Chief Information Security Office

Fraud and Cybersecurity Case Study: Business Email Compromise (BEC)

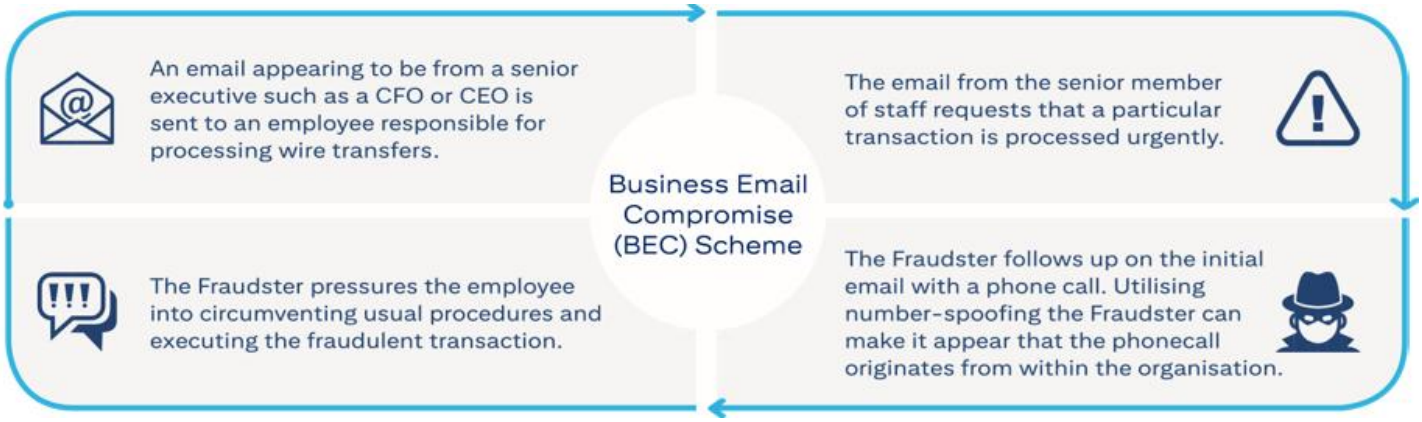
Overview

Business Email Compromise (BEC) remains one of the most financially damaging cyber threats facing organizations today.

In this type of scheme, a criminal impersonates a senior company executive, typically the CEO or CFO and attempts to manipulate an employee, often in finance or accounts payable, into processing an unauthorized wire transfer or performing some other type of action.

The attacker uses convincing social engineering, including urgent language, secrecy tactics (e.g., confidentiality requests or NDAs), and/or phone number spoofing techniques, where the number on the caller ID is spoofed to match a known contact or number to the victim, to make their communications appear genuine.

These emails often look identical to legitimate corporate correspondence, using the same tone, signature, trademarks, and formatting as an internal message. Increasingly, attackers may also use deepfake-enabled voice or video impersonation to reinforce credibility and pressure victims into taking action.



Modern Real-World Scenario

In a recent real-world incident (2024), a U.S. manufacturing firm lost over **$3 million** after a finance manager received what appeared to be an urgent email from the **Chief Operation Officer (COO)**.

The message claimed the company was finalizing a confidential overseas acquisition and needed a same day wire transfer to a law firm.

Shortly after sending the email, the fraudster **followed up with a spoofed phone call**, displaying the COO's actual telephone number on the employee's caller ID. The fraudster reinforced the urgency and confidentiality of the deal (a common tactic to suppress independent verification), warning that "any delay could jeopardize the acquisition."

Believing the request to be genuine, the employee bypassed the usual two-person approval process and initiated the transfer. The funds were immediately routed through several international accounts by the fraudster and became unrecoverable.

Tactics Used

- **Executive Impersonation**: Attackers mimic internal executives using similar domain name or compromised email accounts including the use of deepfake voice or video to impersonate business leaders or colleagues.

- **Urgency & Authority**: Phrase such as "This must be done today" or "Don't involve others" are used to override normal verification steps.

- **Number Spoofing**: Attacker's calls appear to originate from the executive's official line, adding credibility.

- **Emotional Pressure**: Fraudsters often appeal to the victim's sense of loyalty ("I'm counting on you") or fear of delay to manipulate employees.

Key Lessons

- Always verify high value or urgent requests through a separate, trusted channel such as calling the executives known internal extension or messaging them directly. Be extremely cautious where requests involve urgency, confidentiality, or executive authority.

- Establish two-person approval for all wire transfers or payment changes.

- Educate staff regularly on BEC tactics and emerging fraud trends, including deepfake-enabled impersonation and evolving social engineering techniques.

- Implement technical controls such as email authentication (DMARC, SPF< DKIM) and advanced threat detection.

- Simulate BEC exercises regularly to test employee awareness and procedural compliance.