**WHAT CAN YOU DO?**

**AS A BUSINESS**
- Ensure that employees are informed and aware of this type of fraud and how to avoid it.
- Implement a procedure to verify the legitimacy of payment requests.
- Instruct staff responsible for paying invoices to always check them for any irregularities.
- Verify all requests purporting to be from your creditors, especially if they ask you to change their bank details for future invoices.
- For payments over a certain threshold, set up a procedure to confirm the correct bank account and recipient (e.g. a meeting with the company).
- Restrict information that you share about your employer on social media.
- Review information posted on your company website, in particular contracts and suppliers. Ensure your staff limit what they share about the company on their social media.
- Always contact the police in case of fraud attempts, even if you did not fall victim to the scam.

**AS AN EMPLOYEE**
- Do not use the contact details on the letter/fax/email requesting the change. Use those from previous correspondence instead.
- Set up designated Single Points of Contact with companies to whom you make regular payments.
- When an invoice is paid, send an email to inform the recipient. Include the beneficiary bank name and the last four digits of the account to ensure security.