

Verifying What's Real in 2026



AI can clone a voice from three seconds of audio and a face from one good photo. This guide won't stop that, but it will stop you from wiring money to it.

Est time:
90 sec

Skill level:
All

Tools needed:
A lukewarm IQ

Inspect each part of an interaction before trusting it

Every digital interaction consists of six parts. 4 come standard. 2 are provided by the user (you). Lay them out on a flat surface, away from small children and wire transfers.



A: A familiar face



Standard on every video call, but increasingly so are fake ones. Both look identical at first glance.

B: A familiar voice



3 seconds of audio is enough material to clone a voice. Tone and cadence are no longer proof of identity.

C: A high-stakes request



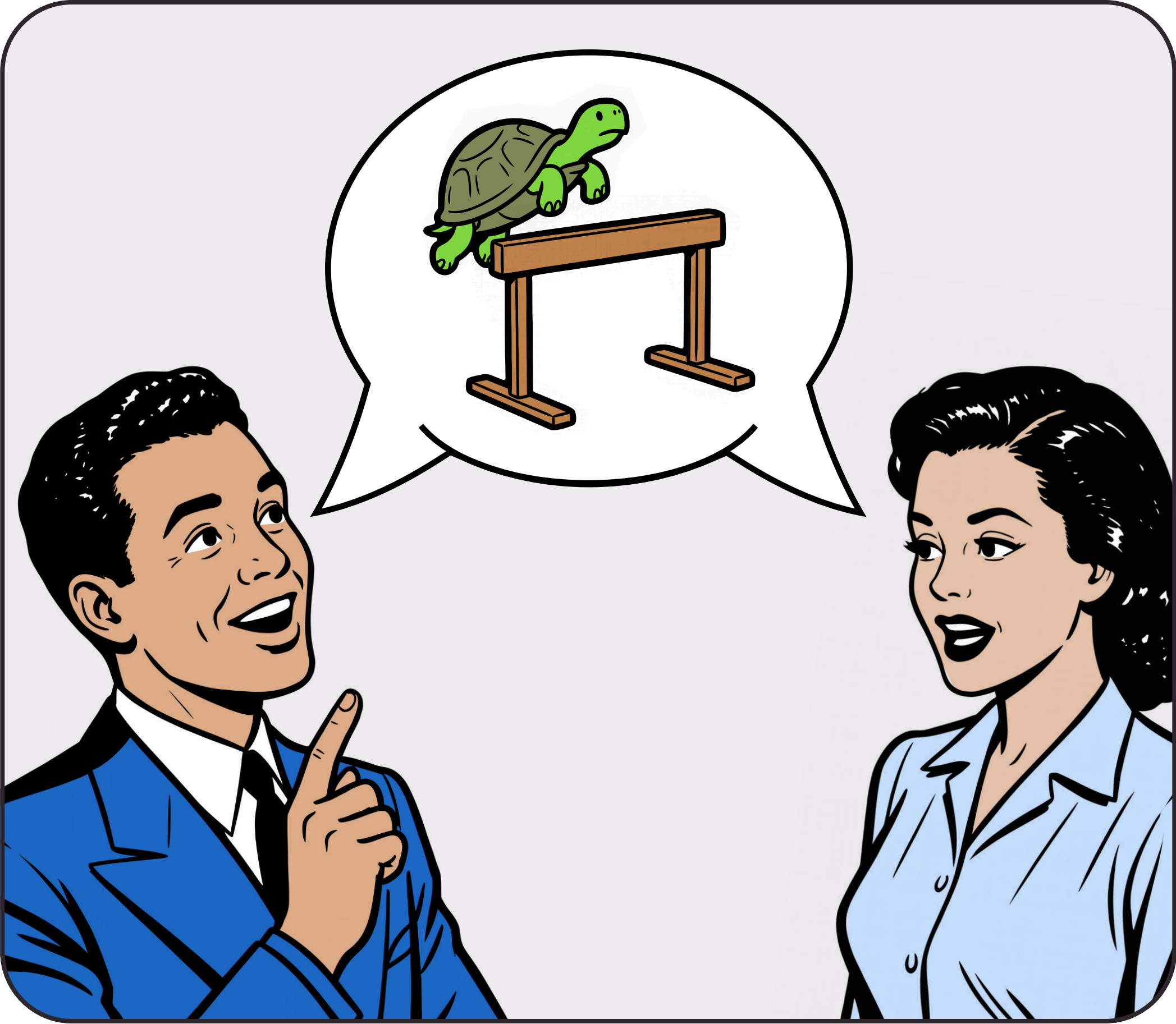
Comes with almost every scam, at no extra cost. Legitimate requests can almost always wait for verification.

