THE WISDOM EDGE



A FREE LARGE-PRINT GUIDE

The AI Scam Shield Guide

Simple ways to spot and stop AI-powered scams

◆ ◆ ◆

Your wisdom, supercharged. Your memories, preserved.

By Glenn Lee · thewisdomedge.com

A NOTE FROM GLENN

A warm welcome

Hello, and welcome. I'm Glenn Lee, and I'm so glad you're here.

You have spent a lifetime learning whom to trust. That good judgment is still your best protection. This guide simply adds a few new tools to it.

Today, some scammers use computer programs called AI to sound and look more convincing. That can feel unsettling. But here is the good news. The habits that stop these scams are simple. They work no matter how clever the trick is.

In these pages, we go one step at a time. You'll see how the most common AI scams work, the warning signs to look for, and exactly what to do. You'll make a family safe word plan. You'll also get a checklist to keep by the phone.

There are no tests here, and no silly questions. Read a page, set it down, and come back later. You stay in charge.

Warmly,

Glenn Lee

The Wisdom Edge · support@thewisdomedge.com

THE BASICS

AI scams, in plain words

AI stands for **artificial intelligence**. It is computer software that can write, talk, and make pictures in a way that seems human.

An AI scam is an old trick in a new disguise. The scammer still wants the same things: your money or your private information. AI just helps them sound more real. The FBI warns that AI can even fix the spelling mistakes that used to give scams away.[3]

Three words to know

Voice cloning

Using AI to copy a real person's voice from a short recording. The copy can then "say" anything.

Deepfake

A fake video, photo, or recording made with AI. It shows a real person saying or doing something they never did.

Phishing (said "fishing")

A fake email or text that tries to get you to click a link or share private details.

In 2025, people 60 and older filed **201,266 complaints** with the FBI and reported **$7.7 billion** in losses.[1] The good news: the same few calm habits work against every scam in this guide.

AI SCAM 1 OF 7

The voice-cloned family emergency call

Your phone rings. A frightened voice sounds just like a younger relative, your child, or a friend. They've had an accident or been arrested, and they need money now. Sometimes a "lawyer" or "officer" takes over the call.[7] With voice cloning, a scammer needs only a short clip of your loved one's voice, which they may find online.[5] (You may hear officials use another name for it. We call it the family-emergency scam.)

Warning signs

- Panic, tears, and a push to act right now.
- "Please don't tell Mom and Dad."[7]
- A request for a wire transfer, gift cards, a payment app, or cash picked up in person.[7]

What to do

- Don't trust the voice. Hang up.
- Call your loved one on the number saved in your phone. Can't reach them? Call another family member.[7]
- Ask for your family safe word (page 11).

In 2025, people told the FBI they lost more than **$5 million** to "distress" calls that used voice cloning.[1]

AI SCAM 2 OF 7

Deepfake videos and fake celebrity endorsements

You see a video online. A famous actor, TV doctor, or business leader seems to recommend an investment, a cure, or a free gift. It looks and sounds real. But it may be a deepfake. The FBI warns that criminals make AI videos of well-known people to make their scams more believable.[3]

! Warning signs

- Odd details: strange hands, teeth, or eyes, or shadows that don't match.[3]
- Lips and voice that are slightly out of step.[3]
- A famous face urging you to pay or invest quickly.

✓ What to do

- Never invest or buy just because someone famous says so.[9]
- Don't use the ad's link. Visit the company's real website yourself.
- Talk it over with someone you trust first.

"It is never a good idea to make an investment decision just because someone famous says a product or service is a good investment." **SEC, NASAA and FINRA investor alert**[9]

AI SCAM 3 OF 7

AI-written phishing emails and texts

A message says your package is stuck, your account is locked, or you owe a toll. It has a link to click or a number to call. Scam messages used to be full of mistakes. Now AI can write a smooth, polished one in seconds.[3] Some scammers also use **spoofing**, which means faking a phone number or email address so it looks familiar.

Warning signs

- A message you didn't expect, with a link or a number to call.
- Rushing words, like "Act within 24 hours."
- A request for passwords, account numbers, or your Social Security number.

What to do

- Don't click the link or call the number in the message.[6]
- Use the company's real website, or the number on your card or statement.[6]
- Delete the message.

