The Sentinel

MIAA's Anti-Fraud Newsletter Spring 2022

MIAA case features in BBC Fraud Show

With NHS resources fully stretched after a two-year Covid pandemic, it is more important than ever to ensure that the NHS budget (of over £150 billion a year) is not diverted from its proper purpose of services for patients. NHSCFA estimates that more than one percent of this budget is vulnerable to fraud every year, which equates to over £1 billion a year.

Independent production company Brown Bob Productions has been closely working for several years with the NHS Counter Fraud Authority (NHSCFA) and its partners, who present real cases on the show to shine a light on fraud against the NHS budget.

Successful MIAA fraud investigations have featured in series 1 and 2 of BBC's Fraud Squad; now the latest series, available on iPlayer, features another recent case of an NHS manager who sold hospital phones for personal gain and which MIAA has been instrumental in bringing to justice.

This fraud was uncovered after mobile phone company officials made contact with MIAA's Anti-Fraud team. The investigation uncovered fraudulent sales of NHS mobile phones between 2010 – 2018. Over an eight-year period alone the manager had made £8,981 from selling 43 mobile phones. He also gave his son an NHS phone worth £950 and put him on an NHS phone contract, where he ran up a data bill and telephone costs of £4,650.

Roger Causer, MIAA's Anti-Fraud Specialist who investigated the case, said: "*Following an extensive investigation, the case came to court where the manager admitted to three charges of fraud by false representation.*"

continued on next page

In this edition:

Virginia Martin
Anti-Fraud Specialist
☎ 07551 131109
✉ Virginia.Martin@miaa.nhs.uk

MIAA case features in BBC Fraud Show

Roger Causer continued: *"He was given 12 months jail suspended for 18 months, was ordered to payback £16,777 and was given 250 hours of community service. This prosecution shows that any NHS employees found to be misusing their position for personal gain will be held to account for their actions."*

Darrell Davies. MIAA's Regional Assurance Director (Anti-Fraud) commented: "*We are pleased that our successful prosecution is featured in the current series of Fraud Squad. The series helps drive up understanding of the work of all who fight fraud in the NHS system. Previous episodes have resulted in spikes of people reporting their suspicion of fraud to the NHS Fraud and Corruption Reporting line."*

Fraudsters exploit Ukraine crisis to steal money

Fraudsters are pretending to be victims of the war in Ukraine in an attempt to steal money from well-meaning UK residents. Criminals are also exploiting the desire to help victims of the crisis by creating false charity websites to trick people into donating.
Three specific scams have emerged as fraudsters attempt to exploit the situation.

Donation scams
Fraudsters bombard people with emails or text messages encouraging them to give money to victims of the war. The messages include a link to a false charity website. The messages may be directed to people who have previously been tricked, or are vulnerable targets for fraudsters.

Emotional pleas
Fraudsters are creating emotional posts pretending to be victims of the war asking for money.

Requests for assistance to move money
A variation of a common scam in which an individual is supposedly a Ukrainian businessman trying to move money out of the country, and who needs to use a bank account outside the country. This is a well know way for a fraudster to steal bank details and drain the account.

If you wish to support Ukraine, donate via the established website of a well known charity organisation working in the country such as Disasters Emergency Committee
https://www.dec.org.uk/appeal/ukraine-humanitarian-appeal

NHSCFA Chief Executive CEO sets out his vision

Alex Rothwell reflects on the challenges of fighting fraud and calls on NHS leaders to ramp up collaboration.

In a four-page spread, in NHE magazine Mr Rothwell set out his broad vision, NHSCFA faces the challenging years ahead, reflects on the challenges of fighting fraud and calls on NHS leaders to ramp up collaboration.

His message is that he is encouraged by his first few months in the job, but doesn't underestimate the enormity of the task of fighting the criminals, and calls on all partners to ramp up their collaboration.

The pillars of intelligence, prevention, investigation and recovery are all articulated, and he makes the call to action to keep reporting fraud to NHSCFA's reporting lines.

