LCFS NEWSLETTER

Your Counter Fraud Service **April 2016**

In this issue:

Please report any concerns or suspicions you may have.

You will be helping to protect NHS funds.

Fraud Awareness Survey – The Results Are In!

We would like to thank everyone that took part in our Fraud Awareness Survey. This year we received an excellent **35** responses representing approximately **62%** of NBT's workforce.

We have provided some key highlights below:

64% of the respondents knew where to find the CCG's Anti-Fraud and Bribery Policy. Clearly we need to do more to improve awareness and we will continue to work alongside the Communications Team to publicise this Policy.

We asked those who had attended awareness sessions to rate them out of 5 (5 being excellent). **96%** of rated the presentation as 3, 4 or 5! This is extremely encouraging and we will continue to update and improve our sessions welcoming any feedback.

Disappointingly however, **27%** either could not remember attending, or had never attended a fraud awareness presentation. **28** respondents indicated that they would like the LCFS to come to a future team meeting.

However the survey, which is anonymous, did not provide your contact details. If you would like the LCFS to come to your team meeting please get in touch! Our contact details are on the back page.

We will continue our efforts to ensure that all staff have received some form of fraud and bribery awareness.

We asked staff 'how would you rate the CCG's stance on fraud and bribery'. **100%** of respondents rated the CCG's stance as 3, 4 or 5 (rigorously pursued); while this is encouraging, it also reflects the need for more to be done to demonstrate the CCG's approach to tackling fraud and bribery.

This year's survey suggests that there is a general knowledge of fraud and bribery with most staff understanding the importance of raising any suspicions to the LCFS.

Thank you again for taking part and providing your input!

Email Phishing Scams

Phishing is a type of email scam, whereby victims are targeted from seemingly genuine persons or services, with the aim of tricking you to either provide personal details or click on something that will allow the attacker to do something you may not be aware of.

Some examples might include an email:

- Claiming to be from a bank requesting you log into your account - a link provided will direct you to a website that looks very similar to the genuine site, but records all your key strokes such as your password;
- Stating that you have been charged for a service you did not use, with an attached document that is supposed to be an invoice - upon opening the attachment a virus is installed on your the computer without your knowledge; or
- Appearing to come from a senior person within your own organisation - this requesting a payment is made urgently into a particular bank account.

What should you look out for in an email?

The Sender: Were you expecting this email? Not recognising the sender is not necessarily a cause for concern, but look carefully at the sender's name - does it appear legitimate, or is it trying to mimic something you are familiar with?

The Subject Line: Often alarmist, hoping to scare you into an action without much thought. It may promote a way to 'get rich quick' or you have won a luxury prize. They may use excessive punctuation.

Any Logos: The logo may be of a low quality if the attacker has simply cut and pasted from a website. Is it even a genuine company?

The 'Dear You': Be wary of emails that refer to you by generic names, or in a way you find unusual, such as the first part of your email address. However, do not forget that your actual name may be inferred by your email address.

The Language Used: Look out for bad grammar or spelling errors, but bear in mind modern phishing looks a lot better than it used to. Many phishing campaigns originate from non-English speaking countries, but are written in English in order to target a wider global audience, so word choice may be odd or sound disjointed.

London Mental Health Worker Jailed for £297,000 Right to Work Fraud (NHS Protect)

A mental health worker who used false documents to get a job in the NHS has pleaded guilty and immediately been jailed for 15 months at Snaresbrook Crown Court, London, after an investigation by local NHS fraud specialists.

On 25 February 2016, Francis ADEKOLA, 57, pleaded guilty to a total of six accounts of fraud and forgery under the, Fraud Act (2006), Theft Act (1968), Forgery and Counterfeiting Act (1981) and Identity Documents Act (2010).

ADEKOLA was employed as a Band 3 Social Therapist at the Newham Centre for Mental Health in East London, and was arrested at his workplace in January 2016.

He was employed for 10 years at the Newham Centre for Mental Health, earning nearly £300k in gross salary including extra bank shifts. During this time, ADEKOLA presented three false passports - two British and one from the Ivory Coast - to his employers as proof of his identity.

Suspicions were raised during a routine document checking exercise. Copies of the passports were sent to the Home Office's National Document Forgery Unit for further checking, which confirmed that all three documents could not be relied upon as evidence of ADEKOLA's nationality. Further checks revealed that ADEKOLA was a Nigerian national and had no legal right to remain or to work in the UK.

The Department for Work & Pensions confirmed that the National Insurance number he had provided did not exist, and his National Insurance card was also a forgery.

Kevin Cane, Area Anti-Fraud Manager of NHS Protect, said: 'The NHS and public expect the highest standards of probity and honesty from its employees, especially those working with the vulnerable. ADEKOLA's sentence sends a message to others who might consider entering the NHS on false papers'.

Be Aware of Signature Identity Fraud (Professional Security Magazine)

Beware of fraudsters that turn up on your doorstep and ask for your signature, warns the National Fraud Intelligence Bureau's (NFIB) Proactive Intelligence Team.

Your signature could be the final piece to a fraud - once they get hold of it, the fraudsters could drain your bank account or commit identity crime. Your identity is a precious commodity; you should take every precaution to ensure that it is not abused or stolen.

A convicted fraudster who was recently interviewed said: 'If we want to get someone's signature, it's really easy. All we do is put on a fluorescent coat or vest, knock on the door and ask the person to sign for a letter or a flyer. They don't need signing for, but nobody ever questions why and we don't hang around for a chat! Once we have the signature, we can make changes on their bank accounts and authorise fraudulent money transfers'.

Not expecting a delivery?

The police suggest:

- Be suspicious;
- Question what you are signing for;
- Look for official identification and if you do sign, just print your name; and
- Check your bank and financial statements carefully and report anything suspicious to the bank or financial service provider concerned.

Your Counter Fraud Contacts

Brendan Harper LCFS

Tel: 07917 790112

brendan.harper@mazars.co.uk or

brendan.harper@nhs.net

Shelly Rai LCFS

Tel: 07788 301124

Shelly.Rai@mazars.co.uk or

Shelly.rai@nhs.net

Report NHS fraud
0800 028 40 60
NHS Protect