SPOT the Spoof BEFORE It Happens!

TEXAS COMMUNITY BANK
6721 MCPHERSON ROAD
LAREDO, TX 78041

Be Aware!

What is Phone Spoofing?

- **Caller ID Falsification and Deception:** Used by scammers to manipulate the information displayed on the recipient's caller ID, to hide and mislead the caller's true identity.
- **Common in Scams:** Frequently employed in fraudulent activities, such as phishing and robocalls.
- **Intention to Deceive:** Spoofers often mimic phone numbers of trusted organizations or familiar contacts to gain trust, aimed at tricking individuals into divulging personal information or taking specific actions.
- **Risks:** Fraud and identity theft. Financial loss from scams. Personal information being compromised.

Be Alert!

Be aware of Spoofing Attack Red Flags.

- **Request for Personal Information**: Callers asking for sensitive personal information such as Social Security numbers, bank account details, or passwords.
- **Requests for Payment Methods**: Requests to make payments through unconventional methods like gift cards, wire transfers, or cryptocurrency.
- **Urgent or Threatening Language**: Calls that use aggressive, urgent, or threatening language to elicit immediate action.
- **Pressure Tactics**: High-pressure tactics to make you act quickly, such as claiming your account and/or debit card will be negatively affected if you do not comply.

Don't Get SPOOFED!

Assess the severity of a phone spoofing attack.

- **Hang Up on Suspicious Calls**: If you receive a call that seems suspicious, hang up immediately and do not engage.
- **Verify Caller Identity:** Always verify the identity of the caller by calling back the known and official number, even if this means calling same "trusted' number you received the call from.
- **Do Not Share Personal Information**: Avoid sharing personal or financial information over the phone, unless you are certain of the caller's identity.
- **Evaluate Personal Information Shared**: Assess whether you shared any personal or financial information during the call and notify your TCB Account Officer/Representative to help evaluate the potential impact of that information being compromised.
- **Analyze Caller Intent**: Determine if the caller's intent was to gain immediate financial information, solicit payments, or scam you into providing other sensitive data.
- **Check for Follow-Up Actions**: Monitor if the spoofing call was followed by other suspicious activities such as emails, texts, or additional calls.
- **Inspect Financial Accounts**: Review your bank statements and account history for any unauthorized transactions or suspicious activities.
- **Impact on Personal Data**: Consider whether the spoofing attack could lead to identity theft or unauthorized access to your online accounts.

Don’t Hang on, HANG UP! Defend Yourself!

TCB Security Tools and Resources

- **Innovative Fraud Detection**: TCB utilizes advanced fraud detection and monitoring systems to identify and alert our customers of suspicious debit card activities in real-time. Automatic enrollment.
- **Customizable Transaction Alerts:** We encourage customers to utilize their Card Management feature to enable preferred transaction alerts, used to monitor account activities. Ready to use and suit each customer’s preference.
- **Customizable Transaction Restrictions:** We encourage customers to utilize their Card Management feature to enable preferred transaction restrictions and controls based on personal usage. Ready to use and suit each customer’s preference.
- **Immediate Debit Card Lockdown:** Log into your TCB Online/Mobile banking profile > scroll down, locate **Card Management** > select the debit card > use the slider icon to lock your card. Ready to use and can be reactivated.
- **24/7 Customer Support:** We offer around-the-clock customer support to address any concerns or to report suspicious activities immediately.
- **Immediate Debit Card Cancelation:** To report a lost, stolen, or compromised debit card please call toll free 1-888-297-3416 or contact a TCB representative. If calling from outside the United States, please dial +1-206-389-5200.
- **TCB Online/Mobile Banking:** Log into your TCB Online/Mobile banking profile > locate and select **Support** > based on your preference either call the reference phone number or select Send us a message. Ready to use and is a secure message.
- **Secure Account Lockdown:** If any fraudulent activity is detected, please notify your TCB Account Officer/Representative to assess the situation and determine if an immediate account lock down is also recommended to prevent further unauthorized access.
- **Two-Factor Authentication** (2FA): Our TCB Online/Mobile banking feature is enhanced with the required usage of two-factor authentication to secure your accounts, providing an extra layer of protection.

Scan Me!

TCB Fraud Protection

Find Me!
https://www.tx-communitybank.com/services/fraud-protection

Scan Me!

FCC Spoofing Video

Find Me!
https://www.fcc.gov/spoofing

Scan Me!

TCB Mobile Banking

Find Me!
https://www.tx-communitybank.com/services/mobile-banking

Federal Resources

- File a Complaint with the Federal Communications Commission (FCC): Go to the FCC’s website (fcc.gov) and file a complaint about the spoofing call through their Consumer Complaint Center.
- Report to the Federal Trade Commission (FTC): Visit the FTC’s official website (ftc.gov) and use the online complaint assistant to report phone spoofing.