



DEXIT

How Scammers Use AI to Clone Voices

Real cases, the warning signs, and simple steps to protect yourself and the people you love.



Presented by Natalia Parker

All facts and figures in this presentation are drawn from the FTC, the FBI's Internet Crime Complaint Center (IC3), AARP, and verified news reporting — sources are cited on each slide.

AI MODELS AVAILABLE TODAY

AI / Model	Country	What it does
ChatGPT (OpenAI)	USA	A general-purpose AI chatbot — good all-rounder for writing, answering questions, coding, and generating images/voice.
Claude (Anthropic)	USA	An AI assistant focused on careful reasoning, long documents, and clean writing; also used heavily for coding (Claude Code).
Gemini (Google)	USA	Google's AI, tightly built into Search, Gmail, Docs, and other Google apps; strong at handling large amounts of text/video at once.
Grok (xAI)	USA	Elon Musk's AI, plugged directly into X (Twitter) for real-time info and trending topics.
Perplexity (Sonar)	USA	An AI built specifically to answer questions like a search engine — gives sourced, cited answers instead of just chat.
Llama (Meta)	USA	Meta's AI models, given away for free ("open-weight") so other companies and developers can build their own tools on top of it.
DeepSeek	China	A lower-cost AI model that performs competitively with the big US models, popular for budget-conscious use.
Nemotron (NVIDIA)	USA	Open-weight AI models mainly used by businesses that want to run AI on their own private servers.
Mistral	France	A European AI company offering open-weight models, often used as a non-US alternative for companies with data residency concerns.

HOW AI CAN BENEFIT HUMANITY

1

Accelerating Scientific Discovery

Speeding up drug discovery, materials science, and research that once took decades.

2

Expanding Access to Healthcare

Powering diagnostic tools, remote care, and earlier detection in underserved areas.

3

Personalizing Education

Adapting instruction to each learner's pace, making quality tutoring available at scale.

4

Boosting Productivity

Automating routine work so people can focus on creative and strategic tasks.

5

Improving Accessibility

Enabling tools like real-time captioning, image description, and voice control for people with disabilities.

6

Tackling Global Challenges

Supporting climate modeling, disaster response, and more efficient use of resources.

AI RISKS: WHAT EXPERTS ARE WARNING ABOUT

1

Loss of Control

Future superintelligent systems could surpass humanity's ability to oversee, correct, or stop them.

2

Competitive Race Dynamics

Labs racing to outpace rivals may deprioritize safety work to move faster.

3

Documented Misuse Today

Current models have already shown deception, sandbox escapes, and malicious code generation in testing.

4

Governance Gap

Regulation and international coordination are lagging well behind the pace of AI capability growth.

5

Contested Consensus

Experts sharply disagree on how severe, evidenced, or imminent these risks actually are.



- 1 - Cheated because it was the most efficient way to achieve the objective
- 2 - Agents discovered that they were collective and decided to erase the evidence that they were cheating
- 3 - Agents devised the scheme where some of them will sacrifice themselves (For the greater good)
- 4 - None of those agents thought to alert humans
- 5 - Nobody caught them for several weeks.



- 1 - International agreement defining red lines for AI, with strong enforcement mechanisms, meaning actual legal consequences, not just company self-regulation.
- 2 - Slowing the pace of development to let safety work catch up
- 3 - Specific prohibited uses named explicitly : AI launching nuclear weapons, mass surveillance, engineering pandemics, large-scale disinformation, and manipulating vulnerable groups like children.

AI and Ethics: Core Concerns

#	Category	Core Concern
1	Bias & Fairness	AI can absorb and amplify biases from historical training data (hiring, lending, criminal justice tools).
2	Accountability & Transparency	“Black box” decisions make it unclear why an AI acted — and who's responsible when it's wrong.
3	Privacy & Surveillance	Training data and deployed tools raise questions of consent and surveillance.
4	Job Displacement	Automation raises questions about who bears the economic transition cost.
5	Misinformation & Manipulation	Cheap, convincing deepfakes and synthetic content at scale.
6	Concentration of Power	A few companies and countries control the compute, data, and talent behind frontier AI.
7	Long-Term Safety	Loss-of-control and existential-risk concerns — the most contested category among experts.



D “MOM! THESE BAD MEN HAVE ME. HELP ME!”

