

DEEPFAKE & VOICE-CLONING FRAUD.



A voice or face is no longer proof of identity — **a few seconds of public audio or video is enough to generate a convincing clone, so verification has to move to a channel synthetic media can't reach.**

- VOICE CLONING
- REAL-TIME FACE SWAP
- SYNTHETIC MEDIA DETECTION
- CALLBACK VERIFICATION

01 THE MECHANISM

Voice & Video Cloning

A short public sample of someone's voice or face is enough to train a model that **generates new, convincing audio or video in real time.**

Real-Time Delivery

Cloned audio and video can be streamed live into a phone call or video meeting, not just pre-recorded, so **the target is interacting with what feels like a live conversation.**

Callback Verification

Confirming identity through a pre-established, separate channel — not the call or video itself — is **what actually catches a synthetic impersonation.**

02 THE FLOW

The Verified Call

VERIFIED

1

An urgent call or video request appears to come from an executive or family member, asking for money or credentials.

2

The recipient hangs up and calls back using a previously known, independently verified number rather than continuing the conversation.

3

Because the callback uses a channel the attacker doesn't control, **a synthetic voice or video cannot follow them there.**

The Unverified Call

DEFRAUDED

1

An urgent call or video request appears to come from an executive or family member, asking for money or credentials.

2

The recipient trusts the voice or face they hear and see, and acts within the same call under time pressure.

3

Funds or credentials are handed over in real time, and **the fraud isn't discovered until the real person is reached hours or days later.**

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Callback Verification Protocol	Requires confirming any unusual request through a separate, pre-established channel before acting, regardless of how convincing the call sounds.
Synthetic Media Detection Tools	Analyzes audio and video streams for artifacts, latency patterns, and inconsistencies characteristic of generated media.
Executive & High-Risk Voice Protection	Limits how much clean public audio or video of high-value targets exists to train a convincing clone against.
Real-Time Deepfake Awareness	Trains staff that live, convincing audio or video is no longer proof of identity, updating decades-old "voice on the phone" trust assumptions.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Trusting a Familiar Voice or Face	No	The exact assumption deepfake fraud is designed to exploit; familiarity is no longer evidence of authenticity.
Caller ID or Meeting Invite Verification	No	Confirms only the call's origin metadata, which can be spoofed independently of the audio or video content.
Post-Incident Media Forensics	No	Confirms fraud after the money or data is already gone, too late to prevent the loss.
Awareness Training Without a Verification Process	No	Raises suspicion but gives no actual mechanism to resolve it in the moment.
Mandatory Callback Verification + Synthetic Media Detection	Yes	Removes the attacker's control of the channel and adds a technical check before any high-risk action.

DEEPPAKE & VOICE-CLONING FRAUD.

CLONE · VERIFY · INTERRUPT

05 PROGRAM OPERATIONS

Detection tools alone can't keep pace with generation quality.

Synthetic media models improve faster than any single detection technique, so process controls matter more than software.

The verification channel matters more than the verification question.

A callback to a number the attacker also controls provides no real protection.

High-risk targets need less public audio and video, not more detection.

Executives and public figures often have the most training data available to clone against.

Time pressure is the actual attack, not the voice itself.

Nearly every deepfake fraud scenario depends on preventing the target from pausing to verify.

06 CONTROL MAPPING

FBI IC3 SYNTHETIC MEDIA ADVISORY

Federal guidance on identifying and reporting AI-generated voice and video fraud.

NIST AI RMF

Risk management guidance that includes synthetic content and AI-generated media risks.

C2PA

An emerging content-authentication standard for cryptographically labeling the origin of media.

FFIEC BANKING GUIDANCE

Wire transfer and payment verification expectations applicable to voice-authorized transactions.

07 WHAT THIS DOES NOT SOLVE

Text-Based Impersonation

Callback verification and media detection do nothing for a **written email or chat impersonation with no voice or video involved.**

Legitimate Insider Fraud

An authorized employee misusing real access **isn't caught by controls built to detect external impersonation.**

Detection Tool False Negatives

No current synthetic media detector catches every generated sample, **especially as generation quality improves.**

Public Figure Reputation Damage

Even a debunked deepfake can **cause real reputational or market harm before it's proven fake.**

08 MYTHS VS. REALITY

MYTH "You can tell a deepfake by how it looks or sounds."	REALITY Real-time voice and video cloning quality has advanced past the point where casual observation reliably catches it.
MYTH "This only targets celebrities and executives."	REALITY Family-emergency voice-cloning scams target ordinary people using audio scraped from social media.
MYTH "A video call is safer than a phone call because you can see the person."	REALITY Real-time face-swap technology can convincingly clone video during a live call, not just audio.
MYTH "If detection software says it's real, it's safe to proceed."	REALITY No detection tool has a perfect track record; it should inform a decision, not replace verification.
MYTH "This is a future threat, not a current one."	REALITY Voice-cloning fraud against businesses and families is already an active, documented technique, not a theoretical risk.

09 SPEAK THE PROGRAM — KEY TERMS

VOICE CLONING

Using a short audio sample to **train a model that generates new speech in the same voice.**

DEEPPAKE

Synthetic audio, image, or video generated or altered by AI to **convincingly depict something that didn't happen.**

REAL-TIME FACE SWAP

Live video manipulation that **replaces a speaker's face with a cloned identity** during an active call or stream.

CALLBACK VERIFICATION

Confirming a request by contacting the purported requester through an **independently verified, previously established channel.**

CONTENT PROVENANCE

Cryptographic or metadata-based evidence of **where a piece of media originated and whether it's been altered.**

SYNTHETIC MEDIA DETECTION

Technical analysis of audio or video for **artifacts and inconsistencies indicating AI generation.**