COUNTER FRAUD NEWSLETTER

AUDIT YORKSHIRE
The journey to excellence

October 2021

Welcome to the October 2021 edition of our newsletter. Please feel free to contact your Local Counter Fraud Specialist for advice on any type of fraud, you will find our details on the last page.

Current Scam Trends

Microsoft Teams Invite Fraud

A new phishing email tactic has been spotted at local NHS organisations over the last few weeks. Staff from several organisations received an email stating they needed to join a Microsoft Teams meeting immediately in order to receive urgent instructions about an incident which had occurred.

The email was designed to look like a genuine meeting request and included a link for recipients to click. It is likely that clicking on the link would have resulted in the member of staff being asked to "sign in" to Teams by entering their NHS email address and password. This is very likely to be an attempt to hijack NHS email accounts and to steal passwords. The email was sent from an email account ending @nhs-uk.bar which is not an official NHS email suffix, and did not include a date or time for the meeting.

Please be aware that this is a new tactic and that fraudsters may continue to send similar emails using different wording. Phishing emails often use time pressure (such as the use of words like "immediately" and "urgent") to encourage you to act quickly. If you think you have received a dodgy meeting invite, you can report it to spamreports@nhs.net or speak to your Local Counter Fraud Specialist for advice. If you think your NHS.net email password has been compromised, you can change your password on the NHS Portal. If you have concerns about another work email account please contact your IT team.

DPD/Courier Text Scam

There has recently been a prevalence of text message scams purporting to be from courier firms. Recipients are sent a text message from a UK code (+44) mobile number which start with the firm's name. A typical example will read:

> *'DPD: Your package has a £2.99 delivery fee. To pay this now visit https://dpd.rearrange-parcel-gb473889.com. Package will be returned to sender if unpaid'*

At first glance, the message may appear official, but on examination it is designed to get the recipient to pay the 'delivery fee.' Although the £2.99 fee sounds reasonable, the real intention is to lift your financial information.

Be on your guard and do not click any links. If you are expecting a parcel from DPD, or UPS or Hermes etc., please use the official Apps or websites of those companies for any tracking or queries.

NHS Spear Phishing Email

A member of staff at a Trust has received two identical emails warning her that her mailbox has been blocked and asking her to click on an 'activate now' link to avoid interruption.

This email had all of the hallmarks of a spear phishing email – one that targets an individual with the ultimate intention of stealing data.

- The email contained grammatical and spelling errors
- It created a sense of urgency – act now or you will lose your email access
- The link, when hovered over, was not connected to NHS.net mail

If you have concerns about your NHS.net emails, contact helpdesk@nhs.net. For concerns about your organisation's emails, please contact your local IT department.

Covid Pass Scams

Nationally there have been lots of articles covering the risk of Covid-19 Pass Fraud. There have been recent cases of people receiving texts, emails or phone calls which appear on the surface to be from the NHS and offering the recipient "access" to their Covid-19 Pass.

The NHS Covid Pass is free of charge, as is the NHS App. The NHS will never ask for your payment or financial details. Anyone wishing for advice around the Covid Pass can visit www.nhs.uk/nhscovidpass for further information.

Cyber Security - Frankenstein Frauds

As you might have noticed from previous newsletters, there are some common threads that connect a lot of fraud attempts. Fraudsters have a bag of tricks that they tend to draw on when they're crafting a spam call, text or email. They pick and choose from this collection of tactics (amongst others) to try and create the ideal scam. Common features of a scam include:

- **S**poofing - disguising their details to appear as if they are your bank or an official organisation.
- **P**ressure - using apparent authority, threats and/or time pressure to encourage you to act quickly.
- **O**ffers - offering you exclusive access to a juicy discount, or free vouchers for a big name brand.
- **O**fficial Branding - official logos are easy to lift and insert into fake emails.
- **K**nown initiatives/behaviours - exploiting public interest in the vaccination roll out, assuming that people will be expecting a delivery/parcel when sending out "missed delivery" texts.
- **Y**our curiosity—trying to lure people into opening links or attachments by suggesting important information has been included, such as the Microsoft Teams scam described on the first page.

