Counter Fraud Newsletter – May 2022

Welcome to the May 2022 edition of our Counter Fraud Newsletter for NHS staff. 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

Energy Bill Rebate Scams

Scammers have been impersonating energy companies to try and trick people into applying for what they are led to believe is a £150 bill rebate. This has included fraudsters pretending to be from Ofgem, but they may also impersonate energy suppliers or local councils using this tactic. Advice on what to do can be found in this article: Ofgem advice

Continued Cyber Risk for the Health Sector

The health sector continues to face serious cyber security threats based on the number of reported incidents to the Information Commissioner's Office (ICO). A report from cyber security firm CybSafe has highlighted that 34% of incidents reported last year were experienced by the health and education sectors, an increase on 2020's figures from the ICO.

The report discusses data which pinpoints phishing as the most common form of cyber attack, with ransomware becoming an increasing trend impacting all sectors. We provided some advice on how to avoid ransomware in the March 2022 edition of this newsletter.

As a quick reminder: please don't click on unexpected links/attachments, do make sure you shut down your computer at the end of every working day to allow updates to be installed, and use strong, unique passwords for each online account.

DVLA Scam Email Sent to NHS Address

A phishing email apparently from the DVLA was received by an employee at her work email address. It had all of the warning signs that this is a scam:

- The email address did not correlate to the DVLA.
- It had a confused message as in one section it referred to vehicle tax and in another section spoke about vehicle licensing,
- It was addressed to a full email address rather than the recipient's name.
- A threat was included – the recipient was told to take action or their driving licence would be terminated.
- Hovering over the link included in the email showed that is was not a link to a DVLA website – in fact, this particular one showed an IP address which is based in Poland.
- Clicking on the link would likely have asked for your details (note the email says you cannot use nicknames or short addresses when you complete the form).

We ask that you remain vigilant to emails like this. Please do not click on any links contained within suspicious messages.

From: [DVLA.CO.UK] Electronic Vehicle Licensing [mailto:info@baba.ed.jp]
Sent: 10 May 2022 13:43
To: XXXXXXXX
Subject: Notification of Vehicle Tax DD Application (Ref: 000000-000039-388292-002)

Strictly Private and Confidential

Dear xxxxxxxxxx@york.nhs.uk ,

DVLA.CO.UK routine check has found some irregularities in your current profile, which indicates that the information given is no longer accurate or up to date. You are required to update your profile to its latest form to avoid termination of your motoring license. You must use your valid and official information to complete this form. Using any nicknames or short-addresses can lead to rejection of this update.

Update DVLA.CO.UK Now

Yours sincerely,

Rohan Gye

DVLA | Vehicles Service Manager

Courier Fraud Warning

National police forces are asking people to watch out for Courier Fraud which is very popular at the moment. In 2021 alone, 3,625 people were victims of courier fraud, with losses totalling more than £15.2 million. Courier fraudsters tend to use one of four strategies:

- **Bank card expiry** – the fraudster claims to be calling from the victim's bank and states there is a problem with their bank card. They ask the victim to confirm their PIN number as part of their "verification" process and then arrange for a courier to collect the card which they then use to commit fraud.

- **High end purchases** – the fraudsters impersonate an undercover police officer and ask the victim for their help with an important investigation. They convince the victim to purchase high value items which they believe will be used as "evidence". The victim is persuaded to send the items by courier to the fraudster.

- **Counterfeit cash/bank investigation** - A person claiming to be a police or banking official informs the victim that they need to help with an investigation into banking corruption. The victim is told to withdraw a large amount of money and the cash is picked up later by a courier to "check for fingerprints or to identify counterfeit bank notes".

- **Computer takeover** – The fraudster calls the victim and claims to be from their internet service provider. They claim the victim is due compensation due to an issue with their internet service. The caller persuades the victim to download a remote access application which then lets the fraudster onto the victim's device. They claim that the victim has been paid too much compensation and that they need to withdraw the excess they then arrange to be collected by a courier.

Courier fraud usually begins with a phone call to the victim. The caller will pose as a trusted official such as a police officer, bank manager or computer engineer. These fraudsters often tell the victim that they mustn't say anything to anyone about what they've been told to do. They may also use a

type of jamming software to hold the victims phone line open, so that if the victim hangs up and tries to call their bank, they can intercept the call.

If you receive a call which appears to fit any of the methodologies above, please end the call. Using another phone, take steps to verify whether the caller was genuine (e.g. call your bank's official customer service number, 101 to speak to the police about calls from police officers, or your internet service provider).

