Deepfake Fraud Readiness Checklist

Use this checklist to evaluate your organisation's preparedness for deepfake fraud, AI scams, and digital deception risks.

Check each item currently in place.

Deepfake Fraud Readiness Assessment

☐ 1. Employees understand what deepfake scams and AI impersonation attacks are.

☐ 2. We train employees to verify unusual requests before acting.

☐ 3. We have documented payment verification procedures.

☐ 4. Wire transfers require secondary approval or confirmation.

☐ 5. Vendor banking changes are independently verified.

☐ 6. Employees are trained to recognise urgency-based social engineering.

☐ 7. Executives support verification culture openly.

☐ 8. Employees feel comfortable questioning suspicious requests.

☐ 9. We educate staff about AI-generated phishing attacks.

☐ 10. Remote employees receive fraud awareness training.

☐ 11. Messaging platform fraud risks are addressed in training.

☐ 12. Employees understand that video and voice communication can be manipulated.

☐ 13. Multi-factor authentication is enabled across critical systems.

☐ 14. Payroll and finance systems have strong approval workflows.

☐ 15. Employees know how to report suspicious communication quickly.

☐ 16. Incident escalation procedures are clearly documented.

☐ 17. Leadership reinforces cybersecurity awareness regularly.

☐ 18. Sensitive requests are verified through secondary communication channels.

☐ 19. We conduct realistic phishing or fraud awareness exercises.

☐ 20. Employees understand risks involving fake AI tools and impersonation.

☐ 21. Identity protection is treated as a security priority.

☐ 22. Vendor and partner communication verification procedures exist.

☐ 23. Awareness training is updated regularly to reflect evolving AI threats.

☐ 24. We treat operational discipline as part of cybersecurity resilience.

☐ 25. AI-driven fraud preparedness is reviewed regularly by leadership teams.

Scoring Guide

Strong Maturity

20–25 checked items

Your organisation demonstrates strong preparedness for deepfake fraud and AI-enabled deception risks.

You likely have:

- strong verification culture,
- employee awareness,
- operational safeguards,
- and leadership engagement.

Continue focusing on:

- awareness updates,
- scenario testing,
- and evolving fraud prevention strategies.

Moderate Exposure

12–19 checked items

Your organisation has meaningful awareness of AI-driven fraud risk, but important gaps remain.

You may need stronger:

- employee training,
- financial controls,
- verification consistency,
- or remote work safeguards.

Improving operational discipline should become a near-term priority.

High Vulnerability

0–11 checked items

Your organisation may face significant exposure to AI-enabled fraud and impersonation attacks.

Employees may currently rely too heavily on:

- digital trust,
- urgency,
- or informal approval processes.

Immediate improvement is recommended in:

- verification culture,
- awareness training,
- identity protection,

and leadership-supported operational controls.