WHAT IS CORPORATE ACCOUNT TAKEOVER?

Corporate Account Takeover, or CATO, was first identified in 2005 and is a type of business identity theft. It typically involves the exploitation of businesses of all sizes, especially those with limited to no computer safeguards. Malware may be utilized to infect a business account holder's computer to steal online banking credentials in order to impersonate the business and send unauthorized wire and/or ACH transactions to accounts controlled by the cyber thieves. This type of cyber-crime is a technologically advanced form of electronic theft.

Warning signs visible to a business or consumer customer that their system/network may have compromised include:

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

Resources for Business Account Holders

1. The Better Business Bureau's website on Data Security Made Simpler: http://www.bbb.org/datasecurity;
2. The Small Business Administration's (SBA) website on Protecting and Securing Customer Information: http://community.sba.gov/community/blogs/community-blogs/business-law-advisor/how-smallbusinesses-can-protect-and-secure-customer-information;
3. The Federal Trade Commission's (FTC) interactive business guide for protecting data: http://www.ftc.gov/bcp/edu/multimedia/interactive/infosecurity/index.html;
4. 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;
5. 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) or the FS-ISAC website (http://www.fsisac.com/files/public/db/p265.pdf); and
6. NACHA – The Electronic Payments Association's website has numerous articles regarding Corporate Account Takeover for both financial institutions and banking customers: http://www.nacha.org/c/Corporate_Account_Takeover_Resource_Center.cfm .

Examples of Deceptive Ways Criminals Contact Account Holders

1. The FDIC does **not** directly contact bank customers (especially related to ACH and Wire transactions, account suspension, or security alerts), nor does the FDIC request bank customers to install software upgrades. Such messages should be treated as fraudulent and the account holder should permanently delete them and not click on any links.
2. Messages or inquiries from the Internal Revenue Service, Better Business Bureau, NACHA, and almost any other organization asking the customer to install software, provide account information or access credentials is probably fraudulent and should be verified before any files are opened, software is installed, or information is provided.
3. Phone calls and text messages requesting sensitive information are likely fraudulent. If in doubt, account holders should contact the organization at the phone number the customer obtained from a different source (such as the number they have on file, that is on their most recent statement, or that is from the organization’s website). Account holders should not call phone numbers (even with local prefixes) that are listed in the suspicious email or text message.