

How exposed is your organization to deepfake social engineering?

Ten questions. Answer for what actually happens, not what the policy says. Each Yes is one point. Each No maps to a runbook on page 3.

#	AREA	CONTROL	ANSWER	
01	FINANCE	Every payment or bank-detail change is confirmed by calling back a number already on file.	Yes	No
02	FINANCE	Payments above a set amount need a second approver — no exceptions for executives.	Yes	No
03	SERVICE DESK	Password and MFA resets never rely on knowledge questions alone (ID, manager, DOB).	Yes	No
04	SERVICE DESK	All active sessions are revoked after any password or MFA reset.	Yes	No
05	ALL STAFF	Staff know IT never asks for codes or remote sessions on an inbound call.	Yes	No
06	ALL STAFF	Staff never return a voicemail to the number left in the message.	Yes	No
07	HR / HIRING	Remote hires pass a live ID check matched to the person before an offer.	Yes	No
08	LEADERSHIP	The CEO has told staff in writing they can pause any request without penalty.	Yes	No
09	REPORTING	There is one simple way to report a suspicious call or video, even stopped ones.	Yes	No
10	TESTING	High-risk workflows were tested in the last 12 months with realistic voice or video.	Yes	No

YOUR SCORE

/ 10

NOT SCORED

0–4 · Exposed

A routine “IT support” call likely succeeds today.

5–7 · Inconsistent

Controls exist, but gaps remain. Fix every No.

8–10 · Defined

Now prove it with a live simulation.

THE PRINCIPLE

Detection decays. Verification holds.

Your people will not out-listen an AI voice or out-stare a live synthetic face. Every model release moves that contest in the attacker's favor. A process that verifies the request through a trusted channel works no matter how good the fake gets.

\$893M

AI-related losses reported to the FBI in
2025
FBI IC3 2025

\$25.6M

Moved after one call where every other
face was synthetic
Arup, Hong Kong, 2024

92%

Of organizations we tested were
vulnerable
Breachers.ai, 1,000+ targets

Detection-first

- Depends on the quality of the fake
- Weakens with every model release
- Fails silently: a good fake passes

Verification-first

- Depends on your process
- Holds no matter how good the fake gets
- Fails visibly: a skipped step you can fix

THE STANDARD

The 7-rule verification standard

For any request, on any channel, that would move money, change access, or release sensitive data.

1 Define high-risk requests. Payments and bank changes, password and MFA resets, access, sensitive data.

2 Never verify inside the channel the request came in on. Not the same call, not the same thread.

3 Call back on a number you already had. Never a number, link, or invite the requester supplied.

4 A live face or familiar voice is not proof of identity. Treat it like an unknown sender.

5 Urgency and secrecy add verification. “Keep this confidential” means a second approver.

6 Anyone can pause any request without penalty. Leadership says so in writing. **Closes Q8**

7 Report every attempt, including the ones you stopped. **Closes Q9**

“I need to verify this with our internal team.”

The one line that most reliably ends our simulations — said, then followed through.

Fix every No

Each runbook is what the person on the receiving end does the moment the scenario starts.

01 · HIGHEST RISK

CLOSES Q5

“IT support” calls an employee
Routine pretext, expiring credential, often after an email flood.
Share nothing. Say the line, hang up, call the service desk on the intranet number.

02

CLOSES Q3 · Q4

An “employee” calls the help desk
Locked out, new phone. Knows manager and ID from public sources.
No knowledge-only resets. Call back on the HR number on file. Revoke sessions after.

03

CLOSES Q6

Voicemail asking for a callback
The voice that answers is patient and helpful — possibly an AI agent.
Never call the number left. Look up the department yourself.

04

CLOSES Q1 · Q2

Executive payment request
CEO or CFO on video, urgent and confidential transfer.
End the call. Call back on the directory number. Second approver, no exceptions.

05

CLOSES Q7

Synthetic job candidate
A strong remote candidate whose video doesn’t quite add up.
Live ID check before the offer. Ship only to a verified address.

06

CLOSES Q1

Vendor or payroll bank change
A known contact updates banking details before a big payment.
Callback to the number on file, second approver, hold first payment.

MEASUREMENT

CLOSES Q10

Measure the action, not the click

Test finance, the service desk, HR, and EAs with realistic voice, video, and callback scenarios. Score the deepest step reached, then re-test after every fix.

L0 No response	L1 Answered	L2 Clicked	L3 Engaged or called back	L4 Took the action	L5 Hit the business
-------------------	----------------	---------------	------------------------------	-----------------------	------------------------

Find out which of your controls hold.
We run these exact scenarios and score them on the OSES™ ladder against your peer vertical.



Book Demo

Sources: FBI 2025 Internet Crime Report via PYMNTS (Apr 2026) · Arup deepfake fraud via CNN (May 2024) · NYDFS help desk social engineering alert (Sep 2024) · Breacher.ai benchmark, 1,000+ simulated targets.

BREACHER.AI · BREACHER.AI03 / 03