PEOPLES BANK
"SINCE 1908"

MEMBER FDIC

CORPORATE ACCOUNT TAKEOVER (CATO)

What is CATO?

CATO is a type of fraud where thieves gain electronic access to a business bank accounts and conducts unauthorized transactions. The criminals gain electronic access by stealing confidential security credentials from employees who are authorized to conduct electronic transactions on business bank accounts. Losses from this cyber-crime can be substantial.

What are methods of CATO?

There are several methods being employed to steal confidential security credentials. Phishing mimics the look and feel of a legitimate financial institution's website, e-mail, or other communication. Users provide their credentials without knowing that a perpetrator is stealing their security credentials through a fictitious representation which appears to be their financial institution.

A second method is Malware that infects computer workstations and laptops via infected e-mails with links or document attachments. In addition, malware can be downloaded to a user's workstation or laptop from legitimate websites, especially social networking sites. Clicking on the documents, videos, or photos posted there can activate the download of malware. The malware installs key-logging software on the computer, which allows the perpetrator to capture the user's ID and password as they are entered at the financial institution's website. Other viruses are more sophisticated. They alert the perpetrator when the legitimate user has logged onto financial institutions website, then trick the user into thinking the system is down or not responding. During this perceived downtime, the perpetrator is actually sending transactions in the user's name.

Warning Signs of CATO

- Unusual business account activity
- Dramatic loss of computer speed
- Changes in the way things appear on screen
- Inability to shut down or restart computer
- Computer locks up so user is unable to perform any functions
- Unusual pop-up messages
- Unexpected rebooting or restarting of the computer

Best Practices

- Education for employees
- Secure your computer and networks
- Limit administrative rights
- Install and maintain Spam filters
- Install and maintain Anti-Virus and Anti-Spyware desktop firewall and malware detection and removal software
- Use strong password policies
- Monitor bank accounts daily
- Use multi-layer security

Resources for Businesses

1. The Better Business Bureau website on Data Security Made Simpler: www.bbb.org/data-security/
2. The small Business Administration's (SBA) website on Protecting and Securing Customer Information: http://www.sba.gov/community/blogs/community-blogs/business-law-advisor/how-small-businesses-can-protect-and-secure-cus
3. The Federal Trade Commission's (FTC) Interactive Business Guide for Protecting Data: http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf
4. The jointly-issued Fraud Advisory for Business: 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/Corporate_Account_Takeover_Resource_Center

Contact Peoples Bank if you:

- Suspect a fraudulent transaction
- If you receive an e-mail or phone call claiming to be from the bank and it is requesting personal/Company information

PEOPLES BANK WILL NEVER ASK FOR SENSITIVE INFORMATION, SUCH AS ACCOUNT NUMBERS, ACCESS IDS, OR PASSWORDS VIA E-MAIL.