



Pegasus Protects

Pause before you send

Payment fraud is one of the fastest-growing trends. Scammers rely on urgency and trust to get you to send money before verifying. Taking just a moment to pause can prevent significant loss.

COMMON PAYMENT SCAMS

Business Email Compromise

A sophisticated scam where attackers impersonate executives, employees, or trusted vendors via hacked or spoofed emails to trick victims. These highly targeted attacks rely on social engineering and personalization rather than malicious links, often resulting in significant financial losses.

Zelle Overpayment Scam

Occurs when a scammer sends fake or stolen funds to your account, then demands you return the "extra" money, leaving you responsible for the stolen amount when the initial transaction is reversed. Scammers often use fake screenshots or act as banks to create urgency.

Mortgage Closing Fraud

Mortgage scam artists target homebuyers who are about to close on their home purchase. Using emails or text messages to pose as an actual real estate agent, mortgage loan officer or settlement agent, the fraudster will attempt to steal the homebuyer's down payment or closing costs.

Grandchildren and Elder Fraud

Beware of calls from people attempting to sound like a grandchild or relative asking you to wire money or provide credit card numbers to help them get out of trouble.

Sweetheart Scams

Sweetheart scammers pretend to fall in love with people in order to win their trust and steal their money. These types of scams may unfold over the course of a year or more. They are often initiated on dating websites and apps, or via social media,

Protect Yourself

- Always verify payment changes verbally
- Be cautious of urgency or secrecy
- Use known contact information—not what's provided in the message
- When unsure, pause and confirm

Stay one step ahead.

If something feels off, contact Pegasus Bank directly at (214) 353-3000.