Counter Fraud Newsletter – October 2022

Welcome to the October edition of the Audit Yorkshire Counter Fraud Newsletter for NHS employees. You will find a guide to reporting concerns and contact details for the Local Counter Fraud Specialist team on the last page of this document.

Current Scam Trends

Protecting your Pay from Salary Diversion Fraud
Over the last few years we've covered the topic of salary diversion fraud many times. Fraudsters target salary payments by impersonating payroll departments and pay systems such as ESR. Some NHS organisations have begun offering staff access to financial wellbeing apps which interact with NHS Payroll systems.

Please be mindful that fraudsters are quick to learn the systems we use and may impersonate these organisations. Always double check Apps before you download them to make sure they are legitimate, be wary of links within texts or emails asking you to log into your account, and always make contact using official customer services options if you are notified of a "problem" with your account.

Google Play Voucher Fraud
Back in March this year, a local NHS organisation was targeted by a scam. A fraudster set up a fake email account and used it to impersonate the Chair of the organisation. The imposter contacted the Finance Director to ask if they were free to help with something.

Trending Scams

- Cost of living payments
- Energy bill rebates
- WhatsApp scams
- Impersonating police officers over the phone

Look out for: "missed parcel" scams are likely to increase as we approach Black Friday and the festive shopping period

When the Finance Director replied, the fake Chair then asked if the Finance Director could buy some Google Play vouchers on their behalf as they were working late. The same tactic has been spotted again in recent weeks. Please be mindful that fraudsters may impersonate senior employees in hopes that staff will feel obliged to comply. If you receive an unusual request, please contact the individual using an established contact method. If in doubt, you are welcome to contact your Local Counter Fraud Specialist for advice.

WhatsApp CEO Fraud
CEO fraud is nothing new, but the tactics that fraudsters deploy are innovative and are constantly using new methods, most recently using WhatsApp to commit this type of fraud.

In CEO fraud, the criminal will impersonate a senior member of staff - in many cases the CEO. They use this false identity to pressure staff members to make unnecessary payments or to part with sensitive information held at the organisation.

It has been reported that criminals are now targeting organisations via WhatsApp. In one incident, an employee was sent messages by a WhatsApp account that looked like it belonged to their organisation's CEO. The messages requested that the employee organise and execute a faster payment of £200k. The payment was made but it later transpired that the messages sent to the employee had been fraudulent. The fraudster had set up a WhatsApp account where the profile picture was a photo of the CEO which had been lifted from their genuine Facebook account.

Stay vigilant and follow your organisations policies and procedures when it comes to payment requests. If you receive any messages like this, you must contact the apparent sender using an established contact method to check if it is a legitimate request. Please report any fraud attempts to your Local Counter Fraud Specialist. It is also important to review your social media settings and ensure that you have set up strong privacy controls to protect your personal information from being stolen and misused.

Apple / Google pay frauds
When you transfer funds between bank accounts, most banking apps will run a check to confirm that the payee is named on the account you are sending money to. This check helps to reduce the risk of fraud. In some recent reports fraudsters have requested payments be made using Apple / Google Pay. This is done to bypass bank checks which would alert the payer that the person they were paying was not who they thought it was.

Getting refunds from Apple / Google Pay can be difficult even if you have been scammed, so prevention is the best tactic. If you receive a request to make a payment via Apple / Google Pay, please be mindful of this new type of fraud and make checks through established contact methods to confirm if it is a genuine request.

If you are setting up Apple or Google Pay on your device make sure you do this over a secure network – you don't know who may be lurking on and monitoring public wi-fi.

Cyber Security

Paste Websites

We often advise people to put their email address into the Have I Been Pwnd (HIBP) website. The name of the site may appear to be squiffy, but it enables you to see whether your email has appeared in any security breaches. HIBP will also tell you whether your email address has been found in any 'pastes'. So what does this mean?

In this context, a 'paste' is where information is simply 'pasted' onto a faceless website. These type of websites were designed to share computer code, but can be used for other things which hackers may find of interest. Pastebin.com is the most common one. The benefits of using such a site include being able to post a link to a large amount of text which may be too much for a 'chat' function to handle.

Personal detail sharing is banned, but it is not policed. Paste websites are hosted on the deep web - which means that they are viewable through a browser, but the content is not indexed by google.

If your email address appears on a paste site, it doesn't not mean that it has been leaked for a malicious purpose. If you run your details through HIBP and your information shows up as having been compromised or pasted, change your password.

Other Useful Information for Staff

NFI time – did you know that your information will be included?

The National Fraud Initiative (NFI) is an exercise that matches electronic data within and between public and private sector bodies to prevent and detect fraud. It is run every 2 years and is co-ordinated by the Cabinet Office.

All Trusts and ICBs are mandatory participants along with all Councils, Home Office, Police, Fire and Rescue Service and the NHS Pension Scheme amongst others.