D: A known contact number



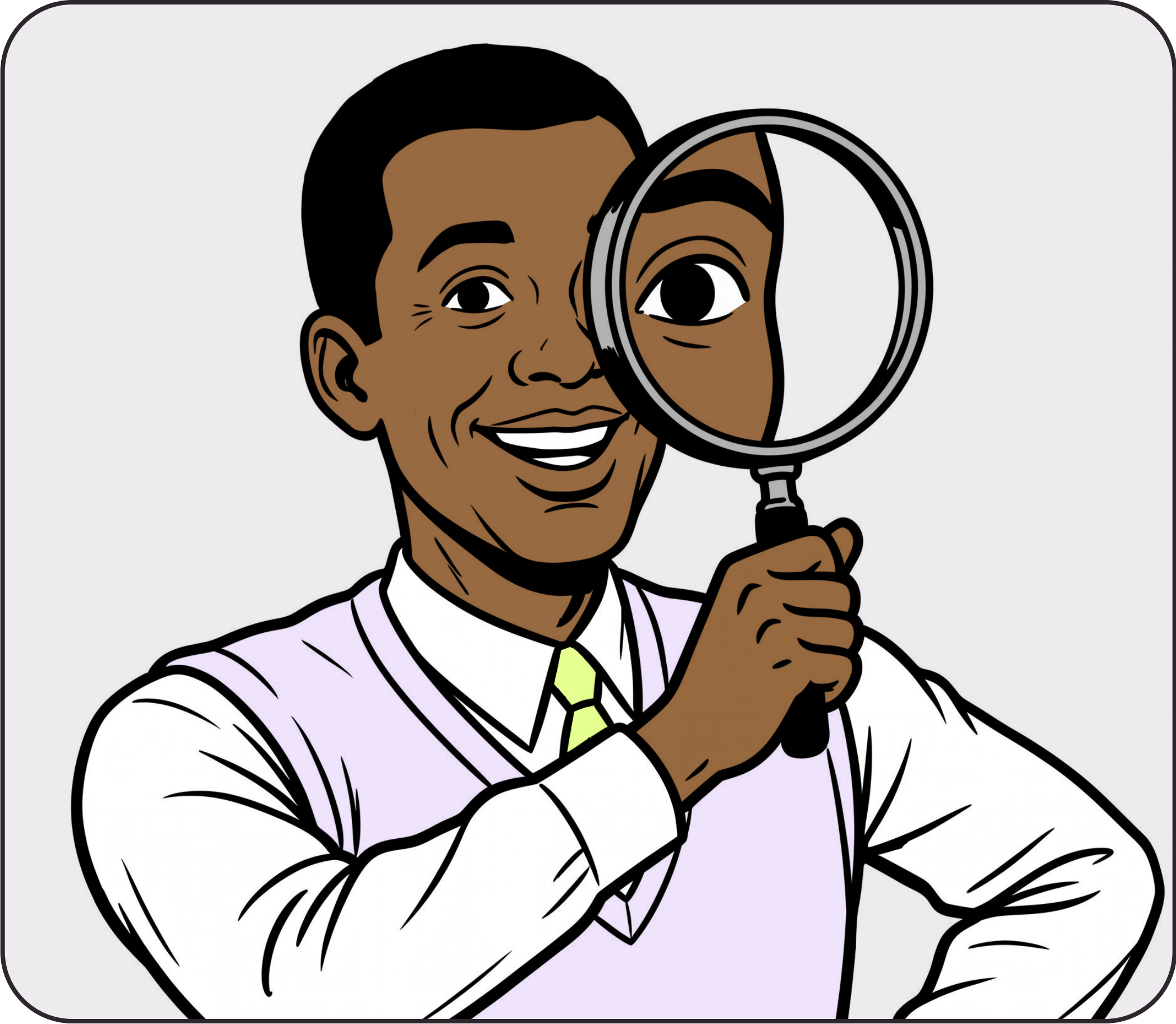
Looks trustworthy. Might even be the “right number.” But caller ID doesn't check ID. Anyone can make it say what they want.

