# Counter Fraud Newsletter June 2023

Welcome to our Counter Fraud newsletter for NHS staff. We hope you find the contents helpful.

## Current Scam Trends

### Car Registration Fraud

Have you ever been sent driving fines or parking tickets that are for a vehicle you don't own?

If so, you may be on the receiving end of car registration fraud. Unfortunately, criminals are aware that they can register a vehicle at any address and under any name if they submit the right paperwork.

This can lead to any driving-related penalties such as speeding tickets and speeding fines being sent to an innocent person who has no link to the vehicle.

You can find out more information about this type of fraud on the Peter Barden website.

**Advice:**

- Contact the DVLA and give them as much information as possible about the car which has been fraudulently registered under your details. You can send them copies of any fines or letters received about the vehicle, but hold on to the originals for your records.
- It may take up to 4 weeks, but the DVLA will be able to issue a letter which confirms that the car is not yours and is not associated to your address.
- Contact the organisation or police force who has issued the fine and let them know that your details have been used fraudulently. Explain that you have contacted the DVLA, and arrange to send them a copy of the proof that the vehicle is not yours once the DVLA has issued it.
- You can find more information on the DVLA website.

### Mobile Phone Fraud

A BBC news article has warned the public to be aware of fraudsters targeting mobile phone users. Thieves may watch you enter your phone's passcode before stealing your device from you when the opportunity arises.

If an unauthorised user gains access to your device, they will try using the same PIN / pattern to unlock your banking apps, will search through any saved notes on your phone looking for passwords and PIN numbers. They can also request password resets if you are logged into your emails on your phone.

The BBC news article includes the story of Jacopo de Simone who had £22k taken from his bank account after losing his phone on a night out.

You can read more on the BBC website.

**Advice:**

Protect your phone with biometric security measures (such as finger print or face unlock) if possible.

- Use strong and unique passwords for each account.
- Enable multi-factor authentication on your email account.
- Don’t store passwords or pin numbers in the notes apps on your phone – consider a password manager instead.
- Be aware of your surroundings when accessing banking apps on your phone.
- Don’t use public wi-fi to access anything sensitive such as financial apps.

**Social Media Scams**

Fraudsters have many ways of carrying out fraud over social media such as posting fake listings on selling pages. They may use hijacked accounts to post these fake items - so that potential buyers feel reassured when they check the sellers profile and see they've been on the platform for years.

They also use social media to find out about you, stealing information such as your name, job title and place of work for use in further fraud attempts, This is especially prevalent on LinkedIn.

**Advice:**

- Use the strongest security and privacy settings available on social media accounts.
- Be wary of offers that look too good to be true.
- Ignore unsolicited messages, and do not click on any links that are sent to you on social media.
- Activate Multi-Factor Authentication if it is available.
- Avoid quizzes that request personal information such as your childhood pet or the street you grew up on.

