

Deepfakes Hit SMEs: Protecting Your Company from AI Fraud

MANAGEMENT SUMMARY & CORE TAKEAWAY

Deepfake fraud is a concrete but manageable threat for Swiss SMEs in 2026. Just three seconds of audio can produce a voice clone. Effective verification rules, a second-channel callback, a code word, and training against manipulative urgency significantly reduce risk without expensive specialty tools.

CONTEXT & EXECUTIVE RELEVANCE

Deepfake fraud uses artificially generated video or audio to impersonate a trusted person. For SMEs, this is no longer a fringe issue. According to Fortune in March 2026, deepfake fraud cost US companies USD 1.1 billion in 2025, a tripling from USD 360 million the previous year. The number of deepfakes rose from 500,000 in 2023 to over 8 million in 2025, and voice cloning fraud grew by 680 percent in one year.

The case of engineering firm Arup shows how far attacks have progressed: a finance employee in Hong Kong paid USD 25 million after speaking with a deepfake version of his CFO in a video call (CNN, February 2024). What used to be forged emails is now a deceptively real video conference. Attackers combine technical deception with psychological pressure, usually urgency and authority.

COMPARISON & BENCHMARK MATRIX

Second-channel callback	Effort: low Protection: very high Cost: none
Secret code word	Effort: low Protection: high Cost: none
Four-eyes principle	Effort: low Protection: high Cost: none
Urgency training	Effort: medium Protection: high Cost: low

SWISS COMPLIANCE & ARCHITECTURE GUIDELINES

- ☑ Full compliance with revised Swiss Data Protection Act (revDSG).
- ☑ Zero vendor lock-in on closed proprietary models.
- ☑ Seamless integration into Abacus, Bexio and M365 ecosystems.

Non-Binding Process Analysis

Let us review in 20 minutes where AI agents create immediate measurable efficiency in your workflows.

ki-outsourcing.ch