Corporate Account Takeover (CATO)

What is CATO (Corporate Account Takeover)?

Corporate account takeover is a type of identify fraud in which criminals steal valid online banking credentials and use those credentials to initiate money movement out of the account.

How to protect your business:

- **Reconcile Accounts Daily**
  - Immediately report suspicious or unknown transactions to Method Bank
- **Protect Your Online Environment**
  - Never open attachments or download files from unknown emails as they may have malware or viruses that could harm your computer
  - Always encrypt sensitive data and use strong passwords that require routine updating for all systems used
  - Install antivirus/anti-malware type software on all computer systems
    - Never download free versions of fraud detection software as these are not actively updated nor do they provide "real time" protection
  - Install firewalls to help limit unauthorized access to your business network
- **Best Practices for Online Banking**
  - Utilize separation of duties within your organization, dual controls for money movement transactions and other transactions deemed high risk
  - Never leave your online banking profile unattended while logged in
  - Avoid using automatic login features that are saved on your computer
  - Perform callbacks on wire / ACH instructions received through email
  - Setup online banking alerts that notify you or your team of any changes being made to online profiles
    - Address changed
    - Account balance below threshold
    - New debit card ordered
    - Email address changed
    - Phone number changed
    - Password changed
    - ACH initiated
    - Wire initiated
    - Many more offered

Tactics used by criminals to gain online access or steal credentials:

- Caller ID spoofing
- Phishing - type of scam that uses emails, text messages, phone calls to trick people into revealing personal information or to install malware
- Malware – malicious software installed by hackers used to disrupt a computer, network, or device
- Credential stuffing - hackers use many different combinations of usernames and passwords until they find one that works. When hackers use this method, it's likely due to the username and/or password being sold on the dark web or obtained from a data breach.

Resources for Business Owners and Staff:

(1.) The BBB**:** https://www.bbb.org/all/cyber-security-resources
(2.) The FTC (Federal Trade Commission): https://www.ftc.gov/business-guidance
(3.) NACHA, the electronic payments association: https://www.nacha.org/content/account-takeover
(4.) Ic3 for filing internet crime complaints: https://www.ic3.gov/
(5.) FFIEC's Cybersecurity Awareness: https://www.ffiec.gov/cybersecurity.htm

Cyber threats change rapidly, it's important that you stay informed, educate your staff, and create procedures that help protect your business.

If you believe your Method Bank account or online access has been compromised, contact us immediately at 469-887-6669 (Dallas branch) or 918-678-2204 (Wyandotte branch). You may also stop by one of our branch locations to discuss with a personal or business banker. It is crucial that we react quickly and implement controls to help mitigate potential losses.