Corporate Account Takeover
Customer Awareness & Education

Warning signs of potentially compromised computer system:

1. Dramatic loss of computer speed
2. Changes in the way things appear on the screen
3. Computer locks up or freezes leaving you unable to function
4. Unexpected rebooting or restarting
5. Unexpected request for a token pass-code in the middle of an online session
6. Unusual pop-up messages, especially a message in the middle of an online banking session that says the connection to the bank system is not working (system unavailable, try back later, down for maintenance, etc.)
7. New or unexpected toolbars and/or icons
8. Inability to shut down or restart the computer
9. Inability to log into online banking (criminals could be blocking access to your account online leaving you unable to see theft and/or fraudulent transactions and keeping them in control of your money)

Best practices for safe business online banking:

- Reconcile banking transactions on a daily basis
- Utilize separation of duties when initiating ACH and/or wire transfers- one person originates the transaction on one computer and another person approves the transaction on another computer
- Immediately report suspicious transactions to Lewisburg Banking Company by calling 270-755-4818 or 270-726-1270
- Install a firewall to help limit unauthorized access to the network and/or computer
- Install anti-virus software on all computer systems
- Do not download “Free versions” of anti-virus programs. Free versions do not provide “real-time” protections
- Ensure that computers are patched regularly, particularly operating systems and key applications
- Install anti-spyware/anti-malware software and update them often
- Be suspicious of Emails purporting to be from the bank or any financial institution requesting account information, account verification or online banking credentials such as user names, passwords, token codes, and similar information. While the institution may contact customers regarding an account or suspicious activities related to an account, institution should never contact customers to provide log-in credentials over the phone or via email.
- Create strong passwords and do not use your business online banking password for other sites

- Change the default login passwords on all network devices
- Limit administrative rights on users' workstations
- Carry out all business online banking activities from a stand-alone computer system- that is, one that is not used for Email and general web browsing and Facebook
- Avoid using automatic login features that save usernames and passwords for business online banking
- Never leave a computer unattended while using any online banking service
- Never access bank, brokerage or other financial services information at Internet cafes, public libraries, airports, etc. Unauthorized software may have been installed to trap account number and login information leaving open the possibility of fraud
- Purchase insurance against electronic banking fraud
- While the institution may contact customers regarding an account or suspicious activities related to an account, institution should never contact customers to provide log-in credentials over the phone or via email.

What to do if you are a victim of Corporate Account Takeover (CATO)

1. Immediately cease all activity from computer systems that may be compromised. Disconnect the Ethernet cable or other network connections to isolate the computer from its Internet access.
2. Immediately contact Lewisburg Banking Company, stating that you believe that you are a victim of Corporate Account Takeover (CATO). Request assistance with the following actions:
    a) Disable online access to accounts
    b) Change online banking passwords
    c) Open new account(s) as appropriate
    d) Request that the bank's security officer and auditor review all recent transactions and electronic authorizations on the account(s), including online bill pay
    e) Ensure that no one has requested an address change, re-ordered checks, ordered debit cards, etc. to be sent to a different address
3. Maintain a written chronology of what happened, what was lost and the steps taken to report the incident to the various agencies, banks, and firms impacted. Be sure to record the date, time, and telephone number, person spoken to, and any relevant report or reference number and instructions.
4. File a police report and provide the facts and circumstances surrounding the loss. Obtain a police report number with the date, time, department, location and officer's name taking the report or involved in the subsequent investigation. Having a police report on file will facilitate dealing with insurance companies, banks, and other establishments that may be the recipient of fraudulent activity. The police report may initiate a law enforcement investigation into the loss with the goal of identifying, arresting and prosecuting the offender and possibly recovering losses.

Small Business Information Security

For additional information on information security, navigate your browser to the link listed below. This guide was published by the National Institute of Standards and Technology (NIST). The guide identifies recommend practices to improve information security in small businesses.

http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf

Should you have any questions regarding Small Business Information Security or Corporate Account Takeover, please feel free to contact one of our representatives at Lewisburg Banking Company by calling 270-755-4818 or 270-726-1270 or visiting one of our office locations. We have staff in our Information Technology and Operations Departments dedicated to the security of your accounts.

Disclosure

This document is for informational purposes, in order to promote business online banking customer awareness and is not intended to provide legal advice. The best practices included within this document are not an exhaustive list of actions and security threats change constantly. Risk assessments should be done regularly to address the changing cyber threat landscape.