COUNTER FRAUD NEWSLETTER

AUDIT YORKSHIRE
The journey to excellence
June 2021

Welcome to the June 2021 edition of our newsletter. 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

Accommodation Fraud

This type of fraud happens when you pay money to book accommodation of any type (such as hotel accommodation), only to later discover that the property or booking is not genuine. This is a particular risk in 2021 due to the highly competitive holiday market. To avoid this type of fraud, it is safest to deal directly with established hotels or travel companies. If you are using a travel company, make sure they are registered with an official body such as ABTA or ATOL. Never pay for accommodation using money transfer agents (such as Western Union or Moneygram) - a credit card gives you the greatest chance of being protected.

"Internet Provider" Impersonation

There have been reports of staff receiving calls which play an automated message when answered. The recorded message states that you need to press 1 to avoid your internet connection being cut off.

Pressing 1 can result in being connected to a premium rate number and/or a fraudster who will then try to persuade you to allow remote access to your desktop, provide sensitive information (such as usernames and passwords), or to provide payment information. Please do not press 1 if receiving these kinds of calls. Please hang up and if you think there is a genuine problem with your connection, please report this to IT using established methods.

Covid-19 "Vaccine Passport" Scam

A new Covid-19 themed scam has started circulating in which members of the public receive an email which directs them to visit a fake (but convincing) NHS website. The website asks the victim to provide their personal and financial details (to pay an "admin fee") in order to access a copy of their "Digital Coronavirus Passport".

One website has already been taken down but it is likely that fraudsters will try other variations of this scam, using new fake websites and potentially changing their method of communication (using text or phone calls).
Your vaccination status is provided for FREE using the NHS App, NHS website, or by calling the NHS on 119. You can find out more about how to access your NHS Covid Pass on the Gov.uk website: Demonstrating your COVID-19 vaccination status - GOV.UK (www.gov.uk)

Cyber Scam Techniques - Team Viewer/Remote Access Software

Cyber criminals who try to persuade you that there is a problem with your computer or your internet connection will often ask you to install a piece of software called Team Viewer (or similar alternatives like LogMeIn, Splashtop, or AnyDesk).

Remote access software is really useful, and you may have seen it in action if your IT team have ever needed to take control of your computer to fix a problem. When used for its genuine purpose, it allows those with the technical knowledge needed to fix issues with your computer remotely.

Unfortunately, fraudsters have identified remote access software as a great way to defraud people. You might have heard about calls from fraudsters claiming to be from Microsoft, reporting that there is an issue with a person's device. The scam works by convincing you to allow the fraudster access to your computer using remote access software. The fraudster can then install malicious software to damage your device or track your movements online (including usernames and passwords), or they may try and persuade you to log into your online bank which allows them to steal your money.

You can read more about this type of scam and how to avoid becoming a victim of a remote access scam by visiting this Which? Article: Victims of remote access scams losing life savings – Which? News

Covid: Birmingham NHS Worker Stole Deceased Patient’s Bank Card to Buy Snacks

A 23 year old healthcare assistant on a Covid Ward in Birmingham has been convicted of theft and fraud after she stole an 83 year old patient’s bank card soon after the patient died. Ayesha Basharat used the card 17 minutes after the time of death of the patient had been recorded to buy snacks from a vending machine. Basharat used the card later that same day and attempted to use it twice more the following day.

When arrested while on shift, Basharat still had the card in her possession. She claimed she had found it and later mistaken it for her own bank card- despite it being a different colour. Basharat had clearly breached hospital rules around patients’ property. She admitted theft and fraud and was sentenced at Birmingham Crown Court to two lots of 18 months in prison, to run concurrently and suspended.

This unpleasant case impacted on the victim’s family and has been in the national media. It highlights the need to adhere to guidelines around patient property and the futility of Basharat’s actions.

