

The Boss Scam

Spot a fake boss, CEO or deepfake video call in ten seconds — **before a cent moves.**

Someone messages, calls or even video-calls claiming to be your boss, a director or the CEO. They sound right. They look right. In 2026, AI can clone a voice from three seconds of audio and fake a face in real time. **The request is always the same: move money — fast, and quietly.**

01 HOW THE SCAM WORKS

- 1 They study you** — your role, your manager, your company — from LinkedIn and the public org chart.
- 2 They make contact** — a new number, a look-alike email, or a real-time deepfake video call.
- 3 They manufacture pressure** — a deadline, a “confidential deal”, and “don’t tell anyone”.
- 4 They move the money** — to a new bank account, gift cards or crypto — then they vanish.

02 THE 10-SECOND CHECKS — IF ANY IS TRUE, STOP

- ◆ The message comes from a **new or unknown number**, or an email domain that’s slightly “off”.
- ◆ You’re **rushed** — a deadline, a threat, “I need this right now”.
- ◆ You’re told to **keep it secret** or skip the normal approval process.
- ◆ The payment goes to a **new or changed bank account**.
- ◆ You’re asked for **gift cards, vouchers or crypto**.

03 WHAT TO DO

- ✓ **Stop.** Real urgency survives a five-minute pause. Fake urgency cannot.
- ✓ **Verify on a channel you already trust** — call back on the number you have saved, or ask in person.
- ✓ **Never** confirm a payment or an account change from the message alone.
- ✓ If money already moved, **call your bank now** and report it.

No real executive will ever rush you to pay in secret. The urgency is the scam.