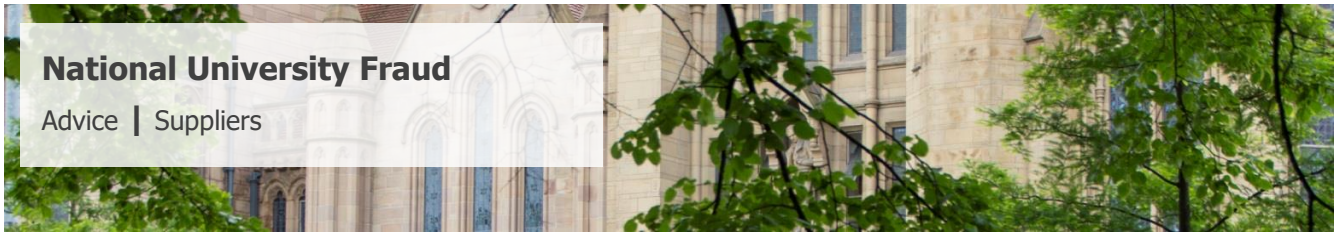

We want to alert you to a **fraud** that is targeting existing and potential suppliers of goods to many Universities in the UK.

The main victims are not the Universities but hundreds of organisations across the UK and Europe. In the UK alone it is estimated that the sums run into £Millions.

The scam

1. A supplier will receive an email or phone call requesting a quotation for goods – on extended payment terms
2. Once the quotation has been provided, a purchase order is emailed to the supplier that is similar to an authentic University purchase order.
3. The purchase order typically instructs delivery to an address that may or may not be affiliated with the University
4. After shipping the goods, they are collected and despatched, usually abroad.

Identifying Fraudulent Emails & POs

The following will be evident in these fraudulent emails and purchase orders:

1. An incorrect domain name (incorrect email extension) will be used to send emails and purchase orders. - **At first glance these fraudulent domains may appear genuine.**
2. Suppliers must always ensure that the email address is genuinely the university email address.
3. Delivery addresses will typically be a **self-storage facility or freight forwarders**, often nowhere near the University.
4. In some cases the delivery address may be a genuine university address, which is later changed or redirected

NEVER **contact the name/number used on the email/purchase order.**
ALWAYS **contact through the main University switchboard**

For High value orders please refer to the Universities guidance on Public Procurement.

We advise all suppliers to consult with their IT or cyber security advisors to ensure they remain vigilant and informed on how to identify suspicious requests.