



How to Protect Your Business from Deepfake Cyber Threats

How to Protect Your Business from Deepfake Cyber Threats

Deepfakes are the fastest growing and most convincing cybercrimes today but, according to the experts, 73% of us can't spot them. One in 10 businesses in the UK have already encountered deepfake attacks. Understanding how they are created and the flaws that signal deepfakes could spare you significant financial and reputational loss.

What is a deepfake?

A deepfake is a form of AI-generated audio or video content that creates realistic impersonations of real people. Criminals are using cheap and freely-available AI tools to closely mimic the voice and mannerisms of executives to deceive employees and bypass security measures.

Interesting fact

53% of us share our voices online or via recorded notes at least once a week. It takes just three seconds of audio to produce an 85% voice match. So before you post your next video, publish your next podcast or simply leave a voice note, check out our checklist for spotting and preventing deepfake fraud.

Examples of deepfakes in action

- **Arup's \$25m fraud attack**

Cybercriminals used a deepfake video call with realistic voices and appearances of senior executives to instruct a junior employee to transfer funds.

- **Headteacher scandal**

An audio deepfake of a headteacher behaving badly went viral on social media, damaging reputation and creating chaos before the truth was uncovered.



Three ways to spot deepfakes

- **Visual Clues:** Look for awkward lip-syncing or unnatural facial movements in videos.
- **Audio Inconsistencies:** Watch for unusual pauses, accents, pitch shifts or robotic tones.
- **Behavioural Clues:** If a familiar person behaves unusually, it could be a sign of a deepfake.

Protect your business using our T.R.U.S.T. protocol

- T**rain your team: Conduct regular staff training to identify deepfake scams.
- R**equire MFA. Insist that every employee uses multi-factor authentication to secure access to data and important information.
- U**se verification protocols. Set up checks for sensitive requests so that employees never act on audio or video instructions alone.
- S**et incident response plans. Prepare a response strategy with practice drills, should you fall prey.
- T**est and update. Regularly review and refine your protocols and adjust to new kinds of threats.

Next steps

- Take our Deepfake Cybersecurity Scorecard test <https://deepfake.scoreapp.com> that helps you assess your readiness and plan for stronger defences.
- Consult the experts: Give us a call on **0203 981 0850** follow us on LinkedIn <https://www.linkedin.com/company/ziptech-services/> or request an appointment info@ziptechservices.co.uk

