

AI scam detection guides

- [The Ultimate Guide to AI Scams: How to Spot and Stop Them](#) – Practical breakdown of AI-enabled phishing, business email compromise, and social engineering, with concrete “red flag” patterns and training ideas for teams.
- [Protect yourself from AI scams - DFPI](#) – Recent government-facing guidance (2026) on common AI scam types (imposter deepfakes, investment scams) and the behavioral red flags to watch for, written for everyday consumers.

Deepfake and AI media spotting

- [How to detect deepfakes: A practical guide](#) – Walks through visual and behavioral cues (eyes, lighting, lip sync, micro-expressions) that still tend to give away deepfake video and images.
- [Don't Be Duped: How to Spot Deepfakes](#) – Short, non-technical set of principles from Northwestern on staying skeptical and cross-checking surprising audio/video before believing or sharing it.

Voice cloning and imposter scams

- [FBI Warning AI Voice Phishing: How To Spot And Stop The Threat](#) – Summarizes current vishing tactics with cloned voices and gives practical verification steps (callback procedures, 2FA hygiene, reporting).
- [How to protect yourself from AI voice scams](#) – Consumer bank-focused guide with scenarios like fake “relative in trouble” calls, plus habits to reduce risk and avoid panic decisions.

Shopping and fake AI products

- [How to Spot AI-Generated Scam Products](#) – Bellingcat-style OSINT approach to spotting AI-generated product photos, fake sellers, and bogus storefronts, with concrete checks on images, listings, and seller history.