The suspect has thrown away her job and reputation for the sake of £6 worth of snacks. All staff are urged to be meticulous when dealing with patients’ property to avoid any misunderstandings or possible criticism. The need to avoid criminal behaviour such as that described above does not need to be highlighted.

Courier Fraudster Jailed

Previous newsletters have covered telephone frauds whereby a victim is called by a fraudster who claims to be either from their bank or a police officer. This method of fraud has been around for many years but is still successful as the criminals are often very convincing and well-rehearsed. In June 2021 a fraudster in Birmingham was jailed for three years for conning victims out of £50,000 under the guise of a police investigation into counterfeit cash.

Rene Cardin, 23, posed as a courier and targeted people in the West Midlands.

An unidentified accomplice called victims, aged between 68 and 85, posing as a police officer telling them to withdraw cash for examination.

Cardin then collected the money from victims' homes but was caught after her car was spotted on CCTV near one of the addresses targeted.

West Midlands Police said Cardin, who already has convictions for a spree of violent robberies, collected tens of thousands of pounds from her victims in just one week in April 2021.

Cardin was sentenced after admitting conspiracy to defraud six victims and to an offence of acquiring, using or possessing criminal property.

NHS employees are urged to be vigilant and not be taken in by such frauds. If you receive a phone call purporting to be from the police or your bank, do not engage with them unless you are satisfied that they are genuine. It would be better to end the call and then call your bank using a number you have on official paperwork and/or call your local police force using the ‘101’ number and then confirming the details relayed to you initially.

£66,000 Recovered from NHS Fraudster

Aled Meirion Jones was convicted of Fraud by Abuse of Position in March 2021. He was featured in a previous edition of the newsletter after it was discovered that he had been diverting cheques into his own account.

The cheques were sent to the hospital as payment to specific doctors who had provided cause of death certificates. Instead of allowing the payments to go to his colleagues, who had rightfully earnt the fees, Jones altered the cheques and paid them into his own account. The value of these cheques came to over £33,000. In addition, Jones had falsely claimed for Locum shifts he had not worked and exaggerated his working hours, resulting in him receiving another £33,000 to which he was not entitled.

Jones was sentenced to two years imprisonment, suspended for two years. He was also sentenced to 200 hours of unpaid work and ordered to repay £66,000 to the NHS. Jones paid the money back, on the last day of the court imposed deadline. Failure to pay would have seen Jones spending the next two years behind bars.

Counter Fraud Training

NEW - Fraud Prevention Masterclasses

The LCFS team are currently scheduling a series of Fraud Prevention Masterclasses, covering key fraud risks within different areas. The masterclasses are delivered via Microsoft Teams and will last around 45 minutes to 1 hour.

The sessions are being delivered on a monthly basis, and cover some key areas that have very specific fraud risks. They include an overview of the various risks which may be encountered, real life case studies and practical advice on the prevention of fraud risks.

If you have an interest in any of the topics below and would like to sign up for a session, please get in touch with Rosie Dickinson (rosie.dickinson1@nhs.net)

Recruitment Fraud

Ideal for staff with responsibility for pre-employment checks

Learn how to spot:

- Identity Fraud
- Qualification Fraud
- Inflation of Skills/ Experience
- Failure to Disclose Criminal Convictions

Payroll Fraud

Ideal for payroll staff who are new or would like a refresher

Covering:

- Timesheet Fraud
- Working Whilst Sick
- Cyber-enabled Salary Diversion
- ESR Fraud

Creditor Payments

Ideal for staff in accounts payable or who deal with invoices/suppliers

Looking at:

- Mandate Fraud
- New and Existing Phishing Tactics
- Social Engineering
- CEO Fraud

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 07484 243 063
Nikki Cooper, Local Counter Fraud Specialist	Nikki.cooper1@nhs.net 07872 988 939
Richard Maw, Local Counter Fraud Specialist	R.maw@nhs.net 07771 390544
NHS Counter Fraud Authority Fraud and Corruption Reporting Line	0800 028 4060