If you receive a call, text or email which you're not sure about take some time to explore whether any of the strategies above may have been used. At home, you can forward spam texts to 7726 and you can report suspicious emails to report@phishing.gov.uk. At work, you can forward suspect emails to spamreports@nhs.net. You can find more information on the Take 5 to Stop Fraud website.

Did you Know?

How to report fraud at work

If you suspect that a fraud is taking place within the workplace, you need to report it. You don't have to know all of the details of what is happening – **if you think something is wrong, please let us know**.

Contacting your Local Counter Fraud Specialist (LCFS) is a good place to start. Details of your LCFS can be found at the end of this newsletter.

The NHS Counter Fraud Authority also provide a 24/7 confidential reporting line (0800 028 4060). If you leave an anonymous report, we ask that you include as much detail as possible to allow us to look into your concerns.

Occasionally, we may not be able to deal with your report if it does not relate to fraud against the NHS, but don't worry, we will be able to assist in directing you to the most appropriate agency to deal with the matter, such as Action Fraud or the local police.

Any report made to us is dealt with in the strictest confidence.

Please bear in mind that we may not be able to keep you updated with the results of our investigations. This is due to confidentiality legislation.

If you do suspect a fraud, please do not discuss it with anybody else – including your manager. This is because more people may be involved than you thought. The fewer people who know about it gives us the best possible chance to preserve evidence and hold offenders to account.

We also ask that you do not confront the person you think is committing the fraud, or try to conduct your own investigations. There are strict guidelines in relation to how crimes are investigated and your LCFS is qualified to undertake them.

Please be assured that any reports made will offer employment rights as per the Public Interest Disclosure Act 1998. Please see your organisation's Whistleblowing Policy for further details.

To make a referral, or for any further advice, support or information, please do not hesitate to contact your LCFS. We are here to listen to your concerns and to take action where necessary to protect vital NHS funding.

If you have a concern about something but you don't think it relates to fraudulent behaviour, your organisation will also have a Freedom To Speak Up Guardian.

More details about the Freedom to Speak Up Guardian can be found on the next page where we look at their role and how they may interact with the Local Counter Fraud Specialist if and when appropriate.

Did You Know? (Part 2)

Whistleblowing

It is essential that any organisation gives staff the freedom to speak up about any concerns they may have about risk, malpractice or suspected wrongdoing- speaking out or reporting your concerns is also known as 'whistleblowing.'

With that in mind, it can be observed that a culture must be created and promoted which allows staff to be confident that they have the freedom to speak up.

Of course, Freedom to Speak up (FTSU) Guardians have a key role in helping to raise the profile of raising concerns in their organisation and provide confidential advice and support to staff in relation to concerns they have.

FTSU Guardians don't get involved in investigations or complaints, but can help to facilitate the raising of concerns where needed. The Guardian will liaise directly with the trusts nominated Counter Fraud Specialist where required to ensure the correct reporting procedure is followed.

The benefits of having a whistleblowing procedure are huge; 50% of tips come from employees and 39% of all frauds are identified from these tip offs- not just in the NHS, but across all organisations.

The NHS is committed to a safe and fair workplace and honest employees are highly valued.

Just one person's behaviour can tarnish the efforts of a whole organisation. It is important to remember that we all have a responsibility to report behaviour that puts the safety of patients or the reputation of the NHS at risk.

We appreciate that you may feel worried about possible negative consequences of whistleblowing; that you may be disbelieved, resented by colleagues or even bullied for speaking up.

We would like to assure you that these worries are very unlikely to manifest as reality; counter fraud will treat all disclosures made in the strictest professional confidentiality and will always seek to safeguard your interests as an honest member of staff who is trying to do the right thing.

If you do wish to report fraud, bribery, corruption please contact your Local Counter Fraud Specialist - their details are at the bottom of this newsletter.

