

A photograph of two men in business attire. The man on the right is in focus, wearing a white shirt and looking towards the man on the left. The man on the left is partially visible, wearing glasses and a dark suit. The background is a blurred office environment.

**Protect your  
business from  
Business Email  
Compromise**



**Bank of  
Ireland  
UK**

# What is Business Email Compromise?

Business Email Compromise, also known as CEO Impersonation Fraud, is a type of fraud where the fraudster pretends to be a senior executive from your organisation. They will send an email to an employee to try to trick them into doing something, like making a payment to either an existing or new client or supplier.

- ▶ The fake emails are well crafted, can be sent from compromised email accounts and may look like they have come from someone you know, generally a senior executive at your company
- ▶ The fraudster usually pressurises you into acting quickly and without thinking
- ▶ Typically, the fraudster instructs you to make an urgent high value payment to a supplier or creditor, and usually includes the payee details, including the IBAN
- ▶ The fraudster usually advises in the email that they will not be available for the following number of hours or days, perhaps running to a meeting or catching a flight and that the payment must be sent immediately.

 New email ▼ |  Reply |  Reply All |  Forward |  Delete

**From: CEO / Senior Executive**  
**To: Chief Financial Officer**

Are you in the office?

I need you to carry out a transaction to a beneficiary. I'm about to go to a meeting. Let me know if you are available and I will forward the details. It's urgent.

Regards

**Name of senior executive**

# Pause and check before you act

Be **sceptical of urgent requests** that do not follow typical company procedures and policies.

**Always verify that the email is from the real sender. Call them before acting on the request.**

## Protect yourself and your business

- ▶ Establish a documented internal process for requesting and authorising all payments. You may need to review existing internal procedures
- ▶ Consider how your business issues and accepts payment instructions. Email is not considered a secure means of communication unless encrypted
- ▶ Phone numbers quoted in the suspicious email should not be trusted; verify the contact internally before making any payment
- ▶ Notify the Bank immediately if you receive a suspicious email relating to payments or Action Fraud or the Police if you think you have been the victim of fraud.

**Always ensure you have up-to-date anti-virus software in place on all your devices and monitor your bank accounts regularly for signs of any unauthorised activity.**

[bankofirelanduk.com/security-and-fraud](https://bankofirelanduk.com/security-and-fraud)

Report suspicious emails relating to payments to [365security@boi.com](mailto:365security@boi.com)

For your security and to improve our service to you, we may record and monitor phone calls. Branch details are given on our website.

Bank of Ireland UK is a trading name of Bank of Ireland (UK) plc. Registered in England and Wales (No. 7022885), Bow Bells House, 1 Bread Street, London, EC4M 9BE.



Protected