COVID-19 Fraud & Security Alerts

Ref: CFMG-002

NHS Counter Fraud Managers Group (CFMG)

Supported by TIAN and 360 ASSURANCE

NHS Tracking App

As reported in last week's alert, a text scam has been reported alerting recipients that they have been in contact with a person with a positive COVID-19 test result. Prior to the national rollout of the NHS tracking app, the scam texts have continued to circulate. Recipients receive a text message stating 'Someone who came in contact with you tested positive or has shown symptoms for Covid-19 & recommends you self-isolate/get tested.' A link is contained within the text to a bogus website, in an attempt to gain personal details.

Read more here

National Crime Agency (NCA) act against COVID-19 scammers

Following two separate NCA investigations a pharmacist and a surveyor have been arrested on suspicion of illegally selling Coronavirus testing kits. The pharmacist was arrested under the Fraud Act 2006, following false claims about the tests capability. In a separate investigation a surveyor was stopped whilst driving and was found to be in possession of 250 COVIID-19 testing kits. Similar to the pharmacist, he was arrested under the Fraud Act 2006.

In a separate incident the NCA also took down a website fooling victims into buying non-existent personal protective equipment through phishing emails.

Read more here

EasyJet cyber incident

This week EasyJet reported that a highly sophisticated cyber-attack had affected around nine million customers. Travel details and email addresses have been stolen, along with a small number of credit card details. The attack occurred in January, however EasyJet have released details in order to warn customers of phishing attacks. The data may be used to take advantage of COVID-19 flight cancelations. Click here to read more

The National Cyber Security Centre (NCSC) has also issued information and advice for customers of EasyJet as follows:

- EasyJet have issued a statement regarding this incident.
- Anyone who thinks they have been a victim of online crime can report a cyber incident using Action Fraud's online fraud reporting tool anytime of the day or night, or call 0300 123 2040. For further information visit www.actionfraud.police.uk.
- If you're an EasyJet customer, NCSC recommend changing your password on your EasyJet account – and if you know you've used that password anywhere else, change it there too. The best way to make your password long and strong is by using a sequence of three random words you'll remember. Of course, remembering lots of passwords can be difficult, but if you save them in your browser then you don't have to. There is more information on the NCSC website.
- It would also be a good time to check if your account has appeared in any other public data breaches. Visit https://haveibeenpwned.com, enter your email address and go from there.
- Two-factor authentication (2FA) is a free security feature that gives you an extra layer of protection online and can stop cyber criminals getting into your accounts - even if they have your password. If it is available use it on all your important accounts.
- If your account has been compromised, your personal details may be used to help craft more convincing scam emails. If you believe you have received a suspicious email then you can report it to the NCSC using the Suspicious Email Reporting Service (SERS) but the NCSC has produced advice which will help you spot the most obvious signs of scam emails.
- EasyJet confirmed that 2,208 credit card details were accessed in this incident. If you were one of them, you should be notified of this by EasyJet. NSCS advise that you monitor your accounts for any unusual activity and if you're worried, get in touch with your bank's fraud department.

Click here to read more on the NCSC website.

Business Against Scams initiative launches to fight COVID-19 scammers

Over 100 businesses and Trading Standards are spearheading a new initiative to combat business fraud, in response to the increase in fraud exposure due to homeworking. Business Against Scams has launched as a new element of Friends Against Scams, an initiative run by National Training Standards. The new initiative provides tools to businesses with the aim of up-skilling and training workforces to identify and prevent scams. Tools include online training modules covering scam examples and guidance on how to prevent falling victim to the scams.

Lord Toby Harris, Chair of National Trading Standards, said:

"Scams not only deceive legitimate businesses, they risk undermining the UK's economic recovery. As more employees work from home, we're urging businesses to protect themselves, their employees and their customers to help prevent significant financial losses or data protection breaches."

