PROJECT LENS

WORKSHOP KIT 02 OF 05 · FACILITATOR GUIDE

AI Scams and Deepfakes Facilitator 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 1.3 · Updated October 13, 2026

projectlensai.org

01

About this workshop

This 60-minute session teaches older adults and their families how AI is changing scams, and the three habits that stop almost all of them: **PAUSE. VERIFY. ASK.** Anyone can lead it with this guide, the slide deck, and the handouts. No technical background needed.

Detail	
Length	60 minutes (a 45-minute version is marked in the run of show)
Best for	Libraries, senior centers, retirement communities, faith and civic groups, family nights
Group size	8 to 40 people. For more than 20, plan one helper for every 10 people during activities.
Facilitators	One lead, plus one helper if possible. Student facilitators work well in pairs.
Devices	Not required. Attendees only need a pencil.

By the end, attendees will be able to:

1. Explain in one sentence how AI makes scams more convincing (voice cloning, fake videos, polished messages).
2. Name at least three red flags of a scam.
3. Use PAUSE. VERIFY. ASK. on a suspicious call or message.
4. Set up a family safe word.
5. Know who to call in Oregon if they or someone they love is targeted.

The tone to aim for: calm, practical, and respectful. Never alarmist. The message is "you can handle this," not "be afraid."

02

What's in the kit

Item	Who it's for	How many to print
This facilitator guide	Lead facilitator and helpers	1 per facilitator
Slide deck with speaker notes	Facilitator (projected)	Also print slides 6 per page as a backup if there's no projector
Participant pack: Spot the Scam cards	Small groups	1 set per table of 4 to 6 people
Participant pack: before and after quiz	Each attendee	1 per person
Participant pack: feedback form	Each attendee	1 per person
Scam Prevention Guide (Guide 3)	Take-home	1 per person, or a stack plus a QR code to projectlensai.org
Scam response card (last page of Guide 3)	Take-home	1 per person, on cardstock if possible
Participant pack: sign-in sheet and flyer template	Host	1 sign-in sheet per 20 people; flyers as needed

Large print: print handouts at 125% on letter paper, or on 11 x 17 paper, for anyone who asks.

03

Before the session

Two weeks before

- [ ] Confirm the date, room, and expected group size with the host.
- [ ] Ask about accessibility: wheelchair access, hearing loop or microphone, large-print needs, interpreters.
- [ ] Send the host the flyer template from the participant pack to fill in and post.
- [ ] Read the Real or AI? answer key in Activity 1, so the reveals feel natural.

The day before

- [ ] Print handouts (see the table above). Add a few extra.
- [ ] Rehearse the full deck out loud with your co-facilitator. Time it.
- [ ] Check the phone numbers on the last slides against the "Who to call" page of the Scam Prevention Guide if it's been more than six months.

At the room (arrive 30 minutes early)

- [ ] Test the projector, laptop, and clicker. Have the deck saved offline in case Wi-Fi fails.
- [ ] Test the microphone. Many older adults have hearing loss; a mic helps everyone.
- [ ] Set chairs so everyone can see the screen. Group tables of 4 to 6 for activities.
- [ ] Put pencils, the quiz, and the sign-in sheet on each table.
- [ ] Find the restrooms and the exit so you can point them out.

04

Ground rules for facilitators

1. **Protect privacy.** Never ask attendees for personal details, account information, or their own scam stories. If someone volunteers a story, keep it general and don't write down names.
2. **No photos without permission.** Ask the host and the group before taking any photo. Never photograph someone who says no. Don't post photos online without written permission.
3. **Educate, don't advise.** You are teaching habits, not giving legal, financial, or medical advice. When someone asks about their specific situation, point them to the right helpline.
4. **Respect experience.** Your audience has decades of judgment. Never talk down. "These scams fool smart people every day" is true and kind.
5. **Stay neutral about AI.** AI is a tool, not good or evil. Avoid scaring people away from technology that could help them.
6. **Use real, safe examples only.** Don't show actual scam links or phone numbers on screen. Use the made-up examples in this kit.
7. **Don't promise outcomes.** Never say "you'll get your money back" or "this will stop every scam."
8. **Never collect money or sell anything.** Project LENS workshops are free and educational.
9. **Hands off other people's devices.** If someone wants help on their phone or tablet, they hold it and they type. Don't log into their accounts, don't create accounts for them, and don't type on their device. Show the steps on your own device or on the slide instead.

