centrexIT

Client Conversation Script

Word-for-word starter language for staff, case managers, social workers, and volunteer coordinators talking AI safety with the older adults they serve.

HOW TO USE THIS SCRIPT

This is starter language, not a script you have to follow word-for-word. Adapt to your voice and your client's circumstances. The italic lines are example phrasing. The bolded sections are the principles behind why we use these words.

The goal is never to scare the client. The goal is to give them tools, restore agency, and make it safe to come to you when something feels off.

Scenario 1 — A client asks if AI can help them

The setup: Client mentions they tried ChatGPT, or saw an ad for an AI tool that promises to help with paperwork, taxes, or a medical question. They want to know if they should use it.

What to say

"It can be really helpful for some things — and risky for others. Let me show you the difference."

"Here's a simple rule: if you wouldn't say it out loud at the bank, don't type it into an AI tool. So asking it to explain a Medicare letter in plain English? Good use. Asking it to fill out the form for you with your Medicare number? That's where it gets risky."

"What I'd love to do is help you figure out which questions are safe to ask an AI tool, and which ones we should walk through together. Sound okay?"

Why this works: You validated curiosity. You gave a memorable rule. You positioned yourself as the partner, not the gatekeeper. The client leaves the conversation feeling more capable, not more cautious.

centrexIT

Scenario 2 — A client got a suspicious call or message

The setup: Client tells you about a call from "Medicare," a text from a "grandchild in trouble," a voice that sounded just like their daughter asking for money, or an email about a package they didn't order. They may have already responded — or be considering it.

What to say first

> *"I'm so glad you're telling me about this. That's exactly the right thing to do."*
>
> *"Before we look at it together — did you send any money, share any codes or numbers, or click any links? It's okay either way. I just need to know so I can help."*

If they did engage with the scam

> *"Okay. Thank you for telling me. This was designed to trick people — they spend a lot of money making it convincing. You are not the only person this has happened to, and the faster we know, the more options we have."*
>
> *"Here's what we're going to do right now: [list the immediate steps — call their bank, change passwords, freeze credit, report to FTC/local PD, etc.]. I'll stay with you."*

If they didn't engage but were tempted

> *"You did exactly right. The fact that you paused and asked someone — that's the protection. These tools are getting really good at sounding real, so the rule is: anything urgent, anything secret, anything involving money — we hang up and call back on a number we already know."*

What to avoid: *"How could you have fallen for that?" "Why did you respond?" "You should have known."* These responses create shame, and shame keeps people from reporting next time. Shame is the scammer's second weapon.

centrexIT

Scenario 3 — A family member of a client has been targeted

The setup: Adult child of a client calls or stops in. Their parent has been scammed, or almost was. They're scared, angry, or embarrassed. They want to know what to do — and often, what your organization can do.

What to say

> *"Thank you for letting us know. This is happening to a lot of families right now — the AI-generated voice calls are especially convincing, and they're catching people who are sharp and careful."*
>
> *"Here's what I'd suggest as a next step: set up a family verification protocol — a safe word, a rule about hanging up and calling back, and a second-person check for anything involving money. I have a one-page handout I can give you. Would it help if I walked through it with both of you together?"*
>
> *"And — please don't bring this up with [parent's name] in a way that makes them feel they did something wrong. Even people who didn't fall for it carry shame about being targeted. The most helpful thing is to make it a family conversation, not a parent-child conversation."*

Why this works: You normalized what happened. You gave them a concrete next step (the protocol). You included the parent in the solution, which protects dignity. And you offered to be in the conversation, which establishes you as a resource for the whole family — not just the older adult.

FOUR PRINCIPLES THAT RUN THROUGH ALL THREE

1. **Lead with thanks for telling you.** Even before facts. The fastest way to lose access to the truth is to make reporting cost something emotionally.
2. **Give them a rule, not a lecture.** "If you wouldn't say it at the bank..." beats five paragraphs about data privacy.
3. **Restore agency.** Frame the moment around what they did right (paused, asked, told you) — not what they almost did wrong.
4. **Avoid shame language.** "How did you..." "Why did you..." "You should have..." These words are the scammer's allies.

WANT A SCORE INSTEAD?

The Elder AI Risk Snapshot is a free 2-minute self-assessment that scores your AI risk across data governance, staff use, and client vulnerability — and tells you which of the items above to prioritize.

Go to **centrexit.com/tools/elder-ai-risk-snapshot**

YOU CALL. WE ANSWER. IT WORKS