COVID-19 Fraud & Security Alerts

Ref: CFMG-008

NHS Counter Fraud Managers Group (CFMG)

Supported by TIAN and 360 ASSURANCE

NHS CFA Fraud Threat Update

The NHS CFA has issued an updated publication covering fraud threats to the NHS as a result of the COVID-19 pandemic. The fifth edition of the COVID Threat Update contains new and interesting fraud threats and identifies potential and ongoing threats to the NHS.

Click here to access the publication

Counter Fraud Functional Standards

The CFA have reported that week that the UK Cabinet Office has published the Counter Fraud Functional Standard (GovS 013). The Standards will result in the whole counter fraud community within the public sector working towards a common counter fraud standard. The intention is to introduce the standards across NHS organisations by the end of the financial year.

Read the CFA update here

Warning over NHS Test and Trace scam that could cost you £500

Cifas has reported that threat actors are trying to scam vulnerable people out of up to £500 by telling them they are at risk of Covid-19 and need to buy a testing kit. The scams range from premium rate phone numbers, to requests for sensitive personal information, and even demands for payments as high as £500 for a testing kit.

CCI Credit Management phishing email

CCI Credit Management are aware of phishing emails that are being sent to NHS organisations purporting to be from CCI Credit Management Ltd asking the recipient to click on a link to download the status of current cases. CCI Management are used by many NHS organisations for debt recovery and they have contacted all affected clients. Be cautious when receiving any email asking you to click on any links.

Malcolm Stamp: Ex-NHS boss charged with corruption in Australia

A former NHS boss has been charged with corruption offences in Australia. Malcolm Stamp faces extradition to Queensland accused of arranging for his daughter to be given a job with a hospital contractor and conspiring to pay her wages from hospital funds.

Mr Stamp, 67, was chief executive of Metro North Hospital in Brisbane at the time of the alleged offences, in 2014. In the UK, he had been the

chief executive of a number of NHS hospitals, including Addenbrooke's in Cambridge. He had previously been chief executive of Mid Essex Hospitals NHS Trust and had also served as boss of the Norfolk and Norwich University Hospital.
Read the full article here

Conman carer ordered to repay almost £12,000 he stole from vulnerable victims

A former care home assistant, at Chataway Nursing Home in Manchester, who stole thousands from vulnerable victims to feed his gambling and drug habit, has been ordered to repay £11,873. Cunningham's role was to manage residents' finances, the 29-year-old took advantage of this power and used the vulnerable victims' bank cards to withdraw money to fuel his vices.

On 8 November 2019, Cunningham was sentenced to two years and four months in prison for the thefts worth almost £45,000 he carried out against three residents at the care home.

On Friday 19 June, Cunningham was ordered to pay £11,873 within three months or face an additional eight months on his sentence.

Read more here

Cisco patches dangerous Webex vulnerability

Cisco is moving to patch a serious vulnerability in version 40.4.12.8 of its Webex video-conferencing Windows client that could allow attackers to open, read and steal potentially valuable or damaging content. The bug, CVE-2020-3347, enables cyber criminals to steal meeting records from within Cisco's Webex service.

Read the full article here

Fraud Advisory Panel

The Fraud Advisory Panel have set up a COVID-19 fraud watch group which is a cross-sector and cross-industry coalition of trusted partners (including the Cabinet Office and City of London Police) who meet weekly to share information on emerging fraud threats and trends affecting business. It aims to act as a conduit to warn the public, private and third sectors about COVID-19 fraud risks and the preventative actions that can be taken.

The latest updated on 25 June 2020 includes; 'current COVID19 fraud risks', most of which we have covered in our weekly alerts; 'Anticipated and/or emerging issues'; and 'some simple preventative tips', with links to some useful documents and contacts.

Read more here

Over £16 million lost to online shopping fraud during lockdown, with people aged 18-26 most at risk

Despite retail and non-essential shops re-opening across the UK, most of the public continues to shop online. Members of the public have reported buying mobile phones (19%), vehicles (22%), electronics (10%) such as games consoles, AirPods and MacBooks, and footwear (4%) on sites such as eBay (18%), Facebook (18%), Gumtree (10%) and Depop (6%), only to have the items never arrive. With a quarter of the victims (24%) aged 18 to 26 residing in cities including London, Birmingham, Manchester, Leeds, Sheffield, Liverpool, Bristol and Nottingham.

Read the full article here

Cifas reveals cases of identity fraud up by nearly a third over last five years

Cifas, the UK's leading fraud prevention service, has revealed that cases of identity fraud rose by 18% in 2019 compared to the previous year – the highest ever increase recorded on the Cifas National Fraud Database.

