SCENIC COMMUNITY CREDIT UNION

4 Ways Bank Imposters Try to Scam You

Here are four ways that a criminal posing as your financial institution may try to scam you into getting you to share your banking info.

1. Phishing (Email) - Phishing emails often use attention-getting subject lines to trick you into clicking on a link or opening an attachment. The message might say that they need to verify your personal information before they can send you a new debit or credit card, that there's an issue with your account, or there's an exciting new promotion they want you to know about.

A scammer might try to get you to reply to the email and provide your account number or other sensitive data.
Or, they might provide a link to an official-looking web page to log in to your online banking – so they can steal your login credentials.

2. Vishing (Phone) - In a vishing scam, a scammer will contact you by phone. Using easily available technology, criminals can show ANY name or phone number they want on YOUR caller ID, so you will be more likely to answer. Scammers can display your town or area code, or even the first few digits of your own phone number, to make it look like it's really your financial institution that's calling.

They might say they need your information or claim your account has been compromised and advise you to transfer your money into a new account – for "safekeeping."

3. Smishing (Short Message Service) - In a smishing scam, criminals will contact you by text message. Many financial institutions are now using text messages to send real-time alerts to their customers – but they will never ask you to provide personal information by text.

4. Snail Mail - While it's not the most high-tech option, scammers can try to steal your information through fraudulent requests by snail mail. You might receive a fake check in the mail with a letter that asks you to deposit the check in your account and wire money to a third party. Don't fall for it. The check will bounce, and you'll be on the hook for the money you wired.

Before transferring any money, always verify that the person you're communicating with is legitimate. Data from the Federal Trade Commission shows that consumers reported losing nearly $8.8 billion in fraud in 2022. Read on to see what Red Flags to watch for and how you can protect yourself from scammers.

Change of our Ooltewah location hours

Beginning October 1, 2023 our Ooltewah branch will no longer be open on Saturdays. The ATM will be accessible and our members have access to the shared branching network.

Visit: https://www.coop.org/Shared-Branch-ATM to find your closest Branch or ATM.

Dividend News

The dividends paid on all regular shares for the third quarter of 2023 will be distributed as follows:

Share Account Balance	Rate*	APY**
$0 to $24.99	0.00%	0.00%
$25 to $9,999.99	0.25%	0.25%
$10,000 and over	0.30%	0.30%

*Rate - disclosed as Annual Percentage Rate
**APY - disclosed as Annual Percentage Yield

Financial Facts

As of July 31, 2023

Members	14,363
Assets	$148,849,917
Shares	$126,766,058
Consumer Loans	$108,442,368
Business Loans (30)	$3,403,365

Fee Schedule Notice

Our fee schedule is available for viewing at any time. Visit mysccu.com/services, or stop by any branch to get a hard copy. We can also mail you a copy at your request; just give us a call at (423) 875-6955

Download the SCCU app

Download on the App Store

GET IT ON Google Play

EQUAL HOUSING OPPORTUNITY

NCUA

Holiday Closings

All branches of SCCU will be closed on the following days:

COLUMBUS DAY
Monday, October 09, 2023

VETERANS DAY
Saturday, November 11, 2023

THANKSGIVING DAY
Thursday, November 23, 2023

CHRISTMAS DAY (OBSERVED)
Monday, December 25, 2023

NEW YEARS DAY
Monday, January 1, 2024

Watch Out for These Red Flags

If you're contacted, be on the lookout for these red flags:

- They ask for sensitive data.
- They use threatening language. For example, the caller may say they'll suspend your account if you don't provide your information. A legitimate financial institution will never do this.
- They use odd phrasing or misspellings – especially in names or addresses.
- They contact you about raising your transaction limit. Financial institutions set default transaction limits and customers may be able to raise them if they want to make larger payments.
- They say they're a financial institution you don't use.
- They pressure you to stay on the line instead of calling back at the institution's customer service number.

How You Can Protect Yourself

Now that you know what to look for, how can you protect yourself from a bank imposter scam?

- If someone contacts you out of the blue, never share sensitive information such as your Social Security number, account number, PIN, password, or verification code. It's only safe to provide details like these if you contact your financial institution yourself.
- Don't reply, download attachments, click links, or log in to a linked website, which could be a dummy site designed to capture your online account information.
- Delete suspicious emails right away.
- Don't be afraid to hang up the phone.
- Don't automatically trust caller ID or official-looking emails.
- Hover your cursor over links or buttons before clicking. If the link destination doesn't look right – don't click.
- If you're ever in doubt, contact your financial institution directly to verify a request or communication. Don't use a phone number, address, or link you've been given – look it up yourself.

Scammers frequently update their methods, so it's important to stay vigilant and practice caution if you receive a suspicious communication. Give us a call or stop by a branch if you feel you may have been scammed.

ENROLL IN ESTATEMENTS

It's Secure- Estatements are protected with anit-phising technology.

It's Convenient- You can access any of your statements anytime.

It's Green- No paper, no mail delivery, lower carbon footprint.