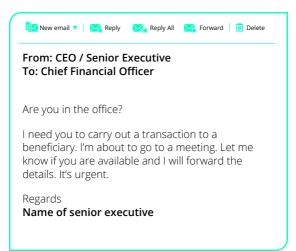




## What is Business Email Compromise?

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
- Often the payee account is located overseas
- ► 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.



## 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 An Garda Síochána 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.

bankofireland.com/security