Corporate Account Takeover

One risk that business customers should be aware of is called Corporate Account Takeover (CATO), a form of business identity theft where cyber thieves gain control of a business' bank account by stealing employee passwords and other valid credentials. Thieves can then initiate fraudulent wire and ACH transactions to accounts they control.

Businesses across the U.S. have suffered large financial losses from such electronic crimes. The vast majority of cyber thefts begin with the thieves compromising the computer(s) of the business account holders. To minimize the threat, businesses should establish processes and procedures to protect, detect, and respond to incidents of actual or suspected CATO.

The following guidelines are provided to help Peoples Bank's business customers better protect themselves when utilizing electronic banking activities. These guidelines are provided to increase awareness of the risks and how to better protect your business, detect potential incidents, and respond to recognized incidents. While Peoples Bank strongly encourages the implementation of these guidelines, it makes no representations or guarantees that the guidelines are all-inclusive or that they will actually prevent losses as a result of CATO. Peoples Bank encourages its business customers to seek the advice of legal counsel, IT staff, and other consultants in implementing safeguards against CATO.

Three Steps to Fight Back Against CATO

Protect

Business customers can help minimize the likelihood of a takeover or other security incident in their online banking activities by incorporating the following activities into regular business operations:

- Provide continuous communication and education to your employees that use online banking systems about good information security practices, including ensuring your employees understand the security risks related to their duties.
- Update your anti-virus and anti-malware programs frequently.
- Update, on a regular basis, all computer software to protect against new security vulnerabilities.
- Communicate to employees that passwords should be strong and should not be stored on the device used to access your online banking.
- Adhere to dual control procedures.
- Use dedicated and isolated devices to originate and transmit wire/ACH instructions.
- Adopt advanced security measures by working with security specialists.
- Use information provided by trade organizations and other agencies to help build an information security program. The Additional Resources section provides links to some of these resources.

Detect

Early detection of a security incident is key to minimizing losses. To help identify any unusual activity, account holders should monitor and reconcile account activity at least daily. In addition, account holders should be alert for red flags related to computer and network anomalies. These signs include, but are not limited to, the following:

- Inability to log in to online banking (thieves could be blocking customer access, so the customer won't see the theft until the criminals have control of the money)
- Dramatic loss of computer speed
- Changes in the way things appear on the screen
- Computer locks up so the user is unable to perform any functions
- Unexpected rebooting or restarting of the computer
- Unexpected request for a one time password (or token) in the middle of an online session
- Unusual pop-up messages, especially a message in the middle of a session that says the connection to the bank system is not working (system unavailable, down for maintenance, etc.)
- New or unexpected toolbars and/or icons
- Inability to shut down or restart the computer

Attackers may also attempt to contact account holders to obtain sensitive information or compromise your systems. Examples of these methods include, but are not limited to, the following:

- Attackers may send electronic messages or inquiries pretending to be from Peoples Bank, banking regulators such as the FDIC, or trade organizations. The messages may ask employees to install software or provide account information. These requests are likely fraudulent and should be verified before any files are opened, software is installed, or information is provided.
- Attackers may make phone calls and or send text messages requesting sensitive information. Peoples Bank will never call, e-mail, or text a customer for sensitive information such as User IDs and passwords. If in doubt, contact Peoples Bank at **270-692-6405** to reach a member or our Operations team. Account holders should not call phone numbers (even with local prefixes) that are listed in a suspicious e-mail or text message.

Respond

If an incident occurs, having established procedures within an Incident Response Plan can help minimize losses. Such a plan provides guidelines for employees to know what to do and who to contact for help. At a minimum, the plan should include:

- The direct contact numbers of key bank employees who can provide online banking support in the event of a compromise (including after hour numbers)
- Steps to limit further unauthorized transactions, such as:
- Changing passwords
- Disconnecting computers used for Internet Banking
- Requesting a temporary hold on all other transactions until out-of-band confirmations can be made
- Requirements for gathering and documenting information about what happened to assist the bank in its response to the compromise and to help in recovering funds
- Steps to contact your insurance carrier
- Procedures for working with computer forensic specialists and law enforcement personnel

Additional Resources

Here are additional resources to consider when developing an information security program:

- The Better Business Bureau's website at https://www.bbb.org/council/for-businesses/cybersecurity/
- The Federal Trade Commission website at https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security
- The Federal Trade Commission's website at https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security

Additional Information

Although implementing security controls for banking and customer information is a good business practice, there may be state, federal, or industry regulations or guidelines requiring specific controls or procedures to be in place. Businesses should ensure they are complying with such requirements.