Don’t Let AI Steal Your Retirement

How to Spot and Avoid the 9 Most Dangerous AI-Enabled Scams Targeting Seniors Today

J. Hutchinson, CISSP, CISSP-ISSMP

PREFACE

Why I wrote this book

Cybercriminals use Artificial Intelligence (AI) to create messages that sound authentic by mimicking the tone, style, and details of real communications. AI analyzes large amounts of data from social media, forums, and leaked databases to craft personalized messages that feel genuine to the target, making scams harder to detect.

After spending over 30 years working in Information Technology, I have retired but want to use my experience to help other seniors, parents, grandparents, and small business owners recognize the warning signs and protect themselves from AI scams.

Stay Safe! J. Hutchinson

Table of Contents

Confidence/Romance Scams

The first four scams are known as Confidence/Romance Scams where scammers are using artificial intelligence (AI) to create convincing fake online profiles and generate realistic conversations that make it easier to gain a victim's trust. AI-written messages often sound natural and persuasive, making these scams more difficult to recognize.
In 2025, victims reported losing more than $19 million to AI-related confidence and romance scams.

These scams continue to evolve. Criminals can now mimic the voices of children, grandchildren, siblings, spouses, close friends, or other trusted individuals to create believable emergency situations designed to pressure victims into sending money before they have time to verify the story.

CHAPTER ONE

01

Grandparent & Family Emergency Scams

Few things grab our hearts faster than a phone call from a grandchild in trouble. That's exactly why scammers love this one. With just a few seconds of audio pulled from social media, AI can now copy a loved one's voice well enough to fool almost anyone. The call sounds real. The panic feels real. And the request for money comes fast, before you have a chance to think.

In this chapter, I'll walk you through what these calls sound like, why they work so well on caring grandparents, and the simple steps that stop them cold.

$5 MILLION

Reported losses by adults 60+ to imposter scams in 2025 (FBI).

A TRUE-TO-LIFE STORY

The 6 A.M. Phone Call

Margaret,72, picked up before the second ring. The voice on the other end was crying, and it sounded just like her grandson Tyler. He said he'd been in a car accident, the other driver was hurt, and he was at the police station. A man came on the line claiming to be Tyler's lawyer. He needed $8,500 in cash for bail, right away, and Tyler was "too embarrassed" to call his parents.

Margaret drove to her bank, withdrew the money, and handed it to a courier who came to her door. It wasn't until she called her daughter that afternoon that she learned Tyler had been at work the whole time. The voice she heard was an AI clone, built from a 30-second video Tyler had posted on Instagram.

"It was his voice. I'd know it anywhere. That's what makes this so cruel."

Five Steps That Stop the Scam

01 **Pause before you act.** Real emergencies survive a 60-second pause. Scams don't. Take a breath and slow the call down.

02 **Hang up and call back.** Call your loved one directly on a number you already have saved. Don't use any number the caller gives you.

03 **Set a family code word.** Pick a simple phrase only your family knows. If the caller can't say it, it isn't them.

04 **Never send cash, gift cards, or wire transfers.** No real lawyer, bail bondsman, or police officer will ask for these. That request alone is the red flag.

05 **Tighten up social media.** Make accounts private. Even a short video gives scammers enough audio to clone a voice.

CHAPTER TWO

02

Deepfake Scams

Deepfakes use AI to clone faces and voices with unsettling accuracy. A familiar boss on a video call, a loved one's voice in a frantic phone message — what you see and hear is no longer proof of who's really there. Verifying through a separate, trusted channel is the one habit that stops these scams cold.

Over $12 MILLION

Reported losses by adults 60+ to AI enabled voice spoofing scams in 2025 (FBI)

A TRUE-TO-LIFE STORY

The $25 Million Video Call

In 2023, an employee at a multinational firm in Hong Kong joined a video conference with his company's CFO — or so he thought.

Scammers had used AI to create a convincing deepfake video of the executive, complete with familiar voice and mannerisms. Other "colleagues" on the call were also AI-generated.

During the meeting, the employee was instructed to transfer funds for an urgent confidential deal. Trusting what he saw and heard, he wired $25 million to a fraudulent account.

By the time the fraud was discovered, the money was gone.

HOW TO PROTECT YOURSELF

Five Steps That Stop the Scam

01 **Watch for visual glitches.** Look for unnatural blinking, odd lighting, or lip-sync that doesn't quite match the voice.

02 **Verify through a second channel.** If a video call asks for money or sensitive info, hang up and call the person back on a known number.

03 **Be skeptical of celebrity pitches.** Famous faces promising fast money or miracle products are almost always deepfakes.

04 **Slow down urgent requests.** Deepfake scams rely on pressure. Pause, breathe, and verify before acting.

