CALLSTRIKE
DEEPFAKE TRAINING

DATA SHEET

SECURITY AWARENESS FOR VOICE AND VIDEO

The Callstrike Platform

Consented voice phishing and deepfake simulations that teach employees to verify a familiar voice or face before they act.

Callstrike runs vishing and deepfake simulations for a company's own employees: AI voice calls at scale, live calls by your own operator in a cloned voice, and live deepfake video calls. Results show who verified and who did not, and training follows the call.

01 SIMULATIONS

Four ways to test the call employees will one day receive

AI voice phishing

A live AI caller phones employees, listens and answers, in seven languages and with an accent matched to each employee's country.

Human-in-the-loop voice phishing

Your own operator, from your security team, red team or MSSP, speaks live and the platform converts their voice into a cloned voice in real time, for high-stakes roles.

Live deepfake video calls

A real-time face swap joins a video call on ten video and messaging platforms, or runs in person in presentation mode.

Deepfake video maker

Generate a short training video in a chosen person's likeness to show employees how convincing a fake can be.

02 RUN THE PROGRAMME

From scenario to result

1 **Bring in your people**

Sync people and groups from your directory, or add them from a CSV file you review first.

2 **Write the scenario**

Start from a pre-built template or write a custom scenario in your own words, then schedule the campaign in your time zone.

3 **Read the results**

Each call's outcome is recorded as shared or refused. The dashboard breaks results down by department and gives each employee a risk score with every factor named.

4 **Follow up**

Each employee's profile keeps a timeline of their simulations, and training is built from their own call transcript.

03 SAFEGUARDS

Training, never an attack

Consent on record

A vishing campaign calls only employees with consent on record. Consent Management is part of every plan.

Stops when asked

The AI caller ends the call when an employee asks it to stop, hang up or end the call, or says the workspace's stop word.

Content policy

Every scenario is checked against a content policy before it is saved. Threats, extortion and content built to distress are refused.

Disclosure and debrief

A campaign can debrief the employee during the call and send a follow-up telling them it was a simulation.

04 FOR THE ENTERPRISE

Built to be run by security teams and their partners

Single sign-on

Configure SSO yourself through a self-service admin portal.

Audit log

A tamper-evident audit log records admin actions and exports to CSV.

Partners and MSSPs

Manage every customer workspace from one partner account, under your own branding.

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

THE CALLSTRIKE PLATFORM · NOVEMBER 2026