The types of fraud and errors previously identified by the NFI include:

- Employees working elsewhere whilst on sick leave
- Fraudulent housing and council tax benefits claims
- Overpayment of invoices resulting from the payment of duplicate invoices and credit notes
- Occupational pension payments paid to deceased pensioners several years after their death

The data is submitted automatically in October. For more information please visit your organisations intranet/website National Fraud Initiative website. If you have any other queries regarding the exercise, please email nikki.cooper1@nhs.net

Keep Your Valuables Safe

We have recently received a report about an NHS employee who was the victim of theft and an attempted fraud. The employee had left their bag in an unlocked room within a health centre, whilst assisting with a covid vaccination clinic. The employee received a call from a male who introduced himself as "David" and said he was calling from Natwest Bank. "David" said that there had been an attempt to use the employee's bank card to withdraw £1000 from a cash machine.

The member of staff checked their bag and discovered that their purse was missing. "David" called from a withheld number, and said that he was calling from "the fraud team at Doncaster". He told the employee to Google a number which would show up as being from Natwest. He went on to say that he could prove he was genuine as he knew the employee's full name, occupation, address etc. He asked the employee to confirm their mother's maiden name but they refused. "David" then said a police officer would be in touch, possibly called "PC Harper" and the call ended.

The employee rang Natwest using their genuine customer services number. The Natwest representative confirmed that the call was a fraud attempt and cancelled the employee's bank cards. "David" would have been able to get the personal details which he quoted during the call using the contents of the employee's purse (such as their driving licence etc.)

The incident was reported to Humberside Police who stated they have received a similar report using the same methodology and referencing a "PC Harper". In other Police Officer impersonation scams, victims have been persuaded to withdraw all their money and to give it to a courier, or move it into a "safe" account controlled by criminals.

Please keep your valuables secure. If any items are stolen from you and you receive phone calls from someone claiming to be from your bank or the police, please hang up and call either organisation using their established contact methods.

Be cautious even if the caller appears to be genuine – it is always better to be safe than sorry. Please report theft to the police, and if fraud is attempted, let your Local Counter Fraud Specialist or Action Fraud know.

In the Press

Fake Psychiatrist Uncovered at Private Mental Health Clinic

George Godwin attended a job interview for a private Mental Health Clinic in January 2021. He told the interview panel that he was a psychotherapist and presented a British Association for Counselling and Psychotherapy certificate. He was taken on by the clinic, who later discovered that he had forged documentation and was not registered with the BACP. He had been paid over £30,000 during his 10 months of employment at the clinic. He admitted fraud by false representation at the magistrates court, and he will be sentenced at Southwark Crown Court. You can read more about the story on the Daily Mail website here.

Office for National Statistics figures reveal phishing trends and targets

The Office for National Statistics (ONS) have published the findings of the Telephone-operated Crime Survey of England and Wales (TCSEW). 50% of respondents stated they had received at least one phishing message in the month before the survey. It also found that the age group most likely to be targeted by phishing messages was the 25-44 age group.

The survey highlighted current trends in the world of phishing. More than half (54%) of those who received a suspicious message said that the sender was posing as a delivery company, a third (32%) said the sender was claiming to be their bank or building society, and a quarter (25%) received messages claiming to be from government services.

The findings also highlighted the impact of the cost of living crisis. In the two weeks to 5 August 2022, over 1,500 reports were made to the Suspicious Emails Reporting Service about scams claiming to be energy rebates from Ofgem. You can read more about the survey on the ONS Website.

A Quick Guide to Reporting Fraud Concerns

I have a concern that fraud may be being committed against the NHS

You can **contact the Counter Fraud team** (our details will be on your staff intranet and in your organisation's Anti Fraud Policy).

You can also report your concerns to the **NHS Counter Fraud Authority** (0800 028 4060).

If you making an anonymous report, **please give as much detail as possible** as we won't be able to contact you for more information.

I have a concern that fraud may be being committed against the general public

These concerns can be reported to **Action Fraud** (0300 123 2040).

If someone has been actively defrauded, it may also be appropriate to report to the **police**.

If it is suspected that the victim's bank account has been compromised, they will need to **speak to their bank as a matter of urgency**.

I have received a suspicious email to my NHS.net email address.

Do not click on any links or attachments.

Forward the suspect email **as an attachment** to **spamreports@nhs.net**. To do this, click on the "More" button which is next to the "Reply, Reply All, Forward" options. Choose "Forward as Attachment".

I have received a suspicious email to another email account (not NHS.net)

Do not click on any links or attachments.

Forward the email to **report@phishing.gov.uk.** You can use this option for any suspicious emails you receive on email accounts that are not NHS.net accounts.

I have received a suspicious text message

Do not click on any links in the text message!

Forward the text message to **7726.**

I have come across something and I'm not sure whether it is fraud-related

You are very welcome to contact the **Counter Fraud team** for advice and support, our contact details will be on your staff intranet and in your Anti-Fraud Policy.