NHE readers are directly called to action too: *"This is what we're collectively up against, and readers of NHE magazine are in a position to make a real difference in this battle. NHSCFA's intelligence experts calculate that over a billion pounds a year of the NHS budget is vulnerable to fraud. What could be happening on your own patch?*"

The CEO makes clear that he is resolute and realistic in facing the problems, drawing on his long experience as a very senior police officer with an ingrained passion for serving the public: *"I intend to add a lot of value to our close, effective working with police forces, the CPS and the justice system as a whole."*

He identifies three standout themes:

- Collaboration
- Working to a clear strategic vision
- The value of empowering people to be brought into that vision

In reaching out to all stakeholders, Mr Rothwell stresses: *"I never forget that the huge majority of NHS workers are unsung heroes, and they are our staunch allies in the fight against fraud."*

His message is also very strong on NHSCFA supporting the local level in an inspiring and empowering way.The CEO closes by thanking the many thousands of NHS people for what they do every day in the fight against NHS fraud and making it clear: *"we are in this together."*

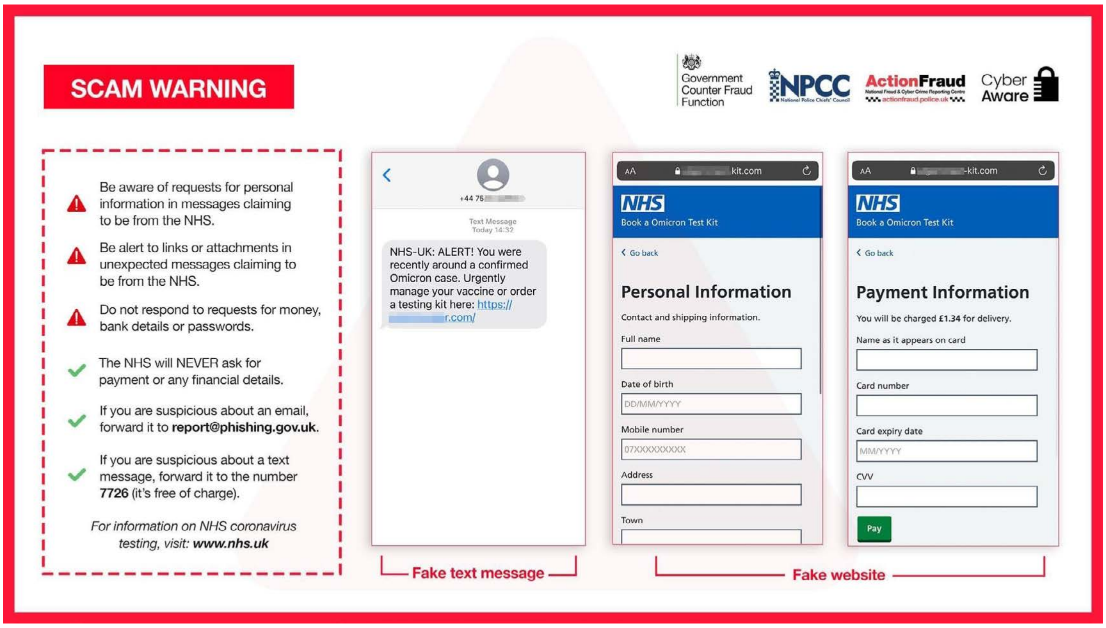
Cyber Fraud & Security Update

Beware of fake NHS text messages

Fake text messages claiming to be from the NHS are still being circulated by fraudsters. Since 1 January 2022, 412 victims have reported losses totalling more than £531,000.

Remember, the NHS will never ask for any payments via a text message.

Here's a reminder of how to spot a fraudulent NHS text message, from demands to reply urgently to requests for personal & financial information.