In the Press - Fraud Hotline Launched

At home, you can report suspicious text messages by forwarding them to 7726 and emails by sending them to report@phishing.gov.uk. A new fraud reporting hotline has now been set up by a number of major banks and telephone companies.

The pilot scheme is designed to help you to double check calls you receive. The 159 service can be contacted if someone calls you claiming to be from your bank, asks you to transfer money, or to discuss any other financial matter with you and they appear to be suspicious.

To access the service, you just need to dial 159 from your phone. This will connect you to the service and you will then be able to check whether the call you received is genuine, if your bank is participating. To date, about 70% of current account holders are covered as Barclays, Lloyds, Halifax, , Natwest, Bank of Scotland, Royal Bank of Scotland, Ulster Bank, Santander and Starling Bank are signed up.

At the moment, the service is live to call if your telephone provider is a member of the pilot scheme. Current suppliers who have signed up include BT, EE, Plusnet, Gamma, O2, GiffGaff, TalkTalk, Three, Virgin Media, Sky and Vodafone.

If the pilot scheme is successful, the intention is to establish 159 as a universal number that is available for customers of all banks and telephone networks.

Details about the new service can be found on the Stop Scams website: 159 - Stop Scams UK Please remember that 159 will never call you. Only a fraudster would object to you calling 159.

At work, fraud matters should be reported to your Local Counter Fraud Specialist. Our details are on the next page. Alternatively, you can report your concerns to the NHS Counter Fraud Authority using the details in the contacts list on the next page.

Counter Fraud Training

MORE DATES ADDED - Fraud Prevention Masterclasses

The LCFS team are currently scheduling a series of Fraud Prevention Masterclasses, covering key fraud risks within different areas. The masterclasses are delivered via Microsoft Teams and will last around 45 minutes to 1 hour. **Due to popular demand, some additional Recruitment Fraud sessions are now available in December and January.**

The sessions are being delivered on a monthly basis, and cover some key areas that have very specific fraud risks. They include an overview of the various risks which may be encountered, real life case studies and practical advice on the prevention of fraud risks.

If you have an interest in any of the topics below and would like to sign up for a session, please get in touch with Rosie Dickinson (rosie.dickinson1@nhs.net)

Recruitment Fraud

Ideal for staff with responsibility for pre-employment checks.

5th November 10-11
15th December 2-3
11th January 2-3
4th February 10-11

Payroll Fraud

Ideal for payroll staff who are new or would like a refresher.

10th November 11-12
12th January 2-3
11th February 10-11

Creditor Payments

Ideal for staff in accounts payable or who deal with invoices/suppliers.

15th November 10-11
10th December 11-12
14th January 11-12
18th February 10-11

NEW

Cyber Enabled Fraud

Tactics used by Cyber Criminals to target us at home and at work.

2nd December 10-11
8th December 2-3
14th December 1-2
20th December 11-12

How to Contact your Local Counter Fraud Specialist

If you would like more information or advice about fraud and the latest scams, or to raise a concern please feel free to contact your Local Counter Fraud Specialist. You can find our contact details below:

Steve Moss, Head of Anti-Crime Services	Steven.moss@nhs.net 07717 356 707
Marie Hall, Assistant Anti-Crime Manager	Marie.Hall15@nhs.net 07970 265 017
Rosie Dickinson, Local Counter Fraud Specialist	Rosie.dickinson1@nhs.net 07825 228 175
Lee Swift, Local Counter Fraud Specialist	Lee.Swift1@nhs.net 07825 110 432
Shaun Fleming, Local Counter Fraud Specialist	Shaunfleming@nhs.net 07484 243 063
Nikki Cooper, Local Counter Fraud Specialist	Nikki.cooper1@nhs.net 07872 988 939
Richard Maw, Local Counter Fraud Specialist	R.maw@nhs.net 07771 390544
NHS Counter Fraud Authority Fraud and Corruption Reporting Line	0800 028 4060 https://cfa.nhs.uk/reportfraud