



**Aware***and* **Safe**

BE AWARE. STAY SAFE.

SAFE IN THE AGE OF AI

# The Everyday Guide to Outsmarting AI Scams



FREE SAMPLE · CHAPTER 1

## The New Face of Scams

*From “The Everyday Guide to Outsmarting AI Scams” — read the full first chapter free.*

# The New Face of Scams

---

Scams are as old as civilization. The con artist used to work street corners; then came the telephone, then email. Each new technology gave criminals new tools, and each time, ordinary people learned the new rules and adapted.

AI is the biggest such shift in our lifetime — not because criminals are smarter, but because the tools got dramatically better, cheaper, and easier to use. Here's what's changed.

## The voice on the phone might not be real

It used to be that a scam call was easy to spot: a stranger with a thick accent reading a script about your "car warranty." AI voice cloning changed that completely.

With just a few seconds of someone's recorded voice — from a voicemail, a social media video, a TikTok — AI can now generate new speech in that person's voice saying anything at all. And it sounds real. Not robotic, not strange. Real.

This is how the modern "grandparent scam" works: a criminal calls an elderly person, and the voice on the line is their grandchild — crying, panicked, saying they've been in an accident or arrested and need money wired immediately. Don't call Mom and Dad, they say. It's urgent. It feels real because the voice is real — or close enough that a frightened grandparent can't tell the difference.

Real families have lost tens of thousands of dollars this way.

**What to do about it:** Agree on a family code word — a silly, secret word that only your family knows. If you ever get a panicked call from a "relative," ask for the code word. A scammer won't know it. And make it a rule: no money moves on the basis of a single phone call, ever. Hang up, call the person back on their known number, and check.

## **The video call might not be real either**

Voice was just the start. AI can now generate realistic video of a person's face, synced to speech, in real time. There have already been cases of criminals joining video calls impersonating company executives — in one widely reported case, a finance employee transferred over \$25 million after a video call with what he believed were his company's executives. Every face on the call was fake.

You probably won't face a \$25 million heist. But the same technology can fake a video message from a "friend" or "relative" on social media, or a clip of a public figure saying something outrageous.

**What to do about it:** Treat unexpected video with the same skepticism as unexpected calls. If a video message asks you for money or sensitive information, verify through a completely different channel — call the person's real number, or message them on a different app. Urgency is the scammer's best friend; slowing down is yours.

## The phishing email got a lot smarter

Classic phishing emails were easy to spot: broken English, strange formatting, obvious lies. AI fixed all of that. Today's AI-written phishing emails are grammatically perfect, personalized with details scraped from your social media, and tailored to your interests, your job, your bank.

Worse, AI lets criminals send thousands of personalized messages at almost no cost. Where a scammer once had to choose targets carefully, they can now carpet-bomb entire populations with messages that feel hand-written.

**What to do about it:** Stop judging messages by how professional they look — AI made "looks legitimate" meaningless. Instead, judge by what the message asks you to do. Any message that asks you to click a link, download something, send money, or share personal information deserves verification through a separate channel. When in doubt, go to the company's website directly (type the address yourself) rather than clicking the link in the message.

## A scam, step by step

To make this concrete, here's how a real voice-cloning scam typically unfolds — based on patterns reported by fraud investigators:

**Days before:** The scammer scrolls social media and finds a grandmother who posts publicly — family photos, comments from her grandson, maybe a video from a birthday party where the grandson speaks. Thirty seconds of audio is plenty.

**The setup:** AI software clones the grandson's voice. The scammer also learns details from the posts: the grandson's name, his college, the family dog's name. All of it becomes script material.

**The call, Tuesday evening:** The grandmother's phone rings. It's her grandson — crying, panicked. He's been in a car accident, he says. He's at the police station. He needs bail money wired right now, and please don't tell Mom, she'll worry. In the background, another voice — the "officer" — confirms the story and gives wiring instructions.

**Why it works:** The voice is right. The details are right. The emotion is overwhelming. And the urgency — don't tell anyone, do it now — blocks the one thing that would expose the fraud: a moment of calm verification.

**How it falls apart:** The grandmother remembers the family code word. She asks for it. Silence — then a hurried excuse, then a dial tone. She calls her grandson's real number. He's in his dorm room, fine, wondering why Grandma sounds so shaken.

Every AI scam follows this shape: research, impersonation, urgency, isolation. Learn to spot the shape, and the specific technology stops mattering.

## THE BOTTOM LINE

AI didn't invent scams. It industrialized them — making them more convincing, more personalized, and vastly more numerous. The good news is that the defenses haven't changed as much as the attacks: slow down, verify through a second channel, and never act on urgency alone. Those three habits would have stopped nearly every AI scam attempted so far.

In the next chapter, we'll go deeper into phishing — the most common AI-powered attack you'll actually encounter — and build your detection skills step by step.



---

# Enjoyed this chapter?

This was Chapter 1 of *The Everyday Guide to Outsmarting AI Scams*, part of the *Safe in the Age of AI* series by Aware and Safe. The complete handbook includes every chapter, all the checklists, and the companion resources — available now in the edition that suits you.

## Ebook + Audiobook Bundle

**\$8.99**

Everything together — the best value.

<https://awareandsafe.com/product/the-everyday-guide-to-outsmarting-ai-scams-ebook-audiobook-bundle/>

## Ebook

**\$6.99**

Premium PDF — read on any device.

<https://awareandsafe.com/product/the-everyday-guide-to-outsmarting-ai-scams-ebook/>