PROJECT LENS

RESOURCE GUIDE 05 OF 06

# AI for Families

## 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 1.2 · Updated October 27, 2026

01

# Welcome

You can be the most important safety tool an older loved one has. This guide helps you learn about AI together, set up simple protections, and keep the conversation open.

It's written for adult children, grandchildren, neighbors, and caregivers.

**Be a partner, not a supervisor.** Older adults have decades of good judgment. The goal is not to take over their phone or their money. It's to explore new tools side by side, and to make sure they always have someone to call before acting on something that feels off.

## How to use this guide

- Read the conversation tips before you start.
- Use the 30-minute session plan for your first time exploring AI together.
- Fill in the family plan card on the last page together, and keep a copy each.

02

# Starting the conversation

Lead with curiosity, not warnings. People open up when they feel respected, and shut down when they feel tested or talked down to.

| Instead of... | Try... |
|---|---|
| "You need to be careful, you could get scammed." | "I read that scammers can copy voices with AI now. Have you heard about that?" |
| "Let me just do it for you." | "Want to try it together? You drive, I'll sit next to you." |
| "AI is dangerous, stay away from it." | "Some of this is really useful. Want to see what it can do?" |
| "How could you not know that?" | "This stuff changes so fast. I'm still learning it too." |
| "Give me your passwords so I can check." | "Let's set up a few safety settings together. You keep your passwords." |

## Good moments to bring it up

- After a news story or a scam call someone in the family received
- When they mention a confusing text, email, or pop-up
- When they ask for help with their phone or computer
- At a family gathering, as a group activity, so no one feels singled out

03

# Your first session together (30 minutes)

Keep it short, hands-on, and fun. Let your loved one hold the device and type.

1. **Pick a tool (5 minutes).** Choose one well-known chatbot, such as ChatGPT, Google Gemini, Microsoft Copilot, Claude, or Meta AI. Download it only from the official app store, or type the web address yourself.
2. **Ask something fun (5 minutes).** Start with a topic they love: "Give me three easy recipes using tomatoes from my garden," or "Tell me about the history of my hometown."
3. **Practice START, IMPROVE, CHECK (10 minutes).** Start with a question. Then improve it: "Make it shorter," "Explain it more simply," or "Ask me questions first." Then check one fact together on a trusted website.
4. **Catch a mistake on purpose (5 minutes).** Ask a question they already know the answer to, such as a family history detail or a local fact. If it gets it wrong, or asks you for more detail, that's a lesson too: it doesn't know your family, and AI can sound sure and still be wrong.
5. **Agree on two rules (5 minutes).** Never type private numbers or passwords. Never trust a phone number or link from AI. Write them on a sticky note by the device.

End by asking what they'd like to try next time. The *Project LENS Prompting Guide* has more practice prompts.

04

# Set up safety together

Work through this checklist side by side. Your loved one stays in control of their own accounts and passwords.

- [ ] **Turn off chat history or training** in the chatbot's settings (look for "Settings," then "Privacy" or "Data controls").
- [ ] **Delete look-alike apps.** Remove any "AI" app that wasn't downloaded from the official app store or that asks for payment right away.
- [ ] **Silence unknown callers.** Turn on "Silence Unknown Callers" (iPhone) or "Call screening" (Android). Ask the phone company about free robocall blocking.
- [ ] **Turn on two-step login** for email and the bank. It sends a code to their phone when someone signs in.
- [ ] **Set up bank and card alerts** for large withdrawals or purchases.
- [ ] **Add a trusted contact to bank and investment accounts.** This lets the bank or brokerage reach you if they suspect fraud. According to FINRA, a trusted contact cannot see account balances or make transactions.
- [ ] **Freeze their credit** with Equifax (1-888-298-0045), Experian (1-888-397-3742), and TransUnion (1-800-916-8800). It's free and can be lifted any time.
- [ ] **Make social media private,** and avoid posting travel plans or long voice videos publicly.
- [ ] **Save key numbers in their phone:** you, their bank's fraud line, and Oregon DOJ Consumer Protection (1-877-877-9392).

05

# Make a family safe word

AI can copy a voice from a few seconds of video. The FBI recommends a secret word or phrase that family members use to prove who they are.

