

M A V E R I C K A I

SCAM-PROOF YOUR FAMILY

THE FOUR-MINUTE SETUP THAT BEATS A CLONED VOICE

AI can now fake a familiar voice on the phone from a few seconds of audio. The good news: the thing that stops it takes four minutes and costs nothing. This guide walks you through it, one step at a time, no tech knowledge needed.

The one-word trick that beats a perfect voice clone

The callback rule that ends the scam instantly

A prompt to check any suspicious message in seconds

A prompt to see what scammers can find about you

The five scams to know right now, and their tells

A one-page checklist to send your whole family

2026 Edition

It Started With a Phone Call

A woman got a call from her daughter. She was crying, saying she'd been taken, that someone had her, and that they wanted money.

It was her daughter's voice. The exact voice she'd heard every day for twenty years.

She paid five thousand dollars. Then she found out her daughter had been sitting at work the whole time. The voice on the phone was a clone.

Here's the part that changes everything: cloning a voice takes a few seconds of audio. A voicemail. A video you posted. A story you told at a wedding. Anything with you talking in it is enough.

THE REASSURING PART, AND IT'S REAL

You do not need to become a security expert. You do not need to delete everything and hide. A four-minute setup, done once with your family, beats this whole category of attack, even when the voice is perfect. That's what this guide is. Let's do it.

Why This Works Now (And Didn't Two Years Ago)

Two years ago, faking someone's voice took a studio, expensive software, and real skill. Today it takes a short clip off social media and a free website. That's the whole shift. The tools got good, and they got easy, at the same time. The people doing this are not geniuses. They just have tools that didn't exist before.

The same thing happened to scam emails. They used to be easy to spot because of the clumsy spelling and broken grammar. AI writes them now, so they read perfectly, in your language, in the right tone. The old "just look for bad spelling" advice is dead.

\$893M

lost to AI-powered scams in one
year

22,000+

complaints in that same year

82%+

of phishing emails now written by
AI

WHERE THESE NUMBERS COME FROM

A U.S. Senate report found that in a single year, Americans lost more than \$893 million to AI-powered scams across over 22,000 complaints, and that more than 82% of phishing emails are now written with AI, which is exactly why they stopped having the bad spelling that used to give them away.

NOT IN THE US? THIS STILL MATTERS

That report was American, but the scam absolutely is not. Voice cloning and AI-written scam messages work in every country and every language. Wherever you are, the same four-minute setup protects your family.

The Safe Word (Start Here)

This is the heart of the whole guide, and it is the single most powerful thing you can do. A safe word is a private word your family agrees on. If someone calls sounding like you and asking for money or help, the other person asks for the word. A scammer with a perfect clone of your voice still does not know it. That's the whole trick, and it works no matter how real the voice sounds.

How to pick one

Pick a word or short phrase nobody could guess and that you have never posted anywhere. Not a pet's name. Not a street you've lived on. Not a kid's birthday. Something random and a little odd is best, two unrelated words stuck together works great (like "purple lighthouse"). Easy for your family to remember, impossible for a stranger to know.

Who needs to know it

Anyone who would actually send money or rush to help if they thought you were in trouble. Your parents. Your adult kids. Your spouse. A close sibling. A business partner. Keep the circle to people you truly trust, that's the point.

How to set it up without it being weird

One group text. One sentence. Done. Send this to your trusted family group and agree on the word together:

COPY AND SEND THIS

Quick family thing, takes 10 seconds. AI can now fake people's voices on the phone. So we're setting up a family safe word. If any of us ever calls in a panic asking for money or help, the other person asks for the word. No word = it's not really us, hang up and call back. Let's use: [OUR WORD]. Keep it between us and never post it anywhere.

TIP

If you'd rather not put the actual word in writing, send the message without it and just say the word out loud on a quick call or in person. Either way, the whole setup takes about four minutes.

The Safe Word (continued)

When to use it

Any call asking for money or pushing you to act fast. No exceptions. Even if the voice is perfect. Especially if the voice is perfect and the story is scary, that urgency is the scammer's main tool. A real loved one in real trouble will not mind you taking ten seconds to ask for the word. A scammer cannot answer it.

IF SOMEONE FAILS THE CHECK

Hang up. Don't argue, don't explain, don't let them talk you out of it. Then call the real person back yourself on the number you already have saved for them. That's it. You've just beaten the entire scam.

TEACH IT TO THE KIDS AND GRANDPARENTS TOO

The people most likely to be targeted are older relatives and younger kids. Make sure they know the word and, more importantly, know that it is completely okay to ask for it, even if the person on the phone gets upset. Getting upset is what a scammer does. Your real family will understand.

The Callback Rule

If the safe word is your shield, this is your sword. It is one sentence, and it beats almost every phone and message scam there is:

THE RULE

Hang up, and call the person or company back on a number you already have saved, never the number that just called you, and never a number they give you on the call.

Here is why this works better than anything else. A cloned voice, a scary story, a fake caller ID, none of it can survive you hanging up and ringing the real person. If it's really your daughter, she answers and she's fine. If it's really your bank, the number on the back of your card gets you the real bank. The scammer only has power while they control the call. The moment you start a fresh one to a number you trust, they're done.

THE NUMBER THEY GIVE YOU IS PART OF THE TRAP

Scammers will say "call us back on this official line" or send a text with a number. Never use it. Always use a number you already had, from your contacts, your bank card, or the company's real website you typed in yourself.

The Scam-Checker Prompt

Got a message and not sure? Don't guess, and don't ask the person who sent it. Paste it into a free AI and let it tell you. Copy this exactly:

PASTE THIS INTO CHATGPT OR CLAUDE

Here's a message I just received. Tell me honestly whether this looks like a scam, and walk me through exactly which parts give it away. Then tell me the safest next step, and the one thing I should absolutely not do in response.

