COVID-19 Fraud & Security Alerts

Ref: CFMG-0015

NHS Counter Fraud Managers Group (CFMG)

Supported by TIAN and 360 ASSURANCE

NHS supplier mandate fraud attempts

This week we have been alerted that two NHS suppliers have warned customers of mandate fraud attempts.

The University of West Scotland has identified a fraudulent attempt requesting changes payment details. The University of West Scotland has confirmed payment details have not changed and will appear on sales invoices.

Infection prevention company Gama Healthcare Ltd has also this week reported a mandate fraud attempt. Citing recent communications attempting to change bank account details, the company has contacted customers to confirm bank account details have not changed.

NHS Counter Fraud Authority (CFA) protecting the NHS against COVID-19 fraud

As a reminder, the NHS CFA has produced guidance on measures to help protect the NHS from fraud during the COVID-19 pandemic. Areas of increased fraud risk include; mandate fraud, procurement fraud, recruitment fraud, payroll and frauds targeting individual NHS staff.

Read the CFA guidance here

NHS staff targeted by Coronavirus fraudsters

Computer Weekly have revealed this week that almost 30,000 fraudulent emails were received by the NHS during the height of the coronavirus pandemic. A Freedom of Information request revealed data from NHS Digital showed almost 30,000 malicious emails were reported in March and April 2020. The article states in one case the St Helens and Knowsley Teaching Hospitals NHS Trust warned staff of fraudulent emails to HR and payroll teams purporting to be from employees in an attempt to change bank details.

Read the article here.

NHS Contact tracing scam

This week consumer goods organisation Which? has alerted members signed up to their scam email service that scams related to the Governments Track and Trace system continue to circulate. Which? has produced an article covering the contract tracing service works and how to identify scams.

Read the Which? article here

Interpol report shift in cyber-attacks during pandemic

Interpol has reported it has seen a major shift in the target of cyber-attacks during the pandemic. The article outlines that an Interpol assessment shows the focus of frauds has shifted from individuals and small business to major corporations, governments and critical infrastructure. The reports key findings include; online scams and phishing methods have been developed to incorporate COVID-19 themes, such as impersonating government and health authorities. In addition the report shows an increase in disruptive malware and ransomware attacks on critical infrastructure and healthcare organisations.

Read the article here

National Fraud Database receives highest number of cases over recorded

Fraud prevention service Cifas has reported that 2019 has seen the highest number of cases recorded on the National Fraud Database. Over 364,000 cases were logged, which represented a rise in fraudulent conduct of 13%. The three main types of fraud identified were identify fraud, misuse of facility and facility takeover. Identify theft rose by 20% in 2019 and represented 61% of all cases recorded. Figures show those aged over 31 were specifically targeted, with victims aged over 60 also on the rise. 68% of identity fraud victims were recorded in the South East of the UK.

Cifas report that misuse of facility frauds, which involves the misuse of bank accounts or other financial products by the genuine account holder, accounted for almost a quarter of all cases. A growth of 64% has been seen in facility frauds over the previous five years. Whilst facility takeover fraud, which results in a fraudster gaining access to the accounts of innocent victims, reached the highest level ever reported in 2019. Facility takeover frauds were up 105% over the previous five years, accounting for almost one in ten cases logged on the database.

Read the Cifas article here.

UK banks inconsistent with transfer scam victims

This week The Guardian has reported that the UK Consumer Association Which? is pressuring all UK banks to adopt a voluntary code to protect victims of bank transfer scams. The article references the increase in fraud related to the UK payments industry, with a significant increase in authored push payment scams. These scams involve fraudsters hacking victims email accounts in an attempt to send false payment details. In one case a home buyer was conned of their house deposit after fraudsters hacked the email account and then sent false payment details purporting to be from the victim's solicitors. The victim lost £300,000, which was eventually paid back following a battle with the victim's bank. Which? claim that many victims have been treated unfairly when trying to recover lost funders and that the voluntary code which most banks have signed up to has failed. The Telegraph has also reported on claims banks are unfairly treating victims of fraud.

Read The Guardian article here. Read The Telegraph article here.

National Cyber Security Centre (NCSC) produce technical advice on cyber insurance

Last week guidance was published by NCSC covering cyber insurance. The guidance covers key questions organisations should be asking should they be considering purchasing cyber protection insurance. Following the rise in the cyber security market and calls for expert technical

guidance, the NCSC has produced the document in partnership with major stakeholders and industry partners. The publication recommends organisations of all types to consider how insurance may help following a cyber-attack and how a policy would contribute to the existing risk management strategies.
Sarah Lyons, NCSC Deputy Director for Economy and Society Engagement said 'businesses rightly want to be as informed as possible before they invest, but when it comes to cyber insurance there simply hasn't been enough information up to now. That's why it's so important for the NCSC as the UK's leading cyber authority to offer our support by providing some clarity on the key issues to consider to ensure cyber security. Cyber insurance may not be right for everyone and it can never replace basic good security practice, but I would urge businesses to consider our guidance to help make the decision that's right for them.'
Read the NCSC technical advice here

