Counter Fraud Newsletter – August 2022

Current Scam Trends

"Hi Mum/Hi Dad" Scam Spotted on Multiple Platforms

This scam, which involves fraudsters impersonating victim's children, was first spotted on WhatsApp. There have now been cases where the same scam has been carried out using SMS text messages and other messaging apps.

The messages often start with "Hi mum" or "Hi dad", and will explain that the person's child has lost or damaged their phone and that they have had to change their phone number. The fraudster will exchange a few messages before saying they are having problems, such as being unable to pay their bills because they can't set up online banking on their new phone. The fraudster will ask the victim to help by paying the bills on their behalf until they can get their online banking sorted out.

This type of scam reinforces how important it is to verify who you're communicating with, even if they're claiming to be a loved one. You could ask a question that only your loved one would know the answer to, try voice or video calling to confirm it's really them, or ask them to send you a voice note. Other warning signs for this scam include urgency, poor grammar, getting vague/evasive replies, and requests which are unusual/out of character.

You can read more information about how the scam operates in this article on the Independent website.

Football Ticket Scam Warning

Football fans have been warned that the return of the Premier League could see a surge in fake tickets for matches.

Criminals often target big games that have already sold out – posting pictures of fake tickets and inventing back stories to explain why they are unable to go themselves. Fraudsters are particularly likely to use social media to dupe victims, and will ask for payment to be made by bank transfer.

Once the fraudster has received the money they disappear – deleting their social media accounts and leaving the victim with no way of contacting them. Victims of these scams have lost an average of £410, with some fans losing up to £2,000.

You can read more about this scam on the This Is Money website, and advice on safely buying tickets can be found on the Premier League website. The same tactics are likely to be used for any major events which experience high demand for tickets, so music fans and festival goers should also be wary of social media ticket sales.

Covid-19 Text Messages

Spam text messages about Covid-19 continue to circulate. A recent message which has been reported reads:

> "Trace Alert: You have been in contact with a confirmed case of the latest variant. Please order a free test-kit via: trace.testkit-pcr-gb.com"

Clicking on the link in the message takes you onto a fake NHS website. The website will claim that although the test is free, a small payment of 99p is required to cover the postage. If you supply your payment details, the fraudster is able to use this information to perpetrate further fraud.

For example, some victims of this scam have received a call a few days later, from a person claiming to be from their bank's fraud team or a police officer. They will be notified that they have fallen victim to a spam text. The fraudster then advises the victim that they must move their money into a "safe account" which is controlled by the fraudster.

The message above has been designed to remain relevant no matter which variant is dominant (previous versions of this message have specifically referenced Omicron). It is also likely that the same methodology could be used to send scam texts relating to other health tests, vaccinations, or energy bill/cost of living schemes.

Please be wary of text messages which contain links. If you think a message is spam, you can forward it to 7726 to report it.

If a link from a text message diverts you onto a page which requests your personal information or financial details, please take a moment to consider if you may be in the process of being scammed.

You can find lots of really good advice about impersonation scams like this on the Take 5 to Stop Fraud website

Cyber Security

Cyber Criminals Targeting NHS Staff with New Tactics

We are currently seeing more sophisticated phishing tactics being used against NHS staff. Trends we have become aware of include:

- **Copying and pasting text/images from genuine NHS Digital emails** about topics such as email accounts being upgraded or transferred between different organisations. In these emails, everything looks exactly as it should on the surface, but the links within the message have been tampered with.

- **Using hi-jacked NHS email accounts** belonging to genuine members of staff to send phishing emails. We have seen examples of hi-jacked accounts being used to send out messages that are designed to look like they have come from central services such as NHSmail or ESR.

- **Monitoring compromised NHS email accounts** over a long period of time, before inserting themselves into ongoing conversations between NHS staff and suppliers to divert payments.

- **The use of "rules" on hijacked NHS inboxes** to divert and conceal messages from colleagues, and to make sure the fraudster's presence stays off the victim's radar.

