Red Flags and Tips to Protect Yourself from Scammers

Every day, thousands of people fall for fraudulent emails, texts, and calls from scammers pretending to be from their bank. Use these tips to make sure you're not one of them.

Emails: Use extreme caution when clicking email links or opening attachments. Do not reply to the sender or call a provided number if you suspect a scam. Contact your bank or financial services provider directly!

Watch for misspelled words. As sophisticated as scammers have become, they may still make mistakes, so watch for typos that can indicate an illegitimate source.

Americans lost **$1.9 BILLION** to phishing and other fraud in 2019

CCB will never ask for the following via email, text or phone call:
PINs, account numbers, passwords, usernames, birthdays, social security numbers, security question answers, one-time security code, etc. Protect this information if someone contacts you purporting to be from a financial organization. NOTE: You may be asked to verify confidential information if you call your bank, but never the other way around.

When dealing with bank card issues, call the number on your credit or debit card for support rather than any numbers sent to you via email or text message. You can also find contact information by going directly to a company's official website (ex: www.countryclubbank.com)

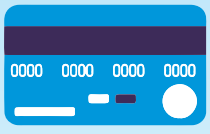
IMPORTANT REMINDER: Never share your login credentials for person-to-person payment apps like Venmo, CashApp, or others. Fraudsters commonly entice individuals to provide login credentials by saying they need it to process a refund, for example. Once they have access, they can quickly transfer money to another account.

Still aren't sure if it's a scam?

Beware of links.

Watch for scare tactics.

Protect your confidential information.



Call the number on your debit or credit card.