

Counter Fraud Newsletter – September 2022

Welcome to the September 2022 edition of our Counter Fraud Newsletter for NHS staff . Please feel free to contact your Local Counter Fraud Specialist for advice on any type of fraud .

Current Scam Trends

National Insurance Number Phone Calls

The Department of Work and Pensions (DWP) has issued a warning about a scam call which is doing the rounds. The call works by using an automated calling system which plays a recorded message if you answer the phone. The recording will say that your National Insurance number has been compromised and that you need to press 1 to be connected to their help team. If you press 1, you will be connected to a fraudster who will pressure you for personal information to “prove” your identity.

The DWP have highlighted that they will never use automated calling systems or recorded messages if they need to speak to you. If you receive a call like this, simply hang up without pressing 1.

Cost of Living Payment Advice

To assist with the cost of living, some households will receive extra support this autumn/winter. This includes payments which are due to be made to those who currently receive tax credits and/or disability benefits, and pensioners in receipt of the winter fuel allowance.

Unfortunately, the Department of Work and Pensions (DWP) has become aware that scammers have been trying to defraud people who are eligible to receive these payments. The DWP have released the following advice for people who are eligible for the payments:

- You do not need to apply for the payment
- You do not need to call the DWP
- Payment will be made automatically
- DWP will never ask you for personal details via SMS or email

The DWP recommend that if you receive a text message asking you to apply for a cost of living payment, that you forward the message to 7726. This is a free service that allows you to report scam text messages.

Sim-swap scam

This happens when a fraudster gathers information about you and contacts your mobile phone provider pretending to be you. They then get the mobile network provider to transfer your phone number to a different sim card which they have control of. They may do this by pretending to be you and claiming that your sim card is damaged or lost.

By doing this, the fraudster will then receive text messages and calls which were intended for you. This could include one time use passcodes to access apps.

The following are signs that could suggest that your sim card has been diverted:

- You can no longer make phone calls or send texts from your phone
- You are alerted that you have activated your phone or sim card on a different device
- If you have multi factor authentication set up (for example, you receive a passcode via text to access your online banking) this stops working

- There are unauthorised transactions on your bank statements

If you suspect that you have had your sim swapped, contact your network provider and bank immediately.

More information can be found in this article: [SIM swap fraud explained and how to help protect yourself | Norton](#)

Cyber Security

Refreshed Guidance from the National Cyber Security Centre – Recovering Hacked Accounts

The National Cyber Security Centre (NCSC) has recently refreshed their guidance on what you should do if you find one of your accounts has been hacked. Losing control of an account can be a stressful experience. The NCSC guidance looks at the steps that you can take if you find one of your accounts has been hijacked.

Some signs that suggest your account may have been hijacked include:

- Being unable to log into your accounts
- Changes to your security settings
- Messages or notifications sent from your account relating to activity you don't recognise
- Logins or attempted log ins from strange locations or at unusual times
- Unauthorised purchases or financial transfers from your online accounts

You can read the NCSC guidance on [their website here](#).

In the Press

NHS Qualification Fraudster Ordered to Repay £96,000

Jon Andrewes was convicted of fraud in 2017 after it was found that he had lied about his qualifications to get a series of senior NHS roles. Andrewes dishonestly claimed to hold a PhD, a first class honours degree, and an MBA from Bristol University. He had also lied about his work experience. Andrewes was found out when discrepancies between the CVs he used at different NHS organisations were noticed.

He was found guilty at court and was originally ordered to repay over £96,000 to the NHS. Andrewes appealed the order and managed to get it overturned. The Court of Appeal ruled that he could keep the money he had been paid during his NHS employment. In response, the Crown lodged their own appeal with the Supreme Court, who have now ruled that Andrewes should repay the £96, 737.24 as originally ordered by the court. You can read more about the case on the [Totnes Times website](#).

Prison Sentence for Fake Sea Captain Holiday Fraudster

Jody Oliver has been sentenced to 6 years in prison after defrauding victims of £320,315. Oliver had perpetrated his scam by dressing up as a Captain of a cruise ship. He would tell victims that he could get them heavily discounted holidays. He would make it seem real by producing fake contracts and paperwork, and by sending emails that he designed to look like they had come from Carnival Line employees who did not exist. He would later state there was an issue with security

or a problem with the ship to delay or cancel the holiday.

Oliver committed the offences whilst he was out on bail for VAT fraud charges. He had also spun a web of lies in his private life. You can read the full story on the [BBC news website](#).

Counter Fraud Training

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.

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. 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 or not it is fraud related.

You are very welcome to contact your Local Counter Fraud Specialist for advice and support, our details are below.