COUNTER FRAUD NEWSLETTER

AUDIT YORKSHIRE
The journey to excellence

September 2021

Welcome to the September 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

Covid-19 Vaccination Passport Scams

Several local news outlets have published warnings about Covid-19 Vaccination Passport scams which are continuing to do the rounds. Reports about this type of scam usually relate to text messages which have been received stating the recipient is "eligible" to apply for a vaccine passport. The text message contains a link which will take you onto a phishing website where personal and financial information is requested.

If in doubt, you can find advice on how to access your Covid-19 Vaccination Passport on the official NHS website. Please remember you do not have to pay for this service: NHS COVID Pass - NHS (www.nhs.uk)

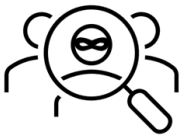
Fake Vehicle Tax Emails

Which? Have warned that phishing emails claiming the recipient has not taxed their vehicle have been popular over recent months. The emails are well designed to appear as though they have come from an official source—either from the DVLA or from the GOV.UK gateway.

You can see some examples of how convincing these emails are by visiting the Which? article which also provides advice from the DVLA :

Vehicle tax phishing emails remain a threat – Which? Conversation

Cyber Security Tips - Social Engineering



When a cyber criminal wants to gain access to a system or an account, they have numerous options to consider. They may look at hacking or using a brute force attack to get into the system. This approach relies on having appropriate technical knowledge and equipment in order to succeed.

An alternative strategy is to manipulate people into accidentally allowing them into secure accounts or systems. Cyber criminals rely on social engineering to help them do this.

An example of this is using official branding and logos on phishing emails, to make the contents of the email appear to be legitimate. If the recipient thinks the email is genuine, they are more likely to open up links and/or attachments contained with the message.

The links included within these emails will lead you to a phishing website. These websites are also cleverly designed to appear genuine. The phishing website will ask you to "verify your identity" by sharing personal data such as your name, address, date of birth, phone number etc.

They may also ask for a small payment to be made. For example, in the recent "missed parcel delivery" scams, people are asked to make a small payment of around £1.50 in order to rearrange the delivery. The low value of this payment is also a form of social engineering.

Because the value of the payment is low, it is easy to assume that the risk of making the payment is also low. People may believe that the worst that can happen if the email turns out to be dodgy is that they have lost £1.50. However, the scam isn't really about getting that £1.50 payment from you, it's about persuading you to hand over your bank details.

If you consider a parcel redelivery scam, the fraudsters will have asked you to confirm your full name and address. This will have seemed plausible, as they are claiming to have a delivery intended for you. If you fill in the payment details, they also receive your card number, card expiration date and security code. Your name, address and bank details can then be used to place orders without your knowledge.

The phishing email and website can also be the starting point for a secondary scam which develops at a later date. In a few weeks, you might get a call from "your bank" alerting you to suspicious orders having been placed. The first 6 digits of your bank card number can be checked online to find out which bank your account is with. When the fraudster calls you, they will say they're calling from your bank, and will start listing out transactions which they know you did not make. This can panic you into thinking the call is real, and transferring money into the fraudsters account thinking they are trying to help you.

The best defence against social engineering is to be suspicious and to take your time. If you receive an email or text message which contains a link or attachment, think carefully about whether you may be dealing with a fraudster. If in doubt, do not click on anything. Instead, contact the organisation who appears to be contacting you using an official customer service phone number.

ESR Fraud Remains Prevalent

ESR remains an attractive target as it holds a lot of sensitive (and therefore valuable) data, as well as containing your pay details.

These emails are highly likely to try and steal your ESR log in details in order to divert your pay into a fraudsters bank account and to steal personal data for use in further fraud offences (e.g. to make expensive purchases or to set up finance agreements etc. without your knowledge, or to try and compromise your NHS email account in order to target colleagues).

Some common tell-tale signs of phishing emails include; poor grammar, lack of personal greeting, use of pressure (authority/urgency/time-limited offers), hidden links, unexpected attachments or unusual email addresses being used.

Please do not click on links or attachments if you are not certain that an email is genuine.

If you receive something like this and you're not sure if it's real, you can find support by opening your web browser and typing in the web address for ESR (https://my.esr.nhs.uk) or you can contact your Local Counter Fraud Specialist.

If you are certain you have received a fraudulent email, you can report this internally by forwarding the message as an attachment to spamreports@nhs.net

Doctor Struck Off for Working Whilst Sick

Dr Joao Muel has been struck off the medical register for behaviour which was described as being "fundamentally incompatible with being a doctor" by the Medical Practitioners Tribunal Service.

In 2018, Muel had told his employer that his diabetes had left him too sick to work. He went onto sick leave and received sick pay. However, during his sick leave, he took up 17 bank shifts at other Trusts. In 2019 he was found guilty of committing fraud, and received a Community Order.

In 2019, Muel applied for a new post at a different health board. However, he failed to notify them that he was facing a fitness to practice investigation.

The Medical Practitioners Tribunal Service panel stated that Muel's dishonest conduct had been "pre-planned and sustained" and that it involved "substantial payments". The service found that his fitness to practice was impaired by misconduct and a conviction. He has now been erased from the register.

Jail Sentence for £1.5 Million NHS Compensation Fraudster

Darren Dommett has been jailed for 29 weeks after he was convicted for contempt of court. Dommett had lodged a compensation claim against the NHS, alleging that a delay in treating a nerve condition had resulted in him being severely disabled.

In 2013, Dommett had gone to hospital due to a compressed nerve in his back. It took several days for his condition to be diagnosed as Cauda Equina Syndrome and for treatment to be delivered.

In 2015 Dommett lodged a claim against the NHS regarding the failure to diagnose and treat his spinal condition in a timely manner. The Trust had admitted liability in 2016 after which Dommett claimed damages of around £1.5 million.

Dommett claimed that he required constant care and supervision, that he had to use a wheelchair due to severe mobility issues, and that he was barely able to walk. He stated he was unable to work and when he was assessed at home, he demonstrated that he couldn't stand up unassisted or manage the stairs.

The size of the compensation claim drew suspicion, and surveillance footage was captured in which Dommett was seen unloading large boxes of flat pack furniture from a van by himself. This included a glass topped table which he moved on his own. Photographs of Dommett on a family holiday in Spain without his wheelchair or other walking aids were also spotted on social media.

Dommett admitted that he had lied about the severity of his condition during previous court hearings regarding his compensation claim. Dommett was sentenced to 29 weeks in jail and has been ordered to repay £20,000 which he had received in compensation payments, as well as being required to pay £65,000 to the NHS to cover their court costs.

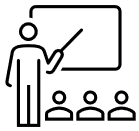
Counter Fraud Training

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.

11th October 10-11
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.

15th October 11-12
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

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