# HSBC Payment Fraud & Scams
# Business Email Compromise / CEO Fraud

## What is Business Email Compromise?

This is an authorised push payment scam where a person or business is tricked into sending money to a fraudster posing as a genuine person or organisation, such as a supplier. For example:

Email address is spoofed or compromised (hacked):

- Spoofing is where the fraudster sets up an email address to trick the recipient. For example, using letters that are similar, such as using 'rn' instead of 'm'- J@rnbusiness.com instead of J@mbusiness.com.
- Compromising/hacking is where a fraudster uses malware (virus) or obtains the email password through another method, such as a vishing call, to take over a genuine email account.

## What is CEO Fraud?

This is where criminals impersonate the CEO or other senior member of staff in an organisation. They often send emails to the accounts department to make a large payment urgently.

The email account of the CEO or another senior member of staff is either spoofed of compromised (hacked). These emails can carry on from previous email trails. Fraudsters use hacking or spoofing to make payment requests, which are often aligned with genuine activities of your business.

HSBC UK

## How can I protect my business?

- **Always** verify new payment details from suppliers by phoning a known contact, on a known telephone number or one from the company's official website, to check the sort code and account number. **Never** use a number in the email as this could be a fraudster.
- **Check** email addresses for subtle differences, such as added letters, numbers, special characters or a different domain like .com instead of .co.uk.
- **Always** check the sender's name/email address – clicking on the name will reveal the full email address of the sender.
- **Use** multi-factor authentication where it's offered to help keep your account safe.
- **Review** email account settings, such as automatic email forwarding, to help protect information.
- When receiving payment instructions from within your organisation, **verify** payment details with the instructing party in person, where possible.

## What if I fall victim?

- **Call** your bank using a trusted telephone number, such as one from their website, to let them know.
- **Report** the incident to **Action Fraud** at actionfraud.police.uk.
- **Change** the password on your email account, check for any other email accounts that could be compromised.
- **Notify** your suppliers and customers that one of your email accounts has been compromised.