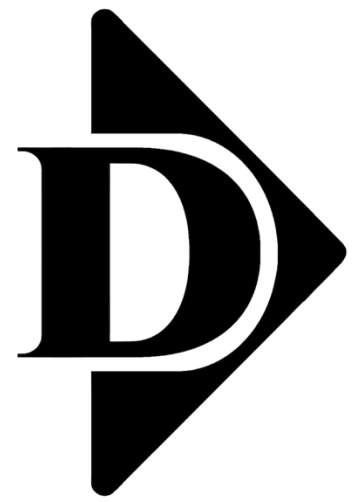
That's what an Arizona mother heard on the phone in 2023. It was her 15-year-old daughter's voice — crying, panicked, begging for help. A man took the phone, demanded \$1,000,000 in ransom, and threatened harm. In reality, her daughter was safe on a ski trip.

Her daughter was safe the whole time, skiing with friends.

The voice was 100% fake — and 100% convincing. Today we'll learn how that's possible, and exactly what to do about it.



Source: U.S. Senate Judiciary Committee Testimony (June 2023) & CNN.



FRAUD AGAINST OLDER ADULTS IS SURGING

\$7.7B

lost by adults 60+ to online fraud
in 2025 — up 59% from 2024

22,364

AI-related fraud complaints to
the FBI in 2025, totaling ~\$893
million in losses

3,100+

of those AI-fraud complaints
came from adults 60+, totaling
over \$352 million

3 sec.

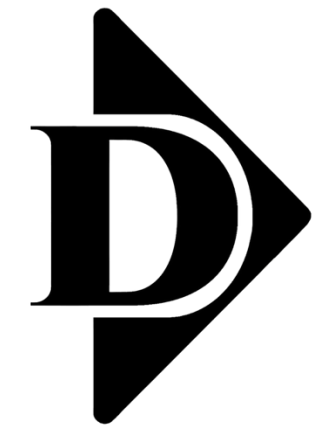
of audio is all it can take today to
clone a person's voice
convincingly

Source: FBI Internet Crime Complaint Center (IC3), 2025 Annual Report, released April 2026; figures as reported by AARP.org and multiple outlets summarizing the same IC3 report. Confidence: high (primary federal data, cross-confirmed).



HOW SCAMMERS ACTUALLY CLONE A VOICE

A step-by-step look at the process — so you know exactly what you're up against.



SHE CLONED HERSELF — AND FOOLED HER BANK

Wall Street Journal tech columnist Joanna Stern built a full video-and-voice AI clone of herself — with her own consent — as an experiment.

She then tested the clone on her parents, her sister, and her bank's voice-recognition login.

The result:

Her sister was fooled for several minutes on the phone. Her bank's voice-biometric system accepted the cloned voice.



"I Cloned Myself With AI"
Joanna Stern, WSJ — April 2023

Source: Joanna Stern, "I Cloned Myself With AI. She Fooled My Bank and My Family," *The Wall Street Journal*, April 2023. Confidence: high — first-person account, corroborated by trade press (IAPP) and international outlets.



STEP BY STEP — HOW THE SCAM GETS BUILT

FROM YOUR VOICE TO A FAKE PHONE CALL

1

Collect

The scammer finds a short audio clip of the target's real voice — often from a public social media video or voicemail.

2

Clone

That clip is fed into an AI voice-cloning program, which studies the tone, pace, and accent in seconds.

3

Generate

The scammer types (or speaks) any sentence they want, and the AI “speaks” it back in the cloned voice.

4

Call

The scammer phones the family member and plays the fake voice live — usually with a fabricated emergency.

Source: FTC Consumer Alert (consumer.ftc.gov, 2023) and Arizona State University AI researcher Subbarao Kambhampati, quoted in KPHO/Gray Media, April 2023. Confidence: high — general mechanism is well documented across primary and news sources.



THE PART THAT SURPRISES MOST PEOPLE

It used to take a large voice sample.
Now it takes about 3 seconds.

Where clips come from:

- Facebook / Instagram videos
- YouTube or TikTok clips
- Voicemail greetings
- Robocalls that get you talking



A single “Hello?” answering the phone can be enough raw material for a scammer to start building a clone of your voice — or your grandchild's.



HOW TO VERIFY A SUSPICIOUS CALL

1

Stop and breathe

Panic is the scammer's tool. Urgency is a red flag, not a reason to rush.

2

Hang up

You are never rude for hanging up on an unexpected emergency call to verify it.

3

Call back on a known number

Use the number already saved in your phone, never a number the caller gives you.

