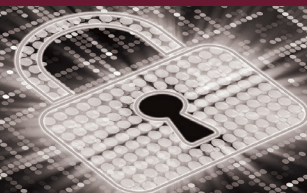


ONLINE SECURITY

What to do if you are the victim of a scam.



If You Paid a Scammer:

♦ Did you pay with a credit card or debit card?

Contact the company or bank that issued the credit card or debit card to report the information so they can begin an investigation as soon as possible.

♦ Did a scammer make an unauthorized transfer from your bank account?

Contact your bank to report the information so they can begin an investigation as soon as possible.

♦ Did you pay with a gift card?

Contact the company that issued the gift card. Tell them it was used in a scam. Keep the gift card itself, and the gift card receipt.

♦ Did you send a wire transfer through a company like Western Union or MoneyGram?

Contact the wire transfer company. Tell them it was a fraudulent transfer.

MoneyGram at 1-800-926-9400

Western Union at 1-800-448-1492

Ria (non-Walmart transfers) at 1-877-443-1399

Ria (Walmart2Walmart and Walmart2World transfers) at 1-855-355-2144

♦ Did you send a wire transfer through your bank?

Contact your bank and report the fraudulent transfer.

♦ Did you send money through a person-to-person money transfer app?

Report the fraudulent transaction to the company behind the money transfer app. If you linked the app to a credit card or debit card, report the fraud to your credit card company or bank.

If You Gave a Scammer Your Personal Information:

♦ Did you give a scammer your Social Security number?

Go to IdentityTheft.gov to see what steps to take, including how to monitor your credit.

♦ Did you give a scammer your username and password?

Create a new, strong password. If you use the same password anywhere else, change it there, too.

If a Scammer Has Access to Your Computer or Phone:

♦ Does a scammer have remote access to your computer?

Update your computer's security software, run a scan, and delete anything it identifies as a problem. Then take other steps to protect your personal information.

♦ Did a scammer take control of your cell phone number and account?

Contact your service provider to take back control of your phone number. Once you do, change your account password.

Also check your credit card, bank, and other financial accounts for unauthorized charges or changes. If you see any, report them to the company or institution. Then go to IdentityTheft.gov to see what steps you should take.

Report Scams to the FTC

If you were scammed or think you saw a scam, tell the FTC at ReportFraud.ftc.gov



www.citizensEbank.com



15 Branches across 13 communities in the Willamette Valley

Member
FDIC