WHAT IS CORPORATE ACCOUNT TAKEOVER?

Corporate Account Takeover (also referred to as CATO) is a type of fraud where criminals gain access to a business' financial accounts to make unauthorized transactions. These types of transactions can include transferring funds from the company, creating and adding new fake employees to payroll, and stealing sensitive customer information that may not be recoverable. Online account takeovers occur when cyber criminals gain access to and/or control of a business' online banking account by stealing employee login credentials. The stolen credentials are then used to initiate fraudulent ACH and wire transactions to accounts controlled by the criminals.

HOW DOES IT HAPPEN?

Cyber criminals will use a number of varying technical and non-technical methods to deceive a user into divulging personal or account/login information. These techniques could include convincing an employee to open a malicious email attachment, accepting a fake friend request on a social networking site, or directing them to a compromised website that installs malicious software on their computer(s).

Cyber criminals will often "phish" for victims using mass emails or phone calls, pop-up messages that appear on their computers, and the use of social networking and internet career sites. For example, cyber criminals often send employees unsolicited emails that:

1. Ask for personal or account / login information;
2. Direct the employee to click on a malicious link provided in the email; and/or
3. Contain attachments that are infected with malware.

Cyber criminals use various methods to trick employees into opening the attachment or clicking on the link, including:

1. Disguising the email to look as though it's from a legitimate business. Often criminals will employ some type of scare tactic to entice the employee to open the email and / or provide account information. For example, cyber criminals have sent emails claiming to be from:
    a. UPS (e.g., "There has been a problem with your shipment.")
    b. Financial institutions (e.g., "There is a problem with your bank account.")
    c. Better Business Bureaus (e.g., "A complaint has been filed against you.")
    d. Court systems (e.g., "You have been served a subpoena.")
2. Making emails appear to provide information regarding current events such as natural disasters, sporting events, and celebrity news to entice employees to open emails and click on links.
3. Using email addresses or other credentials stolen from company websites or victims, such as relatives, coworkers, friends, or executives and designing an email to look like it is from a trusted source to entice employees to open emails and click on links.

The criminal's goal is to get the employee to open the infected attachment or click on a link within the email and visit a fraudulent (or otherwise compromised) website where hidden malware is downloaded to the employee's computer. This malware allows the criminal to see and track the employee's activities across the business' internal network and on the Internet. This tracking may include visits to your financial institution and use of your online banking credentials used to access accounts (account information, log in, and passwords). Using this information, the criminal can conduct unauthorized transactions that appear to be a legitimate transaction conducted by the company or employee.

WHAT TO DO IF YOU FEEL YOU HAVE BEEN COMPROMISED

Please notify us ASAP! Calling us is the best way of keeping any possible losses to a minimum:

- Phone: 906-774-2200
- Toll Free: 877-803-1814

RECOMMENDATIONS & BEST PRACTICES

The following security recommendations and best practices are provided for the safety and protection of your corporate online banking account(s) and confidential information.

A. Layered System Security – It is recommended that a business:

1) Use appropriate tools to prevent and deter unauthorized access to its network and periodically review such tools to ensure they are up-to-date. These tools include (but are not limited to):
    i. Firewalls
    ii. Anti-virus, anti-malware, and anti-spyware programs
    iii. Encryption of laptops, hard drives, VPN's or other communications channels
    iv. Education of all computer users
2) Install robust anti-virus and security software for all computer workstations and laptops and ensure that such software automatically is patched regularly and remains current.
3) Implement multi-layered system security technology. Anti-virus software, alone, will not protect a business from most threats. Layering security software and hardware constructs a multi-level barrier between business' networks and criminals attempting to access such networks.
4) Leverage existing online banking capability / controls for added security:
    i. ACH and Wire Transaction Limits, meaning each company and individual employee / user is limited to an established dollar amount for which they can authorize a transaction (*Required of Both Corporate & Business Online Banking Customers).
    ii. Dual Authorization of ACH and Wire Transactions, meaning two employees / users are required to authorize a transaction before it can be completed.
    iii. Positive Pay, a Cash Management service that matches checks presented for payment against a list of checks previously authorized by the issuing company (designed to deter check fraud).

B. Online Banking Workstations – It is recommended that a business:

1) Create a secure financial environment by dedicating one computer exclusively for online banking and cash management activity. This computer should NOT be connected to the business network, have email capability, or connect to the Internet for any purpose other than online banking.
2) NOT allow any workstation used for online banking to be used for general Web browsing, social networking or email.
3) Verify use of a secure internet browser session ("https") for all online banking.
4) Disallow the conduct of online banking activities from free Wi-Fi hot spots like airports or Internet cafes.

5) Cease all online banking activity if the online banking application 'looks' different than usual. Do not continue and contact the financial institution immediately.
6) Immediately cease all online activity if you detect malware or any suspicious activity, and remove any computers that may be compromised from the network:
    i. Disconnect the Ethernet cable and / or any other network connections (including wireless connections) to isolate the computer from the network & prevent unauthorized access.