SCAM WARNING

Government Counter Fraud Function | NPCC National Police Chiefs' Council | ActionFraud National Fraud & Cyber Crime Reporting Centre actionfraud.police.uk | Cyber Aware

- ⚠ Be aware of requests for personal information in messages claiming to be from the NHS.
- ⚠ Be alert to links or attachments in unexpected messages claiming to be from the NHS.
- ⚠ Do not respond to requests for money, bank details or passwords.
- ✓ The NHS will NEVER ask for payment or any financial details.
- ✓ If you are suspicious about an email, forward it to **report@phishing.gov.uk**.
- ✓ If you are suspicious about a text message, forward it to the number **7726** (it's free of charge).

For information on NHS coronavirus testing, visit: ***www.nhs.uk***

+44 75[redacted]

Text Message
Today 14:32

NHS-UK: ALERT! You were recently around a confirmed Omicron case. Urgently manage your vaccine or order a testing kit here: https://[redacted]r.com/

Fake text message

[redacted]kit.com

NHS
Book a Omicron Test Kit

‹ Go back

Personal Information

Contact and shipping information.

Full name

Date of birth
DD/MM/YYYY

Mobile number
07XXXXXXXXX

Address

Town

[redacted]-kit.com

NHS
Book a Omicron Test Kit

‹ Go back

Payment Information

You will be charged **£1.34** for delivery.

Name as it appears on card

Card number

Card expiry date
MM/YYYY

CVV

Pay

Fake website

Increased cyber security vigilance is vital

As a result of the current world events, the National Cyber Security Centre (NCSC) has recommended that all UK organisations strengthen the security of their Information Technology (IT) systems.

There is an increased likelihood of a cyber-attack and a need for all NHS staff to be vigilant and adopt secure practices.

We can all take precautions to increase our cyber security and reduce the risks. Please familiarise yourself and share with colleagues the following advice: -

Be alert to:

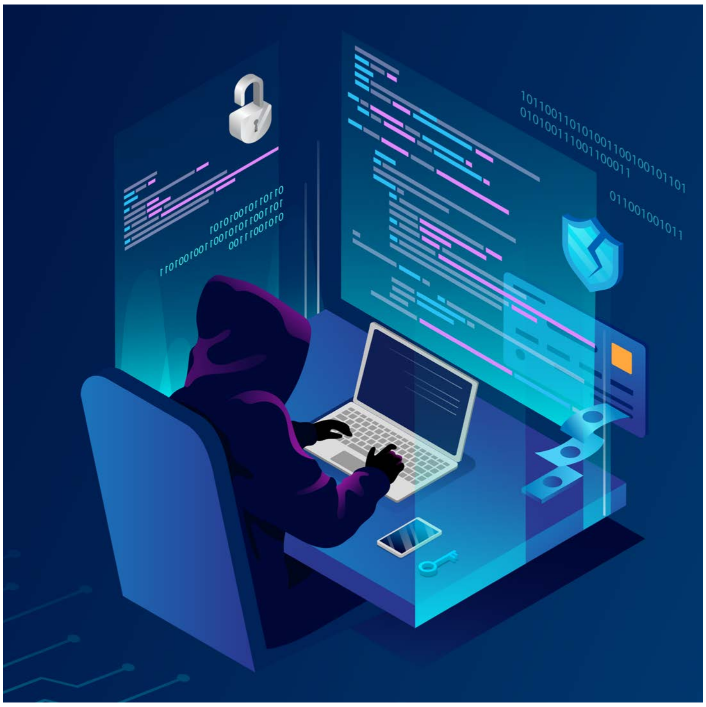
- **Emails containing links that require you to enter your username and password**
- **Unexpected or unusual emails – even from trustworthy email addresses**
- **Emails expressing a sense of urgency**
- **Strange hyperlinks in emails and documents**
- **Unexpected computer behaviour after opening or interacting with an email or document.**

If you are concerned about suspicious texts, forward them to **7726**. 7726 is a number all mobile customers using UK networks can text to report unwanted SMS messages or phone calls on a mobile. The number '7726' was chosen because it spells 'SPAM' on an alphanumeric phone keypad – that's a handy way of remembering it.

Please do not open suspicious emails or click on any of the links they contain. Instead, forward the email to your local NHS IT Team and / or spamreports@nhs.net and delete the original. You can also forward suspicious emails to report@phishing.gov.uk.

Suspicious websites can also be reported here: https://www.ncsc.gov.uk/section/about-this-website/report-scam-website

Please also consider your login credentials. These should be confidential, robust, secure and only to be used where appropriate.



Mitigating insider risk in remote working

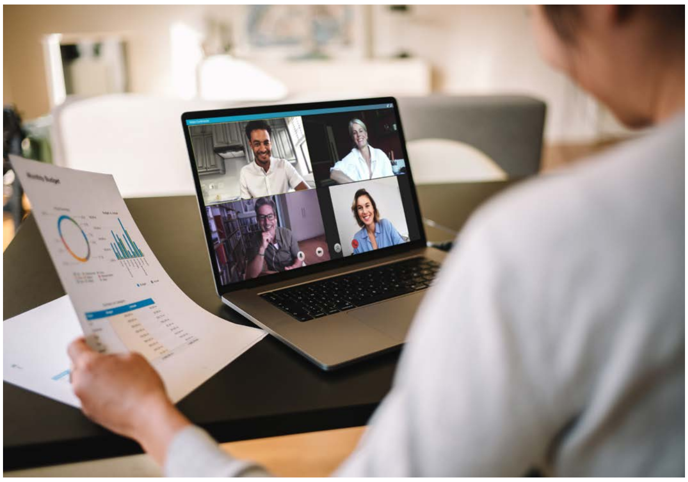
Remote working, whether working from home (WFH) or another off-site location, can bring many benefits to both employers and employees and has been vital for busniness continuity throughout the pandemic. However, remote working can also introduce additional security risks.

Preparation for remote working is the key to avoiding future security problems. At the start of the global pandemic, there was very little opportunity for organisations to plan in advance of moving, at scale, to remote working arrangements.

It's never too late to put security policies and procedures into place, and the starting point is for an organisation to assess the security risks of remote working and, in turn, identify mitigations to reduce those malicious acts taking place. Conducting a role-based risk assessment will help identify specific positions in the organisation where conducting a fraudulent act may be easier or more damaging.

What are the security risks?

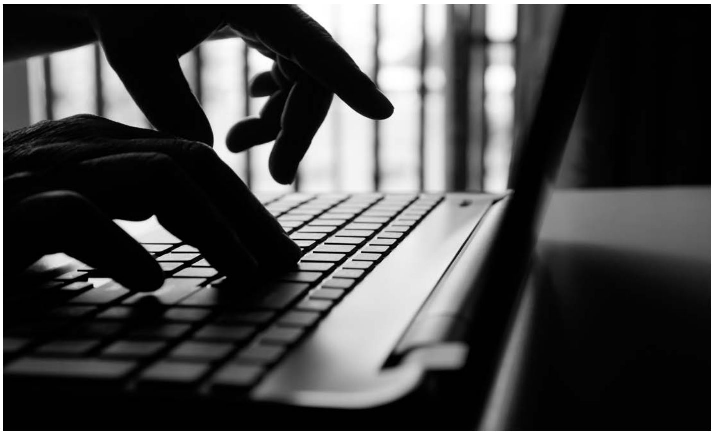
The security risks for remote working are varied. Most line managers will worry that if they have less direct oversight of remote workers it will be difficult to spot poor performance, but fewer managers would consider that remote working could present the opportunity for a malicious worker to conduct an undetected insider act. That is, using legitimate access to an organisation's assets for unauthorised purposes.



Many organisations have recognised that there is an increased risk of loss of IT equipment or sensitive organisational data when staff work remotely. This is usually when an employee may not realise the risk of having sensitive data in their possession outside the workplace, nor adopt the policies and standards appropriate for the use of personal data. By providing staff training, education and support on the safe use of IT, organisations can mitigate the risk of an accidental loss of IT or a data breach.

A frequently recurring theme amongst identified insiders was unhappiness and frustration due to a combination of poor management relationships, unhealthy work/life balances and a perceived lack of recognition.

