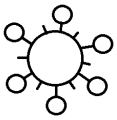
COVID-19 FRAUD ALERTS



Welcome to Issue 10 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

Fraudulent Covid-19 Vaccine Texts

You may have seen warnings circulating on social media about fake Covid-19 vaccination texts. The messages state that the recipient is eligible to receive a vaccination and to follow a web link within the text in order to book their appointment.

The phishing site which has been created is very realistic and uses NHS branding to appear like a genuine NHS website. The recipient is asked for various pieces of personal information as well as their payment details.

You can see screenshots showing examples of the sort of text messages people have received and the layout/design of the phishing page by reading the BBC news article on this scam by clicking here.

In the UK, coronavirus vaccinations will only be available via the National Health Service. You can be contacted by the NHS, your employer, a local GP surgery or pharmacy, to receive your vaccination. Remember, the vaccinations are free of charge and you will not be asked for a payment.

The NHS will never:

- ask for your bank account or card details
- ask for your PIN or banking passwords
- arrive unannounced at your home to administer the vaccine
- ask for documentation to prove your identity, such as a passport or utility bills

If you receive a call you believe to be fraudulent, hang up.

If you are suspicious about an email you have received, forward it to report@phishing.gov.uk.

Suspicious text messages should be forwarded to the number 7726, which is free of charge.

If you think you may already have entered your financial information onto a phishing site, please contact your bank as soon as possible.

Update on a Case - Pharmacist Struck Off after £76k Fraud

A pharmacist in Wales has been struck off the General Pharmaceutical Council register for committing fraud against the NHS, claiming £76,475 by modifying over 1,500 prescriptions.

Michael Grant Lloyd was sentenced to 16 months in prison last year after being found guilty of fraud by false representation.

Concerns about Mr Lloyd's practice were initially referred to NHS Counter Fraud Service (CFS) Wales in November 2017.

It was found that Mr Lloyd had modified more than 1,500 handwritten prescriptions, falsely claiming that a more expensive medication had been dispensed whilst issuing the lower cost version.

The General Pharmaceutical Council noted that although Mr Lloyd has now repaid the money using funds from his own private company, this was not an isolated incident.

They took the decision to remove Mr Lloyd from the register as it was concluded that the public and fellow professionals would find his behaviour "deplorable" and that his removal from the register was necessary in order to "maintain public confidence in the profession".

You can read more about the case here.

HMRC Rebate Scam Alert

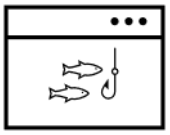
As the end of the financial year approaches, HMRC will provide assistance to those who need to complete a Self Assessment. This includes legitimate tax refunds (also known as rebates) if too much tax has been paid. Unfortunately, cybercriminals are aware that the Self Assessment deadline is approaching and they have stepped up their circulation of HMRC themed scams.

There have been numerous reports of people receiving emails which claim to be from HMRC, and which offer a rebate of £269.23 "as a result of Covid-19 emergency measures". There is also a risk of fake reminder messages or copycat websites masquerading as the correct place to complete a return.

The email contains a link to a phishing site where the recipient is asked to enter their Government Gateway ID and password. Please be aware that there is no Covid-19 tax refund/rebate scheme and that HMRC have confirmed they will not be contacting people using email.

You can read more about HMRC scams using their official website by clicking here and see examples of fake messages in this article from financial advice website, This is Money.

DVLA Phishing Messages Warning



Fraudsters have begun using DVLA branding to carry out scams which ask drivers to verify their licence details, offer vehicle tax refunds, highlight a failed vehicle tax payment and/or ask for bank details.

Customers are advised the only place to access official information on DVLA and its services is GOV.UK. The agency never asks for bank details over email and never sends text messages about vehicle tax refunds. You can read the full article by clicking here.

As well as forwarding any suspicious emails and texts, DVLA has 5 top tips for motorists to stay safe online:

- Never share driving licence images and vehicle documents online
- Never share bank details or personal data online
- Avoid websites offering to connect to DVLA's contact centre
- Only use GOV.UK when looking for DVLA contact details
- Immediately report it to Action Fraud if you think you've been the victim of a scam

As ever, you can report suspect emails to report@phishing.gov.uk and suspicious texts by forwarding them to 7726 free of charge.

Beware "Victim of Fraud" Calls

We have had a local report about a member of staff who was defrauded of £1,000 via a sophisticated telephone call fraud. The victim received an automated call advising them that they were identified as the victim of fraud, and asking them to press 1. When the person pressed 1, they were connected to an individual who claimed to be a police officer. He stated that the victim's ID had been stolen and compromised by criminals operating in the UK and Mexico. He quoted the victims National Insurance number and said a local police officer would call the victim, advising them to Google the phone number for a local police station. A call was then received which appeared to be from the same number. It is very easy to "spoof" a phone number to appear as though you're calling from a legitimate place—and this is what happened in this case.

It transpires that in the month leading up to this phone call, the victim had received a text message which appeared to be from Halifax bank stating there were issues with their bank account. Halifax was mentioned within the call which also made it seem more genuine.

The victim was persuaded to leave work and to purchase £1000 worth of Google Play vouchers, the codes for which were sent to the scammers via WhatsApp. The victim was told they would be sending the codes to the National Crime Agency. The fraudsters also tried to convince the victim to buy more vouchers, but the transaction was declined by the victim's bank. The victim was then pressured to go to a bank to withdraw more money. Luckily, as the victim was on their way to the bank, the call cut off. When the victim rang the number back, they found they were speaking to real police officers who took a report. The victim now has their money back but was shaken up by this incident. This incident was part of a national crime series which Action Fraud and the City of London police have published an alert for. Well over 100 people have been taken in by this fraud so far.

Please be ***very*** wary of these sorts of calls. Remember that phone numbers can be spoofed easily. If you receive a call like this, please hang up and call the police on 101 **using a different phone or after waiting 10 minutes** (in case the fraudsters have jammed the line) to check whether you are recorded as the victim of an ID theft/fraud. Contact your bank using their official number (again using a different phone or after waiting 10 minutes) if you think your financial details have been compromised.

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.

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, contact one of the LCFS team using the details below.

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 / 07484 243 063
Nikki Cooper, Local Counter Fraud Specialist	Nikki.cooper1@nhs.net 07872 988 939
Richard Maw, Trainee Anti Crime Specialist	R.maw@nhs.net 07771 390544