Fraud Protection

1. We will never call you to request information you received via text (SMS) or pressure you to reset your online banking password.
2. A text alert from us warning of suspicious activity on your account or card will never include a link to be clicked. A text alert from us will always be from a 5-digit number and NOT a 10 digit number resembling a phone number.
3. We will never call and ask you for your Debit Card PIN or 3-digit security code on the back of your card. Don't give this out to an unsolicited caller, no matter what they say. Hang up and call us directly.
4. Don't provide your online banking log in credentials, password, debit card number/code, account number or personal information by email, text or on an unsolicited call. Contact your local United Bank & Trust branch directly or call us at 785-562-4312.
5. Use caution when making online purchases. If it sounds too good to be true, it has a high probability of fraud.
6. When being solicited for charitable donations over the phone, don't give your card information directly to the solicitor. Use the charitable organization's website instead.
7. Don't trust caller ID: Caller ID may be modified to show your financial institution's name.
8. Don't give an unsolicited caller remote access to your computer.

Tips to keep your information safe

1. Choose unique passwords
2. Use two-factor authentication when available
3. Avoid public Wi-Fi and computers
4. Sign up for alerts
5. Never give out personal information
6. Avoid clicking links in suspicious emails, text messages, or landing pages
7. Use security software to protect your devices from attack

Monitor your online account

To help detect fraud quickly, we recommend checking your online banking account regularly, and enrolling for alerts to receive notifications of account activity. If anything looks amiss, call us directly for assistance.

United Bank & Trust

Member FDIC

Card Safety Tips

1. Keep cards in a secure place. If you do not need it, leave it at home.
2. Keep cards in sight at restaurants and stores.
3. Do not respond to emails requesting “verification of identity.” Card Issuers and Financial Institutions will never make this request.
4. If someone calls claiming to sell a product or collecting money for a charity, ask the caller to mail the information. Legitimate companies can do this; fraudsters will get angry, try to pressure the Cardholder or victim, or just hang up.
5. Always sign a new card the moment it is received. For protection, some Cardholder’s write “See ID” in the Authorized Signature field. Consider this, if a fraudster steals the card, it will be signed by the fraudster. The card signature will always match the sales receipts. Merchants are not required to, and rarely do, check ID. Sign the card to make it more difficult for fraudsters to forge.
6. The PIN should never be the Cardholder’s date of birth or a series of numbers like 1234 – these numbers are easy to guess.
7. Never write the PIN on the card or on a piece of paper that is in the same place as the card.
8. Cover the keypad when entering your PIN to ensure no one is able to shoulder surf.
9. Check statements promptly to catch and report unauthorized transactions in a timely manner.
10. Shred unwanted pre-approved offers, expired cards, and any correspondence with a card number or details.

Monitor your card transactions

Use these card management features in our mobile banking app to keep track of your finances and help prevent your debit card from fraud. Call us directly if something looks amiss.

1. Lock or Unlock your card
2. Transaction Controls
3. Subscriptions and Card On File Merchants
4. Easy access to Digital Wallet
5. Personalized Alerts
6. In-Depth Spending Insights
7. Travel Plans

Scan for card management videos