05

Run of show (60 minutes)

Times are a guide. Watch the room: if a discussion is going well, let it run and trim the next segment.

Time	Segment	Slides	What happens
0:00 to 0:05	Welcome and before-quiz	1 to 3	Introductions, agenda, 5-question quiz (2 minutes, pencils only)
0:05 to 0:12	How AI is changing scams	4 to 5	The 2025 numbers; what AI can fake: voices, videos, messages
0:12 to 0:22	**Activity 1: Real or AI?**	6 to 11	Two rounds of photo pairs, hands up for A or B, answer slides, then how to check
0:22 to 0:30	Common scams and red flags	12 to 13	Walk through the top scams; ask "has anyone heard of this one?"
0:30 to 0:36	PAUSE. VERIFY. ASK.	14 to 15	The three habits and the exact words to say
0:36 to 0:46	**Activity 2: Spot the scam**	16 to 17	Tables sort six cards, then share answers
0:46 to 0:51	**Activity 3: Family safe word**	18 to 19	Why it works; everyone drafts one
0:51 to 0:55	Protect yourself, and what to do if it happens	20 to 22	Setup checklist, the first hour, who to call in Oregon
0:55 to 1:00	Wrap-up	23 to 25	Three things to remember, after-quiz, feedback form, questions

45-minute version

Every segment gets shorter, so the timings add up to 45 minutes. Keep PAUSE. VERIFY. ASK. and the safe word at full strength; they matter most.

Time	Segment	Slides	What changes
0:00 to 0:03	Welcome and before-quiz	1 to 3	Short introductions; quiz takes 2 minutes

Time	Segment	Slides	What changes
0:03 to 0:07	How AI is changing scams	4 to 5	The numbers and one example only
0:07 to 0:13	**Activity 1: Real or AI?**	6 to 11	Both rounds; ask one person per round instead of two
0:13 to 0:18	Common scams and red flags	12 to 13	One "has anyone heard of this?" question, not one per scam
0:18 to 0:23	PAUSE. VERIFY. ASK.	14 to 15	Full segment
0:23 to 0:30	**Activity 2: Spot the scam**	16 to 17	Three cards per table: B, C, and D
0:30 to 0:34	**Activity 3: Family safe word**	18 to 19	Skip the optional role-play
0:34 to 0:37	Who to call	21 to 22	Skip slide 20; point to the checklist in the take-home guide
0:37 to 0:42	Wrap-up	23 to 25	Three things to remember, after-quiz, feedback form
0:42 to 0:45	Questions	25	Buffer; offer to stay after for longer questions

06

Talking points

The full script is in the speaker notes of each slide. These are the points that matter most.

Welcome (slides 1 to 3)

- Introduce yourselves and Project LENS: a youth-led initiative teaching practical AI literacy in our community.
- "Today isn't about being afraid of technology. It's about three simple habits that protect you."
- The quiz isn't a test. It helps us see what's useful. No names needed.

How AI is changing scams (slides 4 to 5)

- In 2025, Americans 60 and older reported losing $7.7 billion to online fraud. Oregonians 60+ reported more than $77 million (FBI IC3). Most scams are never reported.
- AI doesn't invent new scams. It makes old ones more convincing: a voice that sounds like your grandson, a video of a celebrity, an email with perfect spelling.
- Key line: *"AI can fake a voice or a face. It can't fake a call you make yourself to a number you already know."*

Common scams and red flags (slides 12 to 13)

- Ask the room: "Has anyone gotten a call or text like this?" Hands are enough. Don't ask for details.
- The biggest money-losers for people 60 and older in 2025 were investment scams, tech and customer support scams, and romance scams (FBI IC3). Government impostor scams are also common and costly.
- The universal red flags: urgency, secrecy, and unusual payment (gift cards, wires, crypto, Bitcoin ATMs, cash by courier).

