MIDFIRST BANK Security Measures

Security Measures

MidFirst Bank is dedicated to protecting the financial information you entrust to us and helping protect you from identity theft. We employ a team of professionals dedicated to information security and they use a variety of techniques and processes.

General Website Security

The entire MidFirst Bank website uses a variety of techniques to keep your online banking secure. All of your communications are protected with strong encryption controls validated with digital certificates issued by Symantec. Our servers are constantly monitored, regularly updated, and protected with layers of controls to keep your information private.

The MidFirst Bank website uses a certificate issued by Symantec to validate the encryption system used for all communication. Another way to make sure you are on the MidFirst Bank website is to double-click the padlock icon. The certificate information should state that the certificate was issued by Symantec to www.midfirst.com.

MidFirst Bank regularly updates company systems as new threats emerge. We deploy a variety of protective technologies such as anti-virus, firewall, intrusion detection systems, and others. MidFirst Bank uses audit and other validation processes to ensure that systems are built and maintained securely.

For your safety, MidFirst Bank will never ask for personal information from an email.

Providing convenient and safe customer service is important to MidFirst Bank. Being able to access your account information 24 hours a day in a secure manner is our commitment to you.

Online Banking Security

MidFirst Bank's secure authentication technology adds a layer of security for your personal and financial information when you are banking online. You will create your username and password to use each time you log in to online banking.

Secure Sign-On Tips

- If identity verification is required, a brief process will allow us to verify your identity to help keep your accounts safe. You can choose to simply enter a temporary ID code received by your choice of phone call or text message, and as an alternative, you may answer several security questions.
- Maintain the confidentiality of your username and password
- Only access your accounts from a trusted computer running current anti-virus software
- You can use more than one computer or device to access your accounts; however, each time you log in from an unrecognized computer you may be prompted to verify your identity
- Do not use public computers to access your accounts
- Never write down your password and change it regularly
- Always log off your account when you are finished banking online
- For access to financial information, use different passwords than those for your more common uses, such as email
- Create a password that is at least eight characters in length and that you can remember without writing it down
- Passwords that have uppercase and lowercase letters, plus numbers, are more difficult for attackers to guess
- Do not use a password that contains easily found information, like a birthday, pet's name, mother's maiden name, etc.

Mobile Banking Security

MidFirst Bank's Mobile Banking has many built-in security features:

- Mobile Banking features secure authentication checks, including verifying your identity if your device is not recognized
- Mobile Banking requires "128-bit" encryption technology for all communications – communications are not allowed if a mobile device does not support this level of encryption
- Personal or financial information is retrieved only when requested and is not stored on your phone – information is not at risk if your phone is ever lost or stolen
- Mobile Banking will automatically log off after five minutes of inactivity to protect your information in case your phone is lost or stolen while a valid session is active
- MidFirst Bank will never ask for personal information such as passwords – if you receive a request for such information, immediately report it to MidFirst Bank

Mobile Banking Tips

- Lock your mobile device with a password
- Never share your personal or financial information in a text message, phone call or email
- Avoid storing your banking password or other sensitive information on your mobile device
- If you lose your mobile device or change your mobile number, sign in to online banking or call the MoneyLine at 888.MIDFIRST (643.3477) to remove the old number from your profile
- Keep your mobile operating system up to date to ensure the highest level of protection
- Keep the MidFirst Mobile Banking app up to date
- Always download apps from a reputable source
- Use an anti-virus software
- Do not store your login information on your mobile device
- Always keep a close account of your phone in public places

Debit and Credit Card Monitoring

MidFirst Bank utilizes a series of risk monitoring tools to combat the growing risk of debit and credit card fraud. Debit and credit card authorizations are passed through a series of rules to assess the risk potential of a transaction before it is approved, allowing certain transactions to be declined based on the likelihood of fraud. These risk-monitoring tools will typically target risky foreign transactions, foreign Internet transactions and domestic transactions outside the MidFirst Bank market area. If you are traveling, either domestically or internationally, it is important you notify us so we can provide you with optimal usage of your card. If you are planning to travel, please call us at 888.MIDFIRST (643.3477) for debit cards and 866.762.0492 for credit cards.

Learn more about Debit and Credit Card Security (/information-security/debit-and-credit-card-security)