

# Online Banking Security Bulletin



## Avoid the risk of identity theft and protect your account information.

The Internet offers the potential for safe, convenient ways to shop for financial services and conduct banking business, any day, any time. However, safe banking online involves making good choices – decisions that will help you avoid costly surprises or even scams.

As technology has improved significantly over the last decade, criminals have become proportionately smarter and savvier. This is especially true in the online world - the universe where crooks can hide behind e-mails, websites and fake personas. Unfortunately, these same criminals would like to find their way into your bank account.

Whether you are conducting online financial transactions over the Internet or simply "surfing," some easily implemented precautions can help safeguard your personal information from identity theft and account fraud:

- 🔒 **PASSWORDS**—Security begins with a strong password, which only you know. Experts advise using a combination of letters and numbers, and advise against using easily guessed passwords such as names, birthdays, etc.
- 🔒 **ANTI-VIRUS PROTECTION**—Make sure the anti-virus software on your computer is current and scans your email as it is received. This simple step is critical to your personal safety and security when online.
- 🔒 **EMAIL COMMUNICATION**—Email is generally not encrypted so be wary of sending any sensitive information such as account numbers or other personal information in this way. If you receive an unscheduled or unsolicited email purporting to be from your bank be cautious—take the time to call your bank and make sure the email is legitimate. *You bank will never ask you to verify account numbers or passwords via email.*
- 🔒 **SIGNING OFF**—Always log off after conducting online banking business to ensure the protection of your personal information.
- 🔒 **BE WARY**—Crooks are trying to get your personal information—and they employ some ingenious methods. Don't respond to any unusual requests for personal information. **When in doubt, call your bank.**

## Don't be fooled by impostors

One of the biggest risks in banking online is identity theft. Fraudsters send out emails that look like they come from banks (or other trusted organizations) and which contain links to fake websites which also resemble the real thing. These emails may appear to be from your bank but are really from criminals trying to lure you to a fake website to get your personal information.



Banks will never send you email asking you to disclose your PIN, passwords or other personal information or which link to a page that asks you for this kind of information. If you click on a link in an email that takes you to a page that requires a password or personal information, it is very likely to be a scam. Always make sure you are using a secure internet connection to connect to your bank. Look for 'https' at the beginning of the address and the padlock symbol.

**If you believe your details may have been compromised in some way, always contact the bank.**

## Use common sense!

- ▶ Learn your password and PIN. Destroy any written record as soon as you can. Don't write down your password or PIN.
- ▶ Use different passwords for bank and credit card sites. Don't use the same password for every website.
- ▶ Use strong passwords, comprised of letters & numbers.
- ▶ Set online banking alerts for login events and balance changes.
- ▶ Use extra caution when using public computers to access your bank accounts.
- ▶ Never give your personal security details, such as account number or PIN number, to someone you don't trust.
- ▶ Don't fall for money-laundering scams. Be wary of any 'business opportunity' that involves receiving or holding money for strangers.
- ▶ Keep tabs on your money. Review your bank statements regularly. If you spot any unusual transactions, report them immediately.

**Banking online is very convenient but you have to protect your password and personal details so criminals can't access your account in your name.**

When you travel the Internet to access online banking, you want to be assured, first and foremost, that effective safeguards are in place to make your visit safe, secure, and reliable. When you use Midland National Bank's online banking, you are entering a secure area. Measures Midland takes to protect your private information include:

**PASSWORD PROTECTION & PIN—**

Your password and PIN (personal identification number) are the first line of defense, and are your unique identifier. Be sure not to share them with anyone—most frauds involving hijacked accounts originate with someone the victim knows.

**MULTI-FACTOR AUTHENTICATION—**

This form of identity verification provides added security by requiring multiple forms of identification, such as something you know (password or PIN) and something you have (ATM card, browser cookie, etc).

**ENCRYPTION—**

Once online with Midland, your transactions and personal information are secured by encryption software that converts the information into code that is readable by only you and your bank.

**PRIVACY POLICIES—**

Midland National Bank's privacy policies protecting your personal information are stringent. Your confidential information is treated with the utmost care, meeting or exceeding federal and state mandates.



**IDENTIFYING THE MOST COMMON ONLINE THREATS**

Understanding what criminals are trying to do over the Internet is the first step in building a good defense. Most electronic fraud falls into one of three categories. Experts advise: Understand these threats in order to understand how best to protect yourself.

**PHISHING**—Fraudulent emails purporting to be from your bank or a similar trusted source lures you to a copy cat website (one that may look just like your bank's site). Once there you are instructed to "verify" certain personal information, which is then used to hijack your accounts and your identity. If you receive a suspicious email, delete the message and call your bank to inform them of the email.

**PHARMING**—Also called "domain spoofing," this cyber crime intercepts Internet traffic and re-routes it to a fraudulent site. Once there, the victim is asked to enter personal information, just as with Phishing.

**MALWARE**—This is software designed to infiltrate or damage a computer system without the owner's knowledge. Examples of malware (malicious software) include computer viruses, worms, Trojan horses, spyware, and adware.

***If you notice any unusual or suspicious activity on your accounts, please contact us immediately.***



Midland National Bank  
527 North Main Street  
Newton, Kansas 67114

Telephone: 316-283-1700  
Toll Free: 800-810-9457  
Fax: 316-283-3813  
E-mail: [info@midlandnb.com](mailto:info@midlandnb.com)