C. User Education – It is recommended that a business:
1) Educate all computer users about cybercrimes so everyone understands that even one infected computer can lead to an account takeover.
    i. A user whose computer becomes infected can infect your entire network. For example, if an employee takes their laptop home and accidentally downloads credential-stealing malware, criminals could gain access to the business' entire network when the employee connects at work. All users, even those with no financial responsibilities, should be educated about these threats.
2) Always ask, "Does this email or phone call make sense?" The business should educate all of its employees to think critically about each email and phone call received. A business should advise its employees to:
    i. Not open suspicious emails or emails from unknown persons. Even opening an email may expose a computer and the network to malware.
    ii. Ask, "Does this make sense?" before taking action in response to an email. If an email is suspicious, do not click on any links in the message or open any attachments:
        a. Links can take users to an infected website or download a malware program. Likewise, attachments and .zip files (compressed files) can contain malware.
        b. Users should be instructed to simply delete the suspicious email and not to click links or open attachments. The business also can inquire of a domain lookup service like "whois.net" or similar service that allows users to view the domain registration information of an email sender.
        c. If the user does not stop to think and take appropriate action, criminals may be able to lure an unsuspecting user into an action that may infect their computer and jeopardize the business.
3) Be particularly suspicious of emails or calls purporting to be from a financial institution, government agency or other organization requesting account information, account verification or banking access credentials such as usernames, passwords, Personal Identification Numbers (PINs) and similar information. If such a suspicious email is identified or call received, the business should call the financial institution to verify legitimacy. The business should not call the phone number included in the email, click on any links or reply to the sender of such an email.

D. High Risk Websites – It is recommended that a business:
1) Block access to unnecessary or high-risk websites. At a minimum, a business should prevent access to websites that employees should not visit during work hours. Common sites that carry a high-risk are adult entertainment, online gaming, social networking, personal email, and web based file storage.

E. User Accounts – It is recommended that a business:
    1) Establish user accounts for every computer and limit administrative rights. Many malware programs require the user to have local or network administration privileges to infect the computer.
    2) Employ "user" settings to avoid accidentally downloading a credential-stealing program. Many small and mid-sized businesses allow all employees to be the local or network administrator of their computer. Most malware requires the user to be logged in as the administrator for the malicious program to download.
    3) Require all employees use strong passwords and change their passwords frequently on both the computer and online banking access.
    4) Promptly deactivate or remove access rights from employees that no longer require access (e.g., inactive, transferred, or terminated employees).
    5) Perform periodic (at least annual) reviews of online banking access and privileges to confirm each employee still requires such access as part of their job function.

HOW CAN FIRST NATIONAL BANK & TRUST HELP?

In an attempt to better help you protect your accounts and online activity, we have made a number of security features available to you. We have included a document for you titled "Cash Management Security Features Overview," which identifies each additional security feature available to you, as well as a detailed explanation of each.

Should you have questions about any of this, please do not hesitate to contact one of our customer service representatives. You can call us directly at:

- Phone: 906-774-2200
- Toll Free: 877-803-1814

If a phone call is not convenient for you, you can also reach out to us by submitting a 'Contact Us' form through our website at www.fnbimk.com

First National Bank & Trust

Cash Management Security Features Overview

Security Controls We Apply To All Accounts

The following security controls are applied to all accounts by default. These controls are required and cannot be disabled.

Multi-Factor Authentication

Multifactor authentication (MFA) is a process that requires more than one method of authentication to verify the user's identity for a login or other transaction. A username and password combination is used by default, but any abnormal login activity will trigger a secondary form of authentication. In the event of this scenario, you would be prompted to answer a series of challenge questions that you defined when your account was first established.

New User Held

Most cash management fraud follows the same pattern:

- Fraudster gains access using the Admin credentials obtained via malware, viruses, etc.
- Fraudster changes Admin's email address
- Fraudster creates a new cash management user and logs in
- Fraudster initiates fraudulent transactions as the newly created user

Using the *New User Held* feature prevents new and modified cash management users from logging in until the First National Bank & Trust first verifies their identity.

Transaction Limits

This option allows for maximum business-defined monetary limits to be set for NetTeller Cash Users. If this limit is exceeded the cash management transaction is "held" and not processed until the First National Bank & Trust reaches out to the authorized Cash User at your business to verify the transaction prior to processing.

Security Controls Recommended For All Accounts

The following security controls are optional, but highly recommended for all accounts. These controls can be enabled, disabled, or modified at any time.

IP Restrict

This option allows authorized First National Bank & Trust personnel to establish a series of valid IP addresses for each of your NetTeller Cash Users. If a user attempts to log in and the IP address in which they are logging in from does not match one of the established and trusted IP addresses, a customized message will appear indicating a failure to log in.

Cash Management Security Features Overview

Time Restrictions

This option allows authorized First National Bank & Trust personnel to establish a series of valid days of the week and/or times for each NetTeller Cash User. If a user attempts to log in outside of the enabled days/times, they are presented with a message indicating that they cannot log in.

Dual Control

This option prevents a single user from creating and then initiating or transmitting any ACH batch or wire transfer. One NetTeller Cash User will create the transaction, and another Cash User will approve the transaction. Only after the transaction receives the approval from the secondary user will it be submitted for processing.

Email Alerts

This option will auto-generate and send email correspondence to pre-defined email addresses regarding ACH or wire transaction activity. Within your online banking web session you can setup automated alerts that will notify of various activities. We have made available to you a number of alerts related to ACH and Wire transaction activity. By choosing to enroll in these alerts, you will be notified when each alert is activated through the e-mail address you have defined within your online banking account settings.