COVID-19 Fraud & Security Alerts

Ref: CFMG-009

NHS Counter Fraud Managers Group (CFMG)

Supported by TIAN and 360 ASSURANCE

NHS Trust targeted by mandate fraud

It was reported earlier this month a fraudulent attempt was made to contact a supplier of University Hospital Southampton NHS Foundation Trust, claiming the Trust's bank details had changed. The Trust has confirmed their account details have not changed, nor will they change in the near future.

The NHS Counter Fraud Authority (NHSCFA) digitises the NHS Counter Fraud Manual

The NHSCFA is currently working to digitise the fraud manual, with the digital manual replacing the current version. The mobile friendly resource will provide user friendly guidance which is easy to navigate and is secure and is due to launch in September 2020. The manual is available to Local Counter Fraud Specialists (LCFSs), Directors of Finance (DOFs), Audit Committee Chairs and NHSCFA staff. The resource aims to tackle previously identified issues with the manual around access, ability to download and navigation of the guidance.

Read the full NHSCFA update here

Counter Fraud Champion nomination reminder

The NHSCFA reminds all organisations who have not yet done so to nominate a fraud champion. Although the development of the fraud champion network is delayed due to COVID-19, the CFA continue to welcome nominations. So far over 200 colleagues have been nominated to the role.

Further details on the CFA Fraud Champion role can be found here

NHSCFA 2020 Strategic Intelligence Assessment (SIA)

The 2020 SIA covers activity that occurred within 2018-19. It is estimated that the vulnerability to the NHS in England from fraud, bribery and corruption is £1.21 billion. The estimated vulnerability is a reduction of £85 million from 2018, a further improvement on last year's successful reduction.

Clink here for assessment

Fraud - Social engineering on the rise

The LCFS at Bolton NHS Foundation Trust has been made aware that several Bolton NHS Staff have been approached by fraudsters posing as staff in an attempt to obtain money. The cyber-criminals are approaching staff via Social Media web sites. This type of fraud is called social engineering, whereby the fraudster contacts the victim via social media, to exploit a person's trust in order to obtain money directly. They piece together information from various sources, such as Facebook, Instagram and messenger services, in order to appear convincing and trustworthy to perpetrate the fraud and obtain money from the victim. Staff should be on alert and vigilant when being approached via social media websites by potential fraudsters asking for money.

Contract tracers target the vulnerable

This week the BBC has reported on bogus scams targeting the vulnerable, including bogus contract tracers. The article covers the account of an individual who has been targeted on three occasions with different scams. On one occasion the victim was contacted by a bogus contract tracer attempting to sell a COVID-19 test. The same individual had also been targeted with scams purporting to be from their bank and received an email suggesting they were entitled to a relief fund for the pandemic. Read the BBC article here

Social media: protecting what you publish

The National Cyber Security Centre (NCSC) has published guidance on how to reduce the likelihood of unauthorised and/or damaging content appearing within your organisation's social media channels. Even if your organisation already has an established process for posting social media content, NCSC recommends that you take a moment to review how you're using it. The guidance covers the following:

- Social media: what is the risk?
- Make sure that only authorised staff can publish content.
- Use social media platforms (and management tools) that provide good security features.
- Make sure content can be reviewed and authorised before being published.
- Use corporate devices to create and publish content.
- Put an emergency recovery plan in place.

The guidance is primarily for all staff responsible for setting up social media accounts. However, all staff involved in the creation, review, approval and publication of content for social media channels will also find it useful, especially those staff involved in procurement of social media tools.

Read full guidance here

Cryptocurrency trading platform closed by courts

During the pandemic, investment and cryptocurrency related fraud has seen a significant increase, as fraudsters target victims' economic worries. On 23 June 2020 the High Court wound up GPay Ltd following loses of £1.5 million of investors funds. GPay operated an online

cryptocurrency trading platform and advertised with false claims of entrepreneurial and celebrity backers. David Hill, a Chief Investigator for the Insolvency Service said: “GPay persuaded customers to part with substantial sums of money to invest in cryptocurrency trading. This was nothing but a scam as GPay tricked their clients to use their online platform under false pretences and no customer has benefited as their investments have been lost.”
Read more about the case here

How to avoid pension scams

The Financial Conduct Authority has updated its guidance on how to avoid pension scams and what to do if you suspect a scam. Pension scams can be hard to spot. Scammers can be convincing and financially knowledgeable, with credible-looking websites, testimonials and materials that are hard to distinguish from the real thing. This covers:

- How pension scams work.
- How coronavirus is affecting pensions.
- Pension scam warning signs.
- Four steps to protect yourself.
- What to do if you think you've been scammed.
- Protecting your employees and members.