## Choosing a good safe word

- Pick something easy to remember but impossible to guess: not a pet's name, street, or birthday that could be found online.
- A silly phrase works well: "purple pancakes" or "Grandpa's green canoe."
- Share it in person or by phone. Never post it, text it, or email it.

## The family emergency plan

1. If anyone calls claiming to be family in trouble, ask for the safe word.
2. No safe word? Hang up and call that person directly on the number you already have.
3. Can't reach them? Call another family member before doing anything else.
4. No family member will ever ask for gift cards, wire transfers, crypto, or cash by courier. If someone does, it's a scam.

**Practice it.** Run a quick drill at the next family dinner. It feels silly, and that's what makes it stick.

06

# Signs something may be wrong

Stay in touch regularly, and notice changes. Any one of these is worth a gentle, caring conversation.

## Possible scam warning signs

- New secrecy about money, phone calls, or an online friend
- Unusual withdrawals, wire transfers, or gift card purchases
- Visits to Bitcoin ATMs, or new crypto or "investment" apps
- Anxiety around the phone, or a sudden urgent need for cash
- Remote-access software on their computer they don't remember installing

## AI as company

Some people enjoy chatting with AI, and that can be fine. AI can answer questions, tell stories, or help pass a quiet evening. It is not a substitute for real relationships.

Check in if your loved one:

- Spends hours a day talking with a chatbot instead of people
- Trusts the chatbot's advice over their doctor, pharmacist, or family
- Says the AI "understands them" better than anyone else

The best response is more human connection: regular calls, visits, and invitations to community activities, libraries, and senior centers.

07

# Tips for young helpers

Grandchildren and teens are often the go-to tech helpers in a family. Here's how to make it a good experience for everyone.

1. **Slow down.** Explain one step at a time and let them tap and type. Watching you do it quickly doesn't teach much.
2. **Write it down.** Steps on paper are easier to follow later than remembering what you said.
3. **Skip the jargon.** Say "the settings button that looks like a gear," not "open the config menu."
4. **Be patient with repeats.** Showing something three times is normal. You probably needed help learning to drive.
5. **Share what you know about scams.** You likely see fake videos and scam messages online every day. Your grandparents may not. Show them real examples of what to watch for.
6. **Respect their privacy.** Don't read their messages or look at their accounts unless they ask you to.
7. **Learn from them too.** Ask about their experience: how they spotted a con, managed money, or judged who to trust. Good judgment works with or without technology.

08

# If a loved one is scammed

How you respond in the first few minutes matters. Shame makes people hide the next scam, so lead with care.

## First, the words

- "Thank you for telling me. I'm glad you did."
- "This happens to smart, careful people every day. These are professional criminals."
- "Let's fix this together."

## Then, the steps (do them together)

1. **Stop all contact** with the scammer: hang up, block, don't reply.
2. **Call the bank or card company** using the number on the card. Ask them to stop or reverse payments.
3. **Change passwords,** starting with email, and turn on two-step login.
4. **Freeze credit** with all three bureaus if a Social Security number was shared.
5. **Write down what happened:** dates, names, numbers, amounts, how money was sent.
6. **Report it** to the FBI at ic3.gov and Oregon DOJ at 1-877-877-9392. The National Elder Fraud Hotline (1-833-372-8311) can help you file.
7. **Watch for "recovery" scams.** Anyone offering to get the money back for a fee is another scammer.

**If you think someone is taking advantage** of an older adult (a stranger, caregiver, or even a relative), call Oregon's abuse reporting line at **1-855-503-7233** (1-855-503-SAFE).

> **In an emergency or if someone is in danger, call 911.**

The *Project LENS Scam Prevention Guide* has the full list of Oregon and national help lines.

09

# Family plan card

*Fill this in together. Make a copy for each person.*

## Project LENS Family Plan Card

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

**First person to call before sending money:** _____ Phone: _____

**Second person to call:** _____ Phone: _____

**Bank fraud line (from back of card):** _____

**Our rule:** No one in our family will ever ask for gift cards, wire transfers, crypto, or cash by courier.

**If a call feels off:** PAUSE. VERIFY by calling back on a number you know. ASK family first.

**Never type into AI:** Social Security, Medicare, bank numbers, or passwords

**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 PSA I-120324-PSA (Dec 2024) · FINRA: Why you should consider adding a trusted contact

Version 1.2 · Updated October 27, 2026 · Next review April 2027