Counter Fraud Newsletter – February 2022

Welcome to the February 2022 edition of our Counter Fraud Newsletter for NHS staff. 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

A Reminder - Vigilance Needed

Regular readers will have noticed that there is a strong cyber-fraud element to this newsletter. This is because every NHS email account is a possible target for cyber criminals. NHS email accounts are targeted for a number of different reasons, depending on the motivation of the cyber criminal. They may be trying to:

· Cause damage to NHS IT systems and disrupt NHS services by spreading viruses and malicious software.

· To hold the NHS to ransom by encrypting vital data and charging a fee to release it.

· To gather information to make a financial gain at a later date (e.g. through gathering data on the names of suppliers, invoice numbers, payment due dates, names of other NHS staff to use in a Mandate Fraud, Invoice Fraud, or Salary Diversion Fraud).

· To steal sensitive information about patients and service users which can then be sold on to other criminals.

A lot of these criminal methodologies start with a simple phishing email asking the recipient to click on a link or open an attachment. It is really important that staff are vigilant, and that unexpected emails with links and/or attachments are treated with caution.

If in doubt, please contact your LCFS for advice. You can find our contact details on the last page of this newsletter. If you think you may have clicked on a dangerous link or attachment, please notify your IT team immediately so that steps can be taken to detect and minimise any damage.

Hoax Phone Calls Impersonating IT

The Counter Fraud Team have received a number of reports relating to fraudulent phone calls where the caller has pretended to be from IT over the last few months. These calls have included a few different tactics.

Some callers have been asking for information about colleagues - particularly email addresses. Other callers have instructed NHS staff to type in instructions which they state will “prove” there is a problem with their computer. Another methodology used has been for the caller to try and persuade the NHS employee that their NHS email account password needs to be reset over the phone.

If you are unsure about whether a caller is genuinely from IT, ask for their name and direct dial. Hang up the phone, and contact your IT department or provider using a phone number you know is safe.

If you are certain that a call you’ve received was fraudulent, you can report it to Action Fraud. You are also welcome to seek advice from your Local Counter Fraud Specialist if you are in doubt.

Scam Covid Text Messages

Another month, another Covid-related scam message! One of our team has recently received a new twist on the ever-popular bogus Covid text. This version contained the following wording alongside a dodgy link:

“NHS: You have been with someone who has the Omicron Variant. Order a Test Kit today”

This text message has not originated from the NHS. These messages are designed to trick you into clicking on the link in the text. If you do click on the link, you may be asked to enter personal or financial information, or your device may become infected with malware.

If you receive a text like this, please do not click on any links. You can also quickly report the message by forwarding it to 7726, or by visiting action fraud.

Cyber Security – Watering Holes and Pop Ups

There are lots of strange terms when it comes to cyber security – and Watering Holes are no exception!

Watering Holes are websites that are designed to look legitimate but are used to spread viruses and steal data. They may be fake versions of genuine sites, or they could be official webpages that have been hijacked by cyber criminals.

Visitors to these sites may be tricked into downloading infected files or be faced with alarming pop up messages that try to panic them into making unnecessary payments or downloading viruses. These pop ups can be very disruptive and difficult to close. They rely on causing a sense of panic that makes you more likely to click on something you wouldn't normally interact with.

You may stumble onto a Watering Hole site by accident, or you may be deliberately sent onto one by a link within a phishing email or text message.

Safety tips:

- Make sure your device is updated by switching it off properly at the end of the working day
- If an automatic update requests you to restart your machine, please do so as soon as possible (after saving your work).
- Be wary of unexpected links and attachments on emails.
- On your desktop or laptop it is possible to hover over a link without clicking it, to bring up a grey/white box that will tell you where the link will actually take you (see our example at the bottom of this box).
- Consider how you can verify the sender's details – can you call/message the person on Microsoft Teams or use an established phone number to check they sent you the message and the contents are safe?
- Remember, NHS email accounts can be compromised and even if the email is from a recognised NHS email address, that does not mean it was sent by an NHS employee.
- Do not click on pop ups which appear. To safely close a pop-up window, locate the button in your Taskbar that corresponds to the pop-up. Right click on the button and select **Close**. If this doesn't work, use Ctrl Alt and Delete to open the task manager, identify the task relating to the pop up and click "end task".
- If your browser displays a warning about a website you are trying to access, pay attention to that warning and get your information elsewhere.
- If you are concerned that your device may be infected or compromised, please disconnect your device from the internet and notify the IT team as soon as possible.
- If you are unsure about an email you have received, you can contact your Local Counter Fraud Specialist for support

The “Hover Over” trick in action

You can see in this example that the link claims it will take you to ESR. However, if you hover your mouse over the link (without clicking) a little box will pop up which shows the web address for the link.

In this example you can clearly see that clicking on the link will take you to the Action Fraud website, not the ESR home page as advertised.

It is always worth hovering over links to see if they’re dodgy. Our advice is to always take the long way around. For example, if you got an email with the link above in it and wanted to double check your ESR account, open up a fresh web browser and type the address for ESR into the bar at the top.

