COVID-19 FRAUD ALERTS

Welcome to Issue 8 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 Counter Fraud Authority Warning —Microsoft Teams Emails

The NHS Counter Fraud Authority has been made aware of phishing emails which are circulating and claim to be from Microsoft Teams. The emails appear to be designed to harvest the user's login credentials.

The emails typically advise the recipient that their Microsoft Teams account has been suspended. The email directs them to visit a hoax Office 365 login page.

If the user inputs their login details into this fake Office 365 page, their username and password will be stolen by cyber criminals.

If you receive an email which appears to be from Microsoft Teams stating that your account has been suspended, please treat it with extreme caution.

You can contact your Local Counter Fraud Specialist for advice, and you can read further advice from Microsoft on how to avoid phishing by visiting their help pages here.

ESR Salary Diversion Fraud Risk

Fraudsters are aware that the majority of NHS organisations use ESR to manage employee payslips and personal information. The NHS Counter Fraud Authority recently issued an alert regarding ESR themed phishing emails.

The emails include a link to a fake ESR login screen. If you input your user name and password, your login credentials will be harvested. The fraudster is then able to access your real ESR account and amend your bank details. This would result in your salary being paid directly to the fraudster.

In addition, they can steal other sensitive information such as your full name, address, date of birth, national insurance number and next of kin. This information can then be used in further identity frauds, such as taking out credit cards, loans or phone contracts in your name.

These phishing emails typically contain a threat such as "*you must click on this link and confirm your details or you will not be paid this month*" or a bait, for example "*click on this link to view details of your pay rise*".

If you receive any emails which appear to be from ESR, we recommend that you do not click on any links within the email. Instead, you should open your web browser and navigate to ESR by typing in the web address (https://my.esr.nhs.uk).

If you think you may have clicked on a link to a fake ESR page, you should go to the real ESR site as soon as possible and use the "forgotten password" function to reset your account password. You can then make sure that your bank details are correct.

If you are in doubt about an email you have received and which appears to be from ESR, you can contact your LCFS for advice.

Staying Safe Outside Work

HMRC Investigates 10,000 Covid-19 Scams

HMRC is investigating 10,428 reports of phishing scams designed to exploit the coronavirus pandemic.

HMRC scams have been carried out via text, email and phone call. We have covered many variations of the HMRC scams that have been used in previous newsletters. They include offers of tax rebates due to Covid-19 and phone calls in which the recipient is told they are under investigation for fraud and are threatened with arrest if they do not press 1.

You can read the full article which covers the HMRC investigation by clicking here.

British Gas Phishing Email Results in £12k Loss for Intensive Care Nurse

Unfortunately fraudsters do not care who they target. A nurse who had been working in intensive care during the pandemic was recently targeted by callous fraudsters who cleared £12,000 out of her bank account following a night shift.

The nurse had actually fallen foul of a phishing email a few days earlier, then received a call from the fraudsters who claimed they were from her bank. The caller display on her phone matched the number on the back of her bank card. You can find out more about how this scam was carried out by reading the full article here.

Please remember to exercise extreme caution if you receive a call which claims to be from your bank.

Your bank will never ask you for your PIN, tell you to transfer money to avoid fraud, or be offended if you tell them you are hanging up so you can check the authenticity of the call.

BBC Article Highlights Risks of Spoofing

The BBC recently released an article about a victim of fraud who lost over £25,000 after he received a text allegedly from his bank.

The victim, a former university lecturer who specialised in computer assisted language learning, had received a text message warning him of suspicious activity on his bank account.

The text message had appeared within a chain of text messages he had previously received from his bank.

This was made possible by a fraud technique called “spoofing”. This allows fraudsters to disguise their own number and appear as though they are contacting you from a legitimate customer contact centre.

Spoofing was also responsible for disguising the real identity of the fraudsters who targeted the intensive care nurse from the story above. It is a favourite tool of fraudsters and highlights the importance of not relying too heavily on the information displayed on your phone screen.

The full BBC article contains information and advice on how to protect yourself from similar scams. You can read the full article here.

Fake DVLA Emails Reported

Action Fraud have released information about an email scam which claims to be a warning from the DVLA stating that your vehicle is no longer taxed.

The email contains a threat that if the recipient does not arrange new tax for their vehicle, they will be fined £300. The message also directs recipients to use a credit card rather than a debit card to send payment.

Action fraud received 214 reports regarding this scam over a single weekend. Please be aware of this scam and follow the usual advice on phishing - do not click on any links or attachments if you are being asked for urgent payment. You can make contact with the organisation who claims to have contacted you using their official customer contact details.

New Covid-19 Fraud Hotline Launched

In an initiative between government and the independent charity Crimestoppers, the public can now call a new COVID Fraud Hotline (0800 587 5030) anonymously and free of charge to report suspected fraudulent activity.

Over 150 COVID support schemes have been introduced by the government to help those struggling financially, but a minority of individuals have been abusing these schemes by claiming support illegally.

Chief Executive of Crimestoppers, Mark Hallas OBE said:

> *“Fraud against the public purse denies access to vital funds that benefit us all. It’s crucial that anyone who has information or knows of someone who has fraudulently claimed Government grants or loans to contact our charity completely anonymously and tell us what you know.*
>
> *The COVID Fraud Hotline is open 24/7, 365 days a year on 0800 587 5030 or fill in the simple and secure anonymous form at Covidfraudhotline.org. You’ll be doing the right thing to help ensure the public purse is protected from fraudsters.”*

Counter Fraud Training

Training Sessions

Thanks to the range of conference calling software now at most people's fingertips, we're able to offer online fraud training covering a range of topics. 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.

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
Nikki Cooper, Local Counter Fraud Specialist	Nikki.cooper1@nhs.net 07872 988939
Adele Jowett, Associate Local Counter Fraud Specialist	adele.jowett@nhs.net
Richard Maw, Trainee Anti Crime Specialist	R.maw@nhs.net 07771 390544