NCSC remove 300,000 celebrity investment scam URLs

This week the NCSC has reported it has closed over 300,000 malicious URLs linked to false celebrity endorsements for investment schemes. Celebrities including Richard Branson and Martin Lewis have been referenced in numerous news articles promoting investment scemes which were operated by fraudsters. NCSC Chief Executive Officer, Ciaran Martin said 'These investment scams are a striking example of the kind of methods cyber criminals are now deploying to try to con people. We are exposing them today not only to raise public awareness but to show the criminals behind them that we know what they're up to and are taking action to stop it. I would urge the public to continue doing what they have been so brilliantly and forward anything they think doesn't look right to our Suspicious Email Reporting Service.'
Read the NCSC warning here

The Independent report on COVID job scams

This week The Independent has reported an increase in job related scams is predicted as a result of the pandemic. Following the Bank of England prediction that unemployment could double by Christmas to 2.5 million, there is a risk the job market may continue to be exploited by scammers. The article refers to recent warnings of four common employment frauds, by consumer goods website Which?. One example involves the payment of advance fees, claiming to cover security and police checks and other administration costs such as training. This scam relies on the victim sending money in advance, however no job is available. Another scam example involves fraudsters obtaining bank details from fake job applications.
Read The Independent Article here

Other type of fraud examples

Email scams & Phishing scams

- Following the reintroduction of TV Licence fees to those over 75, it is thought scammers may take advantage of the opportunity. Previous scams have seen phishing emails attempt to gain financial details, by claiming the recipients payment has failed.

- Another TV Licencing scam has been reported to Action Fraud regarding an offer for a years free TV licence. Over 900 reports have been received about the scam, similar to the previous payment failure emails purporting to be from TV Licencing. The latest scam requires users to follow the links providing in the genuine looking emails in an attempt to steal personal and financial information.
- The Driving Vehicle and Licencing Agency have identified a phishing email circulating, attempting to trick users to verify their vehicle tax details through an online link. It is thought such details may be used in future frauds. Another example includes emails purporting to be from DVLA stating the recipient is entitled to a refund from a tax overpayment, in order to receive the payment users are required to submit personal and financial details to a false website.
- Similar to previous scams reported, council tax reduction phishing emails continue to circulate. Councils have warned of emails purporting to be from local authorities or the government offering a reduction in council tax. In order to claim the reduction and refund, users are required to submit false payment and personal details to genuine looking websites via links contained in the email.

Social Media

- Action Fraud has reported it has received 164 reports of investment fraud from Instagram users in June 2020. The investment scams taking place on the social media platform amounted to a combined loss of £358,809. Scammers use the Instagram instant messaging platform to contact victims, or rely on victims to contact them following advertising the service. Typically an investment of a few hundred pounds is required. which it is claimed will be traded on the stock market or trade in foreign currency. Victims are told the investment will multiple several times in a matter of days, which will be paid back to the investor minus a small commission. Typically after payment has been made a range of excuses are used as to why profits could not be returned, eventually resulting in contact ceasing. The scam is complicated as typically fraudsters request amounts are sent through a cryptocurrency platform, making it almost impossible to trace. Read the Action Fraud article here.
- The BBC has reported scammers have recently used fake competitions on social media to obtain personal details. The article states in one case an Instagram user entered a competition to win a holiday to Tenerife. The user was contacted, claiming she had won and fraudsters attempted to obtain personal and financial details. Read the article here

Other

- Action Fraud has received over 200 reports regarding a scam purporting to be from media service company Sky. Automated phone calls use a variety of lures including discounts and free technical support. The calls require the recipient of the call to 'press 1' following the automated message. Victims are then connected to scammers claiming to be representatives from Sky customer service, who attempt to remotely access the victim's computer in an effort to steal personal and financial information. It is reported that fraudsters have already stolen over £270,000 by this scam.

- Scam calls claiming to be from online retailer Amazon continue to be reported. Typically the call will start as a recorded message claiming to offer an update on an order not placed, then request the user to 'press 1' to speak with an operator. Fraudsters claiming to work for Amazon customer services will then attempt to steal personal and financial information.
- Scams have been identified following the introduction of fines by the UK Government for failure to wear face masks in required locations, such as shops. Reports of scammers purporting to work for local authorities have been received. Scammers have used fake identification and clothing in an attempted to issue on the spot fines to members of the public.
- Scams linked to the purchasing of pets have seen a significant rise during the pandemic. As reports of scam adverts continue to rise, Which? has produced an article with tips to spot false adverts and what questions to ask and consider when purchasing a pet. Click here to read the Which? article.
- As covered above UK banks have been pressured to apply a more consistent approach to victims of authorised push payment scams. This week consumer goods organisation Which? has produced an article providing guidance for victims of bank transfer scams. Click here to access the article.