CORPORATE ACCOUNT TAKEOVER

Protecting your business account is very important to CODE Credit Union. That is why we have measures in place to thwart cyber thieves. This includes the ability to set up sub-users on Access24 allowing only specific privileges when logging on to the business account. Online criminals however are using increasingly sophisticated techniques to commit fraud against business accounts.

A shared responsibility between CODE and your business is the most effective way to prevent corporate account takeover. Therefore we are providing the following information to keep you abreast of trends and best practices to protect your CODE business account.

What Is Corporate Account Takeover?

Corporate Account Takeover (CATO) is a type of fraud where cyber-thieves gain access to a business' finances to make unauthorized transactions. These may include transferring funds from the company, creating and adding new fake employees to payroll, and stealing sensitive customer information that may not be recoverable.

Several methods are being employed to infect a business. The most prevalent is malware via infected documents attached to e-mails or links that connect to an infected web site. Even by visiting legitimate websites - especially social networking sites - and clicking on documents, videos or photos malware can infect laptops and users workstations.

Malware can capture keystrokes, enabling criminals to view user names and passwords thus allowing them to impersonate the business in online banking sessions. To the financial institution, the credentials look just like the legitimate user. The perpetrator has access to and can review the account details of the business including account activity along with ACH and wire transfer origination parameters. The cyber-thieves then use this information to initiate funds transfers, by ACH or wire transfer to the bank accounts of associates for the express purpose of receiving and laundering funds.

Small to Medium Sized Businesses, as well as Non-profits are being targeted as they –

- Do not monitor and reconcile their accounts frequently or daily
- Have the capability to initiate funds transfers such as ACH credits and wire transfers
- Do not have a high level of firewalls and monitoring systems

Protecting Your Business Begins with Taking Proactive Steps

- Ensure the most current version of your anti-virus/spyware is installed and is functional
- Install patches regularly
- Choose complex passwords and change them regularly
- Review account transaction history frequently, daily if possible
- Immediately report any suspicious transactions to your financial institution
- Log-off or turn off computers when not in use or unattended
- Use a dedicated computer for financial transactional activity. DO NOT use this computer for general web browsing and email

Recommendations for Corporate Account Takeover Victims

1. Immediately cease activity from computer systems that may be compromised. Disconnect the Ethernet or other network connections to isolate the system from remote access.
2. Immediately contact CODE and request assistance with the following actions:
    - Disable online access to accounts
    - Change online banking passwords
    - Open new account(s) as appropriate
    - Request CODE's agent review all recent transactions and electronic authorizations on the account.
    - Ensure that no one has requested an address change, title change, PIN change or ordered new cards, checks or other account documents be sent to another 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, contact phone number, person spoken to, and any relevant report or reference number and instructions.
4. File a police report and obtain the report number with the date, time, location and officer's name taking the report or involved in the investigation. Having a police report will often facilitate in working with insurance companies and financial institutions. It may also initiate a law enforcement investigation into the loss with the goal of identifying, arresting and prosecuting the offender and possibly recovering losses.

This is provided for informational purposes and is not intended to provide legal advice. The guidance included is not an exhaustive list of actions as security threats change constantly.

In the event of fraud or suspicious activity
please contact CODE Credit Union immediately at 937-222-8971.