UNIVERSITY OF CAMBRIDGE

4th January 2023

Fraudsters are targeting our suppliers – don't get caught out

In the most recent Government report, 27% percent of UK businesses reported that fraudsters had tried to obtain funds by impersonating them (source: gov.uk). Sadly, The University of Cambridge is no exception.

Here's what we know about the latest scam that's been targeting our existing and potential suppliers – along with some tips on how to avoid falling victim to it.

What's the scam?

The fraudsters target a prospective University supplier with an email or telephone call requesting a quote for an order of goods – typically, although not always, on attractive or high-value items like IT or audio-visual equipment.

Often, they'll say they want the goods shipped to a specific location and ask for 30-day payment terms. The supplier gives a quote, and the fraudsters send them a fake University purchase order, which can often be quite convincing.

The purchase order typically instructs delivery to an address that may or may not be affiliated with the University, or a generic self-storage facility. The goods are delivered, but the supplier never receives payment, and the shipped goods can't be recovered from the delivery address.

What the University is doing

The University is reporting known instances of fraudulent activity to the Police via Action Fraud and compiling evidence on reported incidents. To help with this, **please forward any suspicious emails to the Procurement Services team.**

The University is also contacting any existing suppliers who may be at risk of this type of scam and providing regular updates to any University of Cambridge staff members who may come across this in their roles.

How to spot a potential scam

Here's what to look out for:

An incorrect domain name or email address – genuine University of Cambridge emails will come from an address ending with 'admin.cam.ac.uk' or 'cam.ac.uk'. If you receive an email or purchase order from an email address that doesn't look like this – or doesn't come from a nominated individual as per your agreed contract – please contact the Procurement Services team to verify the order.

A suspicious delivery address – fraudulent addresses will typically be a domestic residence or a self-storage facility, often nowhere near the University. More sophisticated scams may use a genuine university address, which is later changed or redirected.

A suspicious phone number – fraudsters will typically call from a telephone phone number that isn't associated with the University. You should never attempt to call any phone numbers contained in a suspicious email, as they may attract a service charge or be listed at a premium rate.

A poorly written email – scam emails often have bad spelling and grammar.

A false or unknown contact from the University – if you receive a request for a quotation, or a purchase order, from a new University contact that raises your suspicion, please contact the Procurement Services team – don't use any contact details from the suspicious communication.

The name of members from the University's senior management team or Council – contact details for the University's senior management team and Council can often be found in the public domain, but they will never be the first point of contact in a genuine purchasing query.

Priority or overnight shipping – fraudsters will often put pressure on a supplier to ship an order very quickly.

We advise all suppliers to remain vigilant and informed on how to identify a suspicious communication by consulting with their IT or cyber security advisors.

Remember, if you're ever unsure about a University of Cambridge quotation request sent by email, or the subsequent purchase order, please contact the Procurement Services team.