Five steps to avoid phishing scams

1 **Be alert.** Phishing messages can use Artificial Intelligence to skillfully imitate an organization you recognize or trust.

2 **Pause.** When asked to "act immediately," do the opposite. Go slow and resist the urge to respond right away.

3 **Verify.** Don't assume communication can be trusted simply because it appears or sounds legitimate.

4 **Stop.** When you receive a request that doesn't seem right, hang up or close the message. You aren't being rude; you are being smart.

5 **Get help.** If you suspect you were the victim of fraud related to your Pegasus Bank account, contact us immediately.

Pegasus Protects

Stay one step ahead

DON'T TAKE THE BAIT

Fraudsters often rely on urgency and familiarity to gain your trust. Emails, texts, or calls may appear to be legitimate—but knowing what to look for can help you recognize a scam before it becomes a problem.

What is Phishing?

Phishing is when fraudsters pose as trusted organizations, like your bank, to trick you into sharing sensitive information.

How to Spot a Scam

- Urgent or threatening language
- Requests for login credentials or passcodes
- Suspicious links or unknown senders
- Messages that don't feel quite right

Protect Yourself

- Never share your password or codes
- Avoid clicking unknown links
- Verify requests directly with your bank
- Enable account alerts and multi-factor authentication

Pegasus Bank will **never** ask for your login credentials, one-time passcodes, or direct you to log in through a link.

If you receive a suspicious call, text, or email, **do not share information**. Call us directly at (214) 353-3000.