

AI FRAUD PREVENTION

Deepfake & AI Fraud Verification Checklist

Attackers now use artificial intelligence (AI) to clone voices, fake video calls, and write convincing emails. In 2024, an employee at engineering firm Arup transferred about US\$25 million after a video call in which every other participant was a deepfake. Use this checklist to make sure no single call, message, or video can move money or data.

Policies to put in place

- ☐ Require call-back verification on a known, saved number for any request involving money, bank details, passwords, or sensitive data
- ☐ Require two-person approval for wire transfers, new vendors, and bank-detail changes
- ☐ Create executive code words or verification questions that are never shared online or in email
- ☐ Ban approving payments or access changes based only on a voice message, text, video call, or chat
- ☐ Tell staff they will never be punished for slowing down to verify a request from a leader

Red flags to train on

- ☐ Urgency, secrecy, or pressure to skip normal steps
- ☐ A new phone number, messaging app, or email address for a known person
- ☐ Video with poor lighting, lag, stiff faces, odd blinking, or mismatched lip movement
- ☐ Voice that sounds right but uses unusual words or avoids personal questions
- ☐ Requests that arrive just before a weekend, holiday, or the end of the business day

During a suspicious call or video

- ☐ Ask the person to turn their head fully sideways or pass a hand across their face
- ☐ Ask a question only the real person would know
- ☐ End the call and call back on a number you already have
- ☐ Do not open attachments or links sent during the call
- ☐ Write down the time, number, platform, and what was requested

If you think you were targeted

- ☐ Call your bank's fraud line immediately if money moved
- ☐ Report to the FBI at ic3.gov and to your security team or IT provider
- ☐ Reset any credentials that were shared and alert the person who was impersonated
- ☐ Preserve messages, recordings, and logs as evidence
- ☐ Request takedowns from the platform if a fake video or audio is circulating

Checking suspicious media

- ☐ Check Content Credentials at contentcredentials.org/verify
- ☐ Run a reverse image search (Google Lens, TinEye, Bing Visual Search)
- ☐ Treat AI-detector scores as one clue, never as proof
- ☐ Confirm through an independent, trusted source before sharing or acting

General guidance for training and planning, not legal advice. Adapt to your environment, contracts, and regulators.