05 **When in doubt, assume it's fake.** Until you've confirmed through another channel, treat any unexpected video request as suspicious.

CHAPTER THREE

03

Social Media Impersonation Scams

If a friend's message on social media asks for money, a code, or a 'quick favor,' pause. Scammers clone profiles of people and brands you trust, then slide into DMs with fake giveaways, investment tips, or urgent requests. The account looks right because it copies real photos and names. Verifying through a second channel is what stops it.

$19 BILLION

Reported lost to the FBI in 2025—with impersonation and f.ake-giveaway schemes leading the rise

A TRUE-TO-LIFE STORY

The Friend Who Wasn't

Carol, 68, got a Facebook message from her longtime friend Diane raving about a government grant program she'd just received — $50,000, no repayment, just a small processing fee. Diane's profile photo, hometown, and family pictures all matched. Carol messaged back excited, sent $750 in gift cards to the "grant agent," and waited.

The grant never arrived. When Carol called Diane directly, Diane was horrified — her profile had been cloned weeks earlier, and dozens of her friends had been contacted. The real Diane never sent a single message. The $750 was gone.

"It looked exactly like her page. Same pictures, same friends. I never thought to call and ask if it was really her."

Five Steps That Stop the Scam

01 **Check for a duplicate profile.** If a friend messages with an unusual request, search their name. Two accounts almost always means one is fake.

02 **Confirm by phone or in person.** A 30-second call to your friend's known number ends the scam before it starts.

03 **Be wary of giveaways and "grants."** Real giveaways never require fees, gift cards, or processing payments up front.

04 **Lock down your own profile.** Set friend lists to private and limit who can see your photos. Cloners need public material to copy.

05 **Report and block impersonators.** Report the fake account to the platform and warn your friends. It protects everyone in your circle.

CHAPTER FOUR

04

Sextortion Scams

If a stranger online pressures you for explicit photos, or an email threatens to share private images unless you pay, pause. Sextortion scammers use shame and urgency to force fast payment. Some have real material from hacked accounts or romance scams; many bluff with old passwords or AI-generated images. Silence is what they count on.

Over $14 MILLION

Sextortion losses for adults over age 60 in 2025

A TRUE TO LIFE STORY

The Grandfather and the Gift Cards

In 2024, a 72-year-old retiree in Arizona received an email claiming a hacker had recorded him through his webcam. The message included an old password he recognized.

The email demanded $2,000 in gift cards within 48 hours or, it claimed, embarrassing footage would be sent to his family, his church, and his former coworkers.

Shaken and ashamed, he drove to three stores, bought gift cards, and read the codes aloud over the phone. The threats kept coming. He paid again. Then a third time.

There was no footage. The password came from a years-old data breach. By the time he told his daughter, he had lost over $6,000 — and the scammer was already gone.

HOW TO PROTECT YOURSELF

Five Steps That Stop the Scam

01 **Stop responding immediately.** Every reply, payment, or apology tells the scammer you're a paying target. Silence is your strongest move.

02 **Do not pay. Ever.** Paying rarely ends the threats and almost always invites more demands. Most threats are bluffs, and even real material rarely surfaces.

03 **Save the evidence before blocking.** Screenshot the messages, usernames, payment requests, and email headers. You'll need them for reports.

04 **Report to the FBI and the platform.** File at **ic3.gov** and report the account on the platform where it happened. For minors, also contact **CyberTipline.org**.

05 **Tell someone you trust.** Shame is the scammer's weapon. A trusted family member, friend, or counselor breaks the isolation and helps you act clearly.

Government Impersonation Scams

Chapters 5 and 6 introduce you to Government Impersonation scams

In these scams, criminals pretend to be government officials or representatives from trusted agencies to steal money or personal information. They may claim to be calling from the Social Security Administration, Medicare, the IRS, law enforcement, or another government agency. Scammers often use threats, false claims, or urgent deadlines to pressure victims into making payments, sharing sensitive information, or providing access to their financial accounts.

During 2025, Government Impersonation scams cost victims $797,948,469 with adults age 60 and over losing $413,206,251; more than any other age group.

AI has made these calls more convincing than ever. Voices sound natural. Scripts adjust on the fly. In this chapter, I'll show you how to tell a real agency from a fake one and what to do the moment something feels off.

05

FakeSocial Security Calls

A call comes in and the caller ID even shows the agency name. A serious voice says it's the Social Security Administration. They tell you your benefits are about to be suspended, there's a warrant out, or someone has stolen your identity. They sound official, they know just enough about you to seem real, and they push you to act right now.

$413 MILLION

Lost by older adults to government impersonation scams in 2025 (FBI).

A TRUE TO LIFE STORY

The Voice From "Social Security"

Harold, 68, answered a call that showed "SSA" on the screen. The agent said his Social Security number had been linked to a crime in Texas and his benefits would be frozen by the end of the day. To "protect" his money, Harold needed to move it to a secure federal account using gift cards from the nearest store.

