CyberGuardLab

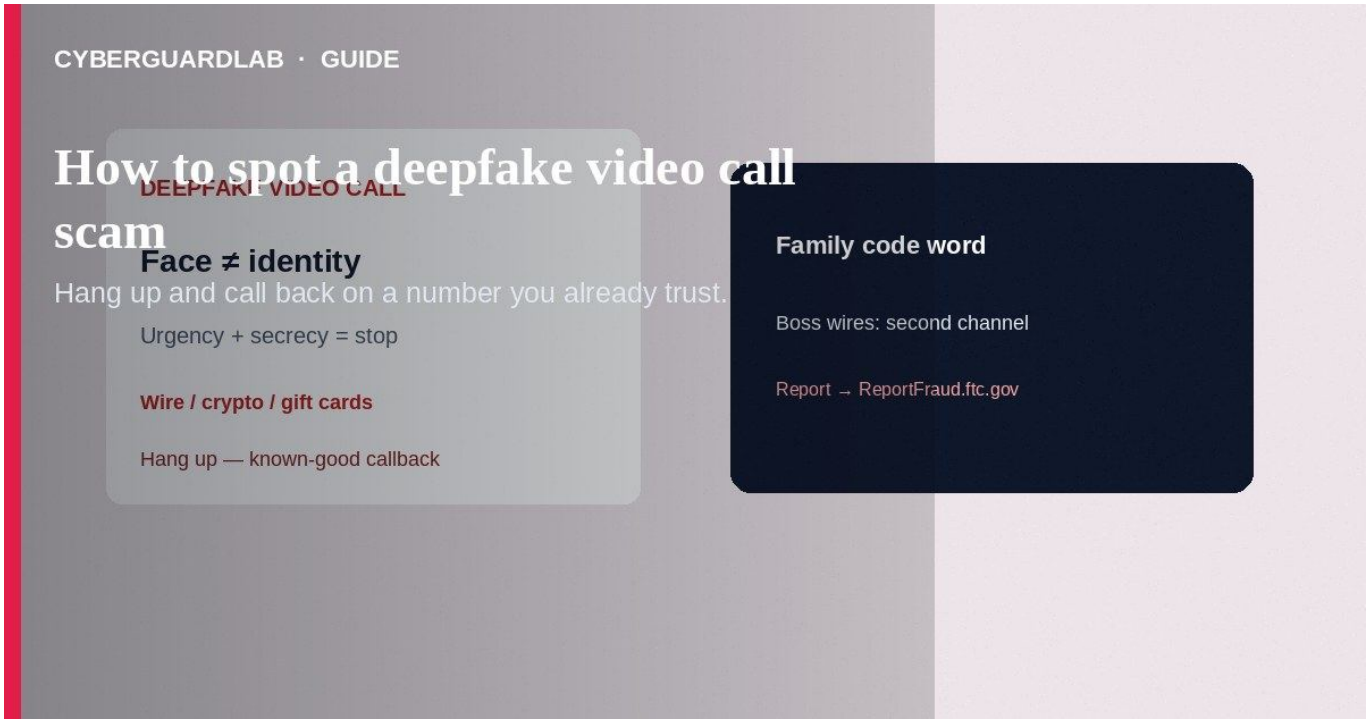
Household antivirus, explained

cyberguardlab.com

How to spot a deepfake video call scam

https://cyberguardlab.com/blog/deepfake-video-call-scam

Independent US household comparison site. Not the vendor. Paid links below may earn a commission. Confirm first-year price, renewal, device limit, and refund terms at checkout.



A deepfake video call scam is when someone uses AI-altered or AI-generated video (and often cloned audio) so a call looks and sounds like a relative, boss, or official-then pressures you to send money, gift cards, crypto, or credentials. The FTC warns that scammers already use AI voice cloning in family-emergency schemes: a short public audio clip can be enough to sound like someone you love. Video deepfakes raise the same rule: do not trust the face or voice alone-verify on a channel you already know is real. This guide covers live/recorded deepfake video-call pressure. It is related to grandparent emergency money scams and tech-support phone scripts, but the focus here is synthetic video/voice on the call itself.