Read the full article here

Ticket fraud warning as venues prepare to re-open

Action fraud are urging people to be wary of fraudsters selling fake or non-existent tickets to events. With pubs, restaurants, cinemas and museums set to reopen with social distancing measures, demand for tickets and reservations is likely to be high. People should take extra care when buying tickets online.

Spot the signs of ticket fraud:

- Only buy tickets from the venue's box office, official promoter or agent, or a well-known and reputable ticket site.
- Avoid paying for tickets by bank transfer, especially if buying from someone unknown. Credit card or payment services such as PayPal offer greater protection against fraud.
- Be wary of unsolicited emails, texts or adverts offering unbelievably good deals on tickets. If it sounds too good to be true, it probably is.
- Is the vendor a member of STAR? If they are, the company has signed up to their strict governing standards. STAR also offers an approved Alternative Dispute Resolution service to help customers with outstanding complaints. For more information: star.org.uk/buy_safe

Thanks a million: British public help reach major milestone in fight against scammers

The National Cyber Security Centre's (NCSC) Suspicious Email Reporting Service has received over a million reports of scam emails in two months. The Suspicious Email Reporting Service was launched as part of the Cyber Aware campaign, which promotes protective behaviours to keep your online accounts and your devices as secure as possible. The service has seen a massive response from the public, receiving a daily average of 16,500 emails and now reaching the milestone of one million. There have also been numerous examples of fake online shops and spoofs involving brands such as TV Licensing, HMRC, Gov.uk and the DVLA.

Latest figures show that 10% of the scams were removed within an hour of an email being reported, and 40% were down within a day of a report. 10,200 malicious URLs linked to 3,485 individual sites have been removed thanks to the 1 million reports received.

Read the full article here

Hackers target Australian school accounts

Following the article featured in last week's alert on Australian cyber-attacks, The Guardian have reported some Australian schools have been targeted in a phishing campaign. A scam email informed recipients a file had been shared, the link took users to a Microsoft SharePoint login

page. It is reported that the login page was a false site, created to collect user login details.
Read the full article here

Syncing phone with car leaves drivers at risk of fraud
Too many motorists are forgetting to erase personal data from their car before handing it on to the next owner, according to new research.
Read more here

Password aware
As we are all spending more time online, and it can be hard to keep track of all your new accounts. Don't re-use the same password - save your passwords to your browser instead. Find out more about how you can stay CyberAware here.

Cyber Security Risks
In this week's update the East Midlands Special Operations Unit (EMSOU) explores some of the most common heard myths today in cyber security, see below.
In an era of misinformation, misleading stories deliberately and inadvertently circulated adding to uncertainty we need to address some of the myths about cyber security.
A lack of information, inaccurate assumptions or inappropriate generalisation are the main causes of security myths.
Myths need to be dispelled, lest we become lax about security and fail to anticipate cyber incidents.
Myth: 'There is nothing on my computer system that is of any interest to an attacker...'
Fact: A compromised computer can be:

- Co-opted with bot software to attack other organizations.
- Turned into a file/web server to host illicit or illegal content, such as child pornography.
- Used to capture audio from a mic or footage from a webcam for extortion or blackmail.
- Harvested as a source of email addresses, which can be used for further phishing attacks or other email-based fraud and scams.
- Used to generate cryptocurrency.
- Commit identity fraud or steal services such as Netflix.

Myth: 'Cloud computing transfers the data security risk to the cloud provider…'
Fact: There is no transfer of liability.
If an organisation uses cloud services and suffers a data breach, then under GDPR, it is the organisation and not the cloud vendor who are deemed responsible. The concept of 'Due Diligence' is important and the customer must ensure that the services provided by the vendor are fit for purpose and secure.
Myth: Cloud computing offers a secure IT environment
Fact: Do not assume that the Cloud service is inherently secure.

Hosting services in the cloud poses any number of important security risks that must be identified and properly evaluated by the customer. For example, most cloud providers make available a pool of resources to multiple tenants, where the risk of data leakage, can be much greater than in a traditional data centre. Access to cloud resources is often device agnostic, and employees may use personal devices to access data - putting organisation systems and information at risk.

Myth: 'Anti-virus is the most important method of preventing a cyber-attack.'

Fact: Anti-virus software alone does not guarantee security.

Instead they must form part of a more holistic approach that seeks defence in depth. Network segregation and strong account authentication prevent the spread of any infection and auditing capabilities detect the issue. Staff training is also part of the defence in depth.

