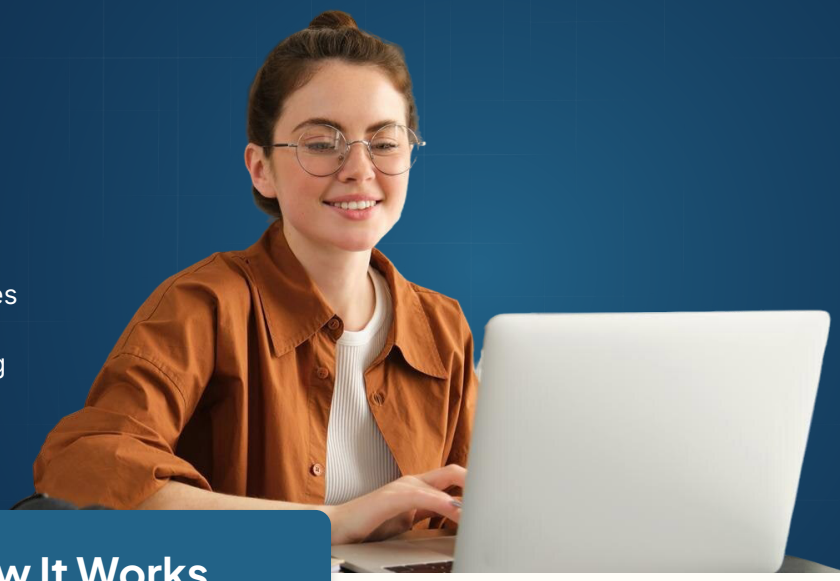
Business Email Compromise (BEC)

Business Email Compromise (BEC) is a targeted scam where criminals impersonate senior executives or trusted partners. By exploiting authority and urgency, attackers trick employees into transferring money, buying gift cards, or sharing sensitive information. These scams have cost organisations billions worldwide.



How It Works

Impersonating Executives

Attackers spoof or hack the email accounts of CEOs, CFOs, or other leaders. Messages appear authentic, making employees feel pressured to act.

Tip: *Always verify financial requests by calling the executive directly on a trusted number.*

Creating Urgency & Secrecy

Emails often stress that action must be taken immediately or that the request should remain confidential. This discourages staff from double-checking.

Tip: *Be suspicious of requests that demand secrecy or rush you into action.*

Domain Spoofing

Scammers register lookalike domains that are easy to miss, such as ***compaany.com*** instead of ***company.com***. Even cautious employees can overlook these small changes.

Tip: *Carefully check email addresses and domains for slight spelling differences.*

The Cost of Compliance

Because the emails appear to come from an authority, staff may follow instructions without question, leading to huge financial losses.

Tip: *Report suspected attempts immediately to your IT or security team to prevent further damage.*