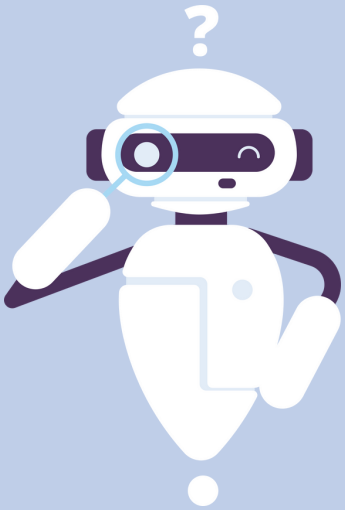
JULY 2023

AUDIT YORKSHIRE

COUNTER FRAUD NEWSLETTER

Welcome to our July 2023 Counter Fraud newsletter for NHS staff. We hope you find the contents helpful. If you need any advice on fighting NHS fraud, you can find our contact details on the final page.



Spot the Bot - one of our newsletter articles was co-authored by Chat GPT this month...but which one? See if you can spot it. You'll find the answer on the Reporting Concerns page.

IN THIS EDITION

WHAT HAPPENS IF I REPORT NHS FRAUD?

If you think a fraud may have occurred, or is currently happening, we would be grateful if you would report it to your Local Counter Fraud Specialist (LCFS) – their details can be found at the end of this newsletter.

Please don't worry about whether what is happening fits the legal definition of fraud. If what you report doesn't really fall within our remit, we will be happy to look at alternative ways of addressing the matter with you. For example, it may be more appropriate for the police or HR to investigate.

We may ask you for some further information, such as copies of emails. We will then look at the information and decide whether to start a formal investigation.

Even if we do not start an investigation, your report may highlight the need to review and improve processes. Preventing fraud is just as important as investigating fraud is.

If you are uncertain, please contact us for advice. Your report to us is treated confidentially.

Where we can, we will keep you updated but please note that we may not be able to share full details due to data protection rules. We are also unable to update you if you choose to make an anonymous report – we really do not know who you are!

The Counter Fraud Team are friendly and approachable and we welcome all reports made to us. We would rather receive lots of referrals which turn out to not to be fraud than miss one which could cause a loss to the NHS.

Further details on how you can report your suspicions are at the end of this newsletter.

Scam Trends

Courier Fraud - Look out for elderly friends and relatives

This type of fraud typically begins with a phone call or email, where the fraudsters pose as bank officials, police officers, or other authority figures when they first speak to the victim. Once they establish contact, the fraudsters manipulate their victims. They will often claim that there has been fraudulent activity on the victim's bank account, create a sense of urgency and coerce the victims into complying with their demands.

A common tactic in courier fraud involves getting victims to withdraw large sums of money from their bank accounts, so that it can be held as "evidence" or moved to "safety". The fraudsters instruct the victims to place the cash in an envelope or bag and hand it over to a courier who will visit their home to collect it. Courier fraudsters have also been known to coerce victims in to using jewellers to purchase high-value items or to attend foreign exchange bureaus to transfer money electronically.

Another variation involves getting victims to hand over bank cards, PIN numbers, or answers to security questions. Once the victims disclose this information, the fraudsters gain access to their funds and can carry out unauthorised transactions. City of London Police recently highlighted the threat that courier fraud poses to people over 70 in England and Wales.

Data from the National Fraud Intelligence Bureau (NFIB- an organisation owned and administrated by City of London Police), revealed that people aged 70 and over lost more than £12.6 million to courier fraud last year. This loss amounts to a staggering 77% of all money stolen by courier fraud.

Indeed, data showed that 153 reports were made by people in their 90s with one report being from someone aged over 100. In 12 months from May 2022 to May 2023, 1,587 reports of courier fraud were made by people over the age of 70 across the UK. A link has been identified whereby courier fraudsters deliberately target locations such as retirement homes and villages, care homes and buildings that provided assisted living. This means that criminals are targeting some of the most vulnerable and oldest members of society.

Advice

We advise all readers to stay cautious and sceptical when contacted by anyone claiming to be from a financial institution or law enforcement. Take time to verify information, seek advice from trusted sources, and never rush into making financial decisions even if you feel you are under pressure. Information on Courier Fraud can be found on the Action Fraud website, the Take 5 to Stop Scams site, and on the City of London Police website.

Deepfake Martin Lewis Scam Warning

Martin Lewis, Money Saving Expert, is warning the public that a video is being circulated which uses deepfake technology to impersonate him. Deepfakes are created using software to steal a person's physical identity and voice, to spread false information or mislead viewers.