How these scams usually work

* Family emergency - "I'm in jail / in a crash / stuck abroad-send money now, and don't tell Mom/Dad." FTC: cloned voices make this more convincing; the fix is still an independent callback.
* Boss / wire request - A "CEO" or coworker on a video meeting asks for an urgent transfer or gift cards. Face and voice are

not proof of identity.
* Tech support or bank "secure video" - Someone insists you must share screens, install remote tools, or read codes during a video session (overlaps with classic phone tech-support scams).
* Hard-to-reverse pay rails - Wire, crypto, gift-card numbers/PINs, or payment apps-FTC flags these payment methods as common scam pressure.
CISA's social-engineering guidance still applies: attackers use urgency, authority, and fear; verify identity with the real organization using contact details you already trust-not numbers or links from the suspicious call.

Red flags on a video call

Cue | What to do

Money, codes, or remote access demanded "right now" | End the call. Real emergencies can wait for a second channel check.

"Don't tell anyone else in the family / company" | Tell someone. Secrecy protects the scammer.

Odd lighting, frozen mouth lipsync, unnatural blinking, metallic/echo voice, delayed reactions | Treat as suspicious-but absence of glitches does not prove the call is real.

Payment only by wire, crypto, gift cards, or payment app | Walk away; those rails are hard to reverse (FTC).

They refuse a family code word or a callback to a known number | Hang up. That refusal is the answer.

What to do (buy-nothing steps)

* Hang up / leave the meeting - Do not send money or read one-time codes during the call.
* Call back on a number you already have - FTC guidance for cloned-voice emergencies: contact the person who supposedly called you using a phone number you know is theirs; if you cannot reach them, try another family member or

friend.
* Use a family/work code phrase - Agree ahead of time on a word only your household or team knows. Ask for it before any money talk.
* For "boss" wires - Confirm via a second channel (known office phone, in-person, or established chat)-never only via the video session that made the ask.
* If you already paid - Contact your bank, wire service, payment app, or gift-card issuer immediately and ask about reversal/refund options; then report at ReportFraud.ftc.gov (FTC what-to-do steps).
* If you shared passwords or remote access - Change passwords, turn on multi-factor authentication, and run a malware scan. Microsoft Defender is enough for many Windows PCs; paid suites are optional.

FAQ

Can a video call still be a deepfake if it looks perfect?

Yes. Glitches help, but polished fakes exist. Identity is proven by out-of-band contact, not by how real the picture looks.

How is this different from a normal grandparent money scam?

Same emotional script; AI voice/video makes the impersonation stronger. FTC still says: don't trust the voice-verify independently. See also grandparent emergency money scams.

Will antivirus detect a deepfake call?

Not as its main job. Antivirus helps with malware after a bad download or remote-tool install. Spotting pressure and verifying people is the primary defense.

What payment methods should make me stop immediately?

FTC repeatedly flags wires, crypto, gift cards, and similar hard-to-reverse methods when someone pressures you in an emergency story.

Where should I report this?

ReportFraud.ftc.gov. Also tell your bank/app and local law enforcement if money moved.

If you still want a paid suite

Spotting a deepfake video call scam does not require paid antivirus. If you still want multi-device paid protection, use only these on-site links: Norton (paid link), Bitdefender (paid link), TotalAV (paid link), McAfee (paid link), Avast (paid link).

Extra caution

A familiar face on a screen is not a payment authorization. End the call, use a known-good number, and never buy gift cards or send crypto because a video stranger (or "relative") told you to.

Sources

* FTC: Scammers use AI to enhance their family emergency schemes
* FTC: Fighting back against harmful voice cloning
* FTC: What to do if you were scammed
* CISA: Avoiding social engineering and phishing attacks
* ReportFraud.ftc.gov

Also read

* Grandparent emergency money scam
* Tech support scam phone call
* Wire transfer / romance advance-fee scam
* Is Microsoft Defender enough?
* Gift card payment scams
* Clicked a phishing link: first hour