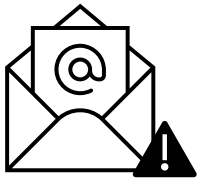
Counter Fraud Newsletter – December 2022

Welcome to the December edition of the Audit Yorkshire Counter Fraud Newsletter for NHS employees. You will find a guide to reporting concerns and contact details for the Local Counter Fraud Specialist team on the last page.

Current Scam Trends

"Unsubscribe" email scams



There have been reports of people receiving emails which are either harassing, i.e. lots are sent close together, or for websites they'd rather not be seen to be viewing, such as those with an adult content. A common tactic has been for an email to be sent advising there are private messages for the recipient to view on an adult dating website. Within this fake email will be a button to click to 'unsubscribe' from receiving future similar emails.

The aim is to get the person to click the 'unsubscribe' button which will either release malware or open a form on which they are asked to provide personal details. These details can then be used to commit fraud offences.

If you receive an email from a company you have not signed up to, do not click on any links or attachments.

If you are receiving lots of emails to try and entice you to hit the unsubscribe button, either block the sender or report as spam in the 'more actions' setting within the email.

Companies House

There has been an increase in concerns regarding information being logged onto Companies House recently. There have been cases of fake companies registering themselves at random addresses – including residential addresses across the UK. Following this, identities can be stolen, or business loans and overdrafts can be drawn. You can read more about this on the Guardian website.

Unfortunately, there is minimal vetting for information which is published on Companies House. There is an economic crime bill going through the House of Commons which is suggesting changes to how Companies House is managed. This will also give Companies House more enforcement powers and to verify information.

You can access Companies House and check that your name and your house haven't been registered for fraudulent purposes – just enter your postcode in the search bar.

If anyone contacts you and claims to be from Companies House, you can contact them on 0303 1234 500 to verify if the call has been genuine.

Information for Staff

A Reminder about Secondary Working

In November the BBC reported that some NHS Trusts were paying up to £2,500 per shift for agency cover, in response to stretched services and staffing shortages.

The BBC reported that it has also seen evidence of aggressive marketing by agencies, which take a cut of the shift pay, with one boasting it is the "best" time to try it, because the fees that can be commanded are increasing.

As the cost of living puts pressure on household finances, people may consider picking up bank and agency shifts. It is important that all staff follow their organisation's policies around secondary employment. In particular:

- You will need to disclose your intention to work elsewhere to your line manager. This is likely to be reflected in your organisation's Standards of Business Conduct or Conflict of Interest Policy, and may also be mentioned in your contract of employment. If you tell your line manager in conversation, you may wish to follow this up with an email to provide an audit trail should one be required.
- If you are signed off sick, it could be viewed as fraud if you work bank or agency shifts during your sick leave. You should tell your GP about your secondary role so that their advice on your fitness to work at each job can be captured on your fit note.

Beware Spoofing Software

When you receive a phone call, your screen will display the caller's details – but can you really believe what you're being shown?

You shouldn't put too much trust in the number you see flashing up on your screen, as it may not be genuine. Fraudsters are able to use "spoofing" software which disguises the number they are really calling from.

Fraudsters can choose to display a completely different phone number, such as a bank's customer services number. They can also place a "name label" over their phone number, so that the caller ID displays whatever text the fraudster wants. Often, they will set it to appear that you are being contacted by a trusted organisation like your bank's customer services team or a police force. During the call, they may even invite you to check that the number or caller ID showing on your phone matches the organisations publicly listed contact number to "prove" that they are genuine.

As we've recommended in the past, if you get any calls from people claiming to be calling from your bank or the police (or other trusted organisations) and asking you for information or to take action, it's best to hang up. You should then either wait for 30 minutes, or use a different phone to get in touch with the organisation through a trusted route. This is because fraudsters can use software to jam your phone line – so although you think that you've hung up, when you try to make a call you are reconnected to another scammer.

Police shut down iSpoof website used by scammers and arrest 100 suspects

In late November one hundred people were arrested in the UK's biggest fraud investigation. The arrests brought down a website described as a "one-stop spoofing shop" used by scammers to steal tens of millions of pounds from Britons via fake bank phone calls.

It is estimated that more than 200,000 potential victims were targeted via the iSpoof fraud website, which was taken down by Scotland Yard's cybercrime unit with the help of the authorities in the US and Ukraine.

At one stage almost 20 people every minute of the day were being contacted by scammers hiding behind false identities created using the site. It is estimated that criminals using iSpoof may have stolen close to £50m.

One victim alone was scammed out of £3m, while the average amount stolen was £10,000. It is estimated that those running the scam website made about £3.2m over a 20-month period.

Fraudsters paid iSpoof for a service that allowed them to disguise their phone number and pretend to be calling from a credible organisation, such as a bank or the tax office. The scammers used bitcoin to pay for the service.

The fraudsters would then trick people into handing over money or giving them access to their bank accounts. In the year to August around 10m fraudulent calls were made globally via iSpoof, with about 3.5m of those made in the UK. Of those, 350,000 calls lasted more than one minute and were made to 200,000 individuals.

The criminals who paid iSpoof for their services believed that they were anonymous. However, that was not the case, and more than 100 people have been arrested as part of Operation Elaborate so far, predominantly in London.