Fraudsters are trying to take advantage of the trust many people place in Martin Lewis' money saving advice. In the deepfake video, Martin Lewis appears to encourage viewers to invest in "Quantum AI" which it claims is an Elon Musk project.

Martin Lewis has warned viewers that the video is a scam by criminals aimed at defrauding the public. The video has been seen circulating on Facebook and Twitter, and uses a caption that looks similar to the font / style used by This Morning (on which Martin often appears).

Advice

You can see screenshots of the video and advice on the Money Saving Expert website. Some top tips include:

- Be aware that Martin Lewis NEVER does adverts or promotes investments.
- If you see the video online, they recommend that you do not interact with it to avoid being further targeted.
- You can report the video on Facebook or Twitter - if you click on the three dots next to the post, you should see an option to report it as spam.
- If you've already fallen victim to the scam, you should contact your bank immediately and cancel any future payments to the fraudster. You should also report it to Action Fraud on 0300 123 20 40.

Cyber Fraud - Fake App Scams

In today's digital age, where smartphones have become an integral part of our lives, mobile applications have gained immense popularity. However, with their rise in popularity, there has been a corresponding increase in fake app scams.

These scams can deceive users, compromise their personal information, and even cause financial losses. This article aims to shed light on the issue of fake app scams, the potential risks they pose, and provide valuable tips on how to avoid falling victim to them.

Understanding Fake App Scams

Fake app scams involve the creation and distribution of fraudulent mobile applications that imitate legitimate apps, often with malicious intentions. Scammers typically design these apps to look identical to popular ones, such as banking, shopping, or social media apps. They aim to trick users into downloading and using them, enabling the scammers to gain access to personal information, login credentials, or even bank account details.

The Risks Involved

- **Data Breach**: Fake apps may request extensive permissions during installation, enabling them to collect and transmit personal data without the user's knowledge or consent.
- **Financial Losses**: Scammers may use fake apps to obtain sensitive financial information, such as credit card details, leading to unauthorised transactions or identity theft.
- **Malware Infections**: Fake apps can contain hidden malware that infects the user's device, compromising its security and allowing cybercriminals to exploit vulnerabilities.
- **Privacy Intrusion:** By using fake apps, scammers gain access to users' personal information, which can be misused or sold to third parties for various malicious purposes.

Tips to Avoid Fake App Scams

- **Download Apps from Official Sources**: Stick to trusted sources such as the Apple App Store for iOS devices and Google Play Store for Android devices. These platforms have rigorous security measures in place to minimize the risk of fake apps.
- **Check App Reviews and Ratings**: Before downloading any app, read reviews and ratings from other users. Be cautious if an app has a low rating or negative feedback, as it could be a sign of a fake app.
- **Verify App Developer Information**: Research the developer of the app you wish to download. Legitimate apps usually provide detailed information about the developer, including their website and contact details.
- **Scrutinize Permissions:** Pay close attention to the permissions requested by the app during installation. Be sceptical if an app asks for unnecessary permissions that are unrelated to its functionality.
- **Examine App Details:** Look for any discrepancies in the app's name, logo, or description compared to the official version. Scammers often create subtle differences that can be easily overlooked.
- **Update Regularly:** Keep your device's operating system and apps up to date. Developers frequently release security patches and bug fixes, minimizing the chances of falling victim to app scams.
- **Use Mobile Security Apps**: Install reputable mobile security software that includes real-time scanning and protection against malware and suspicious apps.

In the Press

13 Year Prison Sentence for iSpoof Fraudster

In our December 2022 newsletter, we included an article on iSpoof - a fraudsters paradise. iSpoof was a website that helped users to commit fraud. This included software that would disguise the fraudsters phone number, allowing them to appear on the victims caller display as though they were calling from an official organisation such as the person's bank or HMRC. Scammers would pay hundreds or thousands of pounds per month to iSpoof for their services.

At one point whilst the site was active, almost 20 people were being targeted every minute of the day by scammers using false identities that they had created on iSpoof. One victim lost around £3 million, whilst the average loss caused was £10,000. It is believed that the website facilitated over £100 million worth of fraud whilst it was active, although it has been stated that this is probably a conservative estimate. The website was closed down in December 2022 and over 100 people were arrested for their involvement with the site.

The website's founder, Tejay Fletcher of East London, has pleaded guilty to four counts of fraud charges. It is estimated that he made around £3 million for himself through the website. He has been sentenced to 13 years and 4 months in prison. More information about the case can be found on the BBC News website.