Social Media Safety – New App Released

Now more than ever, we need to ensure that all public sector staff are mindful of their online presence. Hostile actors can easily use social media to conduct research into an individual's interests, activities, and personal and professional connections. They can then use that information to target the individual.

You may not think of yourself as a target, but all NHS staff have access to information and accounts which would be valuable to cyber criminals and hostile actors. As you'll see in the "In the Press" section of this newsletter, NHS email accounts are particularly attractive as they can be used to send targeted attacks against other NHS colleagues. This makes anyone a potential target.

Espionage conducted on social media is becoming increasingly common. MI5 have warned of adversaries operating on an "industrial scale". LinkedIn has reported that it has recently removed 15.4 million fake profiles from its professional networking site.

You are urged to think carefully about your online activity: your social media profile; your wider presence; and the connections you make. Make sure you review your security settings and consider unexpected requests from unknown accounts carefully.

The Centre for the Protection of National Infrastructure (CPNI) Think Before You Link app is an effective way in which any person can protect themselves against those threats. The app features a series of short learning modules that will help raise your awareness of the threats. It focuses on four key behaviours:

Think Before You Link is available for download from Apple and Android App Stores on both your work or personal phone. Should you wish to, you can consider installing this on your personal devices and work through the courses.

https://thinkbeforeyoulink.app/

In the Press

NHS Email Accounts Hit by Phishing Campaign

An NHS-targeted phishing campaign has been uncovered, with 139 NHS email accounts known to have been compromised. These accounts have been used to distribute at least 1,157 phishing emails. The campaign appears to have started in October 2021 and reached a peak in March 2022. It is believed that here are likely to be more compromised email accounts which have not been identified yet. You can read more about this story on The Register website.

Scammers Set to Exploit Cost of Living Crisis

In an article in the Guardian, DCI Gary Robinson (head of the Dedicated Card and Payment Crime Unit) has warned that it is likely criminals will use the cost-of-living crisis to tailor their attempts when targeting potential victims. This has already been seen with fraudsters impersonating Ofgem (see Page 1).

DCI Robinson points out the way fraudsters moved quickly to capitalise on developments throughout the Covid-19 pandemic, with scams covering parcel deliveries, vaccination appointments and tax rebates. You can read the full article here on the Guardian website by clicking here.

Jail Sentence for Pension Fraudsters who Targeted Critical Care Nurse

Fraudsters Alan Barratt and Susan Dalton have been jailed for tricking people into transferring their pension pots into investment schemes that did not exist. In total, the victims of the scam had over £13 million transferred out of their pensions and into the hands of the fraudsters. One of the victims, Pauline Padden, had been a critical care nurse for 40 years and was conned out of £45,000.

A civil trial in 2018 included the mastermind of the operation, David Austin, who has since passed away. A court order had been issued for Austin, Barratt and Dalton to repay the money which had been taken, but so far the victims are yet to receive a penny. A criminal investigation was launched after the civil trial concluded.

The criminal investigation has now concluded, and Barratt has been sentenced to five years and seven months imprisonment. Dalton has been sentenced to four years and eight months. You can read more about the story on the BBC website by clicking on this link.

Counter Fraud Training

Coming soon! Fraud Prevention Masterclasses to return

The Fraud Prevention Masterclasses are due to return in June 2022. The topics that will be covered this year include:

- General Fraud Awareness
- Fraud Awareness for Managers
- Social Engineering and the Psychology of Fraud
- Cyber Fraud
- Recruitment Fraud
- Payroll Fraud
- Creditor Payment Fraud

The sessions will last roughly 1 hour and will be delivered via Microsoft Teams. Topics will be available throughout the year and dates for the sessions will be announced soon.
If you are interested in signing up for any of these sessions, please email rosie.dickinson1@nhs.net and you will be added to the waiting list for when the dates are announced.

Open offer for bespoke training/fraud awareness input

The counter fraud team is always happy to put together bespoke training for your specific role or

department. We are also happy to attend any team meetings to introduce ourselves and talk about NHS Fraud.

If you would like to arrange a session for your team, please contact one of the Local Counter Fraud Specialists (our details are on the next page)

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. You can also report your concerns to the NHS Counter Fraud Authority via their online reporting tool or hotline. 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 or not it is fraud related.
You are very welcome to contact your Local Counter Fraud Specialist for advice and support, our details are below.