THREATS LIBRARY

JULITH GmbH
Awareness-as-a-Service

CEO fraud & business email compromise (BEC)

BEC attacks often cause more damage than ransomware - and they target accounting, executive assistants, and M&A teams. We show how attackers exploit hierarchy and which process controls actually help.

min read: 8 min **Updated:** 14 March 2026 **Risk:** Very high risk
Source: awareness-as-a-service.com/en/resources/threats/ceo-fraud

What is CEO fraud and BEC?

Business Email Compromise (BEC) describes attacks in which criminals abuse email accounts or identities to achieve fraudulent transfers, data exfiltration, or contract manipulation. **CEO fraud** is the best-known variant: a forged email apparently from the CEO or board demands that accounting make an urgent, confidential transfer.

According to the FBI and ENISA, BEC has been the most financially damaging cybercrime category globally for years - not because individual incidents are spectacular, but because so many organizations are affected and per-incident losses frequently reach six figures. Technical controls are largely ineffective when an attack contains no malware and arrives from a convincingly legitimate address.

Attackers research carefully first: LinkedIn profiles, press releases, annual reports, and company registries supply org charts, ongoing projects, and pending transactions. Armed with this intelligence, BEC emails sound convincingly authentic.

At a glance

01

No malware, no alert

BEC emails contain neither attachments nor links. They look like ordinary business email - which is why no technical system triggers.

02

Average damage in six figures

Per successful BEC attack in the DACH region, average losses reach the high five- to low six-figure range. Reversals are rare.

03

Hierarchy as an attack surface

The combination of authority ("the CEO") and urgency ("immediately, confidentially") overrides critical thinking - regardless of experience level.

How to recognise CEO fraud and BEC

Urgent out-of-cycle transfer
"Please arrange EUR 85,000 to the following account today - we are mid-transaction and this is time-sensitive."

Secrecy requirement
"Keep this between us for now" or "don't go through the usual channels - send directly to me." Any attempt to bypass process is the strongest warning sign.

New or changed bank details
A supplier or partner provides new payment details shortly before a payment is due - often when a transfer is already expected.

Slightly different sender domain
ceo@companyname-ag.com instead of @companyname.com, or a typo domain (companynaem.com). Differences are often just one character.

Unusual time or known absence
Attackers time messages to Friday evenings, public holidays, or when the supposed sender is known to be travelling.

Pressure to skip internal approval
"We have no time for the normal process" - any attempt to sidestep dual-control requirements is a red flag.

How to protect yourself

For employees

- **Never authorise a transfer based on a single email alone** - regardless of who the apparent sender is.
- **Out-of-band verification:** For unusual payment requests, always confirm by phone using a number you already know - not one provided in the email.
- **Challenge new bank details:** Any change to a supplier IBAN must be confirmed through a second, independent channel (phone, in person).
- **Ignore the secrecy demand:** No legitimate manager would be embarrassed that a normal approval process was followed. If someone says "don't tell colleagues", that is the strongest alarm.

For administrators

- **Enforce dual-control above a defined threshold** in the accounting system (e.g. second approval required above EUR 5,000).
- **Supplier master-data process for IBAN changes:** Changes to payment details only after written request and out-of-band confirmation - never on email instruction alone.
- **DMARC** `p=reject` for all domains to make exact domain spoofing harder.
- **Look-alike domain monitoring:** Services that identify typosquatting domains early.
- **BEC training module** with simulated CEO fraud scenarios - accounting, executive assistants, and procurement are primary target groups.

Real cases

CASE 01 · MACHINE MANUFACTURER (SME) · DE · Q4/2025

The executive assistant received an email apparently from her CEO, who was attending a trade fair in Asia. He asked her to transfer EUR 230,000 to an "M&A partner" - already cleared with the CFO, but please keep it quiet. She transferred the money. The real CEO was indeed at the fair - a fact visible on LinkedIn.

Damage: EUR 230,000, of which EUR 60,000 was recovered · **Detection:** the CFO spotted an irregularity three days later · **Lesson:** Out-of-band verification and explicit "secrecy demand = red flag" training would have prevented the loss.

CASE 02 · LOGISTICS PROVIDER · CH · Q1/2026

A supplier emailed accounting with a new IBAN for future payments. The email appeared authentic - same sender domain, similar writing style. In reality, an attacker had compromised the supplier's email account and was waiting for an upcoming payment. CHF 48,000 was transferred to a mule account.

Damage: CHF 48,000, reversal failed · **Detection:** supplier called about a missing payment · **Lesson:** IBAN changes must always be confirmed by phone with the known supplier contact.

What to do if it happens?

THE FIRST 15 MINUTES

1. **Call your bank immediately** (transfer recall): the faster you act, the greater the chance of recovery. Minutes matter.
2. **Document everything:** screenshot of the email, transfer confirmation, timestamps - preserve all evidence, delete nothing.
3. **Inform management and the CFO** - regardless of whether the transfer was apparently authorised by management.
4. **IT Security / SOC:** Check whether a mailbox was compromised (relevant when the genuine domain and sender were used).
5. **File a police report** and notify the relevant authority (BSI in Germany, NCSC in Switzerland).
6. **Notify the supplier** if their IBAN change was part of the fraud - they may also be a victim.

Frequently asked questions

Does DMARC protect against CEO fraud?

Partially. DMARC prevents exact domain spoofing (ceo@yourcompany.com). It does not protect against look-alike domains (ceo@yourcompany-ag.com) or compromised genuine accounts. It is necessary but not sufficient.

Why do banks not reimburse the loss?

An authorised transfer - one you initiated yourself, even if under deception - is generally not treated as a bank error in law. Reversals only succeed if the destination account has not yet been emptied, which is often not the case.

Are certain industries disproportionately targeted?

BEC hits companies with high transfer volumes, decentralised structures, and frequent supplier changes disproportionately: construction, logistics, real estate, M&A-active corporations, and NGOs with international transfers.

What is the difference between CEO fraud and BEC?

CEO fraud is a sub-type of BEC. BEC covers all variants: fake invoices, IBAN manipulation, compromised mailboxes, supplier fraud. CEO fraud specifically means impersonating senior management to subordinates.

Related topics

CEO fraud is the most prominent form of social engineering in a corporate context. Understanding BEC pairs naturally with the psychological foundations of social engineering and the role of insider threats.

© JULITH GmbH · awareness-as-a-service.com · ceo-fraud