PEOPLES BANK
"SINCE 1908"

MEMBER FDIC

CORPORATE ACCOUNT TAKEOVER (CATO)

What is CATO?

- Corporate account takeover is a type of fraud where thieves gain access to a business' finances to make unauthorized transactions, including transferring funds from the company, creating and adding new fake employees to payroll, and stealing sensitive customer information that may not be recoverable.

What are Methods of CATO?

- **Malware**
  - Malicious software designed to infiltrate a computer system without the owners informed consent. Ex. Viruses, Worms, Spyware, Dishonest Adware and most Rootkits
- **Phishing**
  - The fraudulent process of attempting to acquire sensitive information (usernames, passwords, card details etc..) by pretending to be a trustworthy entity in an electronic communication.

How to Identify Fraudulent Messages

- Email address does not match the name of the email sender.
- Poor grammar/punctuation
- Analyze the salutation. Is the email addressed to a vague "Valued Customer"?
- Hover your mouse over any links embedded in the body of the email. If the link address looks weird, don't click on it.
- Is the email asking for personal/account information? Legitimate banks and most other companies will never ask for personal credentials via email. Don't give them up.
- Beware of urgent or threatening language in the subject line. Invoking a sense of urgency or fear is a common phishing tactic.

Business Incident Response

Each business is unique, customers should write their own Incident Response Plan. Each plan should include:

1. Contact numbers for the bank
2. Steps the accountholder should consider to limit further unauthorized transactions, such as:
   - Changing passwords
   - Disconnecting computers used for Internet Banking
   - Request temporary holds on all other transactions and activity

How to Protect your Business

- Education is key. Train your employees
- Secure you computer networks
- Limit administrative rights
- Install and maintain Anti-Virus and Malware detection software
- Use strong password policies
- Monitor and reconcile bank accounts daily
- Use multi-layer security
- Block Pop-Ups

Contact the Bank

Contact IT Security Officer at Peoples Bank (318) 249-2125 if:

- You suspect a fraudulent transaction
- If you receive an e-mail or phone call from someone claiming to be from the bank and is requesting personal/account information

PEOPLES BANK WILL NEVER ASK FOR SENSITIVE INFORMATION, SUCH AS ACCOUNT NUMBERS, ACCESS IDs, OR PASSWORDS VIA-EMAIL.