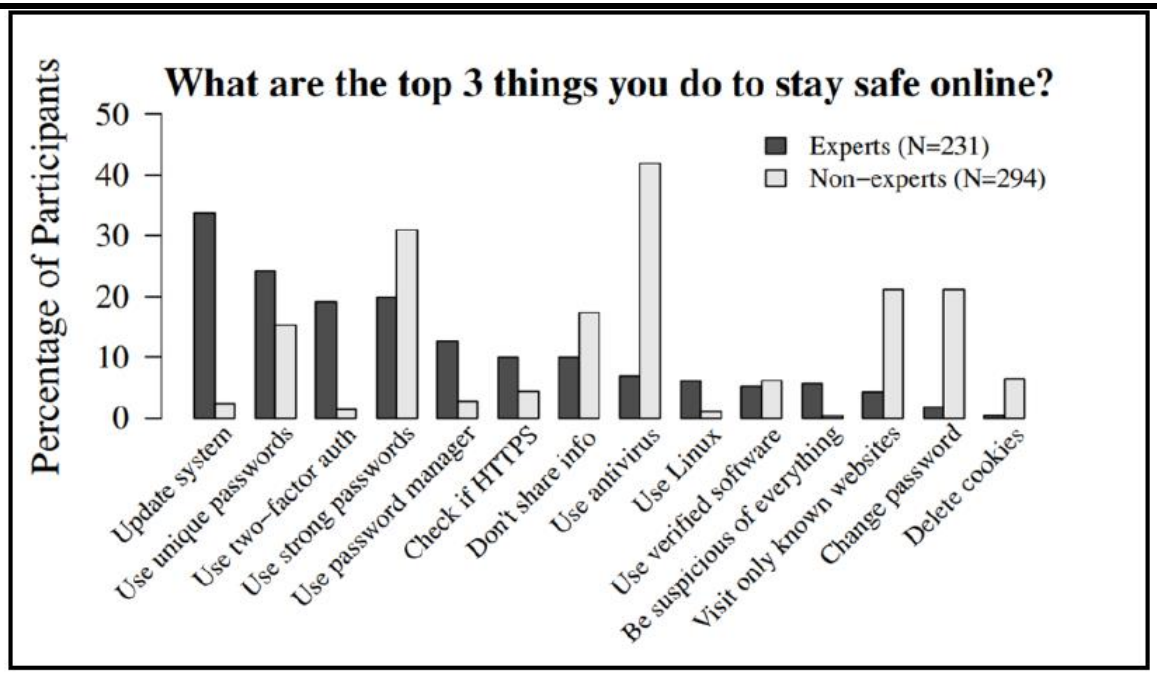
Myth: 'I'd know straight away if my business was compromised.'

Fact: The average time an adversary spends in a network, before detection, is six months.

Attackers will 'live off the land' using inbuilt tools security tools, rather than 'noisy' exploits; scoping network access and valuable resources. Data might be exfiltrated in drip-feed fashion and security logs cleansed to avoid detection or plant false flags. This is another reason why multiple security controls are preferable to a single solution.

Expert vs non-expert opinion

The survey graph below illustrates the cyber professional's security priorities versus those of non-cyber professionals.



Graph from: https://www.usenix.org/system/files/conference/soups2015/soups15-paper-ion.pdf

Other type of fraud examples

Malware / Viruses

- Cyber criminals are exploiting cancelled events as a result of the pandemic to infect users with malware. It is reported that hackers are embedding harmful malware within attachments available online claiming to offer information on cancelled events and ticket refunds.

Email scams & Phishing scams

- Cifas has reported that from 1-8 June 2020 there were 64 PayPal lookalike domains detected. These are domains that are similar to the legitimate PayPal website domain. While such occurrences can be a result of PayPal's brand protection strategy, it could also mean that threat actors are planning to use these domains to support phishing attacks against members of the public. Consumers should always exercise caution when receiving unsolicited emails and double check the URL of any site link included in the email.
- Cifas has reported that a message purporting to be from Instagram's help centre threatens to close your account if you don't hand over personal information. The direct message warns that one of your posts has infringed copyright law and your account will be closed

within 24 hours if you don't dispute the 'breach' by following a link. The message is also signed off with the real address of Instagram's Californian HQ, which gives a false impression of authenticity. The account name used to send the messages is 'Instagramsupportcf' and should ring alarm bells. Instagram contacts its users about account information or account issues over email, not through private message on the platform. The message also contains a number of grammatical errors. Read more here

