May 2021

Oregon State Credit Union **difference**

Oregon State Credit Union

Learn to recognize the signs of a scam

You can avoid falling victim to scams by learning to recognize features common to most of them:

- It involves money, either paying someone or moving money around for them.
- They need your personal information, like your Social Security number, online banking login and password, credit card number or similar.
- It sounds too good to be true – you've won the lottery or a sweepstakes – or it's a get rich quick scheme.
- There is pressure to act fast. Scammers don't want you to have time to think or get a second opinion.
- There's a fear factor such as the threat of police involvement, a problem with your credit union or Social Security account, a virus on your computer or someone in your family needs help.
- You have to pay in a specific way, like a wire transfer or a gift card.

Scam protection begins with knowledge

Getting scammed is an unpleasant experience, but one you may be able to avoid by learning how to recognize fraud and knowing what to do about it. Below are some of the most common scams circulating today. This is not a comprehensive list – new scams are born every day – but being able to recognize these seven scams will help protect you much of the time.

1. Helpful fraud department: In this scam, the caller pretends to be with your credit union's fraud department. The caller is likely using a spoofed phone number to make the incoming number look legitimate. The caller explains that possible fraudulent activity occurred on your credit card or account, and they provide you with fake transaction details or your card number so you believe them. They may even claim they have blocked your card. Under the guise of verifying your identity and helping you get a new card, the caller will attempt to gain your personal and private banking information.

What you can do: Oregon State Credit Union will never ask you for your online banking username and password. Nor will we ever ask for the authentication code you're sent when you log in

to online banking or the mobile banking app. To protect your financial information, never:

- Respond to suspicious or unexpected emails or texts.
- Click on links in a text or email unless you know where those links will take you.
- Share your online banking username and password. Those two pieces of information allow scammers access to your account.

2. Overpayment scam: If you have ever sold something online or through a public advertisement, you may have encountered this. This is when a scammer pays you more than the amount needed to cover the sale. They may say the extra is for shipping or other fees. They may instruct you to deposit a check, money order or cashier's check and send any unused portion back to them. They

Scam protection begins with knowledge, continued on page 2 ➜

Scam protection begins with knowledge, continued from page 1 ➜

will pressure you to complete the transaction quickly – typically within a few days. But after you send the money, the check will bounce or prove to be fraudulent, potentially leaving you responsible for the full amount of the check and any associated fees.

What you can do: Insist on being paid only the amount of money you need to complete the sale. See the "fake check" scam for more information.

3. **Fake check scam:** Similar to the overpayment scam, scammers lure people into depositing a check, cashier's check or money order and then wiring some or all of the money back to the scammer. This may be part of an overpayment scam, online sale, a romance scam or similar. The scammer may pressure you to act fast. By the time you discover the check is fraudulent, the scammer has your money and you may be on the hook for the amount of the check plus any associated fees.

What you can do: Remember, someone you have only met online is a stranger, no matter how authentic or romantic the relationship may seem. If someone wants to pay you with a check, money order or cashier's check, you'll want to wait until the check has fully cleared before you return any portion of the money to the potential scammer. If you've sold something online, the check may be legitimate. If so, the buyer should be willing to wait while you determine the check's authenticity. If they insist you send them money immediately, discontinue the sale or relationship.

4. **Wire transfer:** Scammers love wire transfers because they are are a fast, irreversible way to send money domestically or internationally.

What you can do: Never send money by wire transfer to a stranger or someone you've met online.

5. **Gift and prepaid card:** One popular scam is to solicit payment or donations by pre-paid credit cards or gift cards.

What you can do: Be wary of anyone who asks to be paid in this manner. Gift cards are like cash, and charges cannot be reversed. If someone insists on being paid in this way, break off contact with them.

6. **Amazon scam:** This involves people operating under the guise of Amazon® customer service. They may say you are due a refund, there is a problem with your order or there has been a security breach.

What you can do: If you get a text or email advising you to call Amazon, do not call the phone number in the message, and do not call Amazon at a phone number you found by searching online. If you get a message about a refund you did not expect, do not provide your credit union account information. In all these cases, you should log in to your Amazon account and contact customer service from within your Amazon account. And remember, never click on a link in an email unless you know with absolute certainty who is sending that email.

7. **Tech support:** Tech support scammers want you to believe you have a serious problem with your computer, like a virus. They want you to pay for tech support services you don't need to fix a problem that doesn't exist. They often ask you to pay by wiring money, putting money on a gift card or using a person-to-person app like Pay It Now, Zelle® or Venmo™. Scammers know those types of payments can be hard to reverse.

What you can do: Don't trust anyone who contacts you about a problem on your computer. If you think you have a problem, find a vendor you trust to handle the issue.