COUNTER FRAUD NEWSLETTER

May 2021

Welcome to the May 2021 edition of our newsletter. 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

HSBC Scam

Recently, there have been text scams doing the rounds in the UK. The messages start with 'HSBC' in capitals. They go on to state that HSBC are trying to contact the recipient regarding either an 'attempted payment from a NEW DEVICE' or that a 'NEW PAYEE has been set up.'

The message advises the recipient to click on a link within the text message to confirm that the NEW PAYEE was not set up legitimately or that the NEW DEVICE is not legitimate.

So far, these text messages seem to originate from private mobile phone numbers. The links mention HSBC but do not link to valid HSBC websites. For example, a message from number +447425294339 instructs the recipient to click on this link: 'hsbc.validate-new-devices.com'

Be on your guard and do not click on any links in unexpected messages. If you have concerns, contact your bank through established routes that you have used before.

Census Scam

The UK census took place in March 2021. The census documentation and publicity made it clear that individuals could be fined if they failed to complete the census. It seems that fraudsters have tried to take advantage of this and are sending out a text message scam referring to a £1000 penalty. The text states that the recipient has missed out information from their census and if they do not update their details then the penalty will result. A web link is included in the text: nationalcensus-2021.info

The number that has sent the text appears as a private mobile number: +447485724099. Official government/organisation contact will not present as a private number. Anyone receiving this text should NOT click the link or engage with it in any way.

Cyber Scam Techniques - Flubot SMS Scam

We have previously published articles about fraudsters claiming to be from package delivery services. Unfortunately, the criminals developed this scam further in an attempt to get your personal details.

There are warnings in the media about a text message which is being sent out made to look as though it has been sent by a delivery company. The message asks the recipient to click on a link to track the parcel.

Clicking on the link will download spyware – software which will be able to gather information from your phone, such as online banking log in details and passwords, without you knowing.

This is an advancement on the previous parcel delivery scams which used to trick people into giving their personal and banking details.

This spyware can have a major breach on privacy and can also access your contact list allowing the message to be sent to potential victims at an alarming rate. Millions of these messages have already been sent out.

If you are waiting for a parcel, please only track it by accessing the delivery company's official online website, never by clicking on a link within a text message. text message.

If you receive a message like this, forward it to 7726 then delete it from your phone.

If you have received a text, clicked the link and downloaded the app, do not log into anything until you have 'cleaned' your phone. Further information on how to do this is available here FluBot: Guidance for 'package delivery' text message scam - NCSC.GOV.UK

You can read more about Flubot here: Warning over major 'package delivery' scam - BBC News

Covid-19 Fraudster Jailed

Throughout the pandemic many fraudsters have sought to exploit public anxiety about Covid-19 in order to defraud people.

21 year old Teige Gallagher saw the pandemic as an opportunity to commit large scale fraud, and sent out bulk text messages pretending to be from official organisations, including the NHS.

Gallagher set up phishing websites which mimicked the GOV.UK website and sent out texts which claimed to be from the NHS. Recipients were instructed to go to follow a dodgy link to Gallagher's fake GOV.UK site, in order to enter personal details to prove their entitlement to receive the Covid-19 vaccine. The information requested included their personal financial information including details of their bank cards and banking passwords.

Gallagher had also impersonated various banks and Netflix in other scams. Police found a list of 2000 telephone numbers at Gallagher's home, who are believed to be potential victims of the various scams.

Following his conviction at the Old Bailey, Teige has been sentenced to 4 years and 3 months in prison.

You can read more about the story on the Crown Prosecution Service website: [COVID-19 fraudster jailed for mass cyber scam | The Crown Prosecution Service (cps.gov.uk)]

Arrests following Royal Mail Scam Texts

Eight suspects have been arrested following an investigation into a series of scam text messages which claimed to be from Royal Mail. The messages asked the recipient to click on a link and pay a fee in order to arrange re-delivery of their item.

As you'll have seen from the Flubot article, parcel delivery scams have been very popular over the last 12 months, with fraudsters impersonating several major parcel delivery companies.

You can read more about the arrests here: https://www.bbc.co.uk/news/uk-england-57226704

Fraudsters Sentenced after £18,700 NHS Loss

Two Care Assistants working at Greater Manchester Mental Health NHS Foundation Trust have been sentenced to 8 months each for retaining credits for bank shifts they did not work and defrauding the NHS by over £18,700.

