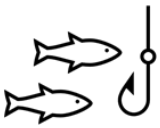
COVID-19 FRAUD ALERTS

Welcome to Issue 7 of our Covid-19 Fraud Alert newsletter.

We have summarised recent fraud trends in this newsletter for you to be aware of. Please feel free to contact your Local Counter Fraud Specialist for advice on any type of fraud, our details are on the last page.

NHS Related Alerts

NHS Organisations Targeted by Mandate Fraud



Mandate fraud is the practice of impersonating a genuine supplier in an attempt to get their bank details altered on payment systems, ultimately diverting payments for invoices. This type of fraud has been really popular throughout the Covid19 pandemic, with the NHS representing a particularly attractive target. In recent months, fraudsters have impersonated various NHS suppliers.

Mandate fraud is often committed via email. Tell-tale signs of mandate fraud usually include:

- The email may appear to have come from an established contact, but their email address has been altered slightly (e.g. joe.bloggs@yoursupplier.com becomes joe.bloggs@yoursupplier.net)
- Other contact details (such as phone numbers included in email signatures) are slightly altered - usually digits are swapped or deleted, or their phone number is completely different from normal
- The email may address you by an incorrect name or there may be a lot of grammatical errors

Please note that fraudsters are becoming more sophisticated in their attempts to commit this type of fraud. They will copy genuine email signatures and use official company logos, and may even hack into legitimate email accounts so the signs above may not be present.

If you are in doubt about the authenticity of an email which is asking for payment details to be updated or pushing for urgent payment of an invoice, **please report it**. You can find our contact details on the last page of this newsletter.

We have put together a 30 minute training session on mandate fraud and phishing in the NHS which can be delivered via Microsoft Teams. It covers practical advice on what to look out for and what to do if you have concerns. If you think your team would benefit from this, please contact one of the team using the details on the last page.

NHS Staff Targeted by Coronavirus Fraudsters

Computer Weekly have revealed that almost 30,000 fraudulent emails were received by the NHS during the height of the coronavirus pandemic. It is worth noting that these figures are based on emails which were reported, the true figure is likely to be much higher.

A Freedom of Information request revealed data from NHS Digital showed almost 30,000 malicious emails were reported in March and April 2020.

The article highlights that several payroll attacks were noted, which lured staff to click on malicious links in order to verify their personal details and ensure payment of their salaries. Please be wary of emails of this nature. If in doubt, visit ESR by typing the web address into your browser rather than by clicking on links in emails. You can read the full article here.

Fraudsters Carrying Out Fake "NHS Survey" Calls

The NHS Counter Fraud Authority has become aware of a fraudulent survey which is being conducted with the aim of harvesting details of vulnerable people. Fraudsters have been calling members of the public and asking them to complete an "NHS Survey" on elderly care and requirements. This includes taking their personal and financial details.

Age UK have reported that following receiving a phone call of this nature, one vulnerable elderly person was then visited by a fraudster who claimed to be from a genuine NHS service. The fraudster then attempted to sell the person thousands of pounds of "NHS equipment".

If you become aware that a member of the public has received a similar call, please encourage them to report the matter to Action Fraud and their bank/the police if they have provided financial details or made any payments to "NHS" visitors.

Staying Safe Outside Work

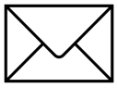
Test and Trace Scam Calls Warning

You may have recently seen posts on social media warning the public about fraudsters pretending to be from the NHS Test and Trace Service. Calls will often start out in a plausible manner—alerting you that you've been in close proximity to someone who has now tested positive, and asking if they can take your address in order to send you a testing kit.

The fraudster will then ask for a payment card, stating that there is a one-off fee for the kit and the test results. Normally they will state that the cost is around £50. If challenged, they may attempt to apply pressure by claiming that you will be fined if you do not get tested.

Please be reassured that there is no cost for NHS testing kits. If you receive a call asking you to pay for a testing kit please hang up. Find out more about the signs of an NHS Test and Trace scam here.

Council Tax Discount Scam Warning

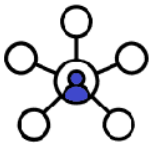


Members of the public are being warned of a new phishing scam which claims you are eligible for a government-funded tax cut. The email is marked up to look like it has come from the "Government Digital Service Team" and promises a "Council Tax Reduction" of £385.50.

The email requests that the recipient provides the details of their debit or credit card in order to receive payment.

If you receive an email of this nature, please do not click on any links or provide your card details. You can report the email to report@phishing.gov.uk.

Trading Standards Report on Covid-19 Fraud Risks



Trading Standards have released a report on the likely tactics which will be used to defraud consumers. They have highlighted that there are several areas which are likely to be exploited by fraudsters in the Autumn and Winter, including:

- Copycat government websites mimicking initiatives like the Green Home Grant announced earlier this year
- Websites and social media posts offering "miracle cures" including products they claim will treat corona virus or offering to accelerate test results
- Fake refund websites offering "assistance" for getting refunds on holiday bookings or insurance claims

You can read more from Trading Standards here.

Flu Vaccination Scam Warning

The seasonal flu vaccination programme has been significantly increased this year to try and reduce the number of potential flu patients. This may result in a repeat of the flu-jab scams which were identified last year.

Last winter, vulnerable members of the public were targeted by fraudsters who pretended to be calling from the NHS regarding their flu jab. Those being called were persuaded to part with their bank details, after being told they needed to make a low value payment to cover the cost of the syringe, vaccine or for the cost of a member of NHS staff making a home visit to administer the jab.

In some cases, a fraudster physically attended the home address of the person, and persuaded them to share their bank details during the visit. People who are contacted about their flu jab should check that it is their surgery contacting them. If they are spoken to about a home visit, they should hang up and call their GP practice directly.

In the News...

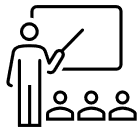
Man who Stole from Nurses During Covid Pandemic Jailed

During the pandemic, a thief attended a series of hospitals and care homes in Birmingham and stole from members of staff. This included entering restricted areas to gain access to steal mobile phones and purses belonging to ward staff, as well as taking a laptop from a Children's Hospital and tablets from a care home. He has now been sentenced to four and a half years imprisonment. You can read more about this story here.

Please remember to keep your belongings and places of work secure, and don't be afraid to ask for identification if you spot someone out of place in your department.

Counter Fraud Training

Training Sessions



A central part of your Local Counter Fraud Specialist's role is to raise awareness of fraud within the NHS. This can take many forms but the most successful and popular method for us to do this is via face-to-face training with staff. Thanks to the range of conference calling software now at most people's fingertips, we're able to offer online fraud training.

Our Fraud Awareness training focuses on:

- How different types of fraud affect the NHS
- Practical advice on what to look out for and methods to protect yourself and your organisation from fraud
- Real life case studies showing how the NHS is targeted
- Information on how to report concerns about fraud

This training can be arranged to suit you and will be delivered via Microsoft Teams. It is part of our normal service and can be delivered to groups of any size. We are also able to design and deliver bespoke training packages based on any fraud related areas of concern that you feel are most relevant for your team.

We are currently running a series of mandate fraud and phishing refresher training sessions via Teams. If you are interested in accessing this training, or to discuss other fraud training requirements, please contact the LCFS team using the details below.

E-Learning Module

If you don't have access to Microsoft Teams, we can explore other alternatives to deliver sessions to your team. Alternatively, you can access our E-Learning module which is available here:

https://www.nwyhelearning.nhs.uk/elearning/yorksandhumber/shared/FraudAwareness/HTML/

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 07970 264 857
Richard Maw, Trainee Anti Crime Specialist	R.maw@nhs.net