Covid-19 Fraud Alert Newsletter

Welcome to Issue 12 of our Covid-19 Fraud Alert 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

The following scams have come to the attention of the Local Counter Fraud Team since the last newsletter was published. Fraudsters change their tactics and update their schemes quickly.

Remember, if something doesn't feel right, it probably isn't.

Covid-19 Vaccine Scam Texts

The fraud team have been made aware of a new suspicious Covid-19 text message that has been sent out to patients. The text message tells the recipient that their vaccination was given from a "suspect batch" and asks them to call a mobile phone number urgently. It is possible that calling the number provided could connect the person to a fraudster.

Compromised National Insurance Number Scam Call

There have been growing reports that people have been receiving automated phone calls. A recorded message plays stating that the person's National Insurance number has been "compromised".

The person is instructed to "press 1" to address the problem. If you do press 1, you may be connected to a premium rate number and further targeted in an attempt to steal your financial information, or to persuade you to send money to a fraudsters account.

You may come across variations on this theme—last month we reported that we had been made aware of a similar scam, in which the caller claimed the person's NHS number had been used fraudulently.

Virgin Media Scam Call

A member of staff has made us aware of a suspicious phone call they received in which they were told they had an "unpaid internet bill" with Virgin Media that needed settling.

The call came from 01914 071 621. There have been other scam calls from people claiming to be

Virgin Media and ringing in order to “fix router issues” or “improve speed”. Virgin Media have a page dedicated to scam calls on their customer website.

TV Licencing Phishing Emails

Members of the public have been targeted by phishing emails which claim to have been sent from TV Licencing. The emails ask the recipient to update their account information, and threaten that failure to comply will lead to their account being suspended.

The fake emails can be spotted using the following information:

1. They do not include your name or postcode that would be included in genuine emails from TV Licencing.

2. They are not sent from an official TV Licencing email account. TV Licencing only use two email addresses to contact customers. These addresses are donotreply@tvlicencing.co.uk and donotreply@spp.tvlicencing.co.uk

These sorts of scams can all be reported to Action Fraud. You can report online using their website or you can call them on 0300 123 2040. You can also report spam emails to report@phishing.gov.uk.

In the Press

Lateral Flow Test Thefts

Three men have been arrested after thousands of lateral flow tests intended for schools across Essex were stolen. The kits had been taken from a parked lorry in the early hours of the morning.

Their arrest in early March followed a news article published in The Mirror in February highlighting that stolen lateral flow tests were being sold online. Tests were being sold at various prices ranging from £45 to £400, on various selling sites.

The tests are all marked with unique lot numbers, so they can be traced back to the supply chain. Journalists from The Mirror had been able to arrange to purchase 50 lateral flow tests and the matter is now being investigated by the police.

A spokesperson for the Department of Health and Social Care has condemned the action, reinforcing that the tests are designed to save lives and their sale is illegal.

Staff are asked to be vigilant to anyone attempting to tailgate into NHS buildings or store rooms. If Covid-19 lateral flow tests are seen being advertised for sale online, please notify the LCFS team. The tests are made by Innova.

Online selling sites such as eBay, Facebook and Gumtree are taking action against those advertising lateral flow tests for sale.

Doctor behind £67k NHS Fraud Sentenced

Dr Aled Meirion Jones has recently been found guilty of Fraud by Abuse of Position at Cardiff Crown Court earlier this month.

The court heard that Dr Jones had diverted cheque payments that had been intended to be paid to his colleagues. As a specialist registrar, Dr Jones had received cheques paid by a funeral home which were to pay individual doctors who had been involved in providing certificates prior to bodies being released for cremation. The standard fee for completing this work is £82 per instance. In total, Dr Jones was found to have altered 27 cheques provided by the funeral home. and paid the money into his own account

Enquiries also indicated that Dr Jones had also stolen and altered other cheques that had been sent to the hospital. The cheques which he had stolen held a total value of over £33,000. On top of this, he had also made false claims for exaggerated hours and locum shifts that he had not carried out. The total value of his fraudulent timesheet claims was over £34,000.

Dr Jones was found guilty and has been sentenced to two years imprisonment, suspended for two years. Confiscation proceedings have been started with a view to recovering the money lost.

Covid Fraud - £34.5 Million Stolen in Pandemic Scams

The BBC have released an article covering the levels of covid-19 related fraud being attempted over the past year.

The article summarises findings from Action Fraud and the National Cyber Security Centre, who have told the BBC that they are dealing with around 30 “significant attacks” per month against the UK’s pandemic response infrastructure. This includes attempts to breach the NHS, vaccine producers, and vaccine supply chains.

Fraudsters may have many different motives for trying to get into NHS systems. They may be hoping to implant malware (such as ransomware, which encrypts your files and demands a ransom for their release), to gain access to financial or sensitive systems, or to divert payments.

It is vital that all staff remain vigilant and follow the advice, guidance and policies produced by IT teams.

You can access some general advice about staying safe online at work on the “Keep IT Confidential” campaign website, which has been provided by NHS Digital.

Action Fraud Advice Following 15,000 Compromised Accounts

Action Fraud have published advice on securing your social media and personal email accounts after receiving over 15,000 reports relating to hacked accounts in a year.

Access was mostly gained by sending phishing emails that were used to harvest log in data. Action Fraud advises that you secure your email and social media accounts using the following advice:

1. Use a strong and separate password for each account you hold - don't forget your email account!
2. Enable two-factor authentication - this means that even if someone gets your password, they will not be able to access your account.
3. If you cannot access your account, seek advice directly from the company.

For more advice, including how to set up two-factor authentication, see the Action Fraud website.

Counter Fraud Training

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 sessions on Mandate Fraud and Phishing via Microsoft Teams. If you are interested in accessing this training, or to discuss any other fraud training requirements, please contact the LCFS team using the details below.

We are also offering out refresher training for any staff who are responsible for carrying out pre-employment checks for new starters. The pandemic has changed how and when identity documents and qualification certificates are presented. The refresher training provides advice on what to look out for.

To register your interest in a session, or to arrange any other fraud-related training, please contact one of the LCFS team using the details below.

How to Contact your Local Counter Fraud Specialist (LCFS)

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.

Nikki Cooper, Local Counter Fraud Specialist. Nikki.cooper1@nhs.net 07872 988 939.

Marie Hall, Local Counter Fraud Specialist. Marie.Hall15@nhs.net 07970 265 017.