CYBERSECURITY 101 · eBuilder Security

Business Email Compromise

Business email compromise is the fraud that does not look like one. A trusted-seeming email asks for a payment or a change of bank details, and the money is gone before anyone checks.

WHAT IT IS

BEC is a targeted scam in which a criminal poses as an executive, supplier or lawyer and uses email to trick staff into transferring money or changing payment details. It usually carries no malware, so it slips past technical defences and targets the payment process instead.

WHY IT MATTERS

$3 billion

reported BEC losses in 2025, second only to investment fraud

FBI IC3, 2025

$55.5 billion

exposed BEC losses worldwide, 2013 to 2023

FBI IC3, 2024

86%

of BEC losses moved by wire or ACH, fast and hard to reverse

FBI IC3, 2025

WHAT HAPPENED

In January 2024 a finance employee at the engineering firm Arup joined a video call with people who appeared to be the chief financial officer and colleagues. Every one of them was an AI-generated deepfake. Following their instructions, the employee made 15 transfers totalling about $25 million, which was never recovered. Source: Hong Kong police and CNN, 2024.

RED FLAGS TO WATCH FOR

BEC emails tend to share a shape. Treat any of these as a signal to stop and verify.

- A sudden change to bank or payment details.
- Pressure to act fast, with a deadline or a threat.
- A request for secrecy or to bypass normal approvals.
- A look-alike domain or a mismatched sender address.

THE ONE RULE THAT STOPS IT

Verify every new or changed payment or bank detail by contacting the sender on a channel you already trust, before you pay.

THEN BUILD THE HABIT AROUND IT

- Use a phone number or contact from your own records, gathered before the request.
- Require two approvers for any payment above a set threshold.

- Turn on multi-factor authentication for every mailbox.
- Set up email authentication (SPF, DKIM and DMARC) to block domain spoofing.

MYTHS AND FACTS

MYTH

Our spam filter will catch it.

FACT

BEC often has no link or attachment, so filters and antivirus miss it. Verifying the payment is what stops it.

MYTH

You can spot a scam by its bad grammar.

FACT

AI now writes flawless messages and clones voices and video, so the old giveaways are gone.

MYTH

The bank will just reverse it.

FACT

Wire and ACH payments clear fast and are rarely recovered, so speed of reporting is everything.

THE LEGAL DUTY

Under Cybersäkerhetslagen and NIS2, a significant incident must be reported to MCF (formerly MSB) within 24 hours, and a mailbox breach that exposes personal data means notifying IMY within 72 hours under GDPR.

GET HELP

eBuilder helps Swedish organisations train their people and monitor for email account compromise.

Read the Full Article →