Harold drove to three different stores buying $4,000 in gift cards, reading each number aloud over the phone as instructed. The agent stayed on the line the whole time, warning him not to tell the cashiers or his family. By the time his son called that evening, the money was gone. Real agencies never ask for gift cards, and they never call you out of the blue with threats.

"He sounded so official. He even had a badge number. I never thought to question it."

HOW TO PROTECT YOURSELF

Five Steps That Stop the Scam

01 **Hang up. Always.** Real government agencies don't call to threaten you. If you're worried, hang up and call the agency directly using the number on their official website.

02 **Caller ID can lie.** Scammers spoof phone numbers and agency names. Don't trust the screen. Trust the action you take to verify.

03 **No agency asks for gift cards or wire transfers.** Not the IRS, not Social Security, not Medicare. Ever. That request is the scam.

04 **Don't confirm personal details.** Never give your Social Security number or banking info to an incoming caller.

05 **Talk to someone you trust.** Before you act, call a family member or friend. Scammers count on isolation. A second voice breaks the spell.

CHAPTER SIX

06

Medicare and Health Insurance Scams

Medicare scams are among the fastest-growing threats facing older Americans. Criminals now use AI-generated voices to impersonate Medicare agents, insurance reps, even doctors' offices, sounding so natural that even careful people get drawn in. They pressure you to confirm your Social Security number, Medicare ID, or banking details before you have time to think it through.

$57+ BILLION.

Estimated loss to Medicare fraud in2025 in the U.S (CMS / NHC AA) — much of it now driven by AI-powered impersonation.

A TRUE TO LIFE STORY

Margaret and the "Medicare" Renewal Call

Margaret, 72, answered a call from someone claiming to be a Medicare representative. The caller, who sounded calm and official, said her benefits were about to expire and she needed to confirm her Social Security number and Medicare ID right away to keep her coverage active.

The voice was so natural it never crossed her mind it could be AI-generated. He even mentioned recent changes to Medicare rules to sound credible.

Something felt off, so Margaret asked for a callback number and hung up. She phoned 1-800-MEDICARE directly. They confirmed it was a scam and that Medicare never calls to ask for personal information.

Scammers use AI to impersonate Medicare agents, insurance reps, and even doctors' offices to harvest personal data, file fraudulent claims, or sell fake supplemental plans.
.

HOW TO PROTECT YOURSELF

Five Protection Steps

01 **Never share personal info on inbound calls.** Medicare and insurers won't call asking for your Social Security number, Medicare ID, or banking details.

02 **Verify by calling official numbers.** Hang up and call 1-800-MEDICARE or the number on your insurance card to confirm any claim.

03 **Be wary of "free" medical offers.** Free braces, genetic tests, or COVID kits in exchange for your Medicare number are common scam hooks.

04 **Guard your Medicare card.** Treat it like a credit card. Only share the number with trusted doctors, pharmacists, and insurers.

05 **Review your statements monthly.** Check Medicare Summary Notices and insurance Explanations of Benefits for services you never received.

AI-Enhanced Investment Scams

Investment scammers are increasingly using artificial intelligence (AI) to make their schemes appear legitimate. AI enables criminals to create personalized conversations with thousands of potential victims at once, making each interaction seem genuine and tailored to the individual.

Scammers also use AI-generated videos, cloned voices, and fake images of celebrities, business executives, financial experts, or other trusted public figures to promote fraudulent investment opportunities. These convincing endorsements often appear on social media, websites, messaging apps, or even during video calls, making the scams more difficult to detect .

In 2025, senior victims reported losing more than $3 billion to investment scams with a reported AI connection.

CHAPTER SEVEN

07

Investment and Cryptocurrency Fraud

If someone promises guaranteed returns, urges you to act today, or pushes you toward an app or platform you've never heard of, slow down. Investment scams have grown right alongside crypto, and they're carefully built to look professional. The website looks polished, the "advisor" is friendly, and the early returns seem real. By the time you try to withdraw, your money is gone.

$3.5 BILLION

Reported lost to investment scams in 2025 for persons over age 60 — the highest of any fraud category tracked by the FTC.

A TRUE-TO-LIFE STORY

The App That Wasn't Real

Linda, 62, met a kind man on a dating site. After weeks of warm conversation, he mentioned the crypto platform that had "changed his life." He helped her set up an account and walked her through her first $500 deposit. The dashboard showed her balance climbing every day. She added more. Then more.

When Linda tried to withdraw $10,000 to help her daughter with a down payment, the platform asked for a "tax fee" first. Then a "verification fee." Then her account was frozen. The man stopped answering. The platform, the dashboard, the gains — none of it was real. Linda lost $47,000 of her retirement savings.

