T2025_21 Beware of deepfake and AI-Generated Scams (September 28, 2025)

Cybercriminals are increasingly using artificial intelligence to create convincing fake audio, video, and images known as deepfakes. These scams can impersonate executives, coworkers, or even family members to trick you into sending money, sharing sensitive information, or granting system access. Unlike traditional phishing, deepfakes exploit human trust by mimicking voices and faces with alarming accuracy.

Always verify unusual requests through a second communication channel before taking action. For example, if you receive a video call or voice message asking for urgent financial transfers, confirm the request via a known phone number or official email address. Organizations should train staff to recognize signs of AI-generated content and establish clear approval workflows for sensitive transactions.

References

- Europol. (2022). Facing reality? Law enforcement and the challenge of deep fakes. Europol Innovation Lab. Retrieved September 27, 2025, from https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes

- Coalition Inc. (2025, February 18). Deepfakes are making cyber scams more difficult to detect. Coalition Security Labs. Retrieved September 27, 2025, from https://www.coalitioninc.com/blog/security-labs/deepfakes-are-making-cyber-scams-more-difficult-to-detect