Why Do We Fall for Scams?

Financial Desperation | This one is a major factor in recent years as inflation continues to rise. When members are faced with financial hardships and a desire for relief or quick financial fixes, they become more vulnerable to falling victim. Desperation can cloud judgement and leaves us susceptible to scammers.

Social Engineering | One thing that scammers are excellent at is social engineering. They can personalize the scams to make them seem legitimate. They also hack social media accounts to come across as someone we already know. They will reach out and ask for personal information or money.

Lack of Awareness | Scammers prey on those that do not keep up with evolving scam techniques. Staying uninformed can increase chances of falling for a scam. Scammers are counting on the fact that we will not understand cryptocurrency or scam red flags making education extremely important.

Emotional Triggers | Scammers use tactics that exploit emotions to manipulate victims. They rely on creating a sense of urgency, fear, or excitement. These emotions can easily impair irrational thinking and causes members to make impulsive decisions. With emotions running high, it can make it harder for us to evaluate the situation.

Trust and Authority | Scammers use a common tactic to gain trust by masking as government officials, law enforcement or company employees. By posing as someone with authority, the member is more likely to feel a sense of trust and comfort. This makes it easier for scammers to gain access to personal information or completing financial transactions.

Lack of Vigilance | In a world of constant distractions and busy on the go lifestyles, it is easy to overlook red flags or suspicious activity. Failing to authenticate or verify offers or communications, not conducting research, and not protecting personal information can leave us vulnerable.

Report Fraud To

Federal Trade Commission
FTC.gov

FBI Internet Crime Complaint Center
IC3.gov

Top Fraud Types for 2023

- Investment
- Social Media
- Email/Text Phishing
- Phone Scams/Impersonators
- Lotteries/Inheritance
- Job Opportunities

A Better Way of Banking

Carolina Trust Federal Credit Union began as Myrtle Beach Air Force Base Federal Credit Union in 1958. We are a unique not-for-profit financial cooperative, and we return credit union profits to our membership through competitive rates, consumer friendly terms, low fees, innovative services, and personal attention. Membership is open to individuals and business owners who live, work (or regularly conduct business in), worship, volunteer, or attend school in Horry, Georgetown, Marion, Williamsburg or southern Florence County (south of Lynches River), South Carolina or Brunswick County, North Carolina. Relatives of members and business owners are also eligible to join our Credit Union.

Deposits at Carolina Trust are federally insured by the National Credit Union Administration (NCUA). This U.S. Government agency federally insures deposits and certain retirement accounts to at least $250,000. According to the NCUA, “Not one penny of insured savings has ever been lost by a member of a federally insured credit union.”

01/24

The Fraud Buster

Fraud Prevention Tips and Scam Alerts

Carolina Trust®
FEDERAL CREDIT UNION
carolinatrust.org • 843.448.2133

EQUAL HOUSING LENDER

This credit union is federally insured by the National Credit Union Administration.

Antivirus, Microsoft & Other Computer Scams

A common scam that is popping up on your computer screens are scams where the fraudster remotely takes over your screen and computer functions.

These scams will contain a warning or error message that pops up on your screen that instructs you to call a number for support. Calling that number is dialing directly into the fraudster. While impersonating a support technician, they will tell you that there have been suspicious activity on your bank accounts and will instruct you to either sign into your online banking which will grant access to your username and password, or they will instruct you to provide them with the number on the back of your debit card and will "transfer" you to your financial institution on a secured line. This transfer is just to another fraudster that is part of their scheme to extort money from you. They may even ask to send information such as debit card number, expiration, or a copy of your ID. This will allow them to then call your financial institution pretending to be you to transfer funds or reset online banking information.

There is no X or esc option that will get you out of the pop up, the best option is to unplug your computer and then have it professionally cleaned to remove any access the fraudster may have. Microsoft, Apple, Norton, McAfee and others will never ask you for online banking information, to purchase gift cards, transfer funds, or pay via cryptocurrency for any services.

Gift Card Scams

Gift card fraud is used to describe scams where the fraudster convinces the victims to purchase gift cards and provide the numbers from the back of the cards. This scam is generally one of the worst as there is no recourse to recover the lost funds. The fraudster pressures you to purchase the cards immediately to avoid you asking too many questions.

Here are three questions to ask yourself when asked to purchase gift cards: Is someone pressuring me to buy these gift cards? Am I being asked to purchase these gift cards immediately? Are gift cards normally accepted as a required payment for this product?

Spoofing Call Scams

How can you feel protected when answering phone calls and not fall victim to a scammer? Anyone skeptical of a call should hang up and dial the number back. Spoofers can only mirror a phone number, but they do not have the ability to answer incoming calls. They even have the ability to mirror the voice of a family member or close friend. **Remember that the Credit Union will never ask you to provide your online banking username and password.**

If you receive a one-time verification code for online banking, never share that code with anyone else, not even someone claiming to be a teammate of Carolina Trust. If you are still unsure if a phone call is valid, please visit us at a branch for assistance or call 843.448.2133, ext. 3.

Fraud Buster Spotlight

Debit Card Skimming Devices

One of the top ways that you can protect yourself from fraud is to know the signs of potential skimming. You want to be on the lookout for anything suspicious or unusual prior to inserting your card into ATMs or POS card readers. Primary targets for skimmers are Pay at the Pump gas stations, Stand-alone ATMs, and POS Card Readers at unmonitored registers. So, what should you look for?

- You should gently pull or wiggle the insert card slot to determine if the cover is loose or can easily be removed. All valid card readers will remain secured to the machine, anything that separates with a gentle pull is likely a skimmer.
- Always check for tape or a sticky substance as that could be an indication a device is taped or glued to the machine.
- You should also be on the lookout for any abnormal stickers or small holes as these can be a camera placed to read the card information when your card is inserted.

Have You Been:

Instructed to purchase gift cards and text the number and PIN from the card:

Be on guard! Many scammers demand that you buy gift cards and send them the PIN numbers. Once the scammer has the PIN, they also have all the funds on the card.

Asked to send money through Bitcoin or other Cryptocurrency network:

Be on guard! Scammers can impersonate businesses, government agencies, and a love interest among other tactics. No legitimate business or government agency is going to demand you pay with cryptocurrency- not to buy something, pay taxes or fines, and not to "protect" your money. ***That's always a scam.***

Asked to send money to an individual you met online but not in person:

Be on guard! Be wary of people who say they cannot meet, talk on the phone, or use video chat. Verify information from dating profiles with independent sources.