Louise Baxter, Head of the National Trading Standards Scams Team, said:

"We've launched Businesses Against Scams as a free tool for organisations to help safeguard their business and protect their workforce and customers. More than 100 businesses have already signed up to the free training, which is empowering businesses and employees – who are

all adapting to new working environments – to take a stand against scams by equipping them with advice and knowledge on how to identify and prevent a scam."
Read more here
Access the Business Against Scams webpage here

COVID-19 scammer charged

A man has pleaded guilty to sending out a large number of fraudulent text messages linked to Covid-19 following an investigation by the Dedicated Card and Payment Crime Unit (DCPCU), a specialist police unit funded by the banking industry. Mohammed Khan, 20, from Camden, London, pleaded guilty to one count of fraud by false representation and one count possession of articles for use in fraud, after being arrested and charged by DCPCU officers last week.

Officers from the unit were also able to recover bank account information that had been harvested through the scams and share them with the banking industry, enabling over 200 customer accounts to be protected. Intelligence work by the DCPCU and Action Fraud identified that the suspect was involved in sending large-scale 'smishing' text message campaigns exploiting concerns around Covid-19 to defraud the public. Some of the fraudulent messages claimed to be from the UK government and offered a tax refund as a result of the pandemic. The messages included a link to a form on a fake webpage imitating official government websites, with the aim of tricking customers into giving away their personal and account details that could later be used to commit fraud. Other messages claimed to be from mobile phone operators offering a refund due to the impact of Covid-19, again including links to fake websites to harvest customer's details.

DCPCU officers executed a search warrant at Mr Khan's home address in Camden, London on Wednesday 13 May and seized a number of digital devices. Analysis of these devices provided evidence that the suspect was involved in the Covid-19 fraudulent messaging campaigns. Mr Khan was arrested by DCPCU officers at his home address on Thursday 14 May and charged with fraud by false representation and possession of articles for use in fraud. He pleaded guilty to both charges at Westminster Magistrates' Court on Friday 15 May. He has now been remanded in custody while awaiting a court sentencing date.

Read more here (UK Finance)

Increase in pandemic pension scammers

Pre-pandemic research from the Pensions Regulator (TPR) and the Financial Conduct Authority (FCA) have already uncovered some concerning statistics around scams targeting those nearing or in retirement. The Investment Association (IA) are now issuing a warning around the further increase of these scams during the Covid-19 crisis. The warning comes as Action Fraud, the UK's fraud reporting centre, recorded total losses of nearly £970,000 owing to Covid-19 fraud in February and March, with a noticeable increase in online fraud specifically. Many of the fraudsters are convincing and appear to be legitimate. If you have any concerns of regarding an investment or pension opportunity being offered, you can check whether the company is genuine at fca.org.uk/scamsmart.

(CIFAS, Leaders in fraud prevention)

COVID-19 benefit and furlough fraud

It has been reported that due to a significant increase in Universal Credit applications during the pandemic, a number of processes have been relaxed. It is believed that because of this the cost of fraudulent claims could reach £1.5bn. The relaxed processing of claims includes carrying out identity checks online rather than face-to-face, whilst other information was taken on trust, such as claimants living costs and self-employed status. It is feared that as payments had been paid out in advance, it would be difficult to get this money back, as some claimants may not be traceable.

Read more here

The Financial Times report that across Europe furlough schemes are plagued with fraud. An economics professor estimates between 8-10% of claimants of the German scheme will be lost to fraud. It is estimated that across the largest five European nations furlough schemes will exceed €100bn. The UK Government report it has received 795 allegations of abuse of the furlough scheme.

Read more here

UK Government Digital Marketplace victim of scam advert

The Cabinet Office confirmed that the UK government Digital Marketplace has been victim of a spoof application to provide services. The website provides public sector organisations a marketplace to find suppliers, people and technology for digital projects.

The spoof fraud consultancy service listed on the portal stated in its advert; "we develop bespoke Cloud-based online fraud solutions to target gullible consumers into parting with their cash, using payment gateways in Russia rotating funds through the Cayman Island to facilitate payment to public sector customers through UK-based institutions untraceable to the fraudulent activities."

Sold at £10,000 per transaction, the advert states the service offers total discretion and significantly increases cash generation opportunities.

The contact on the advert is listed as Frank Abignale, the same name of the fraudster in Steven Spielberg's Catch Me If You Can film.