Phishing and spoofing were the **most-reported** crime type for people 60 and older in 2025, with **48,064 complaints** to the FBI.[1]

AI SCAM 4 OF 7

Fake investment and crypto "AI trading"

An ad, a new online friend, or a group chat tells you about an "AI trading" program. It promises big, steady profits. Often you are asked to pay in **cryptocurrency**, a kind of digital money that is very hard to get back. A website may even show your money growing. But the account can be fake, and the money is gone.[10]

Warning signs

- "Guaranteed" profits, or "Our AI can't lose!"[9]
- High pressure to act fast.[9]
- A stranger online coaching you to invest.[10]

What to do

- Look up the person or firm with the free search tool at Investor.gov.[9]
- Get a second opinion from an advisor, friend, or family member.[10]
- Remember: AI can't predict the future.[10]

Investment scams caused the **largest losses** for people 60 and older who reported to the FBI in 2025: about **$3.5 billion**.[1]

AI SCAM 5 OF 7

Romance scams

Someone kind and attentive reaches out on social media or a dating site. Messages come every day, and you grow close. But they can never quite meet in person. Then a crisis comes, and they need money. AI helps scammers create fake profile photos, write warm messages, and even make videos to "prove" they are real.[3]

Warning signs

- Strong feelings, very fast.
- There is always a reason they can't meet.
- A request for money, gift cards, or crypto, or for "help" with an investment.[2]

What to do

- Never send money to someone you have met only online or by phone.[3]
- Talk to a friend or family member you trust.
- If they ask for money, stop writing back and report the profile to the site.

People 60 and older reported **$584 million** in losses to romance and confidence scams to the FBI in 2025.[1] The FTC found people 60 and older were **48% more likely** than younger adults to report losing money to a romance scam.[4]

AI SCAM 6 OF 7

Fake tech support

A warning pops up on your screen with a phone number. Or an email says a subscription will renew for hundreds of dollars. When you call, a friendly "technician" asks to connect to your computer to fix it or give a refund. Then they say they refunded too much and ask you to send money back, often in gift cards.[6]

Warning signs

- A pop-up with alarms and a number to call.
- A request for **remote access**, which means letting them control your computer from far away.
- Any request for gift cards, wire transfers, or crypto.[6]

What to do

- Don't call the number. If a pop-up won't close, restart the computer.
- Never give control of your computer to someone who contacted you.
- Need help? Call the company's real number, or ask someone you trust.

People 60 and older filed **21,333** tech and customer support complaints with the FBI in 2025, with about **$1 billion** in losses.[1] The FTC found they were **over four times as likely** as younger adults to report losing money this way.[4]

AI SCAM 7 OF 7

Government impersonation

A caller says they are from a government agency, like the FBI or the FTC. They claim your identity was used in a crime, or your savings are at risk. To "protect" your money, you must move it, buy gold, put cash in a Bitcoin ATM, or hand it to a courier.[2,6] AI can make their badges and IDs look real.[3]

Warning signs

- Threats of arrest, or of losing your savings.[2]
- Being passed from "your bank" to "a federal agent."[6]
- Requests for gift cards, gold, cash, crypto, or a courier pickup.[2]

What to do

- Hang up. Real agencies never ask for gift cards or a Bitcoin ATM, or tell you to move money to protect it.[6]
- Find the agency's number yourself, and call it.
- Talk to someone you trust before moving any money.

In 2025, people 60 and older reported about **$413 million** in losses to government impersonation scams to the FBI.[1]

YOUR FIRST SHIELD

Your family safe word plan

A **safe word** is a secret word or phrase that only your family knows. The FBI and the FCC both suggest one.[3,7] A voice clone can copy a voice. It cannot know your word.

1. **Choose it together.** Pick something easy to remember but hard to guess, like "blue teapot." Avoid pet names or anything posted online.
2. **Share it in person,** or on a call you made. Never put it in a text, email, or social media post.
3. **Tell everyone who might call for help:** children, younger relatives, and close friends.
4. **Agree on the rule:** "If you ever call me in trouble, I'll ask for the word."
5. **No word? Hang up.** Then call your loved one on a number you trust.

Who knows our word

_____

_____

Keep the word itself in your memory, not on paper by the phone.

YOUR EVERYDAY HABIT

Stop. Hang Up. Call Back.

One simple habit protects you from every scam in this guide. Practice it until it feels natural.

Step 1

Stop

Take a breath. Scammers need you to rush. A real emergency can wait the few minutes it takes to check.

Step 2

Hang Up

Or close the message. You don't owe a pushy caller politeness. Don't press any buttons or click any links.

Step 3

Call Back

Use a number you already trust: one saved in your phone or printed on your card or statement. Never use a number the caller gave you.[3]

> *"Anyone who's rushing you into paying or giving information is almost certainly a scammer."*
>
> Federal Trade Commission[6]

PRINT ME · KEEP ME BY THE PHONE

My Scam Shield Checklist

Before I do anything, I...

- [ ] Stopped and took a breath. I will not be rushed.
- [ ] Hung up, or closed the message.
- [ ] Called back on a number I trust, not one they gave me.
- [ ] Asked for our family safe word.
- [ ] Talked it over with someone I trust.

