Procurement Matters

University of London Procurement Team Guidance & Information

September 2017

Fraudulent Emails & Purchase Orders

An Important Message For Existing & Potential Suppliers to the University of London

We want to alert you to a fraud scam that is targeting existing and potential suppliers of equipment to the University of London, as well as other Universities and businesses, nationally and globally. 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 specific item/s of equipment. These may be in large or small quantities and of low to high values
2. Once the quotation has been provided, a purchase order is emailed to the supplier that bears resemblance 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 item/s of equipment, the supplier never receives payment and is unable to retrieve the shipped products

Identifying Fraudulent Emails & POs

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

1. An incorrect domain name will be used to send emails and purchase orders. Ensure you verify the order is valid with the University and only accept orders from nominated individuals as per your agreed contract. We advise all suppliers to consult with their IT or cyber security advisors to ensure they remain vigilant and informed on how to identify a suspicious communication
2. The delivery address may or may not be a University address. Fraudulent addresses will typically be a domestic residence or a self-storage facility, often not anywhere near the University. Or, the delivery address may be a genuine university address, which is later changed or redirected
3. The email will often be poorly written with grammatical errors
4. Use of a false or unknown contact from the University. If requests for quotations or purchase orders are received from a new University contact that raises your suspicion, please contact a member of the Procurement Team to verify the validity of the request. Do not contact the name/number used on the email/purchase order
5. The e mail may use names of the University's senior management team or Board of Trustees as contacts – note that senior managers and Board members will never be the first point of contact in a purchasing query
6. Phone numbers not associated with the University may be used
7. Various quantities may be requested but many will be for large orders
8. Rush to ship priority or overnight

UNIVERSITY OF LONDON

If you are ever unsure about a quotation request sent by email, or the subsequent purchase order, please contact the University of London Procurement Team or a known University contact. Please do not attempt to call any phone numbers contained within the fraudulent emails that purport to be University numbers as they may attract a service charge.

What the University is Doing

- The University is reporting all instances of known fraudulent activity to the Police via Action Fraud
- We are compiling evidence for all reported incidents. If you have received any suspicious emails we would also be very grateful if you forward to procurement@london.ac.uk so these can be added to the evidence
- We are contacting existing suppliers that may be subject to this type of fraudulent activity in order to raise awareness and provide basic guidance on how to deal with it
- Keeping relevant University of London staff members aware of all activities and updates to this situation

Caroline Heckscher
Procurement Director
Finance and Planning
University of London
Senate House, Malet Street
London
WC1E 7HU