Having effective policies and procedures, supported by good management is an important mitigation for the risk of employee disaffection and the potential for an insider act occurring.



Writing a remote working policy

Once the security risks for remote working across an have been assessed then appropriate policies can be created. A remote working policy should be robust but flexible and, of course, must comply with UK employment law. A remote working security policy should state whether any jobs or activities are not permitted to be undertaken remotely. For example, those involved in financial transactions, processing of sensitive or personal data, and some IT roles. The decision to exclude certain roles and activities should be based on the outcome of conducting a role-based risk assessment to ensure consistency and evidence of decision making

Policies should also set out arrangements for security and storage of documents, access to sensitive data and IT equipment (including password protection); the sending of documents or sensitive data either in hard copy or electronically; disposal of data; sanctions/disciplinary procedures for breaching security policies, loss of dataor equipment. A remote working policy should state any prohibited locations for remote working, including outside of the UK.

You can find more information about security risks in remote working at the CPNI website: https://www.cpni.gov.uk

This is an edited version of an article by the Centre for the Protection of National Infrastructure (CPNI) published in the February 22 issue of The Public Sector Counter Fraud Journal.

Recent Cases

Doctor struck off for paying bank worker to fake his CV

A doctor's 27 year career in medicine was ended after he was struck off for faking his CV so he could get a new job in finance after being suspended from practising.

Dr Hakeem Lateef was questioned by police after he attempted to get a job in regulatory compliance and anti-money laundering just six weeks after he was suspended from medicine for lying about his involvement in a car crash.

Lateef paid a bank worker £400 to attend a one-day Co-op banking course on due diligence work then gave him a further £100 to 'edit' his CV and include referees. Police were called in when a special Co-op investigator found two copies of Lateef's CV on the computer hard drive of the man who had helped him, one showing the doctor's medical experience and the second with the faked entries.

No criminal action was taken against Lateef for the offence of attempting to obtain a pecuniary advantage by deception but he was referred to the General Medical Council. The doctor denied wrongdoing and denied emailing his faked CV to Bristol-based recruitment agency Emponics which specialises in the finance industry, claiming his PC had been 'hacked'.At the Medical Practitioners Tribunal Service, Lateef, was found guilty of serious professional misconduct and dishonesty.

The hearing was told how in March 2018, Lateef had been suspended when he mislead the General Medical Council about the details of a dangerous driving conviction. finding him guilty of misconduct, Tribunal Chairman, Tim Bradbury said Lateef's account was '*inconceivable'.*

He added: '*The Tribunal did not consider it credible that someone unknown had hacked Dr Lateef's email account and submitted a job application on his behalf without his knowledge. 'He acted in a deliberately dishonest way in order to secure employment he would not otherwise have obtained, and his conduct was properly characterised as fraud."*

Nurse who studied for a degree while sick struck off

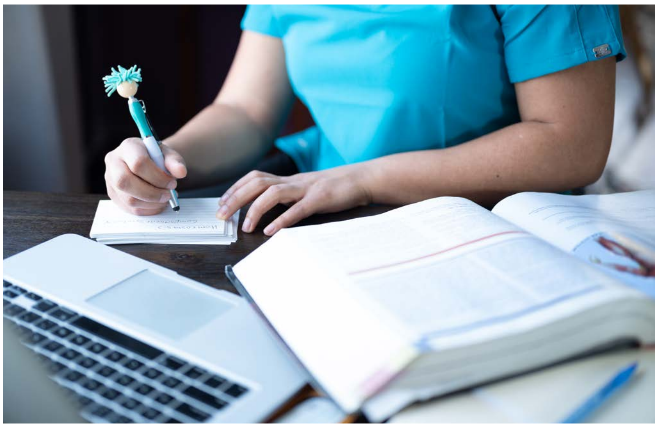
A former nurse at Mersey Care NHS Foundation Trust, has been struck off by the Nursing and Midwifery Council (NMC) after an independent review found that, following her conviction for fraud, her behavior was deemed to be that of a "*dishonest practitioner, which could put patients at unwarranted risk of harm*."

