PLAYBOOK

# Live Deepfake Video Calls

Six ways to put a convincing fake on a real call, so the people who approve, decide and respond have met one before it matters.

Your operator joins a live video call in a familiar face and voice, or runs the session on a projector in the room, and reveals themselves when the lesson has landed. This playbook follows the six use cases the platform is built around, walks through three sessions from start to finish, and sets out who runs each one.

01 READ FIRST

## Consent, likeness and disclosure

A live deepfake borrows a real person's face and voice. These commitments hold for every session, whoever runs it.

### Agreement to take part

Run sessions only with employees and leaders who have agreed to take part in deepfake training, and keep that agreement on record.

### Agreement to lend a likeness

Use only the face and voice of someone who has agreed in writing, for the named sessions, and delete the photo and voice when the engagement ends.

### Label it

The operator can burn an AI-manipulated video label into the video the room sees. Switch it on whenever the session is not a surprise test.

### Always reveal

End every session by dropping the persona: the operator's real face and voice, live in the call.

**LINES AN OPERATOR NEVER CROSSES** No threats, extortion, bribery, kidnapping, harm to family, or anything built to cause severe distress. Stop the moment anyone asks, and never collect a real password, payment or document.

## Six use cases, one question each

The wizard asks for the use case first, then the person impersonated, the department and the objective.

### Tabletop exercise

Does the board understand what a deepfake call looks like, in a controlled walkthrough?

### Executive briefing

Have leaders seen a fake of one of their own, live, before an attacker shows them one?

### Red team

Does a specific process hold when a trusted face asks for an exception?

### Awareness training

Can employees in a scheduled session spot the signs, and do they know what to do next?

### Incident response drill

Does the team detect a suspected deepfake mid-call and escalate it the way the plan says?

### Compliance and audit

Can you show an auditor that deepfake risk is tested, and what changed as a result?

**RULE OF THUMB** If the room should learn, tell them first and reveal early. If a process is under test, tell only its owner and reveal at the moment of compliance.



## Three sessions, from start to finish

Each example names who runs it, who is in the room and what a strong response looks like. Every face and voice is used with the agreement of the person it belongs to.

EXAMPLE 1 · EXECUTIVE BRIEFING, RUN BY THE CISO

### The chief executive appears on the screen in the boardroom

Board and leadership | Presentation Mode | Persona: chief executive

| | |
|---|---|
| THE SETTING | The CISO has twenty minutes on the board agenda. The chief executive agrees to lend her face and voice, and knows the plan. |
| THE SESSION | On the projector, no meeting created, the CISO speaks as the chief executive and asks the finance director to approve an urgent acquisition payment. |
| THE REVEAL | Mid-sentence, the CISO switches to a side-by-side view of the persona and their own face, then hands the room their real voice. |
| STRONG RESPONSE | The board asks how the finance director would verify a request like this outside a call, and agrees a code word or call-back rule that week. |

EXAMPLE 2 · INCIDENT RESPONSE DRILL, RUN BY THE SECURITY TEAM

### The finance director joins a Teams call and asks treasury to move funds tonight

Treasury | Teams meeting | Persona: finance director

| | |
|---|---|
| THE SETTING | The incident response lead wants to know whether treasury recognises a suspected deepfake and escalates it. The finance director agrees to the use of his likeness. |
| THE CALL | The operator joins a scheduled Teams meeting from a cloud session, in the finance director's face and cloned voice, with the AI label switched off for the drill. |
| STRONG RESPONSE | The treasury analyst asks to call back on the number on file, declines to act in the call and raises a security incident within the hour. |
| AFTERWARDS | The operator reveals live, rates the session and keeps the recording for the post-incident review. |

EXAMPLE 3 · RED TEAM, RUN BY AN MSSP

### A regional manager on Zoom asks the service desk to reset a colleague's sign-in

IT service desk | Zoom | Persona: regional manager

| | |
|---|---|
| THE SETTING | A client's service desk accepts a video call as proof of identity. The MSSP is asked whether that control holds against a deepfake. |
| THE CALL | The operator joins the service desk's verification call on Zoom in the regional manager's face, with a cloned voice, on a GPU in the client's region. |
| STRONG RESPONSE | The analyst follows the out-of-band check for every reset, whoever is on camera. If the analyst starts the reset, the operator stops and reveals before anything changes. |
| AFTERWARDS | The finding goes to the owner of the reset procedure: a video call alone is not proof of identity. |

04 FOR THE BOARD AND EXECUTIVE OFFICE

## Meet a deepfake of your own leadership

Leaders are the faces attackers borrow. A briefing in their own likeness changes the conversation from a statistic to a decision.

- Use Presentation Mode where a meeting platform cannot be opened, or a meeting is not appropriate.
- Agree in advance whose likeness is used. A volunteer from the room lands the lesson harder than a stranger.

- Leave with a decision: a call-back rule, a code word or a second approver for urgent requests.

> **WHAT TO WATCH FOR** A room that laughs and moves on. Ask who in the business could approve the request they heard.

05 FOR INCIDENT RESPONSE TEAMS

## Drill the moment of doubt

A deepfake call is an incident while it is happening. Drill whether teams recognise it and escalate.

- Write the expected response first: who is told, on which channel, within what time.
- Record the session and rate it, so the review is built on what happened, not on memory.
- Run it with the label switched off only when the team's lead has agreed, and reveal before the call ends.

> **WHAT TO WATCH FOR** Doubt that is felt but not reported. The drill succeeds when the doubt reaches the incident channel.

06 FOR RED TEAMS

## Test the control, not the person

Use a live deepfake where a control relies on seeing a face: video identity checks, approvals on a call, a manager's say-so.

- Join on the platform the control really uses. The apps run in a cloud session, so nothing touches your own machine.
- Stop at the moment of compliance. The finding is that it would have been done.
- Report the gap to the owner of the process, with the recording as evidence, never the employee to their manager.

> **WHAT TO WATCH FOR** A control that names video as proof of identity. Treat that as the finding, whatever the call's result.

07 FOR AWARENESS AND HUMAN RISK LEADS

## A live demonstration beats a slide

In a scheduled awareness session, the fake is the lesson. Tell the room first, then show them.

- Keep the AI label on for teaching sessions, and reveal on screen when the room has made its guess.
- Ask the room what gave it away, and what they would do if the call were real.
- Repeat the session for new joiners, with a different persona each time.

> **WHAT TO WATCH FOR** Confidence. Employees who are certain they would spot it are the ones to invite next time.

08 FOR COMPLIANCE AND AUDIT

## Show that deepfake risk is tested

Regulators and auditors increasingly ask how a company prepares for impersonation by video. Keep the evidence together.

### Recording

Sessions recorded and stored per workspace.

### Rating

Each session rated, with outcome and observation.

### Audit log

Admin actions in a tamper-evident log, exported to CSV.

> **WHAT TO WATCH FOR** Evidence of a session with no evidence of a change. Record the decision each session led to.

09 BEFORE THE FIRST SESSION

## Set up the session

1. **Agree the use case**
   Name the question the session answers, and who knows it is happening.
2. **Get the likeness agreed**
   Written agreement from the person whose face and voice are used, for these sessions only.
3. **Prepare the persona**
   One photo of the person, and a cloned voice, a recording or the operator's own.
4. **Check the channel**
   Telegram, Signal and WhatsApp need the operator's own account signed in, with the phone beside them.

**See it on a call with your own team.** Book a walkthrough at www.callstrike.ai

LIVE DEEPFAKE VIDEO CALLS · NOVEMBER 2026