Fraud Prevention Masterclasses

The 2023/24 Fraud Prevention Masterclass programme launched this month. The Masterclasses are delivered via Microsoft Teams and sessions typically last around 1 hour. The programme will run until February 2024, further dates will be published later this year. We will be covering the following topics:

General Fraud Awareness	10th August at 2pm
Fraud Awareness for Managers	14th September at 10am
Cyber Fraud	15th August at 11am
Payroll Fraud	8th September at 11am
Procurement Fraud	9th August at 2pm
Creditor Payment Fraud	12th September at 11am
Fraud Awareness for HR	14th August at 10am
Recruitment Fraud	28th September at 2pm

If you'd like to book a place for any of these sessions, please contact yhs-tr.audityorkshire@nhs.net

Bespoke Training Sessions

The Local Counter Fraud Team are always happy to pop along to speak to individual teams. If you would like us to attend one of your team meetings, to deliver a training session on a key fraud risk area, or for any other fraud prevention advice, please contact us using our details (which you'll find on the last page).

REPORTING FRAUD CONCERNS

Fraud vs the NHS

If you think that fraud may be being carried out against the NHS, please **notify your Local Counter Fraud Specialist**. You'll find our contact details on the next page.

You can also report your concerns to the **NHS Counter Fraud Authority** using their online reporting tool or phone number. You'll find these details on the next page.

If you choose to make an anonymous report, please give as much information as possible as we won't be able to get back in touch with you to clarify anything.

Suspicious Emails

Do not click on any links or attachments.

If you have received a suspicious email to your **@nhs.net** email account, you can forward it (as an attachment) to **spamreports@nhs.net**

If you are not sure how to forward an email as an attachment, contact the LCFS team and we will help you.

If you have been sent a suspicious email to another type of email account (not @nhs.net) you can forward it to **report@phishing.gov.uk**

Suspicious texts

Do not click on any links in the suspicious text message.

You can forward suspect text messages to 7726.

Fraud against a member of the public

These concerns can be reported to **Action Fraud (0300 123 20 40),**

If the person has lost money, it may also be appropriate to report the matter to **the police.**

If you suspect that the person's bank account has been compromised, it is important that they **speak to their bank** as a matter of urgency.

I've read the options but I'm still not sure what to do

The Local Counter Fraud team will be happy to advise.

Our contact details are on the next page.

Spot the Bot - Chat GPT helped to write the Fake App Scam article. It can be very hard to spot AI generated material. A tiny giveaway was the spelling of the words "scrutinise" and "minimise" in the advice section - AI often uses American spellings by default.

CONTACT US

Acronym Decoder
LCFS - Local Counter Fraud Specialist
LSMS - Local Security Management Specialist
ICB - Integrated Care Board

Steve Moss
Steven.Moss@nhs.net / 07717 356 707

Head of Anti Crime Services / LCFS

Steve manages the Counter Fraud Team.

Marie Dennis (was Hall)
Marie.Dennis2@nhs.net / 07970 265 017

Assistant Anti Crime Manager covering all clients, and LCFS covering:

York and Scarborough Teaching Hospitals NHS Foundation Trust

NHS Professionals

Nikki Cooper
Nikki.Cooper1@nhs.net / 07872 988 939

LCFS Covering:
Humber Teaching NHS Foundation Trust

Humber and North Yorkshire ICB

Leeds Community Healthcare

Rosie Dickinson
rosie.dickinson1@nhs.net / 07825 228 175

LCFS covering:
Harrogate and District NHS Foundation Trust

Spectrum Community Health CIC

West Yorkshire ICB

Shaun Fleming
ShaunFleming@nhs.net / 07484 243 063

LCFS and LSMS Covering:

Calderdale and Huddersfield NHS Foundation Trust

West Yorkshire ICB

Lincolnshire ICB

Rich Maw
R.Maw@nhs.net / 07771 390 544

LCFS Covering:

Bradford Teaching Hospitals NHS Foundation Trust

Local Care Direct

The Mid Yorkshire Hospitals NHS Foundation Trust

Lee Swift
Lee.Swift1@nhs.net 07825 110 432

LCFS Covering:
Airedale NHS Foundation Trust
AGH Solutions
Bradford District Care NHS Foundation Trust
Leeds and York Partnership NHS Foundation Trust

You can also report fraud concerns to the NHS Counter Fraud Authority:
0800 028 40 60
https://cfa.nhs.uk/reportfraud

Follow us on Twitter - search for @AYCounter Fraud

Scan here to see previous editions of our newsletters