



HOW TO SPOT **five** COMMON SCAMS TARGETING SENIORS

BY JESSICA STEINHOFF

Scammers have been very busy during the COVID-19 pandemic, and unfortunately, seniors are a favorite target. According to the Senate Special Committee on Aging, seniors lose nearly \$3 billion to fraud each year.

Imposter Fraud

Imposters assume fake identities to steal your money, identity, or both. They contact by phone, text message, or email.

- A person claiming to work for the IRS, Medicare, the

sheriff’s department, or another trustworthy agency contacts you, stating you owe a fine or are under investigation.

- A scammer steals your bank account’s online login credentials and uses them to trigger a security code needed to reset your password. They then call you, posing as a bank employee, and ask you to read the code to them. Once they have the code, they change your password, enter your account, and transfer your money elsewhere.

- Someone says they represent a well-known charity and asks for a donation.

- You’re contacted by a person claiming to be a relative, saying they need money right away.

“Thinking carefully and moving slowly are two of your best lines of defense against imposter fraud and many other types of scams,” says Julie Walser, UW Credit Union’s loss prevention manager. “Scrutinize any unexpected messages you receive, and avoid taking immediate action.”

In most cases, government agencies won’t call you out of the blue asking for personal details, legitimate charities won’t ask you to wire money, and it’s unlikely a relative would ask for your Social Security number. To make sure a person is legitimate, do some research. If the person claims to represent an organization, call the organization to verify the person is who they say they are. If a person claims to be a relative, ask to call them back, and do so using the phone number you have, not the one they just provided.

Phishing

Phishing is similar to imposter fraud, but can look a little different. You receive an email or text that looks like it’s from a bank, store, or person you’re familiar with, and you’re asked to share sensitive personal information, such as your username and password or Social Security number. If you’re not expecting a call, be very cautious if you don’t recognize the person. Also, be wary of clicking on email links or attachments. If you’re unsure of the sender, verify their identity by calling the company or organization they say they represent.

Overpayment Scams

These scams involve someone telling you to send money they’ve supposedly given you by accident.

- You receive a fake check, and the person asks you to return it to them as cash.

- You’re told that you’ve won a prize but need to send money to



cover taxes and fees. You might also be asked to share sensitive personal information, such as Social Security, bank account, or credit card numbers.

- Someone who purchased an item from you online claims they mistakenly overpaid and asks you to reimburse them in gift cards.

To steer clear of fraudulent attempts, don’t send money to someone who sends you a check. If you sell an item online or at a garage sale, don’t accept checks for more than your selling price. When possible, use a secure online payment service when you sell something to a stranger.

Debt Collection Scams

A person demands that you send payment for a debt you don’t owe or that you’ve already paid. The person may try to scare or shame you into complying. If someone claims to be a debt collector and pressures you to pay them, don’t give them any money unless you’re certain the person and debt in question are legitimate.

- Make sure the debt you’re asked to pay is a debt you owe. Check your records and ask the person to provide written proof.

- Confirm the collection agency is real. Typically, you’ll be able to locate a legitimate agency online.

- Make sure you’re speaking with a real debt collector by asking

for their name, company name, street address, and debt collector license number, then follow up with the company.

Sweetheart Scams

These are particularly cruel. A scammer pretends to fall in love with the victim to gain their trust and steal their money. They frequently target people who’ve recently lost spouses, and often begin on dating apps or social media. The victim may lose money by sharing bank account numbers or passwords, or the scammer might ask for airline tickets, tuition payments, or money for medical bills. Protect your money and heart by refusing to wire money to anyone you don’t know well, even if you’ve formed a connection online. Also, be wary of emails from people who claim to know you.

Stay informed about the latest scams making the rounds, which can hook not only seniors but their loved ones and caregivers. The Federal Trade Commission’s Scam Alerts web page (consumer.ftc.gov/features/scam-alerts) is a great place to start.

Jessica Steinhoff writes about financial wellness for UW Credit Union, a not-for-profit financial institution that offers checking and savings accounts, loans, and secure online banking tools. See uwcu.org for details.



UW Credit Union
3500 University Ave.
Madison, WI 53705
(800) 533-6773
uwcu.org