Stay Safe From Scams With These Tips

PromiseOneBank
good people, smart banking

Phishing scams today can look as unassuming as a text from your bank asking for a "one-time" code for your two-factor authorization log-in. While there are countless legitimate reasons to receive a text or an email from a business or financial institution, it can be just as easy for scammers to replicate company logos and impersonate trusted businesses under the guise of these generated messages.

It is important to stay on top of the red flags to watch for when it comes to phishing attempts, and familiarize yourself with what banks would never ask you for.

Email Scams

- Avoid clicking suspicious links
- Raise the red flag on scare tactics
- Watch for attachments and typos
- Be skeptical of every email

Phone Call Scams

- Don't rely on caller ID
- Never give sensitive information
- Watch out for a false sense of urgency
- Hang up-even if it sounds legit

Text Message Scams

- Slow down-think before you act
- Don't click links
- Never send personal information
- Delete the message

Mobile Payment App Scams

- Be wary of texts or calls about payment apps
- Use payment apps to pay friends and family only
- Raise the alarm on urgent payment requests
- Avoid unusual payment methods