PROJECT LENS

RESOURCE GUIDE 03 OF 06

Scam Prevention Guide

See AI clearly.

Think clearly in an AI-powered world.

L	Learn	Understand AI.
E	Evaluate	Question and verify.
N	Navigate	Know when and how to use it.
S	Secure	Protect yourself and others.

Version 1.5 · Updated October 27, 2026

01

Welcome

Scammers are using AI to sound more real than ever. A few simple habits still stop almost every scam, and this guide shows you how.

Being targeted is not your fault. Scams are run by organized criminals who do this all day. Smart, careful people get fooled every week. The goal is not to be perfect. The goal is to slow down and check.

How to use this guide

- Read the red flags and the PAUSE. VERIFY. ASK. steps first. They matter most.
- Do the "protect yourself ahead of time" checklist with a family member or friend.
- Keep the response card on the last page by your phone.

02

How AI is changing scams

In 2025, Americans age 60 and older reported losing **$7.7 billion** to online fraud, up 59% from the year before. In Oregon, people 60+ reported losing more than **$77 million** (FBI IC3 2025 report). Most scams are never reported, so the real numbers are higher.

AI doesn't create new kinds of scams. It makes the old ones more convincing.

- **Voice cloning.** With just a few seconds of someone's voice from a video or voicemail, AI can copy it. Scammers use it to sound like a grandchild or child in trouble. The FBI reports these "loved one in distress" calls in its 2025 report.
- **Deepfake videos.** Fake videos show celebrities, doctors, or news anchors promoting investments or miracle products. They are often shared as social media ads.
- **Perfect messages.** Scam emails and texts used to have spelling mistakes. AI now writes them smoothly, in any language, using details from your public social media.
- **Fake chatbots and websites.** Scammers build "customer service" chats and copycat websites that look exactly like your bank, Medicare, or a well-known store.
- **Fake investment "experts."** AI-made videos and chat messages promise big returns from crypto or "AI trading." Investment fraud caused the largest losses for older adults in 2025.

The good news: AI can fake a voice or a face, but it can't fake a call you make yourself to a number you already know.

03

The most common scams

The first three scams below (investment, tech support, and romance) were the biggest money-losers for people 60 and older in the FBI's 2025 report. Government impersonation is also common and costly. The rest are very common too. Learn what each one sounds like.

Scam	What you might hear or see	The giveaway
Investment	"Our AI trading system doubles your money." A friendly stranger on social media or a celebrity video shares a "sure thing."	Guaranteed returns; pressure to move money into crypto
Tech support	A pop-up or call: "Your computer has a virus. Call Microsoft now."	Asks for remote access to your computer, or payment to "fix" it
Romance or friendship	A kind new online friend who is always traveling, overseas, or in the military	Can't meet in person or video chat; soon needs money
Government impersonation	"This is Social Security / the IRS / Medicare. Your number is suspended."	Threats of arrest; demands payment by gift card, wire, or crypto
Family emergency (grandparent)	A panicked voice that sounds like your grandchild: "I'm in jail, don't tell Mom."	Secrecy and urgency; a "lawyer" or "officer" takes over the call
Bank or fraud department	"We've detected fraud. Move your money to a safe account."	Real banks never ask you to move money to protect it
Delivery and shopping	A text: "Your package can't be delivered. Click to reschedule."	A link you didn't expect; asks for card details
Prize or lottery	"You've won! Just pay the taxes and fees first."	You must pay to receive a prize
"Recovery" scam	"We can get back the money you lost, for a fee."	Targets people who were already scammed

04

Red flags

If you notice even **one** of these, stop and check before you do anything.

The message or call...

- Says it's urgent: "right now," "today only," "or you'll be arrested"
- Asks you to keep it secret, even from family
- Came out of the blue, from someone you didn't contact first
- Wants you to stay on the phone while you go to the bank or store
- Plays on strong feelings: fear, excitement, love, or guilt

They want you to...

- Pay with **gift cards, wire transfers, cryptocurrency, a Bitcoin ATM, or cash** handed to a courier
- Click a link, scan a QR code, or download an app
- Share a code that was texted to you (real companies never ask for it)
- Give remote access to your computer or phone
- Move your money to a "safe" account

Something seems a little off...

