How to Protect Your Business Account from Corporate Account Takeover

What is it?

Corporate Account Takeover (CATO) is defined as a form of commercial identity theft. Cyber thieves gain control of a business's bank account by stealing employee passwords and other sensitive credentials. Thieves can initiate fraudulent wire and ACH transactions into accounts they control.

What does this mean to you?

Businesses across the country have suffered large financial losses from electronic crimes through the banking system. The losses range from a few thousand to several million dollars. They have occurred in financial institutions of all sizes and locations.

What can you do to protect your account?

Be vigilant monitoring account activity. You have the ability to detect anomalies or potential fraud prior to or early into an electronic robbery.

Warning signs that may indicate your system/network may have been compromised include:

- Inability to log into online banking (thieves could be blocking your access so you won't see the theft until the criminals have control of your money);
- Dramatic loss of computer speed;
- Changes in the way things appear on the screen;
- Computer locks up so you are 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 credit union system is not working (system unavailable, down for maintenance, etc.);
- New or unexpected toolbars and/or icons; and
- Inability to shut down or restart the computer.

Other examples of deceptive criminal activity

Regulators do **not** directly contact financial institution customers (especially related to ACH and Wire transactions, account suspension, or security alerts), nor do regulators request financial institution 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.

How do you protect your account from cyber-crime?

As a business owner, it is important to have basic online security practices in place. Below are things you should consider:

- Do you provide continuous communication and education to employees using online banking systems - providing enhanced security awareness training will help ensure employees understand the security risks related to their duties;
- Do you update anti-virus and anti-malware programs frequently - update, on a regular basis, all computer software to protect against new security vulnerabilities (patch management practices);
- Do you communicate to employees that passwords should be strong and should not be stored on the device used to access online banking?
- Do you adhere to dual control procedures?
- Do you use separate devices to originate and transmit wire/ACH instructions?
- Do you transmit wire transfer and ACH instructions via a dedicated and isolated device10?
- Do you practice ongoing account monitoring and reconciliation, especially near the end of the day?
- Do you adopt advanced security measures by working with consultants or dedicated IT staff; and utilize resources provided by trade organizations and agencies that specialize in helping small businesses?

What do you do if you suspect a transaction?

Since each business is unique, you are urged to create your own Incident Response Plan. Your template should include:

- ✓ Direct contact information for credit union employees who can assist you (including after hours);
- ✓ Steps to limit further unauthorized online transactions:
  Change passwords, disconnect computers used for internet banking and request a temporary hold on all other transactions;

- ✓ Gather all the information you have surrounding the unauthorized activity, including names of all employees who have password and computer access;
- ✓ Contact your insurance carrier;
- ✓ Consider working with computer forensic specialists and law enforcement to review equipment.

Resources

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; 30 minute online course - http://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses
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 .

Information security laws and standards affecting business owners

Although financial institutions are not responsible for ensuring their account holders comply with information security laws, by making you aware of consequences for non-compliance if the information is breached may encourage you to maintain stronger security. Breaches of credit and debit card information from retail businesses are common. Therefore, the loss of that information or sensitive personal information can create financial and reputational risk for your business.

It is critical that you safeguard your customers' information. If you accept credit or debit cards, you can learn more at https://www.pcisecuritystandards.org/security_standards/index.php. As a business owner, noncompliance may lead to lawsuits, cancelled accounts and monetary fines.