An Important Message for Suppliers: Fraud Alert

UKUPC
UK Universities Procurement Consortia

We want to alert you to a fraud scam that may target existing and potential suppliers. Please take the necessary precautions so that you are not a victim of this scam.

The scam operates in the following way:

1. A supplier will receive an email or phone call requesting a quotation for goods. These may be in large or small quantities and of low to high values.
   - The email may request confirmation of shipment to a specific location (e.g. London).
   - Request acceptance of 30 day payment terms.

2. Once the quotation has been provided, a purchase order is emailed to the supplier that bears resemblance to an authentic purchase order.

3. The purchase order typically instructs delivery to an address that may or may not be affiliated with the Customer.

4. After shipping the goods, the supplier never receives payment and is unable to retrieve the shipped goods.

Identifying Fraudulent Emails & POs:

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

1. An incorrect domain name (i.e. an incorrect email extension).

2. The delivery address may not match the business. Fraudulent addresses will typically be a domestic residence or a self - storage facility. Or, the delivery address may be a genuine business address, which is later changed or redirected.

3. Use of a false or unknown contact from the business.

4. The email may use names of the senior management team.

5. Phone numbers not associated with the business may be used.

6. Various quantities may be requested but many will be for large orders.

7. The email will often be poorly written with grammatical errors.

8. Rush to ship priority or overnight.

Please do not attempt to call any phone numbers contained within the fraudulent emails as they may attract a service charge or be listed at a premium rate.