SCAMS

We continue to see scams in many different forms. Some are phone scams and others are computer scams. No matter how they are reaching you, scammers will do everything in their power to part you and your money. We hope you will find the information here useful and it will help keep you and your money safe.

We want to remove the stigma and any shame that surrounds being scammed. We don't want you feel embarrassed. We just want to keep you from losing your hard earned money. These individuals are very adept at their craft. They will already have found information about you online through internet research, mail theft and other venues that allows them to have enough information to try to scare you into doing something to give them money.

We hope you find the information here helpful and if you have any questions, please reach out to us.

Phone Scams

Clatsop County Sheriff's Office Issues Warning on Recent Phone Scams

April 26, 2024 – Our Office is alerting residents to a surge in phone scams targeting individuals in our community. We have reports of individuals at the bank trying to withdraw thousands of dollars to pay for “fines” to avoid warrants and jail time. This is simply not the way we conduct business as a law enforcement agency. These scams are designed to deceive victims by posing as legitimate entities and using convincing tactics to extract personal information or money.

Scammers employ various strategies to make their scams appear authentic, including spoofing phone numbers to mimic official organizations, using urgency or fear tactics, and providing false promises of prizes or rewards.

Common tactics used by scammers to convince victims include:

1. Threats and Urgency: Scammers may create a sense of urgency by threatening legal action, arrest, or immediate consequences if the victim does not comply.
2. Spoofing and Impersonation: They often spoof legitimate phone numbers or impersonate trusted organizations, making their calls seem genuine.
3. False Promises: Scammers may lure victims with false promises of prizes, rewards, or services, leading them to share personal information or make financial transactions.

To avoid falling victim to phone scams, the Sheriff's Office recommends the following precautions:

1. Verify Caller Identity: If you receive a suspicious call, verify the caller's identity independently using official contact information from trusted sources.
2. Do Not Share Personal Information: Avoid sharing sensitive information such as social security numbers, bank account details, or passwords over the phone.
3. Be Wary of Unsolicited Offers: Be cautious of unsolicited offers, especially those requiring immediate action or payment.
4. Don’t answer the call, let it go to voicemail: This will allow you to verify information before responding to a call.

The Sheriff's Office urges residents to stay informed and share this information with family, friends, and neighbors to prevent falling victim to phone scams. For more information or to report a scam, contact the Clatsop County Sheriff's Office through non-emergency dispatch at 503-325-2061 or visit our website at https://www.clatsopcounty.gov/sheriff

Stay vigilant and protect yourself from phone scams!

Say NO to the "Say Yes" Scam

How the “Say Yes” Scam Operates

The “Say Yes” scam is a telephone scam designed to trick individuals into saying the word “Yes.” Generally, the scam begins with a call from an unknown number, often with a local area code to appear more legitimate. When you answer, the scammer will usually pose as an employee of a company or other organization.

Their main objective is to record you saying “Yes” during the conversation. For example, common phrases include:

- Can you hear me?
- Are you there?
- Are you the homeowner?
- Is this [your name]?

While these questions seem harmless, the scammers do have malicious intent.

How Scammers Use the Audio Recording

Fraudsters utilizing the “Say Yes” scam often already have some of your personal information, such as your credit card number. For example, they could have obtained this data from a security breach or another identity theft ploy.

Then, they enroll you in products or services and charge them to your credit card or other financial accounts. They use your recorded “Yes” as proof that you gave permission to purchase or subscribe to these services.

Tips to Protect Yourself from Telephone Scams

Today’s digital world allows fraudsters to mimic companies and organizations online easily. This makes spotting modern day scams challenging. Fortunately, it’s much easier to protect yourself against telephone scams.

- Always be cautious when answering calls with unfamiliar numbers – even if it’s a local number.
- Most phone companies today provide call-blocking or robocall protection; however, you might inquire about additional spam call protection services or utilize third-party apps.
- If you receive a phone call that begins with “Can you hear me?” or another common “Say Yes” prompt, respond with a question. For example, reply with, “Who is calling?” or “May I ask what this call is about?” Questions like this may result in the fraudster hanging up.
- If you receive an unsolicited call that seems suspicious, hang up and do not engage with the caller. It’s much better to protect yourself from potential scams than to worry about appearing rude.

What To Do If You’re a Victim of a Telephone Scam

If you believe you were a victim of the “Say Yes” scam, don’t panic. Instead, remain vigilant and monitor your financial accounts and credit card statements for potential fraud.

If you engaged with the caller and provided personal or financial information, consider the following steps:

- Enroll in identity theft protection services.
- Obtain a new credit or debit card from your financial institution (if you provided this information to the caller).
- Monitor your accounts daily for possible fraudulent charges.
- Review your credit report for free at www.AnnualCreditReport.com.
- Use a credit score service, such as www.Experian.com or www.CreditKarma.com, to monitor changes in your score.
- If you notice fraudulent charges, contact your financial institution immediately. Also, report the scam to the Federal Trade Commission at www.FTC.gov/complaints/.

What to do if you already paid the scammer

What To Do If You Already Paid a Scammer

Scammers will often ask you to pay in a way that makes it hard for you to get your money back. Don't pay someone who insists that you can only pay with a gift card, cryptocurrency, a payment app, or a wire transfer service like Western Union or MoneyGram. It's a scam.

If you paid someone one of these ways, act quickly to report it to the company or bank behind the gift card, cryptocurrency, payment app, or wire transfer service. Depending on how you paid, you might be able to get your money back. But no matter how you paid, it's worth asking.

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. Tell them it was a fraudulent charge. Ask them to reverse the transaction and give you your money back.
Did a someone make an unauthorized transfer from your bank account?	Contact your bank and tell them it was an unauthorized debit or withdrawal. Ask them to reverse the transaction and give you your money back.
Did you buy a gift card and give someone the numbers off the back of the card?	Contact the company that issued the gift card. Use this list of contacts. Tell them the card was used in a scam and ask for your money back. Keep a copy of the gift card and the store 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. Ask them to reverse the wire transfer and give you your money back. • 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. Ask them to reverse the wire transfer and give you your money back.
Did you send money through a payment app?	Report the fraudulent transaction to the company behind the payment app and ask them to reverse the payment. If you linked the app to a credit card or debit card, report the fraud to your credit card company or bank. Ask them to reverse the charge.
Did you pay with cryptocurrency?	Contact the company you used to send the money and tell them it was a fraudulent transaction. Ask them to reverse the transaction.
Did you send cash?	If you sent cash by U.S. mail, contact the U.S. Postal Inspection Service at 877-876-2455 and ask them to intercept the package. To learn more about this process, visit USPS Package Intercept: The Basics. If you used another delivery service, contact them as soon as possible.

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 someone calls and offers to “help” you recover money you have already lost, don’t give them money or personal information. You’re probably dealing with a fake refund scam.

Source – Federal Trade Commission