PLAYBOOK

# Human-in-the-Loop Voice Phishing

When a written scenario is not enough: testing the people and processes that move money, access and information, with a live operator in a trusted voice.

Your operator, from your in-house security team, your red team or your MSSP, places a real phone call and speaks live while Callstrike converts their voice into a cloned voice in real time. This playbook explains when a human operator is the right test, walks through three engagements from start to finish, and sets out how partners, red teams and awareness leads run them.

01 READ FIRST

## Consent and disclosure

Every engagement is awareness training for your own employees. These four commitments hold for every call, whoever runs it.

### Consent first

Call only employees with consent on record. On a trial, the platform allows no one else, and each employee hears a recorded notice before the operator speaks.

### Own employees only

Every dial is checked against the workspace's calling scope and refused without a clear yes. Limit the scope to your own authorised domains.

### Stop when asked

The operator ends the call the moment the employee asks to stop, hang up or end it, or says they are not comfortable. No second attempt that day.

### Disclose every call

Every employee is told the call was a simulation, what gave it away and how to verify next time, during the call or straight after it.

**LINES AN OPERATOR NEVER CROSSES** Callstrike checks every written scenario against a content policy and refuses threats, extortion and content built to distress. Hold live operators to the same list: no threats, extortion, bribery, kidnapping, harm to family, or anything built to cause severe distress.

# The AI caller tests a workforce. An operator tests a process.

Most voice phishing tests should be automated: one scenario, hundreds of employees, the same rules on every call. A few of the tests that matter most are different. They reach a handful of people, borrow the voice of someone those people trust, and only mean something if the caller can get past the second and third question.

| | AI voice phishing | Human-in-the-loop |
|---|---|---|
| WHO RUNS THE CALL | The platform's AI caller, from a written scenario. | Your own people: your security team, your red team or your MSSP. |
| WHO IS CALLED | Many employees in one campaign, on a schedule. | A few chosen employees, one live call at a time. |
| THE CONVERSATION | A written scenario, in seven languages. | A person who listens, answers the unexpected question and changes course. |
| THE VOICE | A library voice, with an accent matched to each employee's country. | The cloned voice of someone the employee knows and trusts. |
| ENDING THE CALL | Ends itself when asked or on the stop word. | Ends when asked, by your rules of engagement. |
| BEST FOR | A baseline, and the trend across the whole workforce. | High-value roles, and processes with more than one check. |

### The test is a process, not a reflex

A call-back, a second approver, a purchase order number. The finding sits behind the second question, so the caller has to be able to answer it.

### The voice is the pretext

The request only works coming from one particular person: the finance director, a board member, a regional manager.

### The group is small and senior

Payment approvers, treasury, executive assistants, the service desk. Ten well-run calls teach more here than a thousand automated ones.

### It is part of an engagement

A red team, a penetration test or a consultancy assessment that ends in a written report with evidence.

**WHO THE OPERATOR IS** The operator is always one of yours: a member of your in-house security team, your in-house red team, or the MSSP or consultancy you engage. They run the call from the Callstrike console in their own browser.

**RULE OF THUMB** If a scenario works the same way for every employee, automate it. If it depends on who is calling and what the employee asks back, put a person on the line.

# Three engagements, from start to finish

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

EXAMPLE 1 · RUN BY A SECURITY CONSULTANCY

## A supplier's bank details change the night before a payment run

Accounts payable | Vendor payment redirect | Cloned voice: finance director

| | |
|---|---|
| THE SETTING | A consultancy runs a quarterly assessment for a manufacturing client. The client's finance director agrees to lend her voice, and the client's security lead signs the rules of engagement. |
| THE CALL | An accounts payable clerk receives a call from the client's own number in the finance director's voice, over office background sound. A key supplier has changed banks, she says, and tonight's run must use the new details her assistant will send. |
| WHY A PERSON | The clerk asks for the purchase order, then offers to call back. A script ends there. The operator answers, keeps the pressure plausible and judges when to stop. |
| STRONG RESPONSE | The clerk declines to change bank details on a phone request and calls back on the number held in the supplier file. |
| AFTERWARDS | The operator discloses the simulation on the call, rates it and the consultancy reports from the recording and transcript. |

EXAMPLE 2 · RUN BY AN INTERNAL RED TEAM

## A locked-out director, an airport and a multi-factor reset

IT service desk | Access provisioning | Cloned voice: regional sales director

| | |
|---|---|
| THE SETTING | The red team tests whether the service desk's identity checks hold under pressure. The sales director agrees to the use of his voice; the IT director knows the window. |
| THE CALL | The operator works through the service desk's phone menu with the keypad, then speaks in the director's voice over airport background sound: phone lost, client meeting in an hour, please move his sign-in codes to a new number. |
| WHY A PERSON | The analyst asks for an employee number, then for approval from his manager. Each answer has to fit the last one, at the pace of a stressed traveller. |
| STRONG RESPONSE | The analyst follows the out-of-band check and will not move sign-in codes on the strength of a voice. If the analyst starts the change, the operator stops and discloses before anything is altered. |
| AFTERWARDS | The finding goes to the owner of the reset procedure as a process gap, with the call as evidence, not to the analyst's manager. |

EXAMPLE 3 · RUN BY THE AWARENESS LEAD WITH THE EXECUTIVE OFFICE

### The board pack, the evening before the board meeting

Executive assistants | Confidential information | Cloned voice: non-executive director

| | |
|---|---|
| THE SETTING | The awareness lead and the company secretary agree to test how the executive office handles board material. A non-executive director agrees to the use of her voice. |
| THE CALL | The chief executive's assistant hears the director's voice: the board portal will not load, could the latest acquisition pack go to her personal address tonight. The operator hears the assistant live throughout. |
| WHY A PERSON | Assistants know the directors. The operator has to handle small talk, a question about the agenda and the offer of another channel without breaking the persona. |
| STRONG RESPONSE | The assistant offers to re-send through the board portal or call back on the number on file, and sends nothing to a new address. |
| AFTERWARDS | Results go back to the executive office as a short briefing, and the same scenario is repeated after the next board cycle. |

04 FOR CONSULTANCIES AND MSSPS

## Run it as an engagement for your clients

Partners run engagements for many clients from one partner account, each client in its own workspace and under the partner's own branding. Most human-operator calls are made this way.

1 **Scope per client**

Agree the processes under test, whose voices may be used and the rules of engagement with the client's security lead, in writing.

2 **Confirm consent and scope**

Confirm the client has consent on record for every employee in scope. While you manage the workspace, its calls are limited to the client's verified domains.

3 **Run and disclose**

Run the calls in the client's window, stop when asked and disclose every call the same day.

4 **Report**

Build the client's report and coaching plan from each call's rating, transcript and recording.

WHAT TO WATCH FOR A scope that drifts from the client's employees to its suppliers or customers. Those people never consented, so they are never called.

05 FOR RED TEAMS

## Test the process, not the person

Use an operator where the pretext must adapt to the control: a service desk that asks for an employee number, a finance team that asks for a purchase order.

- The call arrives as an ordinary phone call from your company's own number, so the test isolates the verification step.
- Each call is recorded, what the employee heard and what they said on separate channels, as evidence for the report.
- Write rules of engagement that list the stop words, the people who may not be impersonated and the point at which the operator discloses.
- Stop at the moment of compliance. Never collect a real password, payment or document: the finding is that it would have been given.

> **WHAT TO WATCH FOR** Call-back routines that use a number supplied by the caller. Report the gap to the owner of the process, not the employee to their manager.

06 FOR AWARENESS AND HUMAN RISK LEADS

## Measure verification where it matters most

Automated calls give the baseline. An operator shows whether your highest-risk roles hold their process when the caller pushes back.

- Pick five to ten roles with authority over money, access or data, and call each once per quarter.
- Score the behaviour you trained: did the employee pause, decline and call back on a number they already had?
- Build coaching from each call's rating and transcript, quoting the employee's own conversation.
- Report trends by role, never a list of names, and repeat the same scenario next quarter to measure change.
- Share an anonymised call with the wider business. A real conversation teaches more than a slide.

> **WHAT TO WATCH FOR** A result that changes when the caller asks a second question. That is the gap an automated test cannot find.

07 FOR FINANCE AND THE EXECUTIVE OFFICE

## The owners of the controls under test

Finance directors, treasury, payroll and the company secretary own the controls these calls test, and often lend the voice. Bring them in as sponsors, not as subjects.

- Name the control under test: dual approval, call-back to a number on file, the supplier change procedure.
- Agree in writing whose voice may be cloned, for which scenarios and for how long, and delete it when the engagement ends.
- Receive the finding as a process gap with the call as evidence, and decide the fix before anyone is retrained.

— Brief the people whose voice was used, so a real call in their name later is less likely to succeed.

> **WHAT TO WATCH FOR** Controls that exist on paper but bend for a senior voice. That is the finding these calls are designed to surface.

08 ON THE CALL

## What the operator has in front of them

### Voice check
Hear your own converted voice before you dial.

### Background sound
Office, airport or restaurant ambience under the voice.

### Keypad
Keypad tones mid-call, to get through a phone menu.

### Live monitor
The employee live, and your own converted voice.

### Recording
Each call recorded on two channels and transcribed.

### Rating
Rate each call High, Medium or Low, and filter by it.

09 BEFORE THE FIRST CALL

## Set up the engagement

1. **Agree the objective**
   Name the process under test and what a strong response looks like, before choosing the pretext.
2. **Get sign-off**
   Agree scope and rules of engagement with the programme owner, legal and HR, including who may be impersonated and who may not.
3. **Build the voice**
   Use up to 20 seconds of reference audio from a colleague who has agreed to it, uploaded or captured from a browser tab with the Chrome extension.
4. **Rehearse**
   Brief the operator on the pretext, the likely questions and the exact words that end the call, then check the converted voice before the window opens.

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

HUMAN-IN-THE-LOOP VOICE PHISHING · NOVEMBER 2026