Personal Fraud Prevention Tips

SOCIAL ENGINEERING RED FLAGS

98% of today's cyberattacks involve some form of social engineering fraud. If you receive a suspicious-looking email, phone call or text message, do not respond to it. Here are red flags to spot potential fraud.

- Message that create a sense of urgency.
- Requests to work confidentially or work with a person who is introduced in the email or to perform unusual financial tasks such as transferring funds or changing payment information.
- Business-related messages sent from a public domain, such as a free email service.
- Misspellings and poor grammar throughout the email or in the email address.
- Suspicious attachments or links you weren't expecting.

THINK BEFORE YOU CLICK!

Beware of fraudulent emails and texts concerning your account, suspicious transactions or communications regarding payment issues.

Online shopping: Before making an online purchase, ensure the website uses secure technology. Verify the web address begins with https and look for a tiny locked padlock symbol on the page.

Know the sender: Do not click links or open unexpected attachments from senders you don't recognize, or that were forwarded as part of an email chain.

Holiday scams: Check the link for typos and authenticity. Instead of using a link, you can always access the site yourself.

Elder Fraud – Watch out for these fraud tactics directed at senior citizens:

- Unknown loyalty rewards & apps
- Cheap gift cards
- Unsolicited messages about payment errors
- Sweepstakes & Lottery winnings
- Family Distress Calls

ATM SKIMMERS

Don't let an ATM skimmer ruin your holiday cheer. Do a quick scan of your surroundings when visiting an ATM, and check the card slot and keypad for evidence of tampering. Make sure to block your PIN from public view.

WIFI NETWORKS

As you travel this year, make sure your WiFi settings are set to ask before joining a network. If you join an unsecured network, your personal data could be accessed. While on a public network, do not access any personal or financial information.

PRO TIP:

Set Up Alerts

- Set up alerts within CCB Mobile and Online Banking

Card Controls

Did you know you can prevent fraud by using Card Controls located in the CCB mobile app? Control where your card can be used:

- Through your phone GPS
- Authorized Zip Codes
- Set approved merchant types
- Instant notifications when your card is used