These tactics show an increasing level of sophistication from the fraudsters. It's worth remembering that for the cyber criminal, this is their full time job. Things you can consider when you receive an unusual email are:

- Is it likely that the sender would have a genuine reason to send me this email? (e.g. have you had an email about problems with your NHS.net account or payroll details which seems to be from an unknown NHS employee working at another Trust/ICB/GP practice?)

- Have I got a safe route to check this email with the sender? (e.g. via Teams call or phone call using details from the Outlook address book)

- Are any of the links suspicious? (You can check where a link is going to take you by hovering over it with your mouse)

It is more important than ever that we all stay vigilant to the risks posed by cyber criminals. If you want to brush up your cyber-fraud spotting skills, you are very welcome to sign up to one of our Cyber Enabled Fraud Prevention Masterclasses (please see page 3 of this newsletter), or to contact your LCFS to discuss bespoke training for your team.

You can also get in touch with us if you receive something and you're not sure about whether or not it is fraudulent. There is further advice on how to report a spam email on page 4 of this newsletter, and you'll find our contact details on the same page.

Ransomware

Ransomware is a type of malicious software that encrypts your files and demands that a ransom is paid. The attacker will claim that if you pay the ransom, your files will be restored to you.

Ransomware can be hidden in attachments on phishing emails sent by cyber criminals. It is important that if you receive an email with an unexpected attachment, that you consider whether it is safe to open. If in doubt, seek advice from your Local Counter Fraud Specialist or IT provider.

Ransomware is viewed as a significant online threat to UK organisations. The NHS 111 system was recently put under additional pressure after Advanced, a firm who provide digital services for the 111 system, were successfully targeted by ransomware. The attack left clinicians with reduced access to crucial information needed to make decisions. You can read more about the attack and the impact it has had within the "In the Press" section on page 3 of this newsletter.

The National Cyber Security Centre (NCSC) has also seen evidence of a rise in payments being made to criminals behind these sort of attacks. The NCSC and the Information Commissioner's Office have therefore called for help from the Law Society, after concerns that some victims were being advised by legal teams to pay.

Though it may be tempting to pay to get systems back up and running quickly, it's important to remember that the UK Government does not encourage nor condone the payment of these malware related ransoms.

There's no guarantee you'll get your data back, the fraudsters are likely to target you again the future, you would be giving money to criminals, and your system will remain infected.

You can find more information on ransomware and advice on what to do if you are targeted by this sort of attack on the NCSC website

In the Press

NHS IT supplier held to ransom by hackers

On the 7th of August, Advanced, an IT company who provide support to NHS services including NHS111, experienced a cyber attack. The attack included the use of ransomware, a type of malicious software that locks files and then charges a fee to recover the contents.

An NHS psychiatrist told the BBC that the attack had left them making clinical decisions "*nearly blind*". You can read more about the attack on the BBC news website.

Doctor struck off after claiming for £47,500 of work he had not done

Ashir Patel was a superintendent radiographer for Chelsea and Westminster Hospital NHS Foundation Trust.

In 2019 he was convicted of Fraud by False Representation after it was found that he had claimed money for reviewing 20,000 patient images. He had claimed £44,535.33 for doing this work.

In addition, Patel had submitted false on call claims which generated a further £3,500. He admitted to committing the offences and was given two 16 month sentences, both of which were suspended for 24 months.

Following the expiration of his suspended sentence, the Health and Care Professions Tribunal Service (HCPTS) met to determine whether Patel could continue to practice.

They highlighted that whilst Patel had admitted wrong doing, he had demonstrated escalating and persistent dishonestly over a significant period of time.

In addition, they felt that his insight into the impact of his actions on patients was limited. The HCPTS have therefore struck Patel off the register. You can read the full story on the My London 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** for support. 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 it is fraud-related

You are very welcome to contact the **Counter Fraud team** for advice and support, our details are below.