E: A shared code word (not included)



Pick something you'd actually remember and an attacker would never guess. Think “**Green Turtle Hurdle**” not "password123.”

F: A healthy dose of suspicion (not included)



Supplied by you and required for assembly. No warranty covers a kit assembled without it.

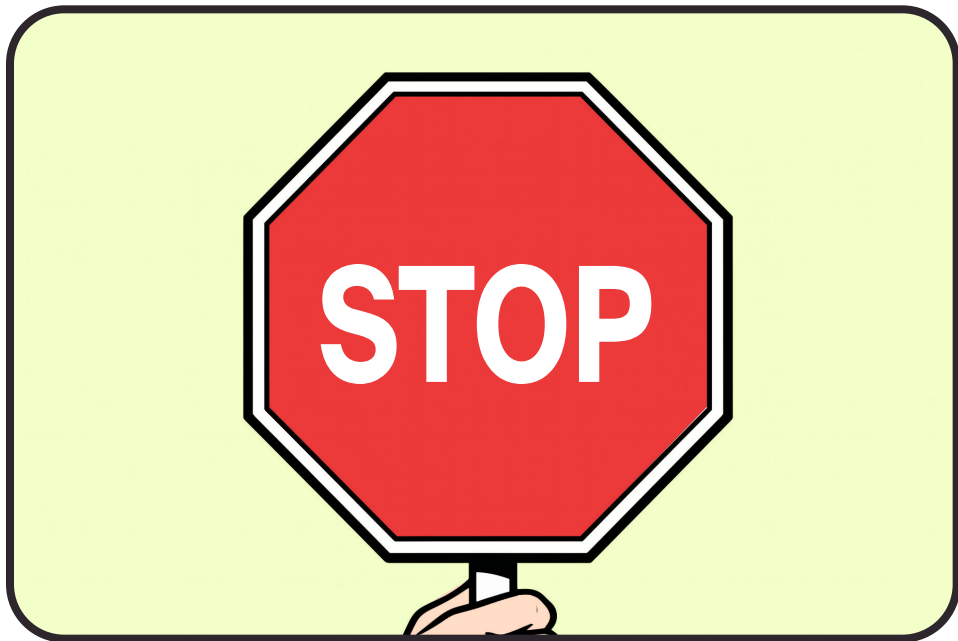
NOTE

The manufacturer cannot guarantee the authenticity of any face, voice, or written message received over email, phone, or video call. Parts A and B are the easiest to counterfeit convincingly. Proceed to assembly.

How to assemble a proper reaction

Follow steps in order. No skipping. Verification only holds if every step before it was completed.