Once contacted by The Reg (an online technology publication) the Cabinet Office removed the listing.

Read the full article here

Suspicious email reporting service

The suspicious email reporting service was launched on April 21 by the National Cyber Security Centre (NCSC) with the objective of gaining information on scam emails from the public. Recipients of suspicious emails are urged to forward the messages to report@phishing.gov.uk

In two weeks 160,000 suspicious emails have been flagged to the service and reports significantly increased following backing from Martin Lewis from MoneySavingExpert. Reports have led to the removal of over 300 bogus websites.

Ciaran Martin, Chief Executive of the NCSC, said:

"This really is a phenomenal response from the British public. I would like to thank them for embracing our reporting service as well as the many organisations which have promoted it. While cyber criminals continue to prey on people's fears, the number of scams we have removed in such a short timeframe shows what a vital role the public can play in fighting back. I would urge people to remain vigilant and to forward

suspect emails to us. If it looks too good to be true, it probably is."
Read more here

Other type of fraud examples

Email Scams – Phishing emails

- UK Government COVID-19 tax relief scam emails are reportedly still being sent. The latest communications require recipients to click on malicious links in order to get a 'free tax relief evaluation'.
- The World Health Organisation (WHO) phishing attempts have been reported, emails state that the WHO are offering $450,000 to selected individuals. Recipients are asked to email the sender for more information quoting reference W.H.O-511.
- We reported last week that a number of scams had been identified centred around false COVID-10 business funding. It has also been found that fraudulent applications have been made for government grants using legitimate business details, likely to have used information gained in phishing campaigns.
- File sharing phishing campaign: With many workforces transitioning to a remote environment, tools such as online file sharing and cloud storage devices are being used more frequently. Threat actors are choosing to target users of these platforms by using phishing emails. The emails look legitimate and trick recipients into clicking links by stating someone has just shared an important file with them. The link directs the recipient to a page harvesting personal & company credentials.
- A new phishing campaign, found in environments protected by Microsoft and Symantec, that not only impersonates a company's management but also suggests that a fellow employee has tested positive for the disease, urging users to read an enclosed malicious attachment posed as "guidelines" or "next steps."

Online Retailers / Counterfeit goods

- In last week's alert, we reported fraudsters advertising pets for sale. This continues to be a problem with Action Fraud stating that 669 people lost a combined total of £282,686 when putting down deposits to purchase pets that end up to be fake advertisements. The fraudster advertise puppies and kittens for sale on social media platforms and selling platforms, including websites dedicated to pet sale. The victim will be asked to pay a deposit to secure the purchase. The fraudster will not let the pet be collected in person due to the lockdown. More funds will be requested to cover delivery costs, pet insurance or vaccinations. Be alert and trust your instincts - look for any suspicious behaviours, and ask for a video of the pet. Choose your payment method wisely, use payment methods with more protection e.g. PayPal or credit card.
- Vehicles for sale that cannot be viewed due to COVID-19.

Spoof websites / software / emails

- Newly updated Microsoft 365 and Azure AD log in pages have been spoofed by attackers. By replicating updated sign in pages the attacks appear more convincing. Various phishing campaigns have been used incorporating the spoof sign in pages. One method involves PDF email attachments with the subject 'Business Document Received'. The documents then require the user to sign in on spoof pages mimicking the new Microsoft sign in page design. Read more here.
- People sometimes choose to install apps that are not available in their region or any official store, opening their system up to malware that will steal private data. A recent fraudulent Android application offered fake Covid-19 information, but its real goal was to steal users personal data including SMS messages, call logs, contacts, and more.

Social media and other messaging platforms

- Fraudsters claiming to be from Aviva are contacting people through social media and other messaging platforms (such as WhatsApp), asking them to share their personal details or pay money in order to apply for a job. To appear more legitimate job adverts use the Aviva name and other public information from the Aviva official website. Unfortunately, these are not legitimate. If you're contacted by someone you don't know or trust asking you to apply for a role at Aviva, do not reply to their message. Instead report this to Aviva immediately.
- Similar to the phishing email scams highlighted last week, associated scams have been identified using social media platforms. One example uses the Department of Work and Pensions branding.