CONSUMER FRAUD & SECURITY PROTECTION

United Bank

Fraud & Security

Here at United Bank, it is our goal to ensure that you are educated on how to protect yourself and your account from falling victim to identity theft and fraud schemes.

United Bank considers your account security of primary importance and offers multiple ways for you to monitor your accounts.

Our options include online banking*, mobile banking*, and 24-hour telephone banking.

United Bank will **NEVER** call, email or text you and ask for your debit or credit card number, account number, expiration date, security code or PIN. Additionally, United Bank will not call and ask you for personal information such as your Social Security Number. If YOU CONTACT US, you may be prompted to verify your information, for example, we may ask for the last four numbers of your Social Security Number or to verify your address.

If your card has been lost or stolen after hours, call 833-933-1648 and follow the prompts to report it as lost or stolen.

*Fees may apply for some services within Online Banking or Mobile Banking. Cell phone text and data rates may apply.

4 Primary Ways to Protect Your Personal & Account Information

1. Know who you share information with.
2. Store your personal information securely, especially your Social Security Number.
3. Ask questions before deciding to share your personal information.
4. Maintain appropriate security on your computers and other electronic devices.

6 Ways to Lessen the Chance of Check Fraud

1. Pay your bills online if possible.
2. Deliver your mail to a post office box.
3. Use a pen with blue or black non-erasable gel ink if writing a check.
4. Don't let delivered mail sit in your mailbox.
5. Monitor your bank accounts.
6. Report incidents quickly.

Questions to Ask Yourself

- Does the payment/reward make sense for the task involved? Does it sound too good to be true?
- Is this offer out of the ordinary?
- Does this offer require me to send money to someone that I am unfamiliar with?
- Am I being asked to send money via wire transfer, gift card, official check, Western Union, or other methods?
- Does the person insist that I am not to tell my financial institution details about the transaction?
- Did this person call me and request my personal information? (Social Security Number, address, DOB, account number, card number, etc.)

Tips to Help You Recognize Fraud & Cybersecurity Threats

- Be alert to impersonators.
- Don't overshare on social networking sites.
- Secure your Social Security Number.
- Use security software on your devices.
- Create strong passwords - avoid using important names and dates.
- Be wise about WiFi - always use a secure network when possible and avoid logging into your online banking when connected to public WiFi networks.
- Don't open files, click on links, or download programs when you are unaware of the sender.
- Keep financial documents and important documents stored in a safe place.
- Enable biometrics (fingerprint sign-on or facial recognition) or multi-factor authentication.
- Keep your personal information up-to-date with United Bank.
- Set up email and text alerts for account balance and transaction notifications.

Find Helpful Tips to Avoid Cybersecurity Threats and Get Trusted Guidance on How to React to Problems

To find answers to urgent questions about missing cards and stolen identities, information on how United Bank is protecting your accounts, and suggestions on what you can do to best protect yourself along with educational tips, the most up-to-date information, and useful links, **scan the QR code below**!

Scan Now to Learn More!

UnitedBank.com