Counter Fraud Newsletter – June 2022

Welcome to the June 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.

Current Scam Trends

Monkeypox Scams

Fraudsters have started to send out a new batch of scam text messages which are designed to look as though they have come from the NHS. These messages warn people that they have come into close contact with a person who is infected with the monkeypox virus. The recipient is directed to click on a link in order to pay for a test. The victim is then contacted by a fraudster claiming to be from their bank. The caller claims to be calling to warn the person that they have been conned into sharing their bank details via a fake text message. They then try to convince the victim to transfer their money into a "safe account". This is an established tactic which has been used to great success during the Covid-19 pandemic. You can read about a nurse who was recently targeted by a Covid-19 PCR scam message on page 3 of this newsletter.

The UK Health Security Agency, the national body responsible for monitoring monkeypox cases, would never need to take payment or card details as part of contact tracing. Your bank will not ask you to move money into a "safe account". If you receive a call claiming to be from your bank's fraud team, end the call and either wait 10 minutes or use a different phone to call them back using the customer services number that you will find on the back of your bank card.

Cost of Living Scams

As mentioned in the last edition of this newsletter, the cost of living crisis is very likely to be exploited by fraudsters. At the start of the pandemic, many of us were targeted by emails and texts that claimed to be offering discounts, rebates and grants as a result of Covid-19. Organisations who were impersonated include TV Licencing , British Gas and the UK government. Fraudsters are likely to adapt these messages to claim that discounts, rebates and support payments are being offered due to the cost of living crisis. Action Fraud received 750 reports of fake Ofgem emails in just 4 days.

Please be very wary of texts and emails claiming that you are due to receive a refund, rebate, discount or support payment. Take steps to verify the message, such as making contact with the organisation using their central customer contact details, googling the company name and "scam", and looking closely at the senders details. Please never click on links in these messages. You can read more about cost of living scams on the Daily Record website here.

Ticket and Holiday Fraud

Now that the summer is here many of us will be looking forward to booking some time off and making the most of the weather (when it cooperates!) Unfortunately, fraudsters are keen to take advantage of our summer plans. They may sell fake event tickets that either don't exist or that are not legitimate. This is particularly likely to happen on social media, where profiles are easy to set up and quickly delete. They may also advertise holiday deals or accommodation by stealing images and details from legitimate hotels, travel companies, or Airbnb listings. Fraudsters will often try and pressure you into acting quickly – for example, by saying the deal is only valid for a short period of time, the price is only discounted for the first 5 people to book, or by implying that someone else is very interested and is likely to book soon.

Remember, if a deal looks too good to be true, it probably is. If you are being pressured to act quickly, be extremely cautious. There are loads of tips on how to avoid holiday fraud on the ABTA website. You can read this advice by clicking here. You will find detailed advice and information on ticket fraud on the Take 5 to Stop Fraud site by clicking here.

Missed Parcel Delivery Scam Update

Over the past few years missed parcel delivery scams have become very common. These started life as text messages which were designed to look as though they had been sent by major delivery companies such as Royal Mail, UPS, Hermes and DPD. The message would say you had missed a delivery and needed to pay a fee to organise redelivery, or that insufficient postage had been paid and you need to pay a small fee to ensure delivery took place.

A new version of this scam has now appeared. This time, they don't mention a fee until you have clicked on the "redelivery" link. You can see examples of these texts in this Wales Online article which includes a warning from finance expert Martin Lewis.

Cyber Security

End of support for Internet Explorer 11 browser

On 15 June 2022, Microsoft retired the Internet Explorer (IE) 11 desktop application, and certain versions of IE 11 on Windows 10 will also go out of support. Internet Explorer was first launched back in 1995.

Once technical support to a product or service ends, a vendor no longer provides security updates, which makes systems and devices more vulnerable to attack. The NCSC has guidance about the risk of obsolete products.

Microsoft is advising IE users to move to its newer browser Microsoft Edge. Other browsers such as Chrome and Mozilla not owned by Microsoft are not affected.

New Safeguards Introduced to Battle Cyber Criminals

The National Cyber Security Centre (part of GCHQ) has announced that they are launching a new data sharing initiative which will share details about malicious websites. This will allow Internet Service Providers such as BT the ability to instantly block these sites.

Malicious websites are a key part of many phishing attacks. We have seen fake NHS websites being set up and used as part of Covid-19 text scams since the early days of the pandemic.

To learn more about the new safeguards, read the full article on the National Cyber Security Centre website.