Then paste the message in exactly as you got it, including who it's from. This works in ChatGPT or Claude, on the free plans, no payment needed. The AI will point out the red flags you might have missed, and it stays calm when you're rattled, which is exactly when scams work best.

TIP

It's free and it takes seconds, so use it any time something feels even slightly off. A surprise invoice, a "your package is held" text, a message from your bank, a too-good job offer. When in doubt, paste it in.

The Exposure Prompt

Scammers need raw material: your voice, your face, your family's names, where you work. This prompt has an AI look at what's publicly visible about you and tell you what a scammer could actually use. Copy this:

PASTE THIS INTO CHATGPT OR CLAUDE

```
Search for me online and tell me honestly what  
someone could realistically use to target me or my  
family. Focus on what's publicly visible: photos,  
any video with my voice in it, family members'  
names, where I work, anything that hints at my  
routine. Then tell me what I should take down first.  
My name is [YOUR NAME] and I live in [YOUR CITY].
```

THE ANSWER WILL BE UNCOMFORTABLE

Seeing it laid out, your voice in that video, your kids' names, your workplace, your daily routine, is a little unnerving. That's the point. That's exactly what a scammer sees, and now you get to do something about it.

What to actually do with the results

You don't need to delete your whole life. Focus on the things that give a scammer the most, and let the rest go:

Worth removing: videos where your voice is clear and easy to grab, posts that name your family members alongside you, anything that shows your regular routine or location, and old accounts you don't use anymore. Setting your main profiles to private does a lot on its own.

Not worth the stress: a photo here and there, a normal amount of being online. You can't and shouldn't erase yourself. The goal is to make yourself a harder target, not an invisible one.

The Five Scams to Know Right Now

You don't need to memorize a hundred scams. These five cover most of what's out there. For each one: how it works, and the tell that catches it.

1. The cloned-voice emergency call

How it works. A panicked call in a loved one's real voice, saying they're in trouble and need money now.

The tell. Urgency plus a money request. Ask for the safe word, or hang up and call them back. The voice can't survive that.

2. The fake boss or family member

How it works. A text or email from "your boss" or a relative asking you to buy gift cards, send a payment, or move money quietly and quickly.

The tell. An unusual request for money or gift cards, plus "don't tell anyone" or "I'm in a meeting, just do it." Verify on a channel you trust.

3. The AI-written bank phishing email

How it works. A perfect-looking email from "your bank" about a problem with your account, with a link to "fix" it.

The tell. It wants you to click a link or log in right now. Don't. Go to your bank the way you normally do, or call the number on your card.

4. The deepfaked celebrity or expert

How it works. A video of a famous person or doctor promoting an investment, crypto, or a miracle health product. The face and voice are faked.

The tell. A public figure personally promising you easy money or a cure. Real ones don't DM you deals. If it's selling something, assume it's fake.

5. The bot romance or friendship

How it works. A warm, attentive new online friend or love interest who, over time, needs money for an emergency, travel, or an "investment."

The tell. They never video call or meet in person, and eventually money comes up. Real connections don't need your bank details.

How to Check If Something Is AI

Let's be honest up front: there is no tool that reliably catches AI fakes every time. The technology to make them is ahead of the technology to detect them. So treat these as helpful extra checks, not a guarantee.

Ask the Gemini app

You can upload an image, video, or audio clip into the free Gemini app and ask if it was made with AI. It's best at spotting content made by Google's own AI tools (they leave a hidden watermark), so it will catch some fakes and miss others.

Check the file at contentcredentials.org/verify

Some photos and videos carry "Content Credentials," a kind of digital label showing how they were made. Upload a file at contentcredentials.org/verify and it'll show that label if there is one. No label doesn't prove anything either way, but a label can help.

THE REAL DEFENCE IS THE HABIT, NOT THE TOOL

Neither check catches everything, so don't rely on them. The thing that actually keeps you safe is the habit: if a message or call makes you furious, scared, or is asking for money, that is the exact moment to stop and verify another way, with the safe word or a callback. Strong emotion and urgency are the scam. Slow down and the scam falls apart.

The One-Page Family Setup Checklist

Screenshot this page and send it to your family. The whole setup, in order.

The setup (about 4 minutes)	Done?
Pick a family safe word nobody could guess	☐
Send the group text to your trusted people	☐
Agree everyone can ask for the word, even if the caller gets upset	☐
Save the callback rule: hang up, call back on a number you already have	☐
Save the scam-checker prompt somewhere easy to reach	☐
Run the exposure prompt on yourself, take down the worst items	☐
Set your main social profiles to private	☐
Send this guide to the family member most likely to be targeted	☐

THE ONE RULE THAT COVERS ALMOST EVERYTHING

If a call or message is scary, urgent, and about money, stop. Ask for the safe word or call back on a saved number. That single habit beats the vast majority of these scams, no matter how real they look or sound.

Your Action Plan Tonight

Don't file this away to do later. It genuinely takes a few minutes. Do it tonight.

DO THESE FOUR THINGS

1. Pick your family safe word right now. 2. Send the group text to your trusted people. 3. Run the exposure prompt on yourself and take down the worst one or two things. 4. Send this guide to the one person in your family most likely to fall for a scam. That last one might be the most important thing you do all week.

That's it. Four minutes of setup against a very sophisticated attack, and the four minutes win. You don't have to be scared of this. You just have to be set up for it. Now you are.

Want More AI Tips Like This?

I post daily AI content, tool breakdowns, and simple guides that actually help you and your family stay ahead. Follow me for the latest.

@MavGPT

TikTok | Instagram | Facebook

Four minutes tonight beats a perfect fake tomorrow.