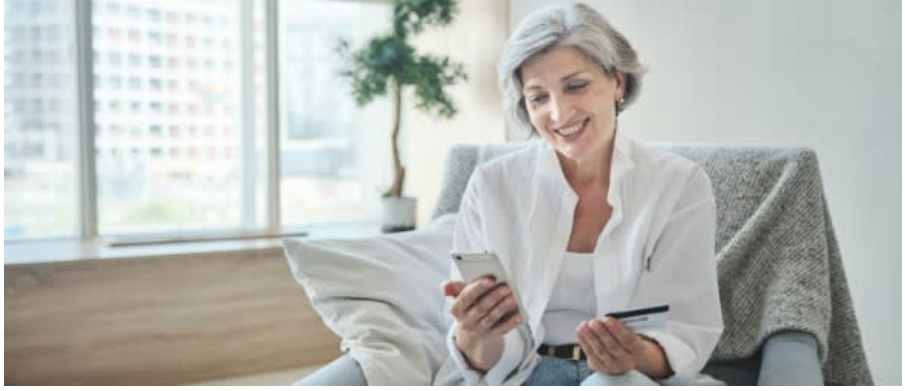
People's CREDIT UNION

LOCATIONS & HOURS

Protecting You From Fraud & Scams

Welcome to your Fraud and Scams Prevention newsletter. With an increase in fraud and scams, we have put this together to provide information on the most recent fraud schemes, risks, and preventive strategies. We aim to increase awareness and promote good practices that can help protect our members and help you stay informed, alert, and empowered to safeguard your assets and personal information.



Beware the Long Con!

Sometimes, when lonely people meet someone online, instead of being asked for money in a short period of months, they are asked for it after several years. This is considered a long con often called “the pig butchering scam” because fraudsters are seen as “fattening the pig” before going in for the kill.

Don’t trust that unexpected text or direct message from a stranger. They often start with solicitations of modest investments intended to bolster your confidence, involving some type of fake claim or falsified dashboard that shows assets exponentially growing, with the intent being to encourage larger and larger investments.

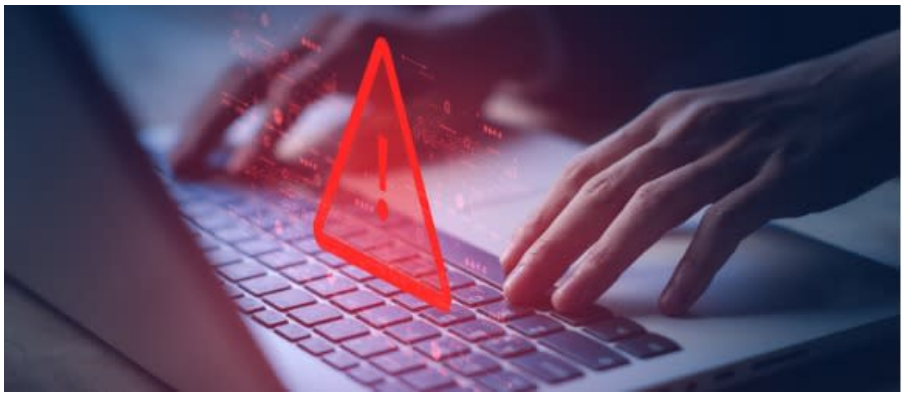
The next phase of the scheme is twofold: to create the perception that you’ll make money by following their instructions and to ensure that you are able to invest into the scam. They want to entice you to put your money toward the “opportunity” they’ve shared, all the while manipulating your decision-making. Once you’ve deposited increasingly larger amounts, they flip the switch and leave you facing devastating losses.

Watch for Warning Signs

To avoid becoming a victim of a pig butchering scam, watch for these red flags:

- Unexpected contact
- Refusal to participate in video chats
- Request for financial information
- Invitation to invest in specific financial products
- Unknown or confusing investment opportunity
- Unfamiliar trading platforms
- Exaggerated claims and elevated emotions
- Sense of urgency about an upcoming news announcement or share price increase

Learn more about how to protect your money **from fraud and get more insight on pig butchering schemes involving cryptocurrency from the FBI and the Financial Crimes Enforcement Network (FinCEN).**



Protect Yourself from Much-Too-Common Cyber Fraud

Scams and phishing attempts are everywhere these days. It’s important to stay alert to potential attempts in your day-to-day life.

Subscription Service Alert Scams

You receive an urgent email that your subscription or membership has expired, and the email asks you to click a link to provide your payment information in order to renew. To avoid these types of impostor email phishing scams, here are three best practices:

1. Take a second and third look at the email. If the sender’s email address is a long string of numbers and letters that don’t make sense, or if it just doesn’t look right, it’s likely an impostor.

2. Keep track of your subscriptions and any auto-renewing payments. That way, you can better determine when a subscription renewal email is fake.
3. Think twice before providing payment for something you didn't initiate. If you're being asked to pay with your bank account number, prepaid credit cards, digital wallet apps, or wiring money, this is a red flag.

Lottery Winnings Scams

Scammers will take advantage of the promise of winning a lot of money or a big prize to get your money or personal information. It's a scam if

- You have to pay a fee for "taxes," "shipping and handling charges" or "processing fees."
- Someone asks you to pay to increase your odds of winning.
- You have to give your financial information.

Scammers will say anything to trick you into thinking you really won a prize.

If you're not sure about a contest or the company sending you a prize notification, search online to see if you find anything about them. Type the name with terms like "review," "complaint," or "scam."

Auto Warranty Scams

If you own a vehicle, you may receive calls from scammers posing as representatives of a car dealer, manufacturer, or insurer, telling you that your auto warranty or insurance is about to expire. During the call—which often begins automatically or pre-recorded—you may be instructed to press a certain number or stay on the line, then asked to provide personal information. Do NOT provide any personal information unless you can verify you are dealing directly with a legitimate company with which you have an established business relationship.

Legitimate telemarketers are required to transmit or display their phone number and the name and/or the phone number of the company they're representing. But be cautious even if a number appears authentic. Criminals may engage in caller ID "spoofing" – deliberately falsifying the information transmitted to your Caller ID display to disguise their identity.

You can file a complaint with the FCC about suspected scam calls. In addition to being fraudulent in nature, these calls likely violate telemarketing and robocall rules.

Government Imposter Scams

According to the Federal Trade Commission, in 2023 alone, older adults reported losing a total of $200 million to imposter scams, with fraudsters posing as the IRS, Medicare, or the Social Security Administration.

It should be a huge red flag if someone you don't know immediately starts pressuring you by phone, text or any other way. Approach any of these types of messages with a healthy dose of skepticism. Hang up. Delete. Ignore. If the IRS, Social Security Administration, Medicare, or other government agency needs you, they'll send a letter.

Fraudulent Transaction Alert Scams

A new and complicated scam starts with a call or text message about a suspicious charge on one of your online accounts, like Amazon. But it's not really Amazon. It's scammers spoofing their phone number to make it look like it's Amazon calling. Don't trust the number in your caller ID and don't trust what the caller tells you. If you're worried about a suspicious purchase on Amazon, check it out through the website or app. Don't call back the number that called you or a number someone left in a voicemail or text message.

To scare you and get your information, scammers will tell you that someone used your name or Social Security number to open fraudulent accounts in your name. Do not transfer money or drain your savings to protect it from fraud. You can get an instant copy

Contact us:

Email: memberservice@peoplescu.com

Phone: 800.498.8930

Follow Us: