COVID-19 FRAUD ALERTS

ISSUE 3

Welcome to our third Covid-19 newsletter. We know that these are anxious and uncertain times for many of us and we are not wanting to scare people with news of fraud.

Our aim in these communications is to raise awareness and to offer advice so that you can look after yourself and our NHS.

Test and Trace App

The NHS Test and Trace Service is now up and running. The official phone number is 0300 013 5000 and there is more information on their website https://www.gov.uk/guidance/nhs-test-and-trace-how-it-works. You may be contacted by phone, text or email.

Please bear in mind that the genuine testers will **NOT** -

- call you from any premium rate number, such as one starting with 07 or 087
- ask you for any financial information such as a debit or credit card number
- ask you to set up a password or pin number

If you do receive a genuine call and are uncomfortable, you can always ask to complete the information on the official web based service instead - https://contact-tracing.phe.gov.uk/

You can report suspicious texts by forwarding the original message to 7726, which spells SPAM on your keypad.

Questions have been asked about the security of the NHS tracking app. Please be assured that –

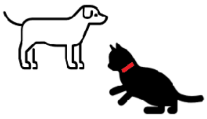
- You remain anonymous and your personal data will not be collected
- The data of people you interact with will not be collected on the app
- Any data in the app is encrypted
- Systems which the anonymous data is uploaded onto is secure and will not be enough to identify individuals
- It is not linked to other data which the NHS holds

For more information about the security of the app and how contact tracing works, please read this article from the National Cyber Security Centre: https://www.ncsc.gov.uk/blog-post/security-behind-nhs-contact-tracing-app

Pet Purchase Frauds

As many people are going to be housebound for the foreseeable future, it is appealing to some to welcome a new pet into the family. Unfortunately, as demand has risen online pet sales have become an attractive target for fraudsters.

Action Fraud have reported that over March and April, 669 people have reported paying £282,686 between them in deposits for pets which have been advertised online. The victims have been told they cannot see the animals due to lockdown restrictions and after paying a deposit, some have parted with more cash as they have been asked for further money to cover vets bills, insurance or delivery of the pet.



If you do decide to add a bundle of fluff into your house, we advise the following –

- Research the seller - genuine advertisers should be able to provide background details of the litter, and are usually happy to send you regular photos and videos of the pup/kitten as they grow.
- If you cannot go and see the animal you are interested in buying, ask the seller for a video call. If they refuse or come up with excuses, be alert that this may be a scam.
- Make any payments by credit card or PayPal. A bank transfer will offer less protection.
- Trust your gut—if something doesn't feel right, chances are - it's not!

Join the Fight to Bring Down Bogus Sites

We referred to fake email sites in our first Covid-19 newsletter. Scams which are currently doing the rounds include offers of goods such as testing kits and PPE and links to bogus official websites such as the HMRC which will then capture any personal details which are input.

The public are being asked to forward any suspicious emails via the National Cyber Security Centre's (NCSC) new Suspicious Email Reporting Service. As a result of the 160,000 referrals they have had so far, they have been able to remove 1,400 links to scams.

The NCSC are only able to remove malicious URL's if they are made aware of them so they are urging the public to forward any suspicious emails to report@phishing.gov.uk

What is Social Engineering?

Social engineering is essentially hacking a person. A criminal will manipulate people into opening email links or parting with personal details.

One way of social engineering is "phishing", a way in which criminals will contact you to obtain details or encourage you to access fake sites. If you want to know more about phishing, please view this 2 minute video – https://youtu.be/AsUNFVhdfao

"Spear phishing" is a more advanced version of phishing – and more convincing. This happens when a criminal will specifically target you. They may send an email which appears to be from a named person you know – such as a senior member of staff or from somebody in the IT department.

One way of identifying if an email is genuine is to check the sender's email address. To do this, hover your mouse cursor over the email address shown and it should bring up full details.

Often emails will have been generated by copying a genuine address and making minor amendments which the criminal hopes will go undetected. For example, an email looking as though it has come from the police may be showing as @westy0rkshire.police – the 'o' in police has been changed to a zero.

Also be wary of suffixes such as @yahoo.co.uk or @gmail.com. Companies tend to use .co.uk or .com.

If in doubt, research the contact details of the company on the internet or contact them to check whether they have sent you the email by using an established contact – not one contained in the body of the email.

Counter Fraud Training

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.

As we are all currently trying to maintain social distancing, this is obviously not something we can offer at the moment. However, 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 free of charge and can be delivered to groups of any size. If you are interested in organising a session, please contact one of the team using the contact details on the next page

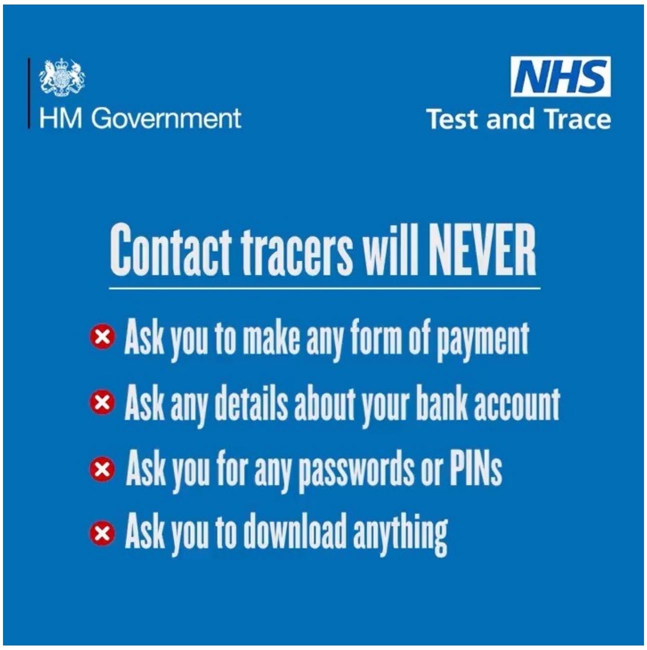
If you don't have access to Microsoft Teams, you can access our E-Learning module which is available here:

https://www.nwyhelearning.nhs.uk/elearning/yorksandhumber/shared/FraudAwareness/HTML/index.html

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
Olivia Townsend, Local Counter Fraud Specialist	Olivia.Townsend@nhs.net 07717 432 179
Lee Swift, Local Counter Fraud Specialist	Lee.Swift1@nhs.net 07825 110 432
Shaun Fleming, Local Counter Fraud Specialist	Shaunfleming@nhs.net 07970 264 857
Richard Maw, Trainee Anti Crime Specialist	R.maw@nhs.net



HM Government

NHS
Test and Trace

Contact tracers will NEVER

- ☒ Ask you to make any form of payment
- ☒ Ask any details about your bank account
- ☒ Ask you for any passwords or PINs
- ☒ Ask you to download anything

Find out more about Covid-19 Fraud and how to report scams you may come across outside of work on the Action Fraud website:

https://www.actionfraud.police.uk/covid19

For information on how to spot Covid-19 phishing emails, please read this helpful BBC article:

https://www.bbc.co.uk/news/technology-51838468

Handy tips and helpful advice from the National Cyber Security Centre can be found here:

https://www.ncsc.gov.uk/cyberaware/home