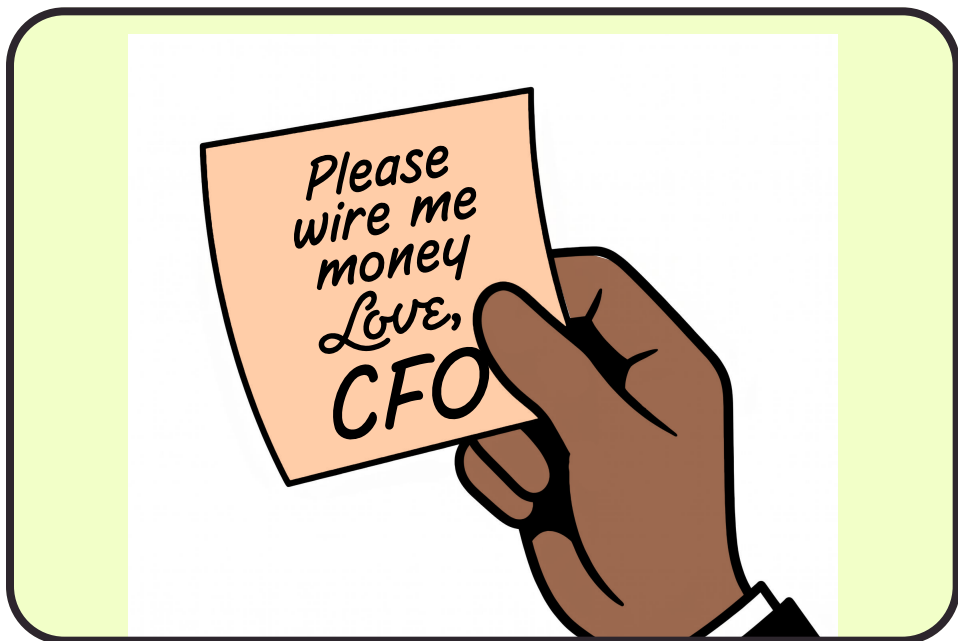
1



Pause

Stop before you act. No reply, click, transfer, or approval happens in the next sixty seconds. Urgency is a design feature of the attack, not a reason to skip this step.

2



Check the channel

Notice how the message actually arrived. If your CFO has never once texted you and is suddenly texting you about wire transfers, that's a huge red flag.

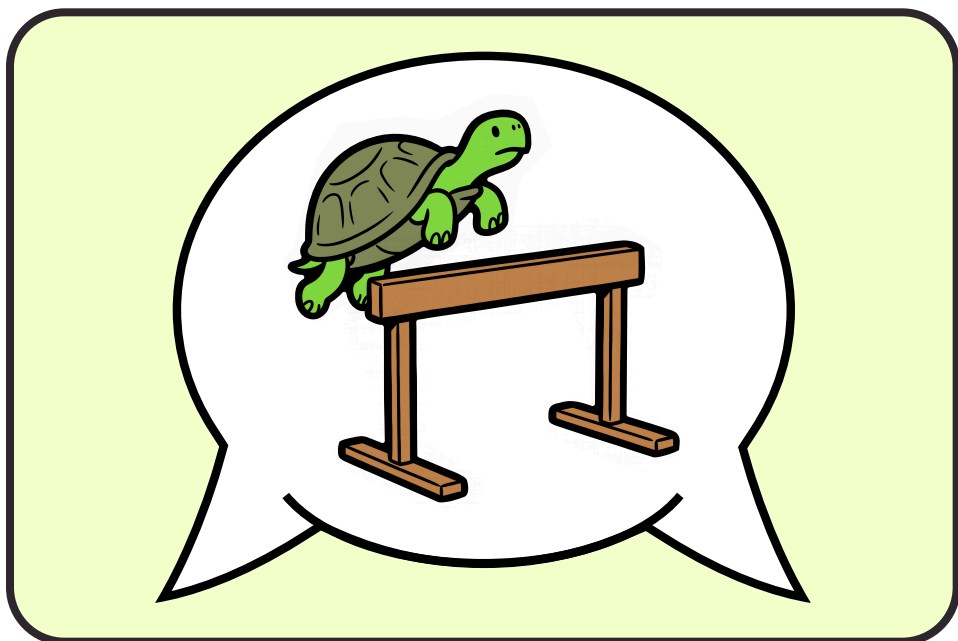
3



Call back on a known number

Hang up. Dial the number you already had saved, not one provided in the message itself. This one act defeats most spoofed numbers and cloned voices.

