# Checklist: Processing Payments – 1 of 2

It is important to adopt a general mindset of awareness and action in the parts of your business that could be vulnerable. The checklist below has been created to support individuals responsible for making payments and to encourage a culture of fraud awareness.

- ☐ **Ask yourself – is the request unusual or out of context? Does it make sense?** Any email relating to payments or accounts that uses urgent language or provides excuses for the lack of a call back option should be treated as suspicious. If you are not expecting the communication and/or do not recognise the sender, **do not click any links or open any attachments**.
- ☐ **Check that the email address is legitimate**. If the name attached to the email is familiar (someone you regularly correspond with), check to **be sure the email address matches**. Fraudsters will pretend to be reputable individuals. If it's a co-worker, the email address should be listed in the company email directory (if you have one).

  Also, be sure the domain name is spelt correctly. Often, fraudsters will create fake domains that closely resemble the real one but will alter a letter or two so that the recipients don't notice. E.g. J@rnbusiness.com vs J@mbusiness.com. Be aware that the displayed name can be hiding the actual sender's email address.
- ☐ **Question the payment if you are unsure, even if it's coming from senior management**. Fraudsters know you are more likely to act on instructions from senior individuals. As such do not trust payment instructions via email, even if they are from a senior executive or business partner. Fraudsters may also use common messaging platforms to facilitate fraud.

**Remember, the fraudster might have access to the inbox you are corresponding with**

# Checklist: Processing Payments – 2 of 2

Verification of new and amended payment details is vital to limiting the impact of payment fraud and scams. Whilst it’s important to perform callbacks, there are a number of additional considerations to ensure you minimise the risk.

**Verify all new payees and all requests to change account details**
Check with the instructing party using known contact details. Where possible, try to speak to the individual accountable individuafor the change in details. If it is from a supplier and you speak to your normal contact, ask them to confirm with the accountable I via telephone. Remember, the fraudster might have access to the inbox of that individual, so validating the instructions via email could mean the response is coming from the fraudster!

- Don’t reply to the email or invoice, use contact details within the email. If the fraudsters have gained access to soe else's account then they will likely change the contact details and you could end up speaking to thmeone fraudster.
- Call the requesting party; do not rely on them calling you. Fraudsters know that a call-back could be part of the process so might try to navigate this step by contacting you first.

**Remember, the fraudster might have access to the inbox you are corresponding with**