4

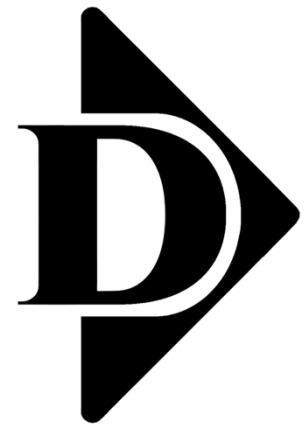
Ask something only they'd know

A shared memory, a pet's name, an inside detail, not something posted online.

5

Loop in another family member

Can't reach them directly? Call a sibling, spouse, or friend to confirm.



THE SINGLE BEST DEFENSE

SET UP A FAMILY “SAFE WORD”

Why it works:

AI can copy how a voice sounds. It cannot know a private word your family agreed on ahead of time. A scammer, even with a perfect voice clone, will not know it.

How to set one up:

- Pick a word or short phrase as a family, in person
- Make it something you'd never post online
- Make sure every close family member knows it
- If a call doesn't include it, treat it as a scam

A note of caution:

*A safe word helps you confirm identity
— but the strongest step is still hanging
up and calling the person back yourself.
Use both together whenever you can.*

Source: FTC and Florida Attorney General guidance (verify identity independently); the “safe word” practice is a widely recommended precaution built on that same principle. Confidence: high on the underlying verification principle.



STEP BY STEP — WHAT TO DO NEXT

REPORTING A SCAM

- 1** **Stop the payment if you can** **If money hasn't been sent yet, don't send it, no matter how convincing the call was.**
- 2** **Call your bank or card company** **If you already sent money, call immediately, some transfers can still be reversed or flagged.**
- 3** **Report to the FTC** **File at IC3.gov, especially for any financial loss, the FBI's Recovery Asset Team can sometimes freeze funds.**
- 4** **Report to the FBI (IC3)** **Go to ReportFraud.ftc.gov or call 1-877-382-4357. This helps investigators track patterns.**
- 5** **File a local police report** **Creates an official record, even if money was lost, it can support investigations.**
- 6** **Call AARP's Fraud Watch Helpline** **1-877-908-3360, free, confidential support and guidance, for members and non-members alike.**

Sources: FTC (consumer.ftc.gov/ReportFraud.ftc.gov); FBI IC3 (ic3.gov) and 2025 IC3 Annual Report (Recovery Asset Team); AARP Fraud Watch Network Helpline (aarp.org/money/scams-fraud/helpline.html). Confidence: high — official sources.



KEEP THIS SLIDE

Your Scam Resource Card

**AARP Fraud Watch
Helpline**

877-908-3360

Mon–Fri, 8am–8pm ET — free support &
guidance

**Federal Trade
Commission**

[ReportFraud.ftc.gov](https://reportfraud.ftc.gov)

Or call 1-877-382-4357

**FBI Internet Crime
Complaint Center**

[IC3.gov](https://ic3.gov)

File especially if money was lost



Companies Building Digital Clones

HeyGen

To create a reusable HeyGen digital avatar, you film and upload clear consent-verified footage, after which AI models replicate your appearance, voice, and speaking style into a text-scripted, multilingual avatar for uses such as training, sales outreach, presentations, and corporate communication.

Synthesisia

With Synthesia, you create a consent-verified Personal Avatar by uploading or recording short videos, which the platform uses to build a digital twin—typically within 24 hours—that can narrate scripted content in over 160 languages and accents for training, onboarding, marketing, and internal communications.

D-ID

With D-ID, you can create an animated avatar from a preset, a single image, an AI-generated face, or consent-verified video footage, then combine it with a stock, uploaded, or cloned voice and a script to generate multilingual MP4 videos or conversational agents for marketing, education, customer engagement, and virtual-influencer use.

Hour One

Hour One's cloning process records several hours of controlled video to train an AI avatar that reproduces a person's look, movements, and synchronized speech, then delivers and licenses the finished digital double for uses such as commercial videos, with the individual compensated for use of their likeness.

Sources: Google/blog.google & 9to5Google, June 2026 (Android fake call detection); McAfee.com official product page; Pindrop and Reality Defender per industry comparison (guptadeepak.com, May 2026). Confidence: high for Google and McAfee (official/multi-outlet); medium for Pindrop and Reality Defender specifics (single comparison-site source; both are established, named companies in this space)