

Protect Your Accounts: Know the Signs of an Imposter Scam



Scammers may pretend to be American Bank employees to gain access to your personal information or money. Knowing the warning signs can help you protect yourself and your accounts.

Fraudsters may contact you by phone, text message, or email claiming to be from American Bank's fraud department. They may even make their phone number appear legitimate. Just because a message looks like it's from your bank doesn't mean it is.

American Bank Will Never Ask You To:

- **Share your online banking password, PIN, or one-time verification code.** These are intended for your use only.
- **Transfer money to a "safe" or "secure" account.** We will never instruct you to send money through Zelle, wire transfer, or another payment method to protect your funds.
- **Withdraw cash or purchase gift cards to prevent fraud.** These are common tactics used by scammers.
- **Download software or provide remote access to your device.** Never allow unexpected or unknown callers to access your computer or phone.
- **Keep a transaction secret or mislead bank employees.** Be cautious of anyone claiming to be investigating fraud who asks you not to tell others or directs you not to contact the bank yourself.

How You Can Protect Yourself:

Fraud prevention best practices:

- Never share one-time passcodes, security codes, or authentication codes with anyone, even if they claim to be from your bank.
- Take advantage of security features. Set up account alerts and enable multifactor authentication (MFA) for added protection.
- Monitor your accounts regularly. Review transactions for unfamiliar activity, password changes, or updates to your personal information.
- Recognize unusual requests. Be alert to situations that seem out of character for your bank, especially requests involving urgency, secrecy, or actions outside normal banking procedures.

Be Aware: Fraudsters use spoofing to disguise phone numbers, email addresses, and caller ID information to impersonate or imitate trusted sources.

What Should You Do?

STOP. Do not share information, click suspicious links, or send money.

VERIFY. End the conversation and contact American Bank directly using a trusted phone number from your bank statement, debit card, or our official website.

REPORT. If you believe your account information has been compromised or you've been targeted by a scam, contact American Bank immediately. Change your online banking and email passwords, and secure any compromised cards or accounts. Keep a record of suspicious communications, including phone numbers, messages, dates, and transaction details.

When in Doubt, Contact Us Directly

Your account security is important to us. If something doesn't feel right, take a moment to verify before taking action. End the call or stop responding to suspicious texts, and contact American Bank directly at 214-358-3111.