

SCENARIO 3 | ALL INDUSTRIES, ESPECIALLY THOSE WITH PUBLIC-FACING EXECUTIVES

# Deepfake Executive Voice and Video Fraud

An employee joins a video call with what appears to be the CEO and CFO, who instruct a confidential urgent transfer.

|                         |            |                               |                          |
|-------------------------|------------|-------------------------------|--------------------------|
| <b>Suggested length</b> | 60 minutes | <b>NIST CSF 2.0 functions</b> | Govern, Protect, Respond |
|-------------------------|------------|-------------------------------|--------------------------|

## Exercise objectives

- Test whether payment controls hold up against convincing AI impersonation
- Establish verification steps for voice and video requests
- Prepare communications if a deepfake of an executive circulates publicly

## Recommended participants

Facilitator and scribe, Executive Sponsor, Incident Commander, IT Lead / MSP, Security Lead / vCISO, Legal / Privacy Counsel, Communications, Finance / CFO. Add the roles named in the discussion questions below. Smaller teams can combine roles; see "Scaling roles to your company size" in the Facilitator Guide.

## Injects

Read each inject aloud, then pause for discussion before moving to the next. Facilitators may add or skip injects to fit the time available.

| # | When              | What happens                                                                                                                                                                     |
|---|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Friday, 4:40 p.m. | A finance specialist receives a message from the CEO's personal phone number asking them to join a quick, confidential video call.                                               |
| 2 | 4:50 p.m.         | On the call, the 'CEO' and 'CFO' explain a confidential acquisition and ask for two transfers totaling \$240,000 before the weekend. The video is slightly laggy but convincing. |
| 3 | Monday, 9:00 a.m. | The real CEO has no knowledge of the call. A second deepfake video of the CEO making false statements about a product recall begins circulating on social media.                 |

## Discussion questions by role

| Role                    | Questions                                                                   |
|-------------------------|-----------------------------------------------------------------------------|
| Finance / CFO           | • What controls should have stopped this, and did they?                     |
| Executive Sponsor       | • Do executives have a verbal code word or verification process?            |
| Communications          | • How do we prove the video is fake and correct the record quickly?         |
| Legal / Privacy Counsel | • Which platforms and authorities do we contact for takedown and reporting? |

| Role     | Questions                                                                                                                                                                                                                                        |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Everyone | <ul style="list-style-type: none"> <li>• What information do we need that we do not have?</li> <li>• Who outside the company must we contact, and do we have their numbers offline?</li> <li>• What would we do differently tomorrow?</li> </ul> |

## Key decisions and good practices to look for

- Require dual approval and out-of-band call-back for all urgent or confidential payments
- Create executive code words or verification questions
- Report to the bank and to IC3
- Request platform takedowns and publish an official statement
- Train staff on deepfake red flags (urgency, secrecy, new channels)

**Hotwash (last 15 minutes):** What went well? What surprised us? Which three action items will we complete in the next 30 days, and who owns each? Record them in the After-Action Report template.

**Document it:** the scribe keeps the Exercise Log (see the Facilitator Guide) so the next exercise builds on this one.

This scenario is fictional and for training purposes. Legal and regulatory references are general information, not legal advice; confirm requirements with counsel.