Investigators infiltrated the website – which was set up in December 2020 and had 59,000 users – and discovered 70m rows of data and bitcoin records. This allowed them to begin to trace the suspects.

Police have a list of 70,000 UK phone numbers who they believe were targeted by iSpoof fraudsters. The Metropolitan Police were due to contact potential victims via text on the 24th and 25th of November 2022. Unfortunately, the fact that they are contacting victims by text could give fraudsters an opportunity to impersonate the police and to try and further defraud people. The police have therefore warned that if you receive a text saying you have been a victim of this scam **after** the 25th of November, **it will not be a genuine text from the police**.

Anyone who is not contacted by the Met but believes they have been the victim of a number-spoofing scam should report the incident to Action Fraud.

The police force said it plans to use the Proceeds of Crime Act to recoup the money where possible.

In the Press

Pharmacy Worker who Defrauded Employer of £1.3m Sentenced
Darren MacKenzie worked for his friend, who owned a chain of pharmacies in Somerset. He was originally taken on as a medicines counter assistant, and over time was given more responsibility – including dealing with finances for the pharmacy where he worked.

Over a 10 year period, MacKenzie abused that position in order to siphon over £1.3 million from the company. He spent the money on over £300k worth of renovations at his home, designer goods, and luxury holidays.

The owner of the pharmacy chain had viewed MacKenzie as a "little brother" and had taken him in when he had been experiencing personal problems. As a result of MacKenzie's actions, the owner had to cut staffing hours whilst working 16 hour days 7 days a week, and two colleagues went without pay in an effort to keep the business afloat.

MacKenzie has been sentenced to 5 years and 8 months in prison, and will face proceedings under the Proceeds of Crime Act to see if any of the money which he took can be recovered. You can read more about the case on the ITV site.

Fraudster who impersonated nurse jailed

In May 2020 Maria Davis approached a partially-sighted man and introduced herself as "Claire Taylor". She informed him that she was a registered nurse and offered to do his shopping for him. The victim, who also has learning difficulties, gave Davis his bank card. Davis later called and claimed that contactless payments weren't working, which led to the victim providing her with his PIN number. Davis then used his card to make cash withdrawals and to pay for cigarettes and scratch cards.

The victim's care workers noticed that over £1,000 was missing from his bank account and raised the alarm. Davis has been sentenced to 8 months in prison after admitting six counts of fraud. You can read more on the Mirror website.

Counter Fraud Training

Fraud Prevention Masterclasses

Our Fraud Prevention Masterclass Programme covers key fraud risks which may be encountered at work. Training dates are listed below. We are planning to deliver sessions until February 2023.

All of the sessions are delivered by Microsoft Teams and last roughly 60 minutes.

If you would like to be informed of any future sessions please don't hesitate get in touch by contacting your LCFS. To make a booking, please contact audityorkshire@york.nhs.uk.

General Fraud Awareness	1st December 10am-11am	6th February 10am-11am
Fraud Awareness for Managers	24th January 10am-11am	14th February 10am-11am
Cyber Enabled Fraud	11th January 10am-11am	1st February 10am-11am
Creditor Payment Fraud	18th January 2pm-3pm	8th February 2pm-3pm
Recruitment Fraud	13th December 2pm-3pm	21st February 10am-11am
Payroll Fraud	6th December 2pm-3pm	16th February 2pm-3pm

Open offer for bespoke training/fraud awareness input

The counter fraud team is always happy to put together bespoke training for your specific role or department. We are also happy to attend any team meetings to introduce ourselves and talk about NHS Fraud.

If you would like to arrange a session for your team, please contact one of the Local Counter Fraud Specialists (our details are on the next page).

A Quick Guide to Reporting Fraud Concerns

I have a concern that fraud may be being committed against the NHS

You can **contact the Counter Fraud team** using our details below. You can also report your concerns to the **NHS Counter Fraud Authority** via their online reporting tool or hotline. If you making an anonymous report, **please give as much detail as possible** as we won't be able to contact you for more information.

I have a concern that fraud may be being committed against the general public

These concerns can be reported to **Action Fraud** (0300 123 2040). If someone has been actively defrauded, it may also be appropriate to report to the **police**. If it is suspected that the victim's bank account has been compromised, they will need to **speak to their bank as a matter of urgency**.

I have received a suspicious email to my NHS.net email address.

Do not click on any links or attachments.

Forward the suspect email **as an attachment** to **spamreports@nhs.net**. To do this, click on the "More" button which is next to the "Reply, Reply All, Forward" options. Choose "Forward as Attachment".

I have received a suspicious email to another email account (not NHS.net)

Do not click on any links or attachments.

Forward the email to **report@phishing.gov.uk.** You can use this option for any suspicious emails you receive on email accounts that are not NHS.net accounts.

I have received a suspicious text message

Do not click on any links in the text message!
Forward the text message to **7726.**

I have come across something and I'm not sure whether it is fraud-related

You are very welcome to contact the **Counter Fraud team** for advice and support, our details are below.

How to Contact your Local Counter Fraud Specialist

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
Rich Maw Local Counter Fraud Specialist	R.Maw@nhs.net 07771 390 544
NHS Counter Fraud Authority	0800 028 4060 https://cfa.nhs.uk/reportfraud