How to minimise fraud risk when making payments

Minimise payment fraud risk

There are steps every business can take to minimise payment fraud and scam risk that do not need to be complicated or expensive. Everyone has a role to play.

- Foster a sense of vigilance in the parts of your business that could be vulnerable.
- Educate employees about how to identify and avoid scams, and make sure they are aware of the company's security policies and procedures.
- Query any request that is unusual or out of context.
- Critically, **any new payee or account details need to be verified through known sources (known contact and phone numbers) that business has established prior to the request.**
- The next few slides provide more detailed guidance to support individuals responsible for payments.

Check the email address

Fraudsters will pose as reputable individuals.

- If the name attached to the email is familiar (someone you know or regularly correspond with), check **to be sure the email address matches.**
- If it's a co-worker, the email address should be listed in the company email directory (if you have one).
- 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 hoping that recipients don't notice. For example, J@rnbusiness.com vs J@mbusiness.com.
- Be aware that the displayed name can be hiding the actual sender's email address.

Check the email thoroughly

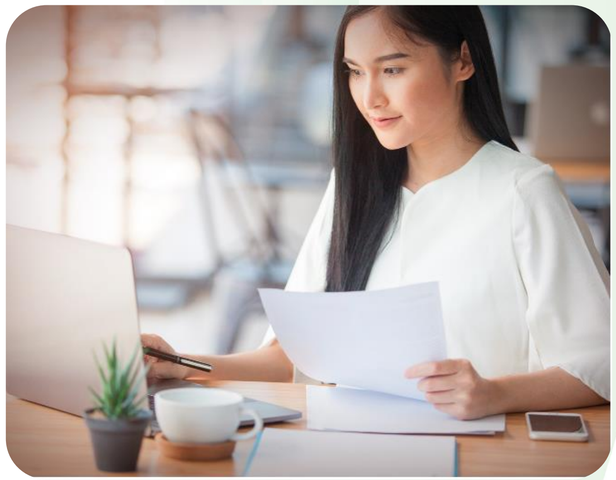
Urgency is a red flag.

- Treat any email relating to payments as suspicious if it uses urgent language, or provides excuses for the lack of a call back option.
- Some phishing emails are poorly written. Even if the spelling is correct, they often contain poor grammar. Treat external emails with extreme caution, especially those containing links or attachments. Be aware that Generative AI is making it easier for attackers to create convincing malicious emails.
- If you are not expecting the communication and/or do not recognise the sender, **do not click links or open attachments**.

Verify new payee or change of account details

Check with the instructing party using known contact details.

- Where possible, try to speak to someone you know. For example, if the change request is coming from someone within the business, try to confirm it directly with that individual via telephone. If it is from a supplier, speak to your normal contact via telephone. Remember to also check the sort code and account number.
- Don’t reply to the email or use contact details within the email or invoice.
- Often, cybercriminals are sending phishing emails to individuals in the contact lists of the account to which they’ve gained access. That means you may recognise the sender because the email address is accurate, though the message itself is suspicious. Calling your contact verifies the request in the email. It may also alert them that their email account has been compromised.



Minimise the risk of payment fraud

Fraud can happen to any type of business and in many different ways.

Create and embed clear security procedures for payment teams

Ensuring all payments are properly validated is the most important action in fraud prevention. Create a procedure to prevent payment teams authorising new or amended payments without proper validation. Following this procedure should mean that payment teams never move money based solely on unverified email or telephone instructions, even when they appear trustworthy. Best practice is to encourage staff to contact payees directly to confirm new or amended payment requests.

Raise employee awareness

Provide employees with adequate training. Fraud awareness is everybody's responsibility within an organisation. Create a risk-based culture and have a procedure for staff to escalate concerns to management. Staff should feel able to challenge and query instructions.

Consider your digital footprint

Sharing too much information via social media platforms also allows scammers to gather information about you, your friends, family and contacts, and can be used to social engineer or impersonate you. Be less of a target by limiting the personal information you post.

Encourage all staff to think before they click

It's fine to click on links when you're on trusted websites. However, avoid clicking on links that appear in unverified emails and instant messages. If you hover over a link, you will be able to see the hidden URL and verify its legitimacy. Double check email addresses and look out for poor spelling and grammar before clicking on any links or downloading any attachments.

Strengthen your passwords

Consider password managers or using a passphrase – a string of words that is typically longer than a traditional password. Passphrases are easy to remember but very difficult to crack. Encourage employees to choose three random words and to select a mixture of alpha-numeric characters and symbols.

Know what do in an event of a fraud/cyber-attack

If you or your company fall victim, it's important to act quickly. Reporting known or suspected security incidents helps protect the workplace. Contact your financial institution.