COUNTER FRAUD NEWSLETTER

AUDIT YORKSHIRE
The journey to excellence

August 2021

Welcome to the August 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

PayPal Phishing Scam

A current PayPal email phishing scam has been identified. The emails state the recipient's account has been "limited" as a result of a policy violation.

The emails ask for customers to update their account, or check the security of their account by clicking a link in the email. The links provided in the emails lead to genuine-looking websites that are actually phishing sites designed to steal PayPal login details, as well as personal and financial information.

If you receive an email you're not quite sure about, you can report it by forwarding the email to the Suspicious Email Reporting Service at report@phishing.gov.uk. You should not click on links within unsolicited emails or text messages. If you feel concerned about your PayPal account, you can contact them using their official website and customer service number.

Matching Numbers Scam

The National Fraud Intelligence Bureau has circulated an alert warning the public about a new type of scam call. These calls look like they are coming from a phone number which is almost identical to your own.

Usually, the first 7 digits (07xxxxx) match your phone number. If you answer the call, you will hear a recorded message claiming to be from an official organisation (such as the HMRC or the police) asking you to "press 1" to speak to an officer about an unpaid fine or arrest warrant. These calls have also been received via messaging apps such as WhatsApp.

Please remember that official organisations will not notify you about fines or police warrants by texting or phoning you. Suspicious telephone calls should be ended immediately, and can be reported via the Action Fraud website www.actionfraud.police.uk/report-phishing.

Cyber Security Tips - Password Advice

It is really important that you vary your passwords to protect your online accounts.

For example, lets say you receive a phishing text. This message appears to be from Royal Mail, and says that you've recently missed a parcel delivery. It includes a link that you can click to reorganise the delivery. You click on the link, and a webpage opens which has the Royal Mail logo and branding.

The website asks you to fill in a form, including your name, postal address, email address and date of birth (to "prove" your identity). Next, they ask you to set up a password to "secure" the information you've just entered. They might also ask for a small transaction fee—say £1.50 to pay for redelivery.

If you do use the same password for everything, chances are that when you fill this form in, you will automatically use your "go-to" password. All the information you've provided on the form is harvested.

The fraudster will then go to your email account and try the password you just gave them to see if it lets them in. They may also head over to online shopping platforms such as eBay or Amazon, and input your email address and the password you just provided. If they do get access to your email account, they can then request password resets for other online accounts that you hold, locking you out.

The other information you entered on the "redelivery form" can also be used against you. For example, you may be targeted by someone claiming to be from your bank alerting you to suspicious activity a few days after completing the form. If you did pay the small transaction fee, the fraudsters will know who you bank with, your address, and what your date of birth is. If they got into your email account, they will also have a good idea of any recent online orders you have placed and can use all of this to appear more convincing when impersonating your bank.

◦ Please make sure to use strong, unique passwords for all of your accounts.

◦ In particular, make sure your email password is robust and do not recycle this for any other accounts.

◦ Be wary of unsolicited emails and texts, especially if they ask for personal information or payments.

◦ Consider using a password manager to keep on top of your passwords.

◦ If contacted by someone claiming to be your bank, hang up, and use a different phone to call the customer service number for your bank (you'll find this number on the rear of your bank card).

NHS Test and Trace Visit Advice

Action Fraud have released advice for people who are planning international travel over the next few months. If you have returned from an international trip and you are legally required to quarantine for 10 days, NHS Test and Trace may visit your address to ensure that you are complying with the law.

Action Fraud advise that the NHS Test and Trace staff will be wearing NHS Test and Trace branded clothing, and they will visit you at the address listed on your passenger locator form. They will identify themselves verbally and present you with their ID card. They will ask you to confirm your identity too, by showing your passport or driving licence. They may visit a number of times during the 10 day period.

NHS Test and Trace staff will NOT:

◦ Enter your home,
◦ Ask you for anything other than to see and photograph your identity document,
◦ Ask for your financial details
◦ Ask you to make a payment or issue a fine
◦ Inform you of the visit in advance via text or email

If someone attends your home claiming to be from NHS Test and Trace, and you do not believe they are legitimate, Action Fraud advise that you should call the police.

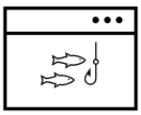
Covid-19 Vaccine Fraudster Jailed

In late December 2020, during the early stages of the Covid-19 vaccination roll out, fraudster David Chambers attended the home address of a lady in her 90s. Chambers was wearing a fake lanyard and claimed that he was from the NHS.

He informed the victim that he was there as part of the vaccination roll out, and pretended to administer the vaccine to her by pressing a “dart-like” implement into the back of her wrist. He then claimed that she needed to pay him £140 which he said would be refunded by the NHS at a later date. The victim paid him the money and he left. A few days later, Chambers came back to her home and told the victim that she needed to pay another £100, but she refused.

Chambers has been found guilty at court and was sentenced to three and a half years in prison. The victim described the incident as “harrowing” and hoped that her experience would not put other people off from accepting the jab.

Mass Text Phishing Fraudster Arrested



A Covid-19 scammer who had sent out thousands of phishing text messages during the pandemic has pleaded guilty to charges of Fraud by False Representation.

Abdisalaam Dahir was charged with the offence after he was linked to bulk phishing text messages impersonating a range of official organisations including HMRC, Royal Mail, HSBC, Nationwide, Three and EE. The HMRC text messages sent out encouraged recipients to provide their personal details in order to access a “Covid-19 grant”.

The phishing texts all included web links that the victims were encouraged to click on, in an attempt to harvest sensitive personal data for use in further fraud offences.

It was estimated that Dahir could have caused up to £185k worth of loss to his potential victims.

Dahir has not yet been sentenced. Members of the public have been reminded to report suspicious texts and emails using the official channels:

◦ Spam text messages can be forwarded to 7726

◦ Phishing emails can be reported to report@phishing.gov.uk

◦ Suspected phishing websites can now be reported using the National Cyber Security Centre online reporting tool: Report a suspicious website - NCSC.GOV.UK

◦ If you think you have been defrauded, you should contact your bank as soon as possible to see if they can stop the money from leaving your account, or return it to you. You can also report the matter to Action Fraud using their phone number 0300 123 20 40 or website: Action Fraud

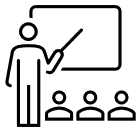
Counter Fraud Training

NEW - Fraud Prevention Masterclasses

The LCFS team are currently scheduling a series of Fraud Prevention Masterclasses, covering key fraud risks within different areas. The masterclasses are delivered via Microsoft Teams and will last around 45 minutes to 1 hour.

The sessions are being delivered on a monthly basis, and cover some key areas that have very specific fraud risks. They include an overview of the various risks which may be encountered, real life case studies and practical advice on the prevention of fraud risks.

If you have an interest in any of the topics below and would like to sign up for a session, please get in touch with Rosie Dickinson (rosie.dickinson1@nhs.net)



Recruitment Fraud

Ideal for staff with responsibility for pre-employment checks.

3rd September 10-11
11th October 10-11
5th November 10-11
4th February 10-11

Payroll Fraud

Ideal for payroll staff who are new or would like a refresher.

9th September 10-11
15th October 11-12
10th November 11-12
12th January 2-3
11th February 10-11

Creditor Payments

Ideal for staff in accounts payable or who deal with invoices/suppliers.

10th September 10-11
15th November 10-11
10th December 11-12
14th January 11-12
18th February 10-11

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 https://cfa.nhs.uk/reportfraud