MODULE 4

Staying Safe from AI Scams

Spotting, checking, and protecting yourself from scams powered by AI.

SENIOR TECH LITERACY SERIES • 90-MINUTE SESSION

TODAY'S PLAN

What we'll do together in the next 90 minutes

1. **How scammers use AI**
   Phishing emails, cloned voices, fake support chats.
2. **The four red flags**
   Urgency, secrecy, payment, authority.
3. **AI as a second set of eyes**
   How to ask — and why to still verify.
4. **Three account habits**
   Passwords, password managers, MFA.
5. **Real or scam?**
   Hands-on activity with a checklist and an AI helper.

Scams haven't changed — their costumes have

Before

Obvious typos.
Clunky grammar.
Generic greetings.

The mistakes were the clue.

Now

Flawless writing.
Perfect spelling.
Convincing voices and videos.

The sound of a message is no longer proof it’s real.

The good news: the four red flags we’ll learn still work — because they’re about what the message asks you to do, not how it sounds.

Three ways scammers use AI today

1

Realistic phishing

Polished emails and texts that look like they're from your bank, Amazon, or Medicare.

2

Cloned voices

A few seconds of audio is enough to imitate a grandchild or a family member on the phone.

3

Fake customer support

Pop-ups and chat windows that feel human — because AI is writing every reply.

TYPE 1

Emails and texts that look too real

Inbox • Amazon Fraud Alert

From: security@amazon-account-check.com
Subject: Unauthorized $749.99 charge — action required

Dear Customer,

A recent charge to your account requires your immediate attention. Click the link below within 30 minutes to cancel this order.

[Cancel Order]

WHAT TO NOTICE

The sender domain

"amazon-account-check.com" is not Amazon.

The thirty-minute deadline

Real companies don't do that.

A link to "fix" it

Log in to amazon.com directly instead.

Generic greeting

Amazon knows your name.

TYPE 2

Cloned voices — the “grandma, it’s me” call

Grandma, it’s me — I’ve been in an accident.

I don’t want Mom and Dad to know. Please wire me $2,000 for bail. Please don’t tell anyone.

The voice sounds just like your grandson.

WHAT YOU DO

Hang up. Call back on a known number.

- Three seconds of audio from a video is enough to clone a voice.
- A real family member will understand — and be relieved — if you pause to verify.
- Agree on a family “safe word” today. Ask for it before you act.

TYPE 3

Fake customer-support chats and pop-ups

⚠ MICROSOFT SECURITY — LIVE SUPPORT

SUPPORT
Hello! I can see your computer is infected. I'll help you right now.

SUPPORT
Please install this program so I can clean the virus remotely.

YOU
I'm not sure. Should I?

SUPPORT
Yes — and please don't tell your bank while we work. We need 8 Google Play gift cards to license the fix.

WHY THIS IS FAKE

Real support never initiates
If you didn't call them, they didn't call you.

No remote-control tools
Real companies will not ask to install AnyDesk, TeamViewer, or similar.

No gift-card payments
Ever. For anything.

No "don't tell the bank"
Secrecy is the scam.

THE BIG FOUR

Red flags that appear in almost every scam

1 Urgency

“Act in the next 15 minutes.”

Real institutions give you time.

2 Secrecy

“Don’t tell your family or the bank.”

Secrecy protects the scammer — not you.

3 Unusual payment

“Pay with gift cards or wire.”

The IRS and your bank never ask for these.

4 Authority pressure

“This is the IRS / Medicare / police.”

Real authorities expect you to call them back.

QUICK SCAN

Phrases that should make you stop

- *“You must act now.”*
- *“Do not tell anyone.”*
- *“We need gift cards to release the funds.”*
- *“I’m with the IRS fraud team.”*
- *“Your account will be closed today.”*
- *“Click this link to verify.”*
- *“Buy Bitcoin and send it here.”*
- *“Don’t hang up — stay on the line.”*

THE GOLDEN RULE

Pause. Verify. Act.

Pause

If a message creates urgency, slow down on purpose. Put the phone down. Take 30 seconds.

Verify

Use a number or website you already trust — not one from the message.

Act

Only when you've checked. If you're still unsure, ask one more person.

FLIP THE SCRIPT

Use AI to check AI-powered scams

THE IDEA

AI assistants can read a suspicious message with you and explain, in plain language, what looks wrong.

1. Open a trusted AI assistant (ChatGPT, Claude, Copilot).
2. Paste the message — the whole thing, including sender.
3. Ask it: “Does this look like a scam? What’s suspicious?”
4. Read the answer — then verify somewhere else.

⚠ But never the last word.

An AI assistant can be wrong. A scam can be built to fool it too.

ALWAYS DO AFTER:

Look up the real number on your bill, the back of your card, or the official website. Call there.

TRY IT YOURSELF

A prompt you can copy and paste

YOUR PROMPT

“I am over 60 and I want to be careful. Please look at the message below and tell me — in plain language — whether it looks like a scam. Point out anything suspicious.

Here is the message:”

Good for:
First opinion, plain-language explanation, spotting classic scam patterns.

Not good for:
The final decision. Always verify with a real person or a known number.

HABIT 1 OF 3

Make your passwords long, not clever

HARD FOR YOU — EASY FOR COMPUTERS

`P@ss1!`

Short. Full of symbols you'll forget. And it's on every password-cracker list.

EASY FOR YOU — HARD FOR COMPUTERS

`porch-lemon-river-candle`

Four unrelated words. A sentence your brain can picture. Adds centuries to the crack time.

Protect these first: email • bank • Medicare • Social Security

Never reuse a password across any two of these. And don't keep them in your wallet or on the back of your laptop.

Two tools that do the hard work for you

2 Password manager

A single, locked notebook for every login

- Remember one password. It remembers the rest.
- Fills logins with one click on your phone or computer.
- Starter choices: 1Password,LastPass, Bitwarden, or the one built into Apple or Google.
- Ask a family member or a librarian to help you set it up the first time.

3 Multi-factor authentication

Something you know + something you have

- A six-digit code from your phone, in addition to your password.
- Even if a scammer steals your password, they can’t get in.
- Turn it on for your email first — email controls every other account.
- Then turn it on for your bank and any account with your money.

If you do only one thing this week — turn this on for email.

ACTIVITY — 10 MINUTES

Real or scam?

1

Round 1 • Sort

In pairs, sort your stack of messages into “real” and “scam” — using only the red-flag checklist.

2

Round 2 • Ask the AI

Pick your two hardest cards. Paste them into an AI assistant and ask: “Is this a scam? Why?”

3

Round 3 • Reveal

We’ll uncover the answers together. For each one that fooled the room, we’ll name the red flag it carried.

WHAT SUCCESS SOUNDS LIKE

“This one had two red flags — urgency and a gift-card request.”

“The AI called it a scam — and I’m still going to call the bank on the number from my card.”

TAKE THIS HOME

Your one-week plan

TODAY	Turn on multi-factor authentication for your email.
THIS WEEK	Pick a family “safe word”. Tell it, in person, to one relative.
THIS WEEK	Tape the red-flag checklist near your phone or computer.
NEXT CLASS	Bring one suspicious message you received. We’ll workshop it together.

QUESTIONS • REFLECTION • ONE SMALL ACTION

Pause. Verify. Act.

You don’t need to be perfect. You just need to slow down and check.
That alone will keep you ahead of most AI-powered scams.

Help: AARP Fraud Watch 877-908-3360 • reportfraud.ftc.gov • Your bank's number on the back of your card