Be Alert: SHIELD Yourself from Debit Card Fraud!

TEXAS COMMUNITY BANK
6721 MCPHERSON ROAD
LAREDO, TX 78041

Debit Card Fraud Can Happen to YOU!

Each year, tens of thousands of consumers fall victim to debit card fraud, with scammers deploying increasingly sophisticated tools and techniques daily. While most debit card fraud occurs online, using your card for in-person transactions also carries risks. In both scenarios, fraudsters aim to obtain your debit card information to drain your bank account. However, there are proactive steps you can take to safeguard yourself. To reduce your risk, it's crucial to familiarize yourself with the various methods criminals use to capture your data.

PHISHING

Phishing involves emails and texts designed to deceive users into divulging financial information. The goal of phishing is to persuade you to click on a link and either log into your bank account or disclose your debit card details.

Tips to Prevent Phishing:

- Staying safe online is important in protecting yourself against debit card fraud.
- Due to phishing emails and messages continuously increasing in complexity, it can be difficult to immediately detect whether it's fake or safe.
- To reduce the likelihood of falling prey to a phishing scam via text or email, consider these two steps: Firstly, confirm familiarity with the sender—whether it's a company or individual. Secondly, verify if the contact details (number or email address) match those previously used by them.
- Whether the text or email is recognized or not, always consider contacting the company or individual directly by phone and/or visiting their official website to verify the authenticity of the message.

HACKING

If you conduct banking or shopping on public or non-secure Wi-Fi networks, hackers can employ keylogging software to capture everything you type, including your name, debit card account number, and personal identification number (PIN).

Tips to Prevent Hacking:

- To protect yourself, especially when you are on public Wi-Fi, be sure to use strong passwords, turn on two-factor authentication (2FA) if available and ensure your security software, operating system, and internet browser are updated. The same rules apply to your mobile phone.
- Be sure to never enter your card details into an unsecure website or store that information within a web browser.

THEFT

Theft occurs when your actual debit card, its PIN, and identifying information is stolen. Thieves then use the card and information to complete fraudulent transactions.

Tips to Prevent Theft:

- Keep your card secure and treat it as you would cash.
- When you receive your card, sign the back of the card immediately, and keep it in a safe place.
- Memorize your personal identification number (PIN) – DO NOT WRITE your PIN down and do not carry it with you.
- Never lend your card to anyone.
- Other than displaying a personal ID if requested by a merchant, do not volunteer any personal information when you use your card.
- Always monitor your card closely during transactions. Handing over your card is comparable to handing over excess cash; ensure it is promptly returned to your possession after each purchase. If you notice anything unusual or concerning during a transaction, please call TCB immediately to report the incident.
- Take your receipt and save it. Always check sales vouchers for the correct purchase amount before you sign them.

SKIMMING

Skimming occurs when devices are installed on ATMs, point-of-sale terminals, and fuel pumps to capture data and steal cardholders' PINs. Scammers then use the information to create counterfeit debit or credit cards.

Tips to Prevent Skimming:

- When paying at the gas station pump, consider selecting the 'credit' option to bypass using a PIN, if available.
- Opting for TAP TO PAY offers the highest security against card skimming and other types of fraud, as your card never makes physical contact with the payment terminal during transactions. If necessary, use the CHIP portion of your card instead of swiping it.
- To prevent your card from being skimmed at a gas station, try using a pump closest to the store, within the attendant's line of sight. These are less likely to be targeted by skimmers. Alternatively, you can pay inside instead of at the pump.
- Check the pump panel for tampering. If the tamper-resistant seal is broken, do not use the gas pump, and advise the attendant that the pump may not be safe to use.
- To avoid using your physical card at the pump, determine if your neighborhood gas station offers mobile app transaction payments for your fuel.
- If you are at an ATM or point-of-sale terminal, do a quick scan for any signs of tampering such as any piece that is loose, damaged, crooked, or scratched. If you spot anything unusual, don't use the machine.
- ATMs in well-lit, indoor locations are typically less likely to be targeted by skimmers. Shield the keypad from prying eyes or cameras when inputting your PIN. When possible, use cards with TAP TO PAY or CHIP technology.

SPOTTING DEBIT CARD FRAUD

Identifying debit card fraud can become easier once you know what to watch for, though it demands vigilance. As the customer, you have the most intimate knowledge of your own transactions.

Tips for Spotting Debit Card Fraud:

- Monitor your transactions daily, if possible, through online banking, the TCB mobile app, or by calling the Bank's 24/7 telephone banking line at 1-844-842-7211. These options are readily available and easy to use.
- Enable Card Management alerts within your TCB Online/Mobile banking profile to receive in-app notifications of transactions on your account. This allows you to promptly address any unauthorized charges.
- Reconcile your bank statements monthly and verify that all debit card transactions were valid in a timely manner.

IF YOU DETECT DEBIT CARD FRAUD ON YOUR ACCOUNT:

- Immediately report a lost, stolen, or compromised card.
- You can cancel your debit card instantly by using the 'report card lost/stolen' Card Management feature within your TCB Online/Mobile banking profile. Alternatively, reach TCB's toll-free number at 1-888-297-3416. For calls outside the United States, dial +1-206-389-5200. You can also contact your TCB Account Officer/Representative to request cancellation of your current card and arrange for a replacement.
- Depending on the type of fraud, you may wish to place a fraud watch on your credit report. When contacting any of the three credit rating agencies – Equifax, Transunion, or Experian – you can instruct that they place a fraud alert on your credit report. This free service will require new lenders to verify it's you before opening any new accounts in your name. You only have to contact one credit bureau to have the alert on all three credit reports. The alert can be removed at any time. If you suspect you may be a victim of fraud or that your personal information may be comprised, freezing your credit profile can be a sound next step. This will prevent new credit lines from being opened in your name.

- Report the fraud to the U.S. Federal Trade Commission (FTC). You can report scams as well as confirmed cases of identity theft. Depending on the size of the fraud, law enforcement will use the reports to investigate the case if warranted.

Debit card fraud is a serious threat that is anticipated to rise in frequency. However, by remaining vigilant, you can potentially avoid becoming a victim of this trend.

	Scan Me!	Find Me!
FTC Efforts on Fraud		https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public
FTC Snapshot of Fraud		https://www.ftc.gov/system/files/ftc_gov/images/CSN-1pager-2023.png
TCB Fraud Protection		https://www.tx-communitybank.com/services/fraud-protection