During the investigation it was found that both had signed up to work a large number of night shifts between April 2016 and July 2018 but failed to work most of them. When interviewed each admitted to being paid for shifts they hadn't worked and that they had not notified their manager or the payroll department of this. They both pleaded guilty to retaining wrongful credits in Manchester Magistrates Court.

The male pleaded guilty to retaining £9,732.33 in monies paid to him for shifts that he didn't work. The female pleaded guilty to retaining £9,004.17. Both have repaid the monies in full, which was taken into consideration by the judge when handing down the sentences.

They both received 8 month prison sentences (suspended for 12 months). The male, who had recently qualified as a nurse, has also been referred to the Nursing and Midwifery Council which will instigate its own disciplinary process and has the authority to remove him from the NMC nursing register. This could jeopardise his recently acquired staff nurse position, which he additionally failed to declare previous convictions/investigations on his application for.

For more about the offence of Retaining a Wrongful Credit, see the "Did You Know?" article below.

Did You Know? Retaining a Wrongful Credit

You might remember that there is a chance card in Monopoly which announces you've got £200 after a bank error in your favour – however, if that happened in real life, you would be breaking the law by keeping hold of that money.

It is a criminal offence to keep money which has been accidentally paid to you. If you know or believe that you have been credited money incorrectly, you could be prosecuted under the Theft Act 1968 if you do not take steps to rectify it. Money can be wrongfully credited due to a mistake at a bank, or a payroll discrepancy if you leave a job but continue to get paid.

There has been a recent case in the news of a Doctor who was accidentally paid after losing his job. He kept the overpaid £41,000 saying that he had believed it to be a 'gift'. He has since been struck off the General Medical Council register. You can read more about his case by clicking the link below:

Doctor mistakenly paid for two years after losing job at Royal Liverpool Hospital - Liverpool Echo

Counter Fraud Training

Training Sessions

A central part of your Local Counter Fraud Specialist's role is to raise awareness of fraud within the NHS. This can take many forms but the most successful and popular method for us to do this is via face-to-face training with staff. Thanks to the range of conference calling software now at most people's fingertips, we're able to offer online fraud training.

Our Fraud Awareness training focuses on:

- How different types of fraud affect the NHS
- Practical advice on what to look out for and methods to protect yourself and your organisation from fraud
- Real life case studies showing how the NHS is targeted
- Information on how to report concerns about fraud

This training can be arranged to suit you and will be delivered via Microsoft Teams. It is part of our normal service and can be delivered to groups of any size. We are also able to design and deliver bespoke training packages based on any fraud related areas of concern that you feel are most relevant for your team.

We are currently running masterclasses on several different topics. These are being delivered remotely on Microsoft Teams and WebEx. The current set of masterclasses cover how to identify and prevent:

- Cyber enabled fraud - phishing and mandate fraud
- Recruitment fraud
- Payroll fraud (designed for new starters in Payroll teams or as a refresher for Payroll staff)

To register your interest in a session, contact one of the LCFS team using the details below.

How to Contact your Local Counter Fraud Specialist

If you would like more information or advice about fraud and the latest scams, or to raise a concern please feel free to contact your Local Counter Fraud Specialist. You can find our contact details below:

Steve Moss, Head of Anti-Crime Services	Steven.moss@nhs.net 07717 356 707
Marie Hall, Assistant Anti-Crime Manager	Marie.Hall15@nhs.net 07970 265 017
Rosie Dickinson, Local Counter Fraud Specialist	Rosie.dickinson1@nhs.net 07825 228 175
Lee Swift, Local Counter Fraud Specialist	Lee.Swift1@nhs.net 07825 110 432
Shaun Fleming, Local Counter Fraud Specialist	Shaunfleming@nhs.net 07484 243 063
Nikki Cooper, Local Counter Fraud Specialist	Nikki.cooper1@nhs.net 07872 988 939
Richard Maw, Local Counter Fraud Specialist	R.maw@nhs.net 07771 390544
NHS Counter Fraud Authority Fraud and Corruption Reporting Line	0800 028 4060