- The voice sounds right, but the way they talk doesn't
- The caller ID shows a real company or agency (these can be faked)
- A video looks slightly unnatural: strange blinking, blurry edges, lips out of sync
- The deal is too good to be true

05

PAUSE. VERIFY. ASK.

Three steps stop almost every scam. You can use them on any call, text, email, video, or knock at the door.

1. PAUSE: urgency is a scammer's best tool

You are always allowed to hang up, close the message, or say "I'll call you back." A real emergency will still be real in ten minutes.

Words to say: "I don't make decisions on the phone. I'll call you back." Then hang up.

2. VERIFY: check using a number you already have

Never use the number, link, or email in the message itself.

If they say they're...	Verify by...
Your grandchild or family member	Calling their own phone, or another relative. Ask for your family safe word.
Your bank	Calling the number on the back of your card
Medicare, Social Security, or the IRS	Calling the number on the official .gov website or a letter you already have. They mail letters first.
A company (Amazon, Microsoft, a utility)	Logging in to your account yourself, or calling the number on a past bill
Police, a lawyer, or a court	Looking up the agency's number yourself. Real officials don't demand payment by phone.

Words to say: "What's your name and department? I'll call the main number myself."

3. ASK: talk to someone you trust

Scammers want you alone and in a hurry. Before you send money or share information, tell a family member, friend, neighbor, or your bank. Saying it out loud often makes the scam obvious.

Words to say: "Let me run this by my daughter first." A scammer will push back. A real person will say "of course."

06

Protect yourself ahead of time

A little setup now makes scams much harder later. Do this checklist with someone you trust, and tick each item when it's done.

- [ ] **Choose a family safe word.** Pick a word or phrase only your family knows. Anyone calling as family in an emergency must say it. Don't post it or text it.
- [ ] **Name a trusted contact.** Choose one person you'll always call before sending money. Ask your bank to add them as a "trusted contact" on your accounts.
- [ ] **Turn on bank and card alerts.** Ask your bank to text or email you for every large withdrawal or purchase.
- [ ] **Freeze your credit.** It's free and stops anyone from opening new accounts in your name. Call Equifax, Experian, and TransUnion (numbers on the last pages).
- [ ] **Block unknown callers.** Turn on "Silence Unknown Callers" (iPhone) or "Call screening" (Android). Ask your phone company about free robocall blocking.
- [ ] **Let unknown calls go to voicemail.** Real callers leave a message.
- [ ] **Limit what you share online.** Make social media accounts private. Avoid posting travel plans, family names, or voice videos publicly.
- [ ] **Use strong passwords and two-step login.** Turn on two-step verification for your email and bank.
- [ ] **Keep devices updated.** Install updates on your phone and computer when asked.

07

If you've been scammed

Act quickly, but don't panic. The sooner you act, the better the chance of stopping the damage. **It is not your fault, and you are not alone.**

In the first hour

1. **Stop all contact.** Hang up, don't reply, and block the number or email.
2. **Call your bank or card company** using the number on your card. Tell them it's fraud. Ask them to stop or reverse payments.
3. **If you paid with a gift card,** call the company on the back of the card right away and keep the card and receipt.
4. **If someone has remote access to your computer,** turn it off or disconnect it from the internet.
5. **Tell your trusted person.** You don't have to handle this alone.

In the first day

1. **Change passwords** for email, banking, and any account you shared. Start with email.
2. **Freeze your credit** with all three credit bureaus if you shared your Social Security number.
3. **Write down everything:** dates, times, names, phone numbers, amounts, and how you paid. Keep screenshots and messages.
4. **Report it** to the FBI at ic3.gov and to the Oregon DOJ at 1-877-877-9392. The National Elder Fraud Hotline (1-833-372-8311) can help you file.

In the first week

1. **Watch your accounts** and statements closely for anything new.
2. **If your identity was stolen,** make a recovery plan at IdentityTheft.gov.
3. **Beware of "recovery" offers.** Anyone who promises to get your money back for a fee is another scammer.
4. **Get support.** The AARP Fraud Watch Helpline (1-877-908-3360) offers free, caring help for victims and families.

