CEO/BEC fraud occurs when an employee authorised to make payments is tricked into paying a fake invoice or making an unauthorised transfer out of the business account.

HOW DOES IT WORK?

A fraudster calls or emails posing as a high ranking figure within the company (e.g. CEO or CFO).

They require an urgent payment.

They use language such as: 'Confidentiality', 'The company trusts you', 'I am currently unavailable'.

They refer to a sensitive situation (e.g. tax control, merger, acquisition).

WHAT ARE THE SIGNS?

Unsolicited email/phone call
Pressure and a sense of urgency
Direct contact from a senior official you are normally not in contact with
Unusual request in contradiction with internal procedures
Request for absolute confidentiality
Threats or unusual flattery/promises of reward

WHAT CAN YOU DO?

AS A COMPANY

Be aware of the risks and ensure that employees are informed and aware too.
Encourage your staff to approach payment requests with caution.
Implement internal protocols concerning payments.
Implement a procedure to verify the legitimacy of payment requests received by email.
Establish reporting routines for managing fraud.
Review information posted on your company website, restrict information and show caution with regard to social media.
Upgrade and update technical security.
Always contact the police in case of fraud attempts, even if you did not fall victim to the scam.

AS AN EMPLOYEE

Strictly apply the security procedures in place for payments and procurement. Do not skip any steps and do not give in to pressure.
Always carefully check email addresses when dealing with sensitive information/money transfers.
In case of doubt on a transfer order, consult a competent colleague.
Never open suspicious links or attachments received by email. Be particularly careful when checking your private email on the company’s computers.
Restrict information and show caution with regard to social media.
Avoid sharing information on the company’s hierarchy, security or procedures.

If you receive a suspicious email or call, always inform your IT department.

#CyberScams