- Recent reports suggests victims are being targeted by compromised emails that look like they are sent by a friend in hospital, reports Cifas. The email asks the recipient to purchase Amazon Gift cards for a disabled family member as the sender is in hospital, their debit card is not working and they cannot organise purchasing it themselves. The victim is asked to purchase gift cards to the total amount of £300 or £400 and the email states they will pay them back shortly once they have forwarded the details of the gift cards.
- Costco Loyalty Reward Scam Message - "Your Costco Package Loyalty Reward Will Be Delivered" is a scam message. The fake message is a phishing scam that goes to malicious website H7svz info. Cybercriminals are sending out fake Costco messages attempting to trick victims into visiting the link and completing surveys that steal personal and financial information, steal account credentials or infect their devices with malware.
- Parents and carers around the country have received an email asking them to provide their bank details by clicking on a link. The email says: "If your child's school is closed and your child is entitled to free school meals, send your bank details to the schools and they will help with funding while the schools are closed." The fraudsters are then using these details to try to steal the recipient's money from their bank account.
- The NCSC continues to provide support to victims of a widespread phishing campaign targeting a range of organisations in the UK. The campaign targets victims by sending what appears to be a legitimate email from a known email contact. The email may contain recent communication between recipients and include links that if clicked redirect to a seemingly legitimate login page. Any personal information entered can then be used nefariously by criminals. Click here for links to further information and guidance
- Amazon phishing emails are doing the rounds again. This time the fraudsters are claiming that your Amazon Prime membership is set to renew and states that the card associated with the membership is no longer valid. You are then asked to open the attached document and follow on-screen instructions to update. You are threatened with suspension of your Amazon Prime benefits.

Phone and Text Scams

- Scammers posing as the NCA stole £30,000 from a vulnerable 89-year-old customer in a sophisticated and drawn-out scam. Initially the victim received a call stating she had won a loyalty bonus worth £35 off her next BT bill and the caller quoted the full details of her bank card as well as her full name and address 'to confirm her eligibility'. A few days later, she received a call from the 'National Crime Agency' warning that £400 had been taken from her account due to a series of scams involving BT and complicit banks. The caller explained the authorities knew she had been targeted by the BT scam. They then asked her to help with their investigation into her local bank branch, by moving her money to a 'safe account'. Read more here

- Action Fraud have been made aware of scammers claiming to be from HMRC offering financial support as a result of coronavirus. If you receive a text, email or call claiming to be from HMRC that asks you to click on a link or give info such as your name, credit card or bank details, it's a scam.
- Amazon and Google Scam Calls - A victim received a call from a woman claiming to be from Amazon advising she was about to be charged £39.99 for Google Services. The caller, who phoned from a mobile number, told the victim that if she did not want the payment to go through she could dial "1", which she did. She was then transferred through to a man who explained he could stop the charge, but only if she typed in a code which would allow him to connect his computer to hers to stop the payment. Read more here

Social media and other messaging platforms

- Mobile phone network 02 has reported customers have received text messages reporting payments have failed. The scam similar to those seen by TV Licensing customers and Netflix subscribers, attempt to trick the recipient into providing payment details to false websites.

Online Retailers / Counterfeit goods

- As previously reported, fake goods scans have risen during the pandemic, with fraudsters using lockdown restrictions to prevent buyers from viewing products. The Guardian has reported a rise in these scams, recently targeting purchases of Nintendo Switches and Hot Tubs. The article highlights NatWest has seen a fivefold increase in some purchase scams. Read more here
- During the pandemic members of the public are being targeted by investment fraudsters and advised they could make large profits by investing in pharmaceutical companies during the coronavirus outbreak. Victims are promised that their stake will double or treble quickly owing to the pandemic. Members of the public have also been targeted by investment scams focussed on the current low price of oil.
- It has been reported by The Telegraph that fraudsters are continuing to target holidaymakers during the pandemic. As Phishing emails continue to rise purporting to be from airlines, it is reported that fake holiday websites have also been set up. The purpose of these sites is to replicate reputable websites with a slight variance in the URL. It is reported these fake sites are likely to charge large deposits for accommodation that does not exist. Scammers are also preying on consumers with fake caravan and motorhome listings and bogus holiday refund offers and travel deals. UK Finance states criminals are taking advantage of people hoping to go on a UK-based "staycation", with fake adverts for caravans and motorhomes on auction websites. Read The Telegraph article here
- Fake adverts, payment pages and websites are being used by criminals to trick you into paying them money. Read online reviews to check that websites are legitimate before making a payment and use secure payment channels. Remember, if the deal sounds too good to be true.

- Nottinghamshire Police Fraud have informed the public to be aware of people offering shopping or medication collection services. Don't assume everyone is genuine. It's okay to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- West Sussex residents are being advised of a scam claiming ultra violet lamps could be used to get rid of coronavirus. It's among a large number of instances of fraud reported to West Sussex Trading Standards during the current pandemic. Read local article here