It is recommended that a business:

- Educate all employees about cybercrimes so they understand that even one infected computer can lead to an account takeover. An employee whose computer becomes infected can in turn infect the entire network. For example, if an employee takes a laptop home and accidentally downloads credential-stealing malware, criminals could gain access to the business's entire network when the employee connects again at work. All employees, even those with no financial responsibilities, should be educated about these threats.
- Educate all employees to think critically about each email and phone call received. An employee should always ask "Does this email or phone call make sense?" A business should advise its employees to:

Not open suspicious emails or emails from unknown persons. Even opening an email may expose a computer and the network to malware.

Ask, "Does this make sense?" before taking action in response to an email. If an email is suspicious, do not click on a link or open an attachment. The link could navigate the employee to an infected website or download a malware program. Likewise, attachments and zip files (compressed files) can contain malware. Employees should be instructed to delete the suspicious email and not click a link or open an attachment. The business can also utilize a domain lookup service, such as "whois.net" or a similar

service that allows employees to view the domain registration information of an email sender. If employees do not stop to think and take appropriate action, criminals may be able to lure unsuspecting employees into actions that infect their computers.

Be particularly suspicious of emails or calls purporting to be from a financial institution, government agency or other organization requesting account information, account verification or banking access credentials such as usernames, passwords, Personal Identification Numbers (PINs) and similar information. If such a suspicious email or call is received, the business should call the financial institution or agency to verify legitimacy. The business should not call the phone number included in the email, or click on the link or reply to the sender of such an email. Note that financial institutions and government agencies will not ask customers for login credentials.

Websites:
It is recommended that a business:

- Block access to unnecessary or high-risk websites. At a minimum, a business should prevent access to websites that employees should not visit on work computers. Common sites that carry high-risk include adult entertainment, online gaming, social networking and personal email.
- Promptly deactivate or remove access rights of employees who no longer require access (e.g., inactive, transferred or terminated employees).
- Require all employees to use strong passwords and change their passwords frequently on both the computer and online banking application.
- In some cases a business may determine it is appropriate to utilize a “white-listing” tool to limit employees’ access to only websites that the business has reviewed and deemed safe.

User Accounts
It is recommended that a business:

- Establish user accounts for every computer and limit administrative rights. Many malware programs require the user to have network administration privileges to infect the computer.
- Employ “user” settings to avoid unintentionally downloading a credential-stealing program. Many small and mid-sized businesses allow all employees to be the network administrator of their computers. Often malware requires the user to be logged in as the network administrator for the malicious program to download.
- Take full advantage of options offered by financial institutions to reduce the risk of a large payment being initiated fraudulently. Many financial institutions allow customers to set a “user limit” for ACH and wire transfer initiation via their online banking portal.

Staying Informed
It is recommended that a business:

- Stay informed about defenses to Corporate Account Takeover. Since cyber threats change rapidly, it is imperative that all businesses stay informed about evolving threats and adjust security measures in a timely manner. Among other things, this can be achieved by connecting with alert groups, and business and industry resources about threats and frauds
- Block access to unnecessary or high-risk websites. At a minimum, a business should prevent access to websites that employees should not visit during work hours. Common sites that carry high-risk include adult entertainment, online gaming, social networking and personal email

Account Security

Dual Control
It is recommended that a business:

- Initiate payments under dual control, with assigned responsibility for transaction origination and authorization. Dual control involves file creation by one employee with file approval and release by another employee on a different computer. Avoid having employees initiate and authorize payment transactions with administrator credentials.

Reconcilement
It is recommended that a business:

- Reconcile accounts online daily. At a minimum, pending or recently sent ACH files and wire transfers should be reviewed.

Account Services
It is recommended that a business:

- Take advantage of appropriate account services offered by its financial institution. Financial institutions offer a variety of services including positive pay, debit blocks, call-backs, etc. Financial institutions should be consulted to identify what security services are offered.

Reporting Suspicious Activity
It is recommended that a business:

- Monitor for and report suspicious activity. Ongoing monitoring and timely reporting of suspicious activity are crucial in deterring or recovering from these frauds. A business should report anything unusual to the financial institution, such as log-ins at unusual times of day, new user accounts, unauthorized transfers, etc., so the financial institution can immediately block the account and monitor activity.

Credentials
It is recommended that a business:

- Not use administrator credentials issued by its financial institution for day-to-day processing. Criminals use compromised administrator rights to create new user accounts to facilitate the generation of fraudulent transactions. The criminals can even use the administrator credentials to lock legitimate employees out of the system.

Warning Signs of a Potential Compromise

Warning Signs of a potentially compromised system include (but are not necessarily limited to):

- Inability to log into online banking (thieves could be blocking customer access so the customer will not see the theft until the criminals have control of the money)
- Dramatic loss of computer speed
- Changes in the way things appear on the screen
- Computer locks up so the user is unable to perform any functions
- Unexpected rebooting or restarting of the computer
- Unexpected request for a one time password (or token) in the middle of an online session
- Unusual pop-up messages, especially a message in the middle of a session that says the connection to the bank system is not working (e.g. system unavailable, down for maintenance, etc.)
- New or unexpected toolbars and/or icons
- Inability to shut down or restart a computer

If you notice anything suspicious

- Review all accounts regularly to detect unauthorized activity.
- Notify Bank OZK at (800) 274-4482 immediately if you suspect that your Login ID or Password has become known to any unauthorized person.
- Immediately change all passwords associated with the online account.
- Disconnect from the internet all computers used for Online Banking.
- Request a temporary hold on all other transactions until verbal confirmation is obtained.
- Work with appropriate computer forensic specialist and law enforcement to review impacted equipment.
- If at any time you have questions regarding security or possible fraud, please contact our customer service representatives at (800) 274-4482 or via email at info@ozk.com.

Additional resources available to business account holders:

1. The Better Business Bureau's website on Data Security Made Simpler:
http://www.bbb.org/data-security
2. The Federal Trade Commission's (FTC) interactive business guide for protecting data:
http://www.ftc.gov/bcp/edu/multimedia/interactive/infosecurity/index.html
3. The National Institute of Standards and Technology's (NIST) Fundamentals of Information Security for Small Businesses:
http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf
4. The jointly issued "Fraud Advisory for Businesses: Corporate Account Takeover" from the U.S. Secret Service, FBI, IC3, and FS-ISAC available on the IC3 website.
http://www.ic3.gov/media/2010/CorporateAccountTakeOver.pdf
5. NACHA – The Electronic Payments Association:
https://www.nacha.org/c/Corporate_Account_Takeover_Resource_Center.cfm