Red flags: if I check any of these, I stop

- [ ] They want gift cards, crypto, a wire transfer, gold, or cash.
- [ ] They want to send a courier to pick up money.
- [ ] They tell me to keep it secret.
- [ ] They want control of my computer.
- [ ] They ask for passwords, PINs, or account numbers.
- [ ] They promise guaranteed profits.

Numbers I trust

My bank: _____

Family: _____

AARP Fraud Watch Helpline: 877-908-3360 (free)

Report a scam: ReportFraud.ftc.gov · ic3.gov

IF IT HAPPENS

If you think you've been scammed

First, it is not your fault. These are crimes run by professionals. Act quickly, and be kind to yourself.

1. Call your bank right away

Use the number on your card. Ask them to stop or reverse the payment. With bank transfers, time matters most.[1]

2. Report it to the FBI

File at **ic3.gov**, no matter how much you lost. Include the payment details.[1]

3. Report it to the FTC

Go to **ReportFraud.ftc.gov**.[12]

4. Talk to a fraud specialist

The AARP Fraud Watch Network Helpline is free: **877-908-3360**, Monday to Friday, 8 a.m. to 8 p.m. Eastern.[11]

Speed helps. In 2025, an FBI team worked with banks on cases involving people 60 and older. They helped freeze about **$32.9 million**, roughly half of the money reported lost in those cases.[1]

AI ON YOUR SIDE

Let AI help you check a message

AI can work for you, too. A helper like Grok can read a message that worries you and point out warning signs. You can try Grok at no charge at grok.com or in the Grok app.

1. Copy the words of the message. Leave out names and account details.
2. Open Grok and paste it in, with a question like the one below.
3. Read the answer. Then still use Stop, Hang Up, Call Back.

TRY THIS

"I got this text message. Does it show signs of a scam? Please explain in plain words and tell me what to do next. Here it is: *Your package is on hold for an unpaid $1.95 fee. Pay today at the link below.*"

Keep these to yourself

Never paste passwords, PINs, account numbers, or your Social Security or Medicare number into any AI tool. AI can also be wrong. Treat it as a second opinion, not the final word.

UNTIL NEXT TIME

You've got this

Thank you for reading. Remember, you don't need to know every trick. You only need a few steady habits: a family safe word, and Stop, Hang Up, Call Back.

Please share this guide with a friend or a family member. Talking about scams openly is one of the best ways to stop them.

Join our free weekly newsletter

Each week, we send one short, friendly AI tip in big print. No jargon, no pressure, and you can unsubscribe any time.

Sign up at thewisdomedge.com

Questions? Email support@thewisdomedge.com

Warmly,

Glenn Lee

The Wisdom Edge is an independent education brand and is not affiliated with or endorsed by xAI, X, the FTC, the FBI, or AARP. This guide is for learning and is not legal or financial advice.
© 2026 The Wisdom Edge

WHERE OUR FACTS COME FROM

Sources

Facts were checked in November 2026. Small gold numbers in this guide match the list below.

1. FBI Internet Crime Complaint Center (IC3), *2025 IC3 Annual Report*, including the Elder Fraud section. ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
2. FBI IC3, *Elder Fraud* brochure (2025 data). ic3.gov/Outreach/Brochures/elder_fraud_tri-fold.pdf
3. FBI IC3, Public Service Announcement I-120324-PSA, "Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud," Dec. 3, 2024. ic3.gov/PSA/2024/PSA241203
4. Federal Trade Commission, *Protecting Older Consumers 2025–2026*, Oct. 19, 2026. search.ftc.gov/system/files/ftc_gov/pdf/2026-older-adults-report-10192026.pdf
5. FTC Consumer Alert, "Scammers use AI to enhance their family emergency schemes," Mar. 20, 2023. web.archive.org/web/20261031044027/https://consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes
6. FTC Data Spotlight, "Impersonation scams: not what they used to be," Apr. 1, 2024. search.ftc.gov/system/files/ftc_gov/pdf/imposter-scams-spotlight-2024.pdf
7. FCC Scam Alert, "'Grandparent' Scams Get More Sophisticated." fcc.gov/consumers/scam-alert/grandparent-scams-get-more-sophisticated
8. FCC, "FCC Makes AI-Generated Voices in Robocalls Illegal," Feb. 8, 2024. fcc.gov/document/fcc-makes-ai-generated-voices-robocalls-illegal
9. SEC, NASAA and FINRA, "Artificial Intelligence (AI) and Investment Fraud: Investor Alert," Jan. 25, 2024. investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/artificial-intelligence-fraud
10. CFTC Customer Advisory, "SI Won't Turn Trading Bots into Money Machines." cftc.gov/LearnAndProtect/AdvisoriesAndArticles/SITradingBots.html
11. AARP Fraud Watch Network Helpline. aarp.org/money/scams-fraud/helpline/
12. FTC, report fraud online. reportfraud.ftc.gov