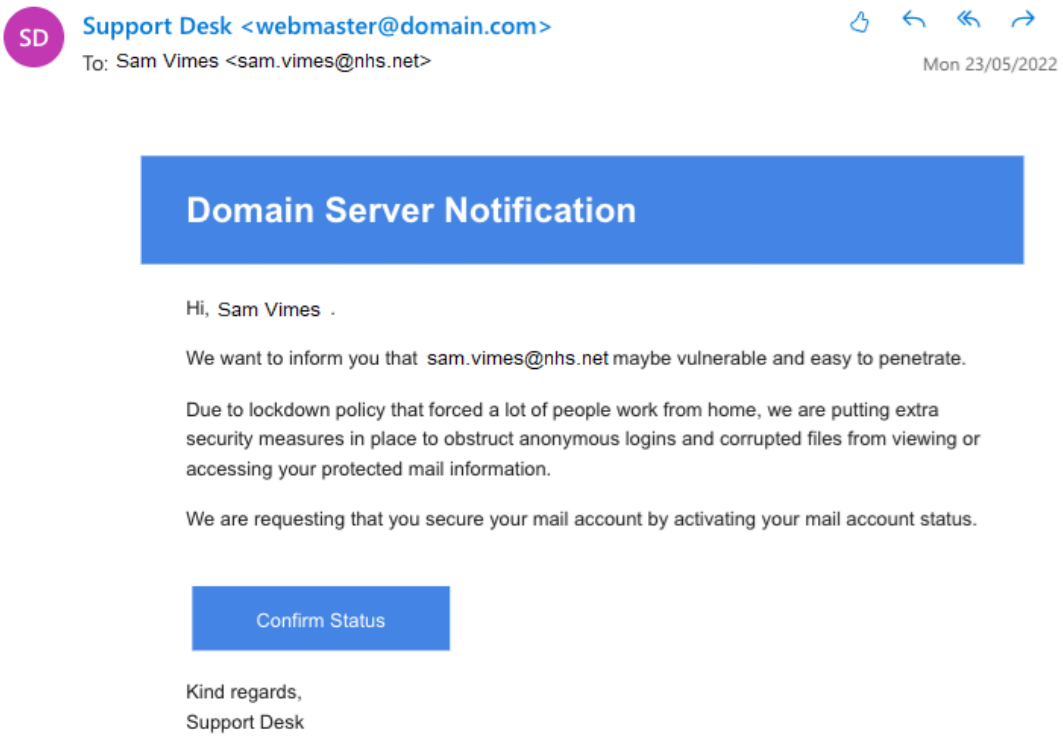
Phishing Email of the Month

The email below was received by a number of NHS employees at the end of May 2022. It claims that the recipients email address may be vulnerable to attack and recommends that they click on a link in order to "secure" their account.

There are a number of tell tale signs on this email. Firstly, it has come from a non-NHS and very generic email address. The formatting is also slightly off, with the email being addressed to the employee using their full name (which has clearly been lifted from their email address). The final sentence about "activating your mail account status" makes little sense.

The email makes a vague reference to "lockdown policy" in an effort to appear legitimate. It also tries to panic the recipient into acting by making them feel worried about their account. Hovering over the link also shows that it will take the recipient to an unknown website, which is likely to be designed to steal their NHS account log in credentials.

If you receive an email like this and are unsure if it is genuine, please contact your LCFS for support. If you are quite happy that you've spotted a phishing email, you can forward it as an attachment to spamreports@nhs.net.


SD

Support Desk <webmaster@domain.com>

To: Sam Vimes <sam.vimes@nhs.net>

Mon 23/05/2022

Domain Server Notification

Hi, Sam Vimes .

We want to inform you that sam.vimes@nhs.net maybe vulnerable and easy to penetrate.

Due to lockdown policy that forced a lot of people work from home, we are putting extra security measures in place to obstruct anonymous logins and corrupted files from viewing or accessing your protected mail information.

We are requesting that you secure your mail account by activating your mail account status.

Confirm Status

Kind regards,
Support Desk

In the Press

Nurse issues warning after losing pay cheque to PCR test fraudsters
A mental health nurse has issued a warning to others after she was the victim of a PCR text message scam. The nurse received a text message asking her to pay for a PCR test. As she'd recently organised a PCR test she thought that the message was genuine. Clicking on the link led her onto a very realistic looking fake NHS website.

After entering her bank details on the site, she received a call from a man who claimed to be from her bank. He told her she'd been tricked into sharing her bank details on a phishing website and persuaded her to transfer all of her wages into what he claimed was a "safe" account. You can read the full story here.

Woman jailed following fake £4m compensation claim against the NHS
A woman who tried to claim over £4 million in compensation from the NHS has been jailed for 6 months for fraud. It was found that she had deliberately exaggerated the effect of injuries which were sustained due to a delayed diagnosis. The patient claimed that the delay had left her unable to walk without a stick and unable to drive for long periods of time without suffering severe pain. She had submitted a claim for compensation on the grounds of medical negligence, and was seeking over £4 million from NHS funds.

Investigators found that although the patient claimed she could not walk more than 10-15 steps without assistance, there was video footage of her walking unaided. It was also found that she had driven for 40 miles without stopping and had lied to four different medical experts. You can read more about this story here.

Counter Fraud Training

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.

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.