Online Security Best Practices for Businesses

Business customers of varying types and sizes who utilize online banking services for electronic transfers are potential targets of cyber thieves. It is important to understand basic security controls when managing your account online. Cyber criminals employ various methods to trick victims into divulging personal or account information. Such techniques may include:

- Using unsolicited emails, thieves can steal employee credentials (e.g., user name, password) and gain control of a business bank account. Thieves can then initiate fraudulent transactions from your bank account.
- Gaining access to a business' computer through malicious software ("malware") that collects and transmits data back to the criminal. One way malware can infect a computer is when a user clicks on a link or opens an attachment within an email from an unknown sender.

In an effort to minimize these risks, please consider the following online security best practices:

- Safeguard access IDs and passwords. Communicate to employees that passwords should be strong (more than 8 characters and a combination of upper and lower case letters, numbers and symbols) and should be securely stored.
- Do not click on links within emails or open attachments from unknown senders.
- Update anti-virus and anti-malware programs frequently.
- Update, on a regular basis, all computer software (e.g., Windows) to protect against new security vulnerabilities (This is also known as patch management).
- Practice ongoing account monitoring and reconciliation.
- Establish controls for conducting online transactions, including the creation of a "dual control" procedure. For example, one employee initiates transactions and another employee reconciles the account.
- Use separate computers to originate and transmit ACH transactions.

You have the ability to detect anomalies or potential fraud prior to, or early in an electronic robbery. Visible warning signs that your system may have been compromised include:

- Inability to log into online banking
- 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

If you notice anything suspicious, please contact the Bank immediately.

For more information, please contact:
Mechanics Bank Information Security Department @ 419-524-0831