CIPHRAVERSE

CIPHRAVERSE WHITE PAPER

CEO Fraud: How It Works and How to Stop It

CEO fraud is a type of email scam known as business email compromise, or BEC: someone impersonates a director or a supplier and asks for an urgent transfer or a change of bank details. No malware is involved. The attack targets people and the payment process, not systems, which is why antivirus and firewalls do not stop it.

How the scam is built

The attacker researches the company on LinkedIn and the corporate website: who signs off payments, who the finance lead is, when the managing director travels. That moment is chosen deliberately, and the message often comes from an address that looks almost right or from a mailbox that was already compromised. It asks for something urgent and confidential: a transfer to a new supplier, an early payment on a deal, or a change to a regular supplier's bank details. A follow up phone call sometimes adds pressure.

Why technical controls miss it

There is no malicious attachment or link to scan. If the director's account was already compromised through phishing, the email is genuine and clears every filter. The attack exploits hierarchy and urgency rather than a technical flaw, so no perimeter security tool stops it on its own.

Controls that work

- Out-of-band verification: confirm any payment or bank detail change through a different channel than the message, calling a number you already had, never the one in the email.
- Dual authorisation: no payment above a set threshold goes out without a second person's approval.
- A culture where saying no to the boss is fine: anyone who questions or delays a suspicious payment should not fear consequences.
- A fixed procedure for supplier bank detail changes: every change is confirmed by phone with a known contact before payment details are touched.

None of these controls need a technology budget. Start with the cheapest one: decide today who authorises payments above a threshold and how a bank detail change gets verified before a single euro moves.