Midland Federal
Savings and Loan Association

Below are some tips that will help you safely use our online banking system and protect your personal information.

Keep your user name and password secure.

Be sure to use a secure password for all of your financial accounts. Never use your pet's name, your child's name or anything else that could be easily found out. Combine letters, numbers, and special symbols (! # % & *). Be sure to change your password on a regular basis.

Never give your User ID or Password to anyone who is not an authorized accountholder.

Don't be tricked into giving your online banking or account information to anyone who is not a bank employee. As your financial institution, we take great care in safeguarding your personal and financial information. No one from Midland Federal will ever call or email you and ask you for any personally identifying information (i.e., your account number, your Social Security number, your online banking log-in credentials, etc.)

Beware of online scams!

Phishing is an attempt to obtain financial or other confidential information from Internet users, typically by sending an email that looks as if it is from a legitimate organization, usually a financial institution, but contains a link to a fake website that replicates the real one. In other words, an attacker might send an email that appears to be from a company that you do business with, such as Midland Federal. The email may ask you to reply with your personal information or ask you to go to a website (that looks like our website, but really isn't) and supply them with your user name, password, account number, Social Security number or other personal information.

Scammers might also contact you by text message or by telephone.

You may receive a text message from a phone number you don't recognize that says your bank account will be closed or frozen unless you respond with your personal and account information.

If you have any doubts about whether an email, phone call or text message is actually from us, **please call us immediately**.

If you receive a questionable phone call or text message that asks you to give or confirm your personal or account information or asks you to confirm, verify or update your account information, or an email that asks you to click on a link or go to a website & enter your personal information, **don't do it**. Contact us immediately and we will offer assistance on how to handle the situation.

You're almost certainly dealing with a scam when you see an email or website that does any of the following: asks you to provide your account information because someone wants to send you money; claims you have a refund coming to you; says that you've won a lottery or contest.

Midland Federal
Savings and Loan Association

Protect Yourself from Identity Theft

Identity theft continues to be one of the fastest growing crimes in the United States, and has ranked as one of the top consumer concerns for the past several years.

These crimes are evolving in more complicated ways that make it harder for consumers to protect themselves, and easier for criminals to set up virtual storefronts on the Internet to sell confidential personal information.

Be proactive - **look over your credit report at least once a year**. You can request a free annual credit report from each of the 3 major credit bureaus by visiting www.AnnualCreditReport.com or by calling 1-877-322-8228.

Check your credit report for inquiries from unfamiliar companies, accounts you never opened and unexplained debts. If you suspect that your personal information has been compromised, or that you have been a victim of identity theft, contact the 3 major credit bureaus and ask that a fraud alert be placed on your account.

If you notice that any unfamiliar accounts have been opened, contact the companies. Make sure to follow-up any telephone calls in writing. File a police report and keep a copy for your records.

For your convenience, here are the Fraud Victims' contact numbers for the 3 major credit bureaus:

Equifax: 1-800-525-6285
Experian: 1-888-397-3742
TransUnion: 1-800-680-7289

Regularly look over your transactions and statements to check for any unauthorized activity. It's important to monitor your account activity. **Contact us immediately** if you see a transaction that you did not authorize or do not recognize.

Please make sure that we have your up-to-date contact information. It is crucial that we are able to contact you if ever we notice any questionable activity on your account.

Make sure that your home computers and mobile devices have up-to-date anti-virus and firewall software installed on them. Use anti-virus software that removes or quarantines viruses and that updates itself automatically, and on a regular basis.

The FDIC has released a video that consumers can use to learn how to better protect their computers and themselves from identity thieves. It also features actions consumers can take if their personal information has been compromised.

Learn more by visiting fdic.gov.

To watch the FDIC's video on Protecting Yourself Online, visit https://www.youtube.com/watch?v=ANaypUUaeAc