Fraud still on the rise

This year's Annual Fraud Indicator report, published by PKF, Experian, and the University of Portsmouth, has estimated that the annual loss to the UK from fraud could be in the region of £193 billion, with over £37 billion of that attributed to the public sector. While estimates of fraud can only ever be that – estimates – owing to its hidden nature, the report still makes sobering reading. Particularly worrying is the 21% increase in Phishing attacks next year – despite it essentially being a very basic trick – and unfortunately one that is being targeted at universities.

Source: Matt Sisson, Projects and Communications Manager, British Universities Finance Directors' Group (BUFDG) 08/06/2016 by

Attempts to raise purchase orders on behalf of the University

Here's a selection of previous experiences from other universities, which have been reported on the BUFDG Fraud discussion board.

29 Jan 2016

The fraudster pretends to be working at the University and tries to raise a Purchase Order to a supplier to look like it is from the University. The delivery address in this case is the other side of the country so the supplier spotted it before any goods were sent.

5 Feb 2016

The fraudster is using other domain names that are very similar to the genuine University domain name, they are typically approaching companies of medical and electronic equipment, most of which are not suppliers to the University, making an initial enquiry for a quote by email using a variety of contact names, some fictitious and some real University employees. They follow it up with a fake Purchase Order giving a delivery address that has nothing to do with the University. They are using multiple domain names and addresses so this is a concerted effort by the fraudster.

17 May 2016

Three suppliers, with which we have no relationship, contacted us this morning after receiving an email purporting to be from the University's Procurement Team. The email was a request for quotations for some high value goods (lab/medical goods).

The three suppliers who contacted us noticed the email address did not seem legitimate, but obviously we don't know how many other companies have been contacted and have not noticed this, as the email address does look similar.

HM Revenue & Customs tax rebate scam

Fraudsters are texting members of the public offering a tax rebate. The text message contains a link to a website and requests to provide personal information, such as bank account information, to claim the non existent rebate. **Protect Yourself**

- Don't click on web links contained in unsolicited texts or emails.
- Never provide your personal information to a third party from an unsolicited communication.
- Obtain the genuine number of the organisation being represented and verify the legitimacy of the communication.
- HMRC will never use texts or emails or tell you about a potential rebate or ask for personal information.

Source: Action Fraud Alert 23 Apr 2016

Forged changes to suppliers bank account details

We have been notified of a number of frauds and attempted frauds involving forged changes to suppliers' bank account details documentation. Examples have used headed supplier stationery, included the university's customer reference number and also been supposedly signed by the supplier's Director of Finance.

The sums of money involved have been quite significant and institutions from across the country have been targeted. Although we are not aware that the frauds are linked, a number have involved construction companies presumably because payments to such suppliers tend to be larger.

We ask all institutions to be alert to this fraud risk and briefly review the controls that they have over changes to supplier details, and ensure that mitigating action is taken where necessary to minimise any fraud risk (for example, by independently verifying with the supplier the change to supplier details before it is actioned).

Source: HEFCE Fraud updates

Guidance from the University's bankers (Lloyds)

We all need to be vigilant to protect ourselves and our business from online fraud. Here are some hints and tips to help your business stay safe.

Think before you respond - beware of screen pop ups that ask you to: log on as another user; perform a software update or download new software; or enter card reader codes. Occasionally we take our online service down for maintenance. Before we do we will give you notice of this; so you will never see a 'maintenance is taking place' message on our website.

Code of silence - we will never ask you to use your LloydsLink card and reader to generate codes on the phone, by email or through a pop up when you try to log on.

Check who you are paying - be extra vigilant regarding the source of your emails. Fraudsters will send emails posing as trusted beneficiaries or colleagues asking for urgent payments to be made. Do not click on any links or provide any details of your Online Banking information. We would always suggest verifying any new beneficiaries, or change in beneficiary details, directly with the requestor or via another communication medium before you make a payment.

Source: Richard Ahern, Director of Fraud and Financial Crime, Lloyds Bank

The University needs your help to stop fraud. For more information visit:
https://leedsbeckett.ac.uk/-/media/files/partners/governance-and-legal-services/compliance-and-legal/anti-bribery-policy/counter_fraud_and_antibribery_policy.pdf

If you have concerns, or think you may have witnessed a fraud, contact:

Caroline Thomas, University Secretary
Tel: +44 (0)113 812 7007 Email: C.M.Thomas@leedsbeckett.ac.uk