

by Erick / The AI Guy...

THE AI VOICE SCAM SPOTTER

checklist

17 actions for the day a familiar voice asks for money: set up now, use on the call, and follow if it already happened. Tick them off.

print it, or screenshot it...

KEEP THIS ON THE *fridge*

THE 4 MOVES

1 A familiar voice

2 An emergency

3 Secrecy

4 Payment you cannot reverse

Spot any one and it is time to hang up.

THE 3 CHECKS

- ☐ **Hang up** and call back on the number saved in your phone.
- ☐ **Ask for the family code word.** No word? Hang up.
- ☐ **Watch for pressure:** urgency, secrecy, gift cards, crypto, wire transfer.

STILL NOT SURE?

Slow down. Ask a question only the real person would know. Call another family member, even if told to keep it secret.

ALREADY HAPPENED?

Do not blame anyone. Call the bank or the company you paid with, then report it at reportfraud.ftc.gov

Do not write your code word on this page.

how the call works...

THE 4 MOVES OF A *fake call*

1

A familiar voice.

It sounds just like your loved one. A short audio clip, maybe from something posted online, is enough to clone a voice.

2

An emergency.

A car wreck, an arrest. You are told it is urgent and you are the only one who can help.

3

Secrecy.

"Do not tell anyone." The scammer does not want you talking to family and realizing it is a scam.

4

A payment you cannot reverse.

Wire transfer, crypto, a payment app, or gift card numbers read over the phone.

*Spot any one of them and it is **time to hang up.***

How to use this checklist

Part 1: do it once, today. **Part 2:** use it on the call, in the order a call unfolds. **Part 3:** only if it already happened.

PART 1 OF 3

SET IT UP *today*

CODE WORD

1 Pick one family code word, in person.

Done when: everyone who will use it has heard the word said out loud, face to face, and it is not typed into any post or comment.



SHARE IT

2 Tell the grandparents and the teens.

Done when: each of them can say the word back to you without looking at anything.



PRACTICE

3 Practice it once.

Done when: one of you has played the caller, asked for the word, and the other answered correctly.



CALL-BACK NUMBERS

4 Save the numbers you would call back.

Done when: your parents, grandparents, kids and siblings are in your phone contacts, so you can call them from there, not from a call log.

PART 1 OF 3

TRIM, THEN *share it*

VOICE ONLINE

5 Make your social accounts private.

Done when: each account you use shows as private, and your followers are people you know.



VOICE ONLINE

6 Cut down your public voice clips.

Done when: you have scrolled your public videos and removed or hidden the ones that do not need to be public.



SHARE IT

7 Send this checklist to the family group chat.

Done when: the people you named in step 2 have the PDF on their own phones.

Why this step

A scammer needs only a short audio clip of someone's voice, and it can come from content posted online. The FBI says to limit online content of your image and voice, make accounts private, and limit followers to people you know.

PART 2 OF 3

ON THE *call*

LISTEN

8 Name the moves as you hear them.

Done when: you can say which of the 4 moves you hear. One is enough to stop.



LISTEN • CHECK 3

9 Watch for the pressure signs.

Done when: you have checked for urgency, secrecy, and a request for gift cards, crypto or a wire transfer. Any one means verify first.



ASK • CHECK 2

10 Ask for the family code word.

Done when: the caller has said the exact word, or you have hung up because they could not.



ASK • STILL NOT SURE

11 Ask a question only the real person would know.

Done when: you asked one, like "Where did you spend Thanksgiving last year?", and a stranger could not find the answer on their social media.

PART 2 OF 3

HANG UP AND *verify*

**HANG UP • CHECK 1**

12 Hang up, or say you will call right back.

Done when: the call is over and no money, card numbers or PINs went to the caller.

**CALL BACK • CHECK 1**

13 Call back on the number saved in your phone.

Done when: you reached the real person on a number you dialed yourself, not the one that just called, and they told you what is going on.

**CALL FAMILY**

14 Call another family member, even if told to keep it secret.

Done when: a second relative or friend has confirmed where your person is and whether the story is true.

Do not trust the voice

The FTC says not to trust the voice on the line, even if it sounds like your family member. The FBI adds: listen closely to tone and word choice.

PART 3 OF 3

ALREADY *happened?***MONEY**

15 Call the bank or the company you paid with, right away.

Done when: you told them a scammer tricked you and asked for a reversal. That is your bank, payment app, wire company, gift card issuer, or crypto exchange or ATM operator.

**REPORT**

16 Report it at reportfraud.ftc.gov.

Done when: you submitted a report. The FBI also takes reports at ic3.gov.

**FAMILY**

17 Tell your family. No blame.

Done when: the person whose voice was copied knows, and nobody was blamed. These calls fool caring people.

Sources

1. [FTC: Scammers use AI to enhance their family emergency schemes](#)
2. [FTC: Scammers use fake emergencies to steal your money](#)
3. [FTC: What to do if you were scammed](#)
4. [FBI IC3 PSA I-120324-PSA: Criminals use generative AI for financial fraud](#)

next step...

PICK YOUR CODE WORD

tonight.

At dinner, say it out loud, practice it once, and send this checklist to your family group chat.

WHERE TO *find me*

SKOOL COMMUNITY

Join the Momentum AI community on Skool

Step-by-step AI systems and real builds you can follow.

skool.com/momentum-ai/about

INSTAGRAM

@erick.killmonger

New carousels and guides like this one.

instagram.com/erick.killmonger

NEWSLETTER

Two Steps Ahead

AI news, useful tools, and security stories worth your time.

momentum-ai.beehiiv.com/subscribe

STAN STORE

All my links

stan.store/Momentum_AI