CARROLLTON BANK

Fraud Prevention Tips

The best defense against fraud or identity theft is a proactive approach. Here are a few steps you can take to help protect yourself.

Protect your identity

- Copy the front and back of the vital information you carry in your wallet or purse and store it in a secure place, so it's handy if it's lost or stolen.
- Don't carry your Social Security card and unused credits cards with you. Store them at home in a safe and secure location.
- Don't give out your Social Security number unless absolutely necessary.
- Don't provide your credit card number or other important information on a call that you did not make.
- Fraud and identity theft often happens as a result of mail and garbage theft. Shred important documents before discarding. Put outgoing mail in an official post office mailbox, instead of your home mailbox.
- Go paperless! Get electronic versions of your bills and financial statements. Sign up for our Bill Pay and free E-Statements.
- Check your credit report at least once a year with a free credit report from each of the three major credit bureaus. Start at www.annualcreditreport.com† or get a copy directly from:
  - Equifax: **1-800-685-1111** or www.equifax.com†
  - Experian: **1-888-397-3742** or www.experian.com†
  - TransUnion: **1-800-916-8800** or www.transunion.com†

  While you are talking to them, ask them to place a Fraud Alert on your account. This lasts for 90 days, so you have to repeat it quarterly. You can lock it down permanently with a Credit Freeze, but it makes getting new credit a little more complicated.

  †Carrollton Bank makes no endorsement or claims about the accuracy or content of the information contained in these sites. The security and privacy policies on these sites may be different than Carrollton Bank.
- If you haven't received a regular bill or statement in a while, contact the company's customer service department.

CARROLLTON BANK

Protect your checking account

- Review your statements carefully. Contact us if you notice any suspicious charges.
- Report lost or stolen checks immediately. Consider having your new checks delivered to the bank, rather than your home mailbox.
- Eliminate junk mail credit card offers that can be stolen from your mailbox by opting out.
- Monitor your account with our online banking or our mobile banking app.
- Don't print your driver's license number or Social Security number on your checks.
- Store checks in a secure location.
- Don't carry your checkbook with you unless it's absolutely necessary.

Protect your Credit Card and Debit Card

- Keep your cards in a safe place. Contact us immediately at 1-800-558-3424 (for Credit Cards) or 1-800-472-3272 (for Debit and ATM Cards) if your card is lost or stolen, or if you suspect unauthorized use.
- Don't send your card number through email, or over the phone unless you made the call.
- Check your statements and contact us if you notice any discrepancies.
- If you have forgotten your PIN or would like to select a new one, please contact your local Carrollton Bank, or call 800-992-3808.
- Change your Personal Identification Number (PIN) every six months. Don't use a number or word that appears in your wallet, such as name, birth date, or phone number.
- Memorize your PIN. Don't write it down anywhere, especially on your card, and don't share it with anyone.
- Cancel and cut up unused credit and other cards. When you receive a replacement card, destroy your old card.
- If you order a new debit or credit card, mark your calendar and check with the issuing company if it does not arrive with 10 days. Ask the issuer if a change of address has been filed.
- Shop with merchants you know and trust.
- When shopping online, make sure the site you're on is secured with encryption. Check for a lock symbol in the lower right corner of your web browser, or "https://…" in the address bar of the website. The "s" stands for "secured" and tells you that the web page is encrypted.
- Then be sure to log off from any website, or close your browser window, after a purchase transaction is made with your credit or debit card to prevent unauthorized access to your information.

CARROLLTON BANK

Protect yourself online…

Follow these tips to stay secure whether you're sending emails, shopping online, using social media, or just surfing the Web.

- Don't use your Social Security number or phone number as a username or password.
- Change your passwords frequently and, where possible, use letters, numbers, and special characters such as # and @. Don't use your Carrollton Bank online banking username and password for anything else.
- To change your Carrollton Bank username please contact your local Carrollton Bank. To change your password:
  - Sign on to an online banking session
  - Click on the **options** link in the upper right hand corner
  - Under "Password", click the Edit button
- Don't write your online passwords down or share them with anyone. Consider using a password management program.
- The same advice goes for the answers to your security questions. Don't share them with anyone. Carrollton Bank will never ask you for your password or your security answers via email.
- When using social media, it's a good idea to keep your personal information private. Avoid sharing details such as your birth date, home address, mother's maiden name, schools attended/mascots and pet's name, because fraudsters know they are often used as answers to security questions.
- Pay attention to the privacy options for any social network you use. They can be complex and change frequently, so use the controls they provide to be adjust who sees what you share.

…and on your mobile device

- Always lock your mobile device when it is not in use. By requiring a password or your fingerprint to unlock your device, you make it more difficult for someone else to view your information.
- Keep your mobile operating system up to date. Always download updates from the company's website to be sure the update is legitimate.
- Delete any text message from Carrollton Bank or other financial institutions. Be sure to clear this and any other confidential information from your phone before loaning, recycling or selling it.
- If you lose your mobile device or change your mobile phone number, sign on to CarrolltonBanking.com to remove the old number from your mobile banking profile or call customer service at **217-942-9106**.
- Where possible, avoid public Wi-Fi networks, as fraudsters can spoof the name of reputable hotspots.
- Never share your account numbers, passwords, Social Security number and date of birth in a text message, phone call or email.
- For your security, sign off when you finish using a Carrollton Bank app rather than just closing it. Our smartphone app and mobile banking site will automatically log you off after 20 minutes of inactivity. This reduces the risk of others accessing your information from your device.
- Download our app by clicking on the appropriate button below…

Available on the App Store

ANDROID APP ON Google play

Prevent Phishing…

- Phishers send an email to a wide audience that appears to come from a reputable company and contains links to a spoof website that imitate that company's website. They hope to convince you to share your personal information with an urgent message about updating your information, which they use to transfer money out of your account.
- If you receive an email like this, don't open attachments, click links, or respond to them. Call your local branch to report the message as soon as possible.

…Smishing

- When fraudsters send an SMS (Short Message Service) or text message to your mobile device it's referred to as smishing. The purpose is the same: convince you to share your confidential information.
- If you receive a text message telling you that you immediately need to update your information, activate an account, or verify your identity by calling a phone number or submitting information, on a website, do not respond and delete it.

…Vishing

- Vishing is a phishing attack made through a telephone call or voice message. Often fraudsters spoof their caller ID so it appears that the telephone call is coming from a reputable company. They may also have information, such as your name or address, which makes the call seem more legitimate. If you are uncomfortable with a phone call, simply hang up.

…and mail or fax phishing

- Phishing attempts can be made through regular mail or fax machines. If you are suspicious about mail or a fax you received requesting confidential information, you should discard it.

CARROLLTON BANK

Computer Security Tips

- Avoid using online banking on shared or public computers.
- Always download programs from reputable sources.
- Set up your network and your devices to prevent unauthorized users from remotely accessing them. If you use a wireless router in your home, consult your manual for appropriate security settings.
- Keep your operating system, software, browser version and plug-ins current, by downloading updates directly from the appropriate company's website.
- Be sure your computer is protected by a firewall and keep anti-virus and anti-malware software up to date.