Minding Your Small Business

Reducing the Risk of Corporate Account Takeovers

Corporate Account Takeover is a type of business identity theft in which cyber thieves gain control of a business's bank account by stealing employee passwords and other valid credentials. Thieves can then initiate fraudulent ACH transactions.

Bank of Cave City has procedures in place to protect, detect and respond to corporate account takeover and fraudulent activity. However, it is important that you and your employees to follow established security practices. Security practices you can implement to reduce the risk of theft include:

1. Never access bank accounts at internet cafes or from public wi-fi hotspots.
2. Install commercial anti-virus, firewall software and anti-malware programs and update all frequently.
3. Teach employees to create strong passwords not to save them to the device used to access online banking. Provide continuous communication and education to employees using online banking systems. Providing enhanced security awareness training will help ensure employees understand the security risk related to their duties.
4. Adhere to dual control procedures. For example, one person to authorize the creation of the payment file and a second to authorize the release of the file.
5. Transmit wire transfer and ACH instructions via a dedicated and isolated device.
6. Monitor and reconcile accounts daily.
7. Create and implement advanced security measures by working with consultants or dedicated IT staff.
8. Use resources provided by trade organizations and agencies that specialize in helping small businesses, such as the Better Business Bureau.

Business account holders should be especially vigilant in daily monitoring of account activity. You have the ability to detect abnormal activity and/or potential fraud prior to or early in an electronic robbery.

Warning signs visible to a business customer that their system/network may have been compromised include:

1. Inability to log into online banking.
2. Dramatic loss of computer speed.
3. Changes in the way things appear on the screen.
4. Computer locks up so the user is unable to perform any functions
5. Unexpected rebooting or restarting of the computer
6. Unexpected request for a one time password (or token) in the middle of an online session
7. 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)
8. New or unexpected toolbars and/or icons.
9. Inability to shut down or restart the computer.

Other sources of info for small business computer security include:

1. 5 Steps to Better Business Cyber Security
2. The Small Business Administration's Cyber Security for Small Businesses Training Course
3. The Federal Trade Commission's Small Business Computer Security Basics

Please contact us should you have any questions regarding Corporate Account Takeover.