CORPORATE ACCOUNT TAKEOVER

What is it? Corporate Account Takeover, or CATO, is the business equivalent of identity theft and is a growing threat to businesses of all sizes and industries. Businesses with limited computer security, such as small businesses, are especially vulnerable to CATO.

How does CATO occur? Cyber thieves commonly use malware to steal online banking credentials or hijack login sessions. Malware can be downloaded from an internet site or email by clicking on infected links or attachments. Criminals use the malware to capture your user IDs and passwords, giving them access to fraudulently transfer funds from your accounts.

How can you prevent CATO? CATO losses are not covered by Regulation E and are generally the responsibility of the account owner. We encourage all our business customers to take steps to protect themselves against CATO. A business' employees are the first line of defense. All your employees should be educated about the threat of CATO, particularly those with access to your financial information. Consider implementing some or all the following best practices* and proactive steps to assist you and your employees protect your business' financial information:

Computer/Network Best Practices

- Protect your computers with strong passwords.
- Use a dedicated computer for online banking activity that is not also used for email or other internet use.
- Turn off the computer when not in use.
- Change the default login passwords on all devices.
- Install a firewall to help limit unauthorized access to the network and/or computer.
- Use a current internet browser and pop-up blocker.
- Perform browser and operating system updates and install security patches regularly.
- Install and update internet security software (e.g. anti-virus, anti-spyware, malware detection, etc).
- Consider utilizing an IT professional to install, configure and maintain your computers, network, firewall, and internet security software.

Behavioral Best Practices

- Be wary of unsolicited emails or pop-up messages.
- Do not open unknown attachments or hyperlinks.
- Be suspicious of emails claiming to be from Citizens Bank or any financial institution requesting sensitive information such as account numbers, user names, passwords, etc.
- Do not provide sensitive information to unknown parties via phone, email, or an unfamiliar website, including credit/debit card numbers, passwords, PINs, or other personal data.
- Watch for unexpected online activity, such as being prompted for a token-generated, one-time password.
- Note changes to PC performance, unusual login delays, and new or unusual icons or toolbars.
- Do not use public internet access points (e.g. internet cafes, public Wi-Fi hotspots, etc.) for online banking.
- Never leave a computer unattended while using any online banking service.
- Avoid using automatic login features for business online banking.
- Stay informed and train your staff about internet fraud scams.

Online Banking Best Practices

- Review banking transactions on a daily basis. Verify all online financial transactions.
- Regularly reconcile your bank statements and review credit reports.
- Require dual-authorization for high-risk transactions such as wire transfers, ACH, and online bill pay.
- Request that access to your internet banking account be restricted to business hours and/or to specific IP addresses, if available from the provider
- Establish company or employee transfer limits.
- Regularly review employee access permissions.

What are the Warning Signs of a Compromised Computer?

- Dramatic loss of computer speed or locking up
- Changes in the way things appear on the screen
- Unexpected request for a token or pass-code in the middle of an online session
- Unexpected rebooting or restarting
- Unusual pop-up messages, especially a message in the middle of an online banking session that says the connection to the bank system is not working
- New or unexpected toolbars and/or icons
- Virus protection software will not run or update
- Inability to shut down or restart the computer

What if my accounts may have been compromised? If you suspect that your business account is a victim of CATO, be proactive and follow the steps below:

- Immediately cease all activity on the compromised computer. Disconnect the network connections to isolate the computer from Internet access.
- Immediately contact us at (270) 298-7429 to report that you may be a victim of Corporate Account Takeover. Our staff will assist you with the following:
  - Disable online access to all accounts.
  - Change online banking passwords.
  - Open new account(s) as appropriate.
  - Assist with a review of all recent transactions.
  - Ensure there are no unauthorized address changes, re-ordered checks, ordered debit cards, etc.
- Maintain a written chronology of what happened, what was lost, and steps taken to report the incident to the various agencies, banks, and companies impacted. Be sure to record the date, time, and telephone number, contact person, instructions received, and reference numbers, if any.
- File a police report, providing the facts and circumstances about the loss. Obtain a copy of the police report with the date, time, department, location and officer's name taking the report or involved in a subsequent investigation. Having a police report on file facilitates communicating with insurance companies, banks, and other businesses that may be the recipients of the fraudulent activity. The police report may instigate an investigation into the loss with the goal of identifying, arresting and prosecuting the offender and possibly recovering losses.

Looking for more information? The following resources can assist in educating you and your employees.

- Better Business Bureau's Data Security Made Simpler: http://www.bbb.org/datasecurity
- Small Business Administration's Protecting and Securing Customer Information: http://community.sba.gov/community/blogs/community-blogs/business-law-advisor/how-smallbusinesses-can-protect-andsecure-customer-information;
- Federal Trade Commission's interactive business guide for protecting data: http://www.ftc.gov/bcp/edu/multimedia/interactive/infosecurity/index.html;
- 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;
- "Fraud Advisory for Businesses: Corporate Account Takeover" from US Secret Service, FBI, IC3, & FS-ISAC: http://www.ic3.gov/media/2010/CorporateAccountTakeOver.pdf or http://www.fsisac.com/files/public/db/p265.pdf; and
- NACHA – The Electronic Payments Association's numerous articles regarding CATO for banks and banking customers: http://www.nacha.org/c/Corporate_Account_Takeover_Resource_Center.cfm.

** This document is for informational purposes in order to promote business online banking customer awareness and is not intended to provide legal advice. The best practices included within this document are not an exhaustive list of actions and security threats change constantly. Risk assessments should be done regularly to address the changing cyber threat landscape as it relates to your business.*