Email Security
How to Protect Yourself

To ensure you receive the most current updates regarding the merger, Lone Star State Bank customers with a current email address on record can expect to receive email communications from Prosperity Bank, contactus@prosperitybankusa.com.

Be skeptical of every email

Fraudulent emails can appear very convincing, using official language, logos, and similar URLs. Check for misspellings, unusual fonts, and different parts of a word that are in the subject line or email body. Always be alert.

Watch out for a false sense of urgency

Banks will never use scare tactics, threats, or high-pressure language to get you to act quickly, but scammers will. Scammers count on getting you to act before you think, usually by including a threat. Demands for urgent action should put you on high alert. A scammer might say. "Act now or your account will be closed," or even, "We've detected suspicious activity on your account" — don't give into the pressure.

Never give sensitive information

No matter how authentic an email may appear, never reply with personal information like your password, PIN, or social security number or a one-time login code with anyone who contacts you unexpectedly via email, phone, or text — even if they say they're from Prosperity Bank. Banks may need to verify personal information if you call them, but never the other way around.

Avoid clicking suspicious links

If an email pressures you to click a link — whether it's to verify your login credentials or make a payment, you can be sure it's a scam. Malicious links are a common technique used by scammers to not only steal usernames and passwords but also to deploy malicious software on your device. When in doubt, visit Prosperity Bank's website directly by typing www.prosperitybankusa.com into your browser.

Watch for attachments and typos

Prosperity Bank will never send attachments such as a PDF or Word Document in an unsolicited email. Misspellings and poor grammar are also sure warning signs of a phishing scam.

If you fall victim to an attack, act immediately

If you have disclosed sensitive information in a phishing attack, contact Prosperity Bank immediately. Place fraud alerts on your credit files and make sure to monitor your bank account statements closely for any fraudulent activity.

Report suspicious e-mails or calls

If you receive a suspicious email, call, or text, report them to the Federal Trade Commission at www.consumer.gov/idtheft, or call 1-877-IDTHEFT.