The nurse had reported sick due to an alleged assault at work. She remained off work for two years until her employment was terminated on ill health grounds. Despite claiming she was incapable of coming to work, she undertook a full-time degree in mental health nursing at the University of Manchester, including 2,300 hours of work placements.

Evidence obtained by MIAA's Fraud investigation team showed inconsistencies in what she was reporting to the Trust HR about her injury in comparison to the work she was undertaking on her course as part of the practical element. She was interviewed under caution by an MIAA Anti-Fraud Specialist, where the allegations were put to her and she admitted to the offences.

She was sentenced to a 16-month imprisonment order suspended for two years and required to undertake 200 hours unpaid work and a 20-day rehabilitation order. A Compensation Order was made for the full amount of the overpayment - £40,533.31. Costs of £3,000 were also awarded, to be added and paid following compensation.

Her case was referred to the Nursing and Midwifery Council (NMC) in January this year, after an independent disciplinary panel review she was struck off the register of nurses able to practice in the UK. Claire Smallman, Senior Anti-Fraud Manager at MIAA who investigated the case said: *"Working elsewhere or undertaking training and education while reporting as sick is fraud. As well as gaining a criminal record, NHS staff who are found guilty of defrauding the service can lose their NHS pension and be stuck off from their professional bodies."*



Contact your Anti-Fraud Specialist

Darrell Davies
Regional Assurance Director (Anti-Fraud)
☎ 07785 286381
✉ Darrell.Davies@miaa.nhs.uk

Paul Bell
Senior Anti-Fraud Manager
☎ 07552 253068
✉ Paul.Bell@miaa.nhs.uk

Claire Smallman
Senior Anti-Fraud Manager
☎ 07769 304145
✉ Claire.Smallman@miaa.nhs.uk

Ruth Barker
Anti-Fraud Specialist
☎ 07584 774 763
✉ Ruth.Barker@miaa.nhs.uk

Roger Causer
Anti-Fraud Specialist
☎ 07768 131806
✉ Roger.Causer@miaa.nhs.uk

Alun Gordon
Lead Counter-Fraud Specialist
☎ 07469 573 678
✉ Alun.Gordon@miaa.nhs.uk

Kevin Howells
Anti-Fraud Specialist
☎ 078257 32629
✉ Kevin.Howells@miaa.nhs.uk

Phillip Leong
Anti-Fraud Specialist
☎ 07721 237352
✉ Phillip.Leong@miaa.nhs.uk

Virginia Martin
Anti-Fraud Specialist
☎ 07551 131109
✉ Virginia.Martin@miaa.nhs.uk

Karen McArdle
Anti-Fraud Specialist
☎ 07774 332881
✉ Karen.McArdle@miaa.nhs.uk

Michelle Moss
Anti-Fraud Specialist
☎ 07825 858685
✉ Michelle.Moss@miaa.nhs.uk

Andrew Wade
Anti-Fraud Specialist
☎ 07824 104 209
✉ Andrew.Wade@miaa.nhs.uk

Paul McGrath
Anti-Fraud Specialist
☎ 07584774761
✉ Paul.McGrath@miaa.nhs.uk

Neil McQueen
Anti-Fraud Specialist
☎ 07721 237353
✉ Neil.McQueen@miaa.nhs.uk

Report Fraud

Report NHS Fraud

https://cfa.nhs.uk/reportfraud

Report fraud or cyber crime to Action Fraud

https://www.actionfraud.police.uk/

Fraud prevention advice

https://takefive-stopfraud.org.uk/

National Cyber Security Centre

- Report a vulnerability with a UK government online service https://www.ncsc.gov.uk/information/vulnerability-reporting
- Report a cyber security incident

https://report.ncsc.gov.uk/

MIAA Anti-Fraud Services

https://www.miaa.nhs.uk/services/anti-fraud/

Check out the latest updates on general frauds & scams www.actionfraud.police.uk/

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

TAKE FIVE TO STOP FRAUD™