PAUSE. VERIFY. ASK. (slides 14 to 15)

- Have the group say it out loud together. It sticks.
- Practice the words: "I don't make decisions on the phone. I'll call you back."
- Emphasize: hanging up is never rude when someone is pressuring you.

Protect yourself and who to call (slides 20 to 22)

- Point to the checklist in the take-home guide rather than reading every item.
- "It is not your fault" is the most important thing to say about being scammed. Say it clearly.
- Read the Oregon DOJ and elder fraud hotline numbers aloud. Point out they're on the take-home card.

Wrap-up (slides 23 to 25)

- Three things to remember: PAUSE. VERIFY. ASK.; the family safe word; never pay with gift cards, wires, or crypto.
- Collect quizzes and feedback forms. Thank the host.

07

Activity 1: Real or AI? (10 minutes, slides 6 to 11)

Goal: show that AI images can fool anyone, so the habit that matters is checking where something came from, not squinting at pixels.

Each round shows two pictures of the same scene, labeled A and B. One is a real phone photo taken by the Project LENS team. The other was made by an AI image tool from a short written description of that photo. The images are already in the deck; there's nothing to find or insert.

How to run it:

1. Show the round for about 20 seconds. Ask: "Which one is the real photo? Hands up for A." Then: "Hands up for B."
2. Ask one person from each side what made them choose. Then click to the answer slide.
3. On the answer slide, point out the clue in the speaker notes. Say clearly that a clue is a hint, never proof.
4. After the last round, show slide 11: how to check (reverse image search, find the original source, look for Content Credentials).

Answer key

Round	Scene	Real photo	Made by AI	Clue to point out
1 (slides 7 and 8)	Rocky tropical shore	B	A	The AI sky is an even, brilliant blue and the water extra turquoise, like a travel ad. The real photo is hazier.
2 (slides 9 and 10)	California coast from a clifftop	A	B	Very few people can tell. If anything, the three rocks sit in a neat, evenly spaced row.

All four images belong to the Project LENS team: the real photos were taken on team members' phones, and the AI versions were made by the team with Canva and Figma AI image tools in October 2026. No faces, house numbers, or license plates appear in any of them. Kit 1 uses different pairs, so a group that takes both workshops sees fresh pictures.

Connect it to scams: after round 2, say: *"If a picture this good can be made in seconds, a scammer can make one too: a fake vacation photo, a fake rental listing, a fake picture of a grandchild. That's why we don't squint. We check where it came from."*

Making your own pairs (optional). Take an everyday photo on your phone (a pet, a garden, a meal, a view), then ask an AI image tool to make a picture from a description of it. No faces, house numbers, license plates, real public figures, fake news events, or anything upsetting. Remove location data before sharing the real photo. Keep a written answer key.

08

Activity 2: Spot the Scam (10 minutes, slides 16 to 17)

Goal: practice using red flags and PAUSE. VERIFY. ASK. on realistic messages. Two of the six cards are probably real, so people practice judging, not assuming everything is fake.

How to run it

1. Give each table one set of the six cards from the participant pack.
2. Ask tables to sort the cards into two piles: "scam" and "probably real." For each scam, name one red flag. (5 minutes)
3. Go around the room: one card per table. Reveal the answer and the red flags. (5 minutes)
4. End with: "Even for the real ones, what's the safe way to check?" (Call a number you already have.)

Answer key

Card	What it is	Answer	Red flags or reasons
A	Text: package held, pay a $1.99 redelivery fee at a link	**Scam**	Unexpected; small fee to get card details; link isn't the real carrier's site. (The card uses a made-up address ending in .example, so no real website is shown.)
B	Voicemail from a crying "grandchild" who's in jail, says don't tell Mom, a lawyer will call	**Scam**	Urgency, secrecy, a second "official" caller; voice could be cloned. Ask for the safe word.
C	Email from your pharmacy: your prescription is ready; call the number on your label with questions	**Probably real**	No link, no payment, no urgency; it tells you to use a number you already have

Card	What it is	Answer	Red flags or reasons
D	Pop-up: "Microsoft has detected a virus. Call support now."	**Scam**	Real companies don't put phone numbers in pop-ups; close the browser
E	Recorded call: "Your Social Security number is suspended. Press 1."	**Scam**	Threat, urgency; Social Security numbers don't get "suspended"
F	Letter in the mail from Medicare with your yearly plan notice; no payment requested; says to call 1-800-MEDICARE	**Probably real**	No payment demand; points to the official number. Still verify by calling 1-800-633-4227 yourself.