In the Press

Doctor struck off after faking his CV in 'elaborate scam'

Hakeem Lateef has been struck off after presenting a fake CV. In 2018, Lateef was trying to gain new employment in the financial sector. He sent his CV to a contact and paid them £100 to update it. The new CV which was produced did not mention Lateef’s 27 years in medicine. Instead, his work history was replaced an alternative version, including 7 years of experience at a variety of major banks. The new CV was sent on to an employment agency. When challenged, Lateef stated that his email account had been hacked, however no evidence of this could be found. The Medical Practitioners Tribunal Service determined that Lateef should be erased from the Medical Register. You can read more about this story here.

Man jailed for more than four years over scam Covid grant texts

Thomas Proudfoot has pleaded guilty to computer misuse, money laundering and fraud. Proudfoot is suspected of being “significantly involved” in selling methods for committing smishing/phishing scams. Proudfoot is believed to have sent out scam text messages offering recipients “Covid-19 Grants” which contained a link to a dodgy website. Proudfoot was found to have committed fraud between June 2020 and July 2021, and has been sentenced to 4 years 8 months in prison. You can read more about the story here.

Scale of Covid-19 Bounce Back Loan Fraud Unfolds

National press coverage has highlighted that the Bounce Back Loans launched during the early stages of the pandemic have been exploited by criminals. A recent criminal case saw six men jailed for their role in an extensive car theft operation. It was noted that one of the gang members (a man with 48 criminal convictions) had managed to secure a £50,000 bounce back loan for a company that did not exist.

In December, two men were jailed for a total of 33 years after their money laundering operation was broken up by the police. £10m of their £70m pot was made up of fraudulent Covid loans. The men were on bail for other offences when they fraudulently applied for Bounce Back Loans.

Did You Know? Theft vs Fraud

As fraud and theft are both criminal offences, it can be easy to get them mixed up. However, knowing the difference can really help if you need to know who to speak to for advice about a crime that has happened.

Of the two, theft is much easier to understand. If someone walks into an empty NHS office and takes £10 out of an unattended handbag without permission, that is theft. The person has just stolen £10. Theft often relies on stealth or force to succeed.

Fraud offences are similar, in that something financially valuable is taken from the victim. However, fraud relies on the criminal persuading their victim to give them something which they do not have a legitimate right to access. For example, a cyber criminal may email you pretending to be from the TV licencing company. They may claim that you're entitled to a refund, and direct you to click on a link and then enter your bank details to allow them to "process the refund". What the criminal has actually done, is to steal your financial data by misleading you into thinking you were applying for a refund.

Fraud in the NHS has lots of different forms. For example:

- A patient submitting travel expenses claims for appointments that didn't take place.
- An employee exaggerating how many hours have been worked on a timesheet.
- A cyber criminal sending emails to Payroll claiming to be a member of staff and asking for their bank details to be updated.
- A supplier deliberately inflating the cost of goods and materials before sending their invoice to the NHS.
- A job applicant falsely claiming to hold an essential qualification when applying for an NHS role.

You can read more about NHS Fraud on the NHS Counter Fraud Authority website.

Counter Fraud Training

The Counter Fraud team are always happy to deliver training and awareness work to staff. This can be in whichever format your team would find most helpful.

We are happy to put together bespoke training to suit your area of work and the risks you're most likely to face during your day-to-day role.

We are also happy to drop into team meetings to introduce ourselves and to give an informal overview of fraud risks affecting the NHS.

If you would like to access any of the above, please don't hesitate to get in touch with a member of the Local Counter Fraud team.

2022/23 Masterclasses

The Local Counter Fraud Team are putting the 2022/23 Fraud Prevention Masterclass programme together. We will be adding two new modules onto the programme, General Fraud Awareness which will be suitable for all staff, and Fraud Awareness for Managers. In addition, the Cyber Enabled Fraud Prevention Masterclass that was available in December 2021 will be added into the regular programme so that more staff can access it.

If you have any suggestions of topics that you'd like us to cover, you're very welcome to get in touch and let us know. You can find our contact details in the section below.

Request for Newsletter Feedback

The Counter Fraud Newsletter has been in this format for 12 months. We would be really grateful if you could let us know what you think. Is the newsletter useful? Are we missing anything that you think would be helpful to include? Would you like to see more or less of anything? If you can spare 5 minutes to fill out the link below, it would be much appreciated. Alternatively, you can email rosie.dickinson1@nhs.net. You can find the Survey here: here

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:

Nikki Cooper, Lead Local Counter Fraud Specialist	**nikki.cooper1@nhs.net** **07872 988 939**
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
Richard Maw, Local Counter Fraud Specialist	r.maw@nhs.net 07771 390544
NHS Counter Fraud Authority Fraud and Corruption Reporting Line	0800 028 4060 NHS Counter Fraud Authority Fraud and Corruption Reporting Line