Managing Your Electronic Banking

As the scale and sophistication of electronic banking cyber attacks increase, we must continue to educate and arm ourselves with the tools to minimize the possibility of fraudulent activities or account takeovers. Criminals are using technology to raid and drain bank accounts of their funds. Common examples include key logging, website hijacking and phishing, to name a few.

We must continue to work to identify and adapt to new and ever changing threats. We ask that you and your family, or your business, familiarize yourself with such threats and proactively implement measures to protect against these types of threats.

Please remember that MidSouth Bank will never ask for your personal information, your account information, your electronic banking user ID and password, or other electronic banking credentials by email or an unsolicited telephone call.

To help protect yourself against fraudulent activities we recommend implementing risk controls such as, but not limited to:

- Monitoring your account activity and statements on a regular basis
- Ensuring that your anti-virus and anti-malware software is current and your computers are scanned on a regular basis
- Ensuring that your computer's operating system software is current or properly 'patched'
- Using strong user IDs and passwords that include a combination of numbers, special characters and upper and lower case letters
- Safeguarding your user IDs and passwords
- Frequently changing your passwords

Our business customers should conduct periodic risk assessments and evaluations of their controls. The risk assessment should identify risks related to your electronic banking processes, for example:

- Is your network protected from outside threats?
- Is your computer's operating system software current and is your anti-virus and anti-malware software current?
- Is your password policy adequate?
- Are the proper checks and balances in place related to electronic banking?
- Are there delays in terminating system access of former employees?
- Have you considered the possibility of internal theft?

Member FDIC
EQUAL HOUSING LENDER

MidSouth Bank

Then strengthen or implement controls to mitigate the risks, for example:

- Using firewalls and intrusion detection monitoring to protect your network
- Implementing a program to manage your computer's operating system updates and your anti-virus and anti-malware updates
- Using a password policy that requires strong or complex passwords and frequent password changes
- Using dual controls or authorizations as a check and balance for electronic movement of funds
- Implementing a process to terminate system access of former employees
- Conducting employee background checks
- Conducting internal or third party audits of your controls

Federal regulations provide consumers (non personal or business accounts are not included in this regulation) with some protections related to electronic funds transfers. The regulations generally apply to electronic banking. These laws establish limits on the consumer's liability for unauthorized electronic funds transfers. These laws also define specific steps you need to take to help resolve an error with your account. Please note that in order to take advantage of these protections you must act in a timely manner and must notify us immediately. Please refer to the Electronic Funds Transfer Disclosure that you received when you opened your account. If you need additional copies we will be glad to provide them.

If you believe your account credentials have been stolen or compromised, notify us immediately, **MidSouth Bank at 888-440-7774.** Please contact us with any questions you may have regarding this information.

Thank you for banking with MidSouth Bank.

The most helpful bank in town.