

INVOICE FRAUD

HOW DOES IT WORK?

Someone pretending to be a supplier, creditor, or provider approaches the university. The fraudster requests that the bank details for a recurring payment be changed to a different account. The new account in question just happens to be controlled by the fraudster.



WHAT CAN YOU DO?

- Verify all requests purporting to be from your creditors, especially if they ask you to change their bank details for future invoices.
- Do not use the contact details on the letter/fax/email requesting the change. Use those from previous correspondence instead.
- 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).
- 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.
- Set up designated Single Points of Contact with companies to whom you make regular payments.
- Restrict information that you share about your employer on social media.