"The numbers on the screen looked so real. I watched my money grow for months. I trusted what I could see."

HOW TO PROTECT YOURSELF

Five Steps That Stop the Scam

01 **Guaranteed returns aren't real.** Every legitimate investment carries risk. "No risk, high return" is the oldest scam line in the book.

02 **Be wary of romance and crypto in the same conversation.** Strangers online who quickly turn talk to investments are following a script.

03 **If you can't easily withdraw, it isn't yours.** Surprise fees to access your own money mean the platform is a trap.

04 **Verify the company before you send a dime.** Check FINRA's BrokerCheck and your state securities regulator. Real firms welcome the question.

05 **Talk to someone before transferring funds.** A trusted family member, your bank, or a fee-only advisor can spot what excitement may hide.

CHAPTER EIGHT

08

Fake Customer Support Scams

Scammers use AI and other technology to impersonate technical support or customer service representatives from trusted organizations. They may contact you about a supposed computer virus, expired antivirus subscription, banking issue, online purchase, utility account, printer, GPS device, internet or cable service, or cryptocurrency exchange. Their objective is to create a sense of urgency, gain remote access to your devices, steal personal information, or convince you to pay for services you don't need.

$1 BILLION

Lost to tech support scams in 2025 by Americans over age 60

A TRUE TO LIFE STORY

Frank and the "Apple Support" Call

Frank got a phone call from someone claiming to be from "Apple Support." The caller said his iCloud account had been hacked and urgently asked him to install a remote access app so they could "secure" his device.

The caller sounded professional and used technical language to build trust. He warned Frank that if he didn't act immediately, all of his photos and personal data would be lost forever.

Frank refused, hung up, and called Apple back using the number listed on their official website. Apple confirmed they never make unsolicited calls like this.

A pop-up warning, a bogus help line, or a chatbot pretending to be "Amazon Support" can trick you into handing over passwords or remote access to your device.

Five Protection Steps

01 **Never call numbers from pop-ups.** Pop-up warnings urging you to call a support number are almost always scams. Close the browser instead.

02 **Use official websites only.** Find support phone numbers and chat links directly on the company's official website, not from search ads.

03 **Never grant remote access.** Don't allow anyone to control your computer unless you initiated the call to a verified support line.

04 **Watch for gift card requests.** No legitimate company will ever ask you to pay for support or services with gift cards.

05 **Hang up and verify.** When in doubt, hang up. Call the company back using a number you trust from their website or a billing statement.

CHAPTER NINE

09

AI-Generated Phishing Emails and Texts

Today's phishing emails are polished, personalized, and grammatically perfect. AI tools let scammers mimic your bank, your boss, or your favorite store with chilling accuracy. The grammar is flawless, the logos look right, and the urgency feels real. Slowing down and verifying through a trusted channel is what keeps you safe.

$77 MILLION

Lost to phishing scams in 2025 by Americans over age 60

A TRUE-TO-LIFE STORY

The Email That Looked Real

Thomas, 85, a retired physician in a southern California senior community, clicked a link in an email offering seniors "exclusive savings on everyday essentials, from groceries to household services." He couldn't quite explain why. "I don't really need a discount," he later said.

Last Christmas, he nearly lost money to a similar phishing message claiming he owed delivery fees on a package. He entered his credit card details before something felt off. His bank flagged and blocked the $200 charge just in time — but the next victim might not be as lucky.

"The email looked completely legitimate — perfect grammar, the right logo. I can't explain why I clicked."

HOW TO PROTECT YOURSELF

Five Steps That Stop the Scam

01 **Hover before you click.** On a computer, hover over any link to see the real address. On phone, press and hold. If it doesn't match the sender, don't click.

02 **Watch for urgent language.** "Act now," "account suspended," or "final notice" are pressure tactics designed to bypass your judgment.

03 **Go to the website directly.** Never use links inside an email. Type the company's address into your browser or use a bookmark you trust.

04 **Never share details by email or text.** Banks, the IRS, and shippers will not ask for passwords, card numbers, or codes through a message.

05 **Report and delete.** Forward suspicious emails to reportphishing@apwg.org, then delete. Reporting helps stop the scam from reaching others.

RESOURCES

1) FBI Internet Crime Report 2025 Internet Crime Complaint Center

https: //www.ic3.gov/AnnualReport/Reports/2025_ IC3Report.pdf

To report a crime:

FBI crime complaint center: www.ic3.gov

REFERENCES

1) FBI Internet Crime Report 2025 Internet Crime Complaint Center

2) Grandparent & Family Emergency Scams

3) The $25 Million Video Call

4) The Email That Looked Real

5) GAO Fraud and Improper Payments

6) Medicare Fraud 2025