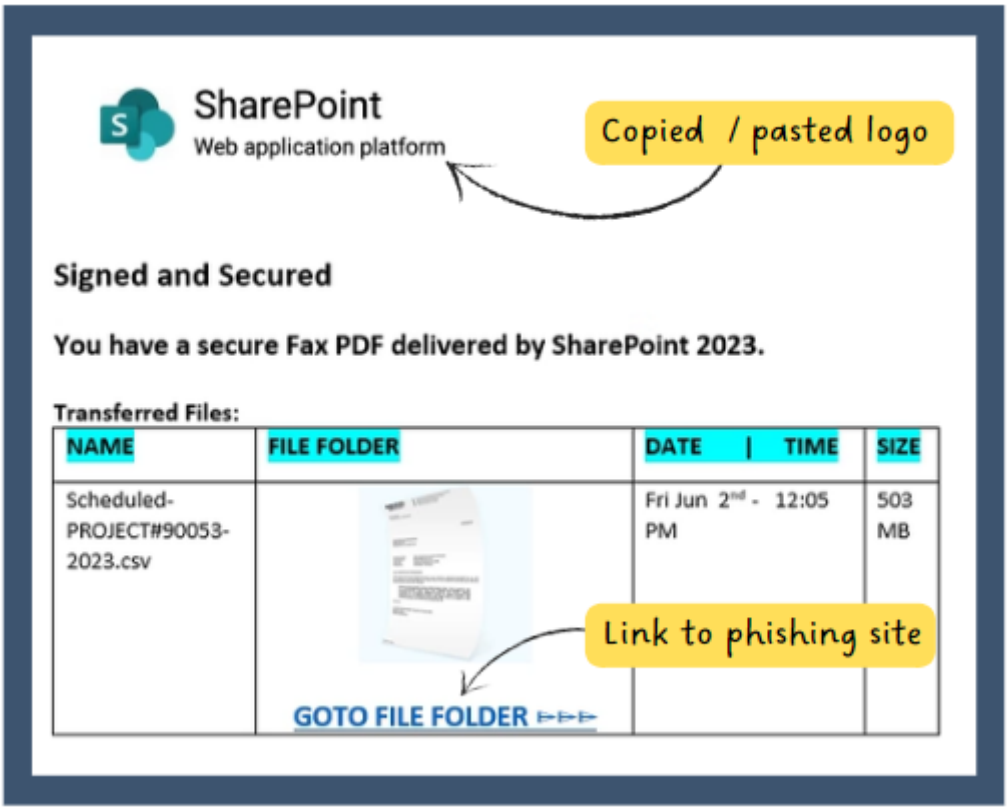
## Cyber Security

**File Sharing Scams**

Phishing emails are often the first step in a fraud attempt. They are designed to trick you into taking action that isn't required - whether that is sharing your log in credentials, making a payment, or disclosing personal or sensitive data. Fraudsters can impersonate NHS colleagues and external partners to try and trick us into taking unnecessary action.

We have recently seen an increase in phishing emails encouraging receivers to click on a link to view a document within SharePoint.

SharePoint is a genuine application which is part of Microsoft Teams which allows documents to be shared and managed amongst users. Fraudsters are emailing NHS staff with a mock SharePoint invite, like the one shown below.




If the recipient clicks on the link, it will ask them to "log in" to SharePoint with their NHS credentials. The person's email address and password will be harvested and used for criminal purposes. Clicking the link may also allow malware to be transferred to NHS systems.

To add credibility to these phishing emails, the fraudster may hack into genuine NHS email accounts to send them from.

**Advice**

- If you receive an email like this which you are not expecting and do not know the sender, **do not click on the link** and contact your IT department or report to spamreports@nhs.net.

- If you do know the sender, give them a call on their **official contact number or Microsoft Teams** to check if the link is genuine. Don't rely on any contact details within the email as these may belong to the fraudster.

**Salary Diversion Fraud**

As it has been reported in the press that many NHS staff are due to receive backdated pay in June, there is an increased risk that fraudsters may try and divert salary payments.

Salary Diversion Fraud often works in a similar way to the Share Point phishing email shown on this page.

Instead of sharing a link to a "secure file" the fraudster sends a link which they claim is for ESR. They often claim that there has been a problem with payroll or that the person's bank details are causing an issue.

This is intended to make the recipient feel anxious, and to click on the "link to ESR" without checking it is safe.

If you hover over the link with your mouse, you should be able to see the web address that it will really take you to.

If you click on the link, you will see a fake ESR page. If you enter your log in credentials, they will be stolen by the fraudster. They can then use your log in to amend your bank details.

**Advice**

- If you get any emails directing you to log into ESR, open a web browser and type in the address manually (https://my.esr.nhs.uk)
- ESR is set up so that if your bank details change, or if a new assignment is added to your profile, you will get an automated email from esr.wfmPROD@nhs.net. If you get an email from this address saying a change has been made and you didn't request it, or if you are not due to start a new assignment, please contact Payroll.
- Use a strong and unique password for ESR.
- Use the strongest privacy settings available on social media accounts.

## 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 using our details below. 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.

## How to Contact Your Local Counter Fraud Specialist:

Your Local Counter Fraud Specialist is: