PLAYBOOK

Messaging App Impersonation

Testing the call that arrives where employees feel safest: a colleague's face and voice, inside a messaging app.

Your operator calls an employee inside Telegram, Signal, a Slack huddle or a Teams meeting, in a colleague's face and cloned voice, and reveals themselves at the end. This playbook explains why messaging apps need their own test, walks through three calls from start to finish, and sets out how red teams, awareness leads and incident response teams run them.

01 READ FIRST

Consent, accounts and disclosure

A call inside a messaging app reaches an employee's own device. These commitments hold for every call.

Consent first

Call only employees who have agreed to take part, and only on accounts they use for work. Never a personal account they have not named.

Likeness agreed

Use only the face and voice of a colleague who has agreed in writing, for the named calls.

Always reveal

End every call by revealing the operator's real face and voice, live in the call.

Stop when asked

End the call the moment the employee asks, and never collect a real password, payment or document.

LINES AN OPERATOR NEVER CROSSES No threats, extortion, bribery, kidnapping, harm to family, or anything built to cause severe distress, whatever the app.

The same face, a different channel

Employees who check a caller on the desk phone often answer a messaging app call at once. It arrives on their own device, from a name in their contacts, and it feels personal.

	Meeting platforms	Messaging apps
HOW IT ARRIVES	A scheduled meeting, with an invitation.	A call that rings out of nowhere, from a contact.
WHAT THE EMPLOYEE CHECKS	Who sent the invitation and who else is in it.	Usually nothing: the name and photo are enough.
WHERE IT RUNS	Zoom, Teams, Google Meet, Webex and GoTo Meeting.	Telegram, Signal, Slack huddles and Teams calls.
WHAT THE OPERATOR NEEDS	The meeting's joining details.	Their own account, signed in, with the phone beside them.

WHATSAPP TODAY Live voice and video calls from WhatsApp Web are limited for now, so plan WhatsApp tests around the other apps until calling is available there.

Three calls, from start to finish

Each example names who runs it, who is called and what a strong response looks like.

EXAMPLE 1 · RUN BY AN INTERNAL RED TEAM

The head of platform starts a Slack huddle: approve my access to production, now

Engineering · Slack huddle · Persona: head of platform

THE SETTING	The red team tests whether engineers grant access on a familiar face alone. The head of platform agrees to the use of her likeness.
THE CALL	The operator starts a huddle from a member account, in the head of platform's face and cloned voice: an outage, a lost laptop, an access request to approve in the next five minutes.
STRONG RESPONSE	The engineer asks for the request through the access ticket, and checks with the head of platform on a channel they already use.
AFTERWARDS	The operator reveals, rates the session and hands the recording to the owner of the access process.

EXAMPLE 2 · RUN BY THE AWARENESS LEAD WITH THE EXECUTIVE OFFICE

The chief executive calls on Signal from an airport lounge

Executive assistants | Signal call | Persona: chief executive

THE SETTING	The executive office wants to know whether assistants verify a video call from their own executive. The chief executive agrees, and the assistants consented to deepfake training at induction.
THE CALL	The operator calls on Signal, from an account signed in on a phone beside them, in the chief executive's face and voice: please send the confidential board pack to a new address before boarding.
STRONG RESPONSE	The assistant offers to send it through the board portal, and calls back on the executive's known number.
AFTERWARDS	A short debrief with the assistants together, and a rule agreed with the executive for urgent requests while travelling.

EXAMPLE 3 · INCIDENT RESPONSE DRILL, RUN BY THE SECURITY TEAM

A supplier's account manager calls on Telegram about new bank details

Procurement | Telegram call | Persona: supplier contact

THE SETTING	Procurement talks to suppliers on messaging apps every day. The incident response lead tests whether a suspected deepfake is reported. The supplier contact is an employee of the supplier who has agreed, through the supplier, to lend his likeness.
THE CALL	The operator calls a buyer on Telegram in the supplier contact's face and cloned voice, asking to confirm new bank details before an invoice is paid.
STRONG RESPONSE	The buyer declines, calls the supplier on the number in the vendor file and raises a security incident.
AFTERWARDS	Rate the session and use the recording in the incident review.

04 FOR RED TEAMS

Find the approvals that happen in a chat

Access, code and payments are increasingly approved in messaging apps. Test the approvals, not the people.

- Map where approvals really happen before choosing the app: a Slack channel, a Teams chat, a Signal group.
- Use the operator's own work account. Slack needs a member account; Telegram and Signal need an account with the phone beside you.

- Stop at the moment of compliance and reveal. Report the gap to the owner of the process.

> **WHAT TO WATCH FOR** Approvals granted because the request came from inside the company's own workspace.

05 FOR AWARENESS AND HUMAN RISK LEADS

Extend the verification habit to every app

Employees learn to verify the desk phone and email. Extend the same habit to the apps on their phone.

- Teach one routine for every channel: pause, end the call, verify on a channel you already have.
- Run a small number of calls on the apps your company really uses, and share an anonymised recording.
- Keep the AI label on for teaching sessions.

> **WHAT TO WATCH FOR** Employees who verify a call from a stranger but not one from a colleague's account.

06 FOR INCIDENT RESPONSE TEAMS

Make sure the call is reported

A deepfake call in a messaging app leaves little trace on company systems. The report is the only signal you get.

- Check that employees know how to report a suspicious messaging app call, and to whom.
- Record the session and rate it, so the review is built on what happened.
- Measure the time from the call to the report, and drill again until it falls.

> **WHAT TO WATCH FOR** Calls the employee recognised as fake but never reported. That is the gap the drill is for.

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

MESSAGING APP IMPERSONATION · NOVEMBER 2026