COMMON MEMBER SCAMS & WHAT TO WATCH FOR

ROMANCE SCAMS:

Using fake online dating profiles with photos of other people to lure their victims, scammers often say they are from the U.S. but are temporarily traveling or working overseas.

Scammers quickly profess their love and tug at the victim's emotions with fake stories and their need for money. They often ask for funds to cover plane tickets and other travel expenses. Other scamming situations may include:

- *Victims are duped into providing online banking login credentials. The scammer then logs into the account and is able to pull money from the account. They may also try to set up mobile remote deposit services in order to transmit images of fraudulent checks.*
- *The victim is instructed to send funds to the scammer by Western Union or MoneyGram.*

If a romance scam is suspected, STOP COMMUNITCATING WITH THE SCAMMER IMMEDIATELY, and speak to a trusted family member, friend or financial advisor.

PHISHING/VISHING/SMSHING:

Social engineering fraud is a range of malicious activities carried out by fraudsters through human interactions. It uses psychological manipulation to trick users into making security mistakes.

Unsolicited emails, text messages and telephone calls allegedly from a legitimate company or individual requesting personal, financial and/or login credentials. Forms of social engineering are outlined below:

- **Phishing**- *One of the most popular forms of social engineering. This form is used to gain usernames, passwords and account/card details by the scammer pretending to be a trusted entity and creating a sense of urgency, curiosity or fear in victims. Recipients are instructed to click on links to malicious websites or opening attachments that contain malware. DO NOT CLICK ON LINKS OR OPEN EMAIL ATTACHMENTS FROM UNKOWN SOURCES.*
- **SMishing**- *A type of phishing attack using mobile phones and text messaging. Recipients may receive text messages with hyperlinks to malicious URL or downloading malware onto the mobile phone. If it appears to come from a credit union or financial institution requesting to call a fraudulent phone number, CONTACT THE INSTITION USING A NUMBER FROM YOUR RECORDS NOT ONE LISTED IN A VOICEMAIL OR TEXT MESSAGE.*

- **Vishing**- *Voice phishing is scammers attempting to get users to surrender personal information via telephone, which is often used in identity theft. The call may come from a spoofed phone number making it seem like the credit union or financial institution is calling. IF YOU RECEIVE A*

CALL FROM A SPOOFED NUMBER CONTACT THE INSTITUTION BY A NUMBER FROM YOUR RECORDS TO VERIFY LEGITIMACY.

SECRET SHOPPER SCAMS:

People looking to earn extra cash are often tricked into participating in secret shopper scams. These scams work by the participant accepting a job where he/she receives a counterfeit check ranging in amounts of $2000 - $5000 and is instructed to cash the check and buy money orders or gift cards.

The scammers request the money order and/or gift cards be sent to them and the participant will receive a percentage of the check amount once the scammer receives the money order or gift card.

ADVANCED FEE SCAMS:

This occurs when the scammer informs a victim that he/she won a large award or is intitled to a large inheritance from a deceased relative. The scammer then demands the victim to pay taxes and fees before they can receive their money.

The victim often wires the funds to cover the fees and taxes and then never hears from the scammer again.

Elderly Scams:

These scams target seniors who receive a phone call from the scammer pretending to be a loved one, often a grandchild. They often say that they have been arrested and need bail money or are traveling and need money to get back into the country. They request money be wired to them, typically through Western Union. Be sure to call the grandchild or relative at a phone number you have on record for them before any action is taken.

This scam my also include an “attorney” calling on behalf of a loved one who is in trouble. Instead of wiring funds the victim may be asked to purchase gift cards or provide account information.