Corporate Account Takeover (CATO) Guide

- **What is Corporate Account Takeover?**

  Corporate account takeover occurs when a criminal obtains electronic access to your bank account and conducts unauthorized transactions. The criminal obtains electronic access by stealing the confidential security credentials of employees who are authorized to conduct electronic transactions on your corporate bank account.

- **How are confidential security credentials stolen?**

  There are several methods being employed to steal confidential security credentials. One is to mimic the look and feel of a legitimate financial institution's website. Users provide their credentials to these sites without knowing that a perpetrator is stealing their security credentials through a fictitious website which appears to be their financial institution.

  A second method is malware that infects computer workstations and laptops via infected emails with links or document attachments. In addition, malware can be downloaded to a user's workstation and laptop from legitimate websites, especially social networking sites. Clicking on the documents, videos or photos posted there can activate the download of the malware. The malware installs key-logging software on the computer, which allows the perpetrator to capture the user's ID and password as they are entered at the financial institution's website.

  Other viruses are more sophisticated. They alert the perpetrator when the legitimate user has logged onto a financial institution's website, then trick the user into thinking the system is down, or not responding during this perceived downtime, the perpetrator is actually sending transactions in the user's name.

- **What does Corporate Account Takeover look like?**

  If robust authentication is not used and a user's credentials are stolen, the perpetrator can take over the account of the business. To the financial institution, the credentials appear to be the legitimate user. The perpetrator has access to and can review the account details of the business, including account activity and patterns and ACH and wire transfer origination parameters such as file size and frequency limits and Standard Entry Class (SEC) codes.

  With an understanding of the permissions and the limits associated with the account, the perpetrator can transfer funds out of the account using wire transfers or ACH files. With ACH, the file would likely contain PPD (Prearranged Payments & Deposits) credits routed to accounts at one or more receiving depository financial institutions (RDFI's). These accounts may be newly opened by accomplices or unwitting "mules" for the express purpose of receiving and laundering these funds. The accomplices or mules withdraw the entire balances shortly after receiving the money and send the funds overseas via wire transfer or other popular money transfer services.

  Perpetrators also send ACH files containing debits in order to collect additional funds into the account that can subsequently be transferred out. The debits would likely be CCD (Cash Concentration & Disbursement) debits to other small business accounts for which the perpetrator has also stolen the credentials or banking information. Given the return timeframe for CCD debits and the relative lack of account monitoring and controls at many small businesses, these debit transactions often go unnoticed until after the return timeframe has expired.

Warning signs of potentially compromised computer system:

- Dramatic loss of computer speed
- Changes in the way things appear on the screen
- Computer locks up or freezes
- Unexpected rebooting or restarting
- Unexpected request for a token pass-code in the middle of an online session
- 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 (system unavailable, down for maintenance, etc)
- New or unexpected toolbars and/or icons
- Inability to shut down or restart the computer

Best practices for safe business online banking:

- Reconcile banking transactions on a daily basis
- Utilize separation of duties when initiating ACH transfers- one person originates the transaction on one computer and another person approves the transaction on another computer
- Immediately report suspicious transactions to Community State Bank of Orbisonia by calling 866-874-5552
- Install a firewall to help limit unauthorized access to the network and/or computer
- Install anti-virus software on all computer systems
- Do not download "Free versions" of anti-virus programs. Free versions do not provide "real-time" protections
- Ensure that computers are patched regularly, particularly operating systems and key applications
- Install anti-spyware/anti-malware software and update them often
- Be suspicious of Emails purporting to be from the bank or any financial institution requesting account information, account verification or online banking credentials such as user names, passwords, token codes, and similar information
- Create strong passwords and do not use online banking passwords for other sites
- Change the default login passwords on all network devices
- Limit administrative rights on users' workstations
- Carry out all online banking activities from a stand-alone computer system- that is, one that is not used for Email and general web browsing/social networking
- Avoid using automatic login features that save usernames and passwords for online banking
- Never leave a computer unattended while using any online banking service
- Never access bank, brokerage or other financial services information at Wi-Fi hot spots such as internet cafes, public libraries, airports, etc. Unauthorized software may have been installed to trap account number and login information leaving open the possibility of fraud

What to do if you are a victim of Corporate Account Takeover (CATO)

1. Immediately cease all activity from computer systems that may be compromised. Disconnect the Ethernet cable or other network connections to isolate the computer from its Internet access.
2. Immediately contact Community State Bank of Orbisonia stating that you believe that you are a victim of Corporate Account Takeover (CATO). Request assistance with the following actions:
    a) Disable online access to accounts
    b) Change online banking passwords
    c) Open new account(s) as appropriate
    d) Request that the bank's security officer and auditor review all recent transactions and electronic authorizations on the account(s)
    e) Ensure that no one has requested an address change, re-ordered checks, ordered debit cards, etc. to be sent to a different address
3. Maintain a written chronology of what happened, what was lost and the steps taken to report the incident to the various agencies, banks, and firms impacted. Be sure to record the date, time, and telephone number, person spoken to, and any relevant report or reference number and instructions.
4. 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 facilitate dealing with insurance companies, banks, and other establishments that may be the recipient of fraudulent activity. The police report may initiate a law enforcement investigation into the loss with the goal of identifying, arresting and prosecuting the offender and possibly recovering losses.

Small Business Information Security

For additional information on information security, navigate your browser to the link below. This guide was published by the National Institute of Standards and Technology (NIST). The guide identifies recommend practices to improve information security in small businesses.

http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf

March 2014