Notice Fraud

Summer 2024

Notice Fraud

Welcome to RSM's Counter Fraud Newsletter for NHS staff. Explore the latest fraud trends and gain valuable insights into the fraud risks impacting the sector. Discover our counter fraud initiatives and recent fraud case to help you stay informed and fight against fraud. In this edition, we focus on cyber enabled fraud prevention and risks, following the cyber-attack in June which impacted some NHS organisations.

Across our 60 healthcare clients in 2023/24 we received 926 fraud referrals from which 7.5% (70) referrals related to 'email scams' and mandate fraud. We shared 19 alerts with our clients on cyber fraud risks. The prompt identification of these fraud attempts and measures to block them prevented losses of £1.8m.

Mandate Fraud – Copycat Domain RSM Alert (02) issued preventing losses of £418K

A recent mandate fraud attempt at one of our NHS clients was unsuccessful. The fraudsters submitted an email from a copycat email domain purporting to be from one of the Trust's regular suppliers. They acquired the domain @octavlus.co.uk, swapping the i for an l. The correct domain is @octavius.co.uk. Email conversations went back and forth before the fraudsters requested that supplier bank details be amended.

The finance team identified the incorrect email address when following their mandate change process. Had this not been identified any future invoices may have been diverted to the fraudsters account, resulting in a significant financial loss.

The domain name was reported to NHS Digital who had the domain blocked, and we shared an alert across our NHS clients to protect other organisations.

> Cyber threats are on the rise in the healthcare sector. The critical nature of healthcare services, combined with the shift to virtual care makes these organisations a prime target for cybercriminals.
>
> **Clive Makombera, RSM's Head of Healthcare, The growing cyber threat and its impact on the sector**

Where can this type of fraud take place?

- Social media
- Emails
- Internet banking
- Mobile applications
- Online shopping
- Mobile phones
- Artificial intelligence
- Cloud services
- Internet of things

21 million malicious emails are blocked across the NHS network every month.

What are the main cybercrime threats?

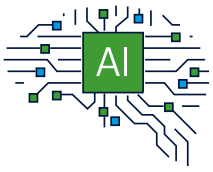
- Mandate fraud and false invoicing – submitting false invoices for payment, or amended supplier payment details to divert payments.
- Phishing / smishing / vishing – fraudsters sending emails, text or voice messages asking for you to click on a link and enter sensitive information such as your username and/or password.
- Viruses / malware / ransomware – sending hidden files within emails or attachments, that when opened cause harmful effects like slowing down your system, corrupting, deleting, or quarantining data, which the fraudsters can use to extort money in return for restoring the disrupted systems.
- Identity theft and impersonation – using your identity or personal information to facilitate fraud, such as an individual pretending to be you to get information from colleagues or suppliers.
- Hacking emails and social media – gaining unauthorised access to systems or networks.
- Online scams – designed to deceive individuals, tricking them into providing money or sensitive information.

Emerging risks – impact of artificial intelligence on fraud

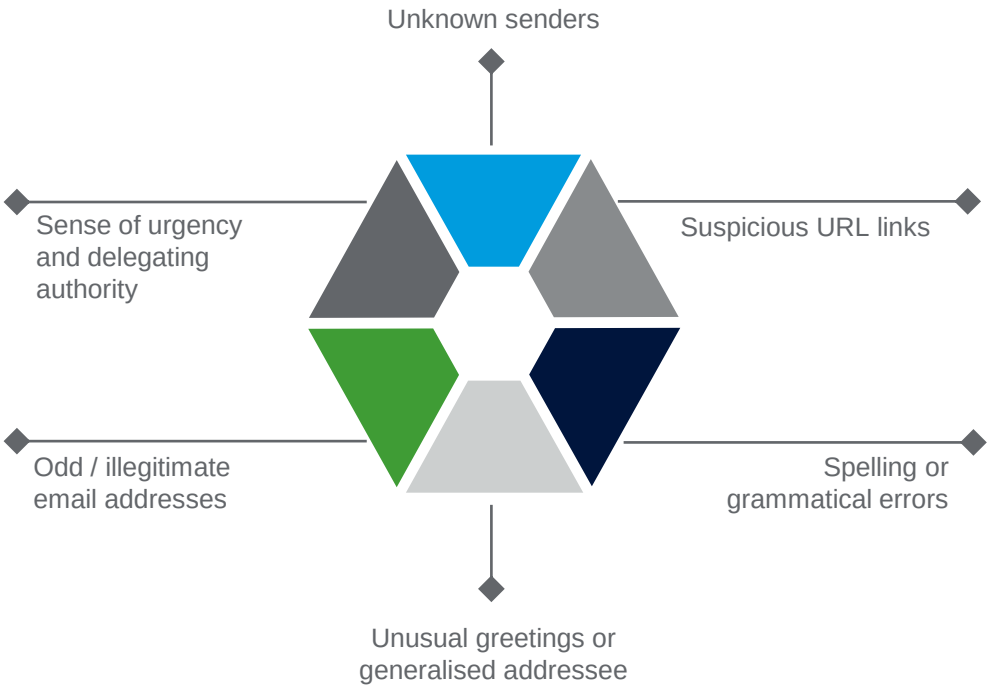
Artificial intelligence (AI) is advancing quickly, with machines now performing tasks which typically required human intelligence. AI can now do a variety of things from problem-solving, recognising patterns and assisting with language, whether that be writing or understanding text.

Whilst AI offers significant benefits and can save time, it also brings with it new fraud risks.

- Using deepfakes to impersonate someone else, such as your manager or a relative. This Involves manipulating audio, video, or images.
- Applicants use AI to generate answers to interview questions and create fake CVs.
- Improving the spelling and grammar on phishing emails to make them harder to identify.



What to look out for?



Top tips for keeping secure

- Set strong, complex passwords. Current guidance is to use three unconnected words, and include numbers and special characters, for example Pa55Th!sW0rd.
- Install software updates as soon as they are released on personal devices.
- Install anti-virus software on all devices.
- Stop and think when you receive an email or text message.
- Avoid clicking on suspicious links, opening messages and attachments from unknown senders.
- Use secure devices and connections and when accessing sensitive data.
- Don't share unnecessary information online and in person.

Upcoming fraud awareness sessions

Cyber security

Cyber fraud and security are important matters both in your personal and professional life. Join our session to learn about cyber fraud risks, data theft, and broader cybersecurity issues.

Session date and time: 30 July 2024 10am – 11:30am

Please click here to register for the Cyber Fraud and Security Awareness Session.

Recruitment and ID verification

Involved in recruitment? Whether you're in HR, a hiring manager, or team lead, don't miss our upcoming recruitment and ID verification awareness session.

Session date and time: 6 September 2024 10am – 1pm

Your LCFS will share details on how to book on to this session.

Contact

To access training or report a fraud you should contact your Local Counter Fraud Specialist (LCFS) directly:

T: 0121 214 3149

E: manjit.sandhu@rsmuk.com

You can also report fraud anonymously on 0800 028 4060, or online via https://cfa.nhs.uk/reportfraud

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM UK Risk Assurance Services LLP

25 Farringdon Street
London
EC4A 4AB
United Kingdom
T +44 (0)20 3201 8000
rsmuk.com