OREGON DEPARTMENT OF JUSTICE
Consumer Outreach & Education | Consumer Advocacy

2026 EDITION

SCAMS, FRAUD & UNLAWFUL BUSINESS PRACTICES

This toolkit offers linked resources and information to help you spot warning signs, ask the right questions and take simple steps to protect yourself.

PROTECT YOURSELF BEFORE YOU CLICK, SHARE SEND MONEY, OR TRUST UNEXPECTED REQUESTS

SPOT WARNING SIGNS

ASK THE RIGHT QUESTIONS

PROTECT YOURSELF

REPORT PROBLEMS

EMPOWERING OREGON CONSUMERS.
BUILDING STRONGER COMMUNITIES.

Protect Yourself. Know Your Rights.

OREGON DEPARTMENT OF JUSTICE

Consumer Outreach & Education | Consumer Advocacy

SCAMS, FRAUD & UNLAWFUL BUSINESS PRACTICES

A PRACTICAL GUIDE FOR OREGON CONSUMERS, WORKING FAMILIES, SENIORS AND OLDER ADULTS.

Scammers and those who adopt unethical business practices want to build false trust to gain access to your personal information or your money. They may contact you by phone, text, email, social media or online.

Learning how scams work is one of the best ways to reduce your risk.

CONSUMER TIP

Give yourself permission to pause.

WHY THIS MATTERS

The Oregon Consumer Advocacy Program receives an average of over 9,000 complaints a year. Many involving fraud, scams, and unethical business practices.

While not every incident is reproted, these complaints show that scams continue to affect individuals, families, older adults and businesses across Oregon.

WHAT'S INSIDE

File a complaint or search Oregon's complaint database: oregonconsumer.gov

1 PART 1: WHAT TO KNOW

Scams, fraud & unethical business practices

Scammers use trust, fear, urgency, and technology to convince people to send money or share personal information. Although many scams may look different, many follow the same pattern. Understanding these tactics can help you recognize suspicious activity before it leads to financial loss.

Scammers use fake trust to gain your trust.

Common impersonations include:

- Government agencies
- Financial institutions
- Utility companies
- Internet/phone providers
- Tech support
- Law enforcement
- Family & friends
- Delivery companies
- Retail or delivery companies.

Create a sense of urgency

They may claim:

- Your account has been locked or compromised
- Your payment is overdue
- You've won a prize
- A loved one is in trouble.
- Your device has a virus.
- You'll be arrested or fined unless you act now.

They want information or your money

They may ask for:

- Wire transfers
- Gift cards
- Cryptocurrency
- Payment apps
- Banking information
- Passwords
- Verification codes
- Social security numbers
- Credit card number, pin or code.

Scams can happen anywhere

- Phone calls
- Text messages
- Emails
- Social media
- Dating apps
- Online marketplaces
- Fake websites
- Messaging apps
- Mail
- Door to door
- In person

REMEMBER: If something feels rushed, confusing, or too good to be true, **STOP** and **VERIFY** information independently.

HOW MOST SCAMS AND FRAUD WORK

Unexpected Contact
You're contacted by phone, text, email, social media, or in person.

→

Build Trust
They try to build a relationship or have you trust what they saying.

→

Create Urgency
They pressure you to act or make a decision quickly or keep it a secret.

→

Request money or information
They ask for money, gift cards, transfers, crypto or personal information.

LEARN MORE: Fraud and Scams:The Basics or Recognize an Impersonator

CONSUMER TIP | **Stop. Verify. Ask questions.** Talk with someone you trust before sending money or personal information.

2 PART 2: WHAT TO WATCH FOR

Warning Signs

SCAM ALERT

Although unethical business practices, scams, and fraud evolve, their warning signs are often similar. Recognizing these signs before sending money, clicking a link, or sharing information can help you reduce the risk of financial loss or compromised personal information.

- **Pressure to act immediately**
- **Ask to keep it a secret**
- **Request for personal information**
- **Romance that quickly turns financial**
- **Request for gift cards**
- **Wire transfers requests**
- **Fake family emergencies**
- **Cryptocurrency payment requests**
- **Threats of arrest, lawsuit, fines or suspended accounts**
- **Investment opportunities promising guaranteed returns**
- **Unexpected calls or texts**
- **Caller ID spoofing, phishing, smishing or fake numbers**
- **"Too good to be this" offers**
- **Fake tech support or pop-up alerts**

Common Type of Scams and Fraud

- Auto Scams
- Solar Scams
- Health and Medical
- Imposter Scams
- Romance Scams
- Telecommunications Scams
- Tech support
- Construction scams
- Online Shopping
- Financial and Investment Scams
- Rental or travel Scams
- Business Scams
- Employment Scams

Create an action plan at FTC WORKSHEET or find out what to do if you been scammed

3 PART 3: BEFORE, DURING & AFTER

PROTECTING YOURSELF, YOUR FAMILY AND COMMUNITY

A few simple steps can help you avoid scams, fraud and unethical business practices while reducing risks and potential financial losses.

