Fraud Prevention - Guidance for Business Banking Customers

Best practices for safe business online banking:

- Use online banking to reconcile transactions on a daily basis
- Report suspicious transactions to the bank immediately
- Employ Dual Control for processing ACH and/or wire transfer transactions (one person originates/saves the transaction and another person approves/processes the transaction using a different login and different computer, if possible)
- Install a firewall, anti-virus and anti-spyware/anti-malware software on all computer systems and update software regularly
- Change vendor-supplied defaults/passwords when installing systems on your network and remove unnecessary applications
- Ensure that computers are updated regularly, particularly operating systems and key applications
- Be suspicious of Emails purporting to be from the bank or any financial institution requesting account information, verification of account or online banking credentials such as user names, passwords, token codes, and similar information
- Create strong passwords and do not use your business online banking password for other sites
- Use a stand-alone computer, if possible, for business online banking - one that is not used for email and web browsing
- Avoid using automatic login features that save usernames and passwords
- Set and review system alerts, such as minimum balance, debit posted, profile information or password changed
- Never leave a computer unattended while logged in to online banking
- Never access bank or other financial services information at Internet cafes, public libraries, airports, etc.
- Purchase insurance against electronic banking fraud

Educate and monitor your employees:

- Review best practices with all employees who have access to online banking
- Limit administrative rights on users' workstations
- Prohibit the use of "shared" usernames and passwords
- Delete online Access IDs when employees leave your company
- If employees use mobile devices for business, require them to password protect their devices and install security apps
- Caution employees against acting on unusual email requests for ACH or wire transfer transactions that appear to be from management

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 passcode 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

Suggestions for what to do if you are a victim of Corporate Account Takeover (CATO)

1. Immediately disable internet access and cease all activity from computer systems that may be compromised

2. Immediately contact the bank to report the suspected compromise. Request assistance with the following:
    - Change online banking passwords or disable online access until compromise is resolved
    - Request that the bank review all recent transactions and electronic authorizations on the account(s)
    - Ensure that no one has requested an address change, re-ordered checks, ordered debit cards, etc.
    - Open new account(s) as appropriate

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. Arrange for a forensic investigation of your computer network to determine the extent of compromise and steps needed to prevent further incidents.

5. 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 similar fraudulent activity.