08

Who to call

Reporting helps you and helps stop the scammer from reaching the next person.

> **If you feel unsafe or someone is at your door, call 911.**

Oregon

Who	Help with	Phone
Oregon DOJ Consumer Protection	Scams, fraud, consumer complaints	1-877-877-9392
ODHS Abuse Reporting	Elder abuse, including financial exploitation	1-855-503-7233 (1-855-503-SAFE)
Oregon Division of Financial Regulation	Investment, insurance, and banking scams	1-888-877-4894
Oregon SHIBA	Medicare fraud (Senior Medicare Patrol)	1-800-722-4134
ADRC of Oregon	Local senior and disability services	1-855-673-2372
211info	Any local help; interpreters available	Dial 211

National

Who	Help with	Phone
National Elder Fraud Hotline	Case managers help people 60+ report fraud	1-833-372-8311 (1-833-FRAUD-11)

Who	Help with	Phone
AARP Fraud Watch Helpline	Free support for victims and families	1-877-908-3360
FBI Internet Crime Complaint Center	Reporting online crime	Online only
Federal Trade Commission	Reporting scams	1-877-382-4357
IdentityTheft.gov	Recovery plan if your identity is stolen	1-877-438-4338
Social Security OIG	Social Security impostor scams	Online only
Medicare	Medicare fraud	1-800-633-4227
FCC	Robocalls and spoofed numbers	1-888-225-5322

Freeze your credit (free): Equifax 1-888-298-0045 · Experian 1-888-397-3742 · TransUnion 1-800-916-8800

Phone numbers verified on official websites, October 1, 2026.

09

For caregivers and family

Shame keeps people quiet, and silence helps scammers. The best protection you can offer is a relationship where your loved one feels safe telling you anything.

Talk about scams before they happen

- Bring it up casually: "I read about a scam where AI copies a grandchild's voice. Have you heard of that?"
- Set up a family safe word together, and practice it.
- Agree on a simple rule: "Before anyone sends money, we call each other first."
- Offer to help with the "protect yourself ahead of time" checklist, side by side.

If a scam has already happened

- Lead with care: "Thank you for telling me. This happens to smart people every day."
- Avoid blame. Skip "How could you fall for that?" It makes people hide the next one.
- Help with the next steps together: calling the bank, reporting, changing passwords.
- Watch for repeat contact. Scammers often target the same person again, sometimes as "recovery" helpers.

Warning signs a loved one may be caught in a scam

- New secrecy about money, phone calls, or an online friend
- Unusual withdrawals, wire transfers, gift card purchases, or visits to Bitcoin ATMs
- Anxiety around the phone, or a sudden urgent need for cash
- New "investment" apps or crypto accounts

If you suspect financial exploitation of an older adult in Oregon, call **1-855-503-7233** (ODHS Abuse Reporting).

10

Scam response card

Cut out and keep by your phone.

Project LENS Scam Response Card

PAUSE. It's okay to hang up. Say: "I'll call you back."

VERIFY. Call back on a number you already have. Never use the one they gave you.

ASK. Talk to someone you trust before you send money or share information.

Never pay with: gift cards, wire transfers, crypto, a Bitcoin ATM, or cash to a courier

Never share: passwords, codes texted to you, or Social Security, Medicare, or bank numbers

We have a family safe word: ☐ Yes (keep it in your head, not on paper)

My trusted person: _____ Phone: _____

My bank's fraud line (from back of card): _____

Oregon scam help: Oregon DOJ 1-877-877-9392

Elder abuse or exploitation: 1-855-503-7233

National Elder Fraud Hotline: 1-833-372-8311

Emergency: 911

Project LENS: Learn. Evaluate. Navigate. Secure. projectlensai.org

This guide is for education only. It is not legal, financial, or medical advice.

AI changes quickly. We review this guide every six months. For the newest version, visit projectlensai.org.

Sources: FBI IC3 2025 Annual Report · FTC: Scammers use AI to enhance family emergency schemes · FTC Protecting Older Consumers 2024–2025

Version 1.5 · Updated October 27, 2026 · Next review April 2027