Teaching point: the "probably real" messages have something in common. They don't rush you, don't ask for payment or private information, and send you to a number or account you already know.

09

Activity 3: Family safe word (5 minutes, slides 18 to 19)

Goal: every attendee leaves with a plan to set up a family safe word, which the FBI recommends to beat voice-cloning scams.

How to run it

1. Explain (slide 18): if someone calls claiming to be family in trouble, ask for the safe word. A voice clone won't know it.
2. Give everyone 2 minutes to brainstorm a safe word *privately* on a scrap of paper they take home and throw away once their family has agreed on a word. Don't use the scam response card: it stays by the phone, where others can see it. Silly phrases work best: "purple pancakes."
3. Remind them: don't say it out loud here, don't post it, and don't text it. Share it with family in person or by phone.
4. Optional: ask a volunteer pair to act out the call. One plays the "grandchild," the other asks for the safe word. It usually gets a laugh, and people remember it.

Facilitator note: never ask anyone to share their safe word, even as an example.

10

Handling tough moments

If someone says they've been scammed

This may happen, sometimes with strong emotion. Your job is to be kind and point them to help, not to investigate.

1. **Thank them and reassure them:** "Thank you for sharing. This happens to smart people every day. It's not your fault."
2. **Don't ask for details in front of the group.** Offer to talk privately after the session, with the host present.
3. **Point them to help:** their bank first if money is involved, then Oregon DOJ Consumer Protection (1-877-877-9392) or the National Elder Fraud Hotline (1-833-372-8311). If

they're worried someone is taking advantage of them, the ODHS abuse reporting line is 1-855-503-7233.

4. **If someone is in immediate danger, call 911.**
5. **Tell the host** afterward so they can follow up. Don't record names in your session notes.

Hard questions and simple answers

They ask...	You can say...
"Is my phone listening to me?"	"Some apps can use your microphone if you allow it. You can check and turn that off in your phone's settings. We can show you how after."
"Should I just stop using the internet?"	"You don't need to. A few habits, like PAUSE. VERIFY. ASK., let you use it safely."
"Is ChatGPT (or another chatbot) safe?"	"The well-known ones are real tools. The safety is in how you use them: no private information, and check anything important."
"Can you tell me if this message on my phone is a scam?"	"Let's look at the red flags together. If you're unsure, call the company using a number you already have." Don't log into their accounts.
"Will I get my money back?"	"I can't promise that, but acting quickly gives you the best chance. Call your bank right away."
"Why don't the police just stop them?"	"Many scammers are overseas and hard to catch. Reporting still helps investigators spot patterns and warn others."
A question you can't answer	"That's a great question. I don't want to guess. Answerland's librarians can help, free, any time, at answerland.org."

11

After the session

Quiz answer key (same 5 questions before and after; the quiz is in the participant pack)

#	Correct answer
1	False: AI can copy a voice from a short recording
2	C: Hang up and call back on a number you already have
3	D: All of the above (gift cards, wire transfers, cryptocurrency)
4	True
5	B: Oregon DOJ Consumer Protection

Scoring: count correct answers before and after for the whole group (not by person). Example: "Before, the group averaged 2.8 out of 5. After, 4.6."

Within one week

- [ ] Record the session in the log below.
- [ ] Read the feedback forms and note one thing to improve.
- [ ] Only quote feedback publicly (for example, on the website) if the person checked the "OK to share" box. Never use names unless they gave written permission.
- [ ] Thank the host by email.
- [ ] Within one week, copy any emails from the sign-in sheet into the Project LENS mailing list, then shred the sheet. The host doesn't keep a copy.

Session log (add a row each time)

Date	Host and location	Facilitators	Attendees	Avg before	Avg after	One thing to improve

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

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

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

Sources: FBI IC3 2025 Annual Report · FBI IC3 PSA I-120324-PSA (Dec 2024)

Version 1.3 · Updated October 13, 2026 · Next review April 2027