INFOGRAPHIC

TrustLayer

BEC stops here: Your 7-step defence

the challenge

BEC isn't just another email threat. It's targeted, convincing, and often looks like it came from the top. One well-timed message can trick someone into handing over money or sensitive data—no malware required.

It's a global problem costing businesses billions. But it's also preventable, with the right approach.

01

Watch the sender — not just the name

Spoofing works because we scan, not study. Always check the full address, not just the display name.

Lock down finance and execs 02

Attackers target those with access or authority. Prioritise training, protection, and policies around finance teams and senior staff.

03

Always verify urgent payment requests

No shortcuts. Always confirm requests out-of-band — especially if it's urgent, unusual, or outside process.

Build in process-level defences 04

Out-of-process invoices? Manual approval gaps? Fix the cracks attackers rely on.

05

Train continuously, not once

BEC lures don't look like spam. Use real examples and keep training short, sharp and frequent.

Secure access to email platforms 06

Enable adaptive MFA for platforms like Outlook Web Access. Block legacy protocols and shared logins.

07

Use smart, layered email protection

Choose tools that go beyond spam filters — flag spoofing, detect impersonation, and alert users in real time.

Bonus checks for high-risk teams

Handling large sums or sensitive data? You'll want to go further:

- Monitor inbox behaviour for unusual replies or patterns
- Buy up key lookalike domains to block spoof setups
- Run BEC-style phishing simulations — not just generic spam tests
- Make it easy to report — visible buttons, instant triage, clear follow-up

TrustLayer