BEFORE

Stay alert and proactive

- [ ] Research any complaints and check reviews.
- [ ] Verify independently who is contacting you and why.
- [ ] Create strong, unique passwords.
- [ ] Talk to someone you trust before wiring any money or sharing personal information.
- [ ] Register for the Do not Call Registry.

DURING

Stay in Control

- [ ] Take notes of names, numbers and dates.
- [ ] Do not click on links or open attachments.
- [ ] If you feel pressured, PAUSE.
- [ ] Ask questions.
- [ ] Do not allow remote access if you did not start the contact.
- [ ] Keep records of calls, emails and texts.

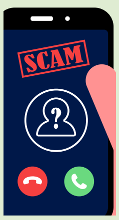
AFTER

Stay informed

- [ ] Contact your financial institutions.
- [ ] Change passwords.
- [ ] Visit identitytheft.gov
- [ ] **Report** scam, fraud or bad business practices.
- [ ] Monitor your accounts, devices and credit reports,
- [ ] Freeze your credit if needed.

REMEMBER:
You have the right to say:
"I need time to think about this."

QUICK REMINDERS



Stay vigilant with unexpected calls, texts, or emails

Verify all information

Talk with someone you trust before taking action

Protect your personal information like your finances.

PART 4: WHERE TO GET HELP

Reporting Problems

Use the guide below to help determine where to report a concern.

Before fling a complaint, Gather:

- Contracts, receipts
- Purchase Agreements
- Loan Documents
- Repair Estimates
- Photos, screenshots
- Emails, text messages
- Notes with dates, names, etc.

REPORTING MATTERS

- ✓ Mediate or resolve disputes.
- ✓ Identify patterns of misconduct.
- ✓ Protect other Oregon consumers.

Scan QR code to file a consumer complaint or file at:

justice.oregon.gov/consumercomplaints

Learn more at: oregonconsumer.gov or email:help@oregonconsumer.gov

WHO SHOULD I CONTACT?

Fraud, scam or unethical business practices	**Oregon DOJ-** oregonconsumer.gov **Federal Trade Commission -** ftc.gov
Identity theft	identitytheft.gov
Financial services or products	**Consumer Financial Protection Bureau** consumerfinance.gov **Division of Financial Regulation** dfr.oregon.gov
Internet crime, phishing, crypto, online fraud	**FBI Internet Crime Complaint Center (IC3) -** ic3.gov
Legal support	**Oregon State Bar Lawyer Referral Services -** osbar.org/public/ris 503.684.3763
Consumer education and advocacy	**Oregon Consumer League -** oclactionfund.org **Oregon Consumer Justice -** ocj.org 503.406.3311 **AARP Fraud Watch -** aarp.org/fraudwatchnetwork 1.877.908.336
Peer support after fraud	**Give an Hour Peer Support -** giveanhhour.org
Scam reporting & community alerts	**BBB Scam Tracker -** bbb.org/scamtracker

Before I respond, I will:

- ✓ Stop and slow down
- ✓ Verify who contacted me
- ✓ Research independently
- ✓ Talk to someone I trust
- ✓ Never share passwords or personal information or send money
- ✓ Keep learning signs it's a scam

REMEMBER: STOP → CHECK → DOCUMENT → REPORT

WORKSHEET:

Scam Prevention Checklist and Verification log

BEFORE I RESPOND, I WILL:

- ☐ Give myself permission to slow down.
- ☐ Verify who is contacting me.
- ☐ Call the agency/institution directly.
- ☐ Research independently.
- ☐ Never send gift cards, wire transfers or share personal information without veirfying first.

CONTACT VERIFICATION LOG

Who contacted me and why? ______________________

How did they contact me? ______________________

Organization affiliation? ______________________

What did they ask me to do? ______________________

Did I feel pressured to act quickly?

☐ YES ☐ NO

They ask for money or personal information?

☐ YES ☐ NO

NOTES: ______________________

WHAT DID THEY ASK FOR?

- ☐ Money
- ☐ Gift cards
- ☐ Crypto
- ☐ Wire transfer
- ☐ Bank account info
- ☐ Home remodel
- ☐ Personal info
- ☐ Other ______________

RECORDS TO SAVE

- Contracts
- Receipts, confirmations or documents
- Screenshots
- Emails, texts, call logs, advertisements
- Names & Dates
- Phone numbers
- Tracking /Transaction ID or reference #

If you've already been scammed

Stop sending money, giving access to your accounts or information.

Contact your bank or financial institutions. Preferably in person.

Change your passwords and save all records and communications.

Report the incident and reach out for support.