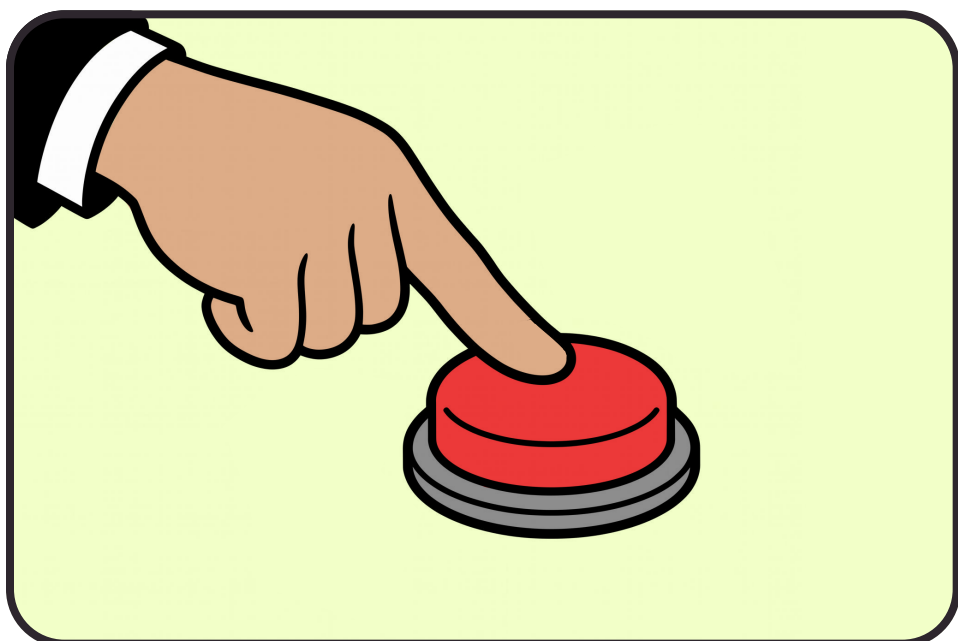
4



Confirm the shared code word

Ask for the word or phrase your team agreed on in advance. If they can't produce it, the part does not fit. Stop assembly.

5



Escalate

Still not sure? Loop in security before you act, not after. A false alarm is better than a missed attack.

CHECK YOUR WORK

Genuine



Pressure-tested. Held.

Synthetic



Pressure-tested. Didn't hold.

Troubleshooting a failed assembly

Common defects reported during assembly, and how to fix each one. If your issue isn't listed below, assume the worst and go back to Step 1 of assembly. You can never be too cautious when there's so much on the line.



SYMPTOM

Manufactured urgency: "There's no time to verify. Act now."



DEFECT

This is an attack feature, not a time constraint. Genuine emergencies still survive a callback. **Return to Step 1.**

Video calls freeze, stutter, or glitch at oddly convenient moments.



Compression artifacts are common when a real-time face swap struggles to keep up. **Ask them to turn sideways, then return to Step 1.**

The writing style feels slightly (but not exactly) off.



Trust that feeling. Verify somewhere else entirely. Verify out of band before responding. **Do not reply in the same thread.**

They refuse to use your callback number or code word.



Incompatible part. A genuine request has never once been damaged by verification. **Skip to Step 5. Escalate immediately.**

RULE OF THUMB

Any defect found



Return to Step 1

The fine print, mercifully short

This verification process carries no expiration date and may be reapplied as many times as needed, including multiple times with the same attack, on the same day. Skipping a step voids the warranty. No coverage is provided for funds wired, credentials shared, or access granted before Step 5.

COVERED

- Requests verified through Steps 1–5
- Calls placed back on a known number or secondary channel
- Actions confirmed with a code word
- Anything escalated before acting
- Your reputation as *"the careful one"*

NOT COVERED

- Requests acted on under time pressure
- Numbers provided by the requester
- Verification skipped "just this once"
- Anything approved after the fact
- *Regret*



AFTER YOU FINISH ASSEMBLY

Final inspection before you trust anyone again

You read this manual. Statistically, you’re already ahead of most people.

Your next step is finding out whether your actual setup would've survived contact with a deepfake CFO.

See how Doppel helps your team catch what this guide can't: the impersonation attempts that don't wait for you to double-check.

Request a demo