Click here for details

Portable Media

In this week’s update, the East Midlands Special Operations Unit (EMSOU) has focussed on danger of portable media and how they can be mitigated:

In 1986 IBM introduced the 3.5 inch floppy disk with 1.44 megabytes of storage space. A big step forward over its predecessor, the flimsy 5.25 inch floppy. Fast forward 20 years or so and we have USB thumb drives that can hold over 350 thousand times more data.

USB drives are small; inexpensive, portable and have massive storage capacity. Small wonder they are immensely popular with IT workers to store and transport files from one device to another. Unfortunately, these same characteristics make USB drives appealing to attackers. Nor is it just thumb drives that poses significant risks to an organisation. SD cards, portable hard drives and mobile phones plugged in by employees can also cause harm.

The Dangers of Portable Media

- Data Loss: Portable media is designed to be small and compact and is easily lost or stolen, a commonly encountered problem that organisations face.
- Sources of Infection: USB products can be plugged into a device and automatically load malware such as viruses, key loggers,

ransomware, rootkits, Trojans and backdoor access. These drives can be left in public spaces, where they will be picked up and used by the unwary, or plugged into unprotected workstations. In an experiment, researchers from the University of Illinois left nearly 300 unmarked USB flash drives around the University campus; half of these were plugged into a host device.

- Attackers have also targeted large manufacturing companies and supply chains to infect new products that are then distributed to customers.
- Data Exfiltration: When attackers physically access a computer system, they can download sensitive data directly onto the storage device. When turned off, a computer's memory is still active for several minutes without power. If an attacker plugs a USB drive in, during that time they can quickly reboot the system from the USB and copy the computer's memory - including passwords, encryption keys, and other sensitive data. Victims may not even realize that their computers were attacked.

<u>How to mitigate the problem of removable storage</u>

- Use Anti-Virus: To automatically scan external storage devices for harmful malware before use. Keep anti-virus software updated to identify and sanitise the latest threats.
- Disable auto-run: To prevent malicious code on an infected item from opening and running automatically.
- Allow only pre-approved USB drives: Purchase from secure vendors and do not permit any others to be plugged into the work environment.
- Use mobile charging stations: Discourage staff from charging mobile phones at company work stations. Who knows what is being synchronised or downloaded.
- Encrypt Storage: Some of the more secure versions of encrypted USB drives will also erase data when an incorrect password is entered multiple times. AES encryption is widely considered unbreakable.
- Training: Staff should identify sensitive data and avoid storing such information on portable media. It is also important to train staff to recognise how users are socially engineered to plug in such devices.

The most sophisticated thumb drives are designed to look and act like any other input device such as a keyboard or mouse. In these circumstances, anti-virus software and disabling auto run will still struggle to detect malicious behaviour.

Other type of fraud examples

<u>Malware / Virus</u>

- Cifas has warned of a Ransomeware that targets macOS users. Named OSX.ThiefQuest (or EvilQuest), this ransomware is different from previous macOS ransomware threats because ,besides encrypting the victim's files, ThiefQuest also installs a keylogger, a reverse shell, and steals cryptocurrency wallet-related files from infected hosts. Once infected, victims are asked to pay a $50 ransom in bitcoins within three days (72 hours) to recover their encrypted files and are directed to read a ransom note saved on their desktops. The ransom note gives a static BTC address and no contact details to obtain the decryptor.

Email scams & Phishing scams

- As COVID-19 restrictions lift and employees begin returning to the workplace, phishing campaigns leverage training programs that are now becoming required for employees to undertake in order to comply with coronavirus regulations. A current specific campaign targets Office 365 users and sends a fraudulent link for registration. According to a report by Check Point Research, the link redirects users and asks for them to input their credentials. Read more here
- Fake Microsoft Covid-19 relief funds: Cifas has reported that emails purporting to be a Senior Director from Microsoft claim "to stop the spread of the COVID-19 pandemic across the globe". An online email beta test is claimed to have been carried out, with the recipient's email address being selected to receive the "Microsoft Coronavirus Relief Fund" (MCRF). Recipients are asked to open a JPEG file to view details and receive further information on how to claim this fund. Fraudsters are sending emails from a variety of addresses, including Microsoft Live accounts and dot com email domains.
- Police have issued a warning about spoof @SpotifyUK emails, asking you to update your account information. Spotify has said it will never said emails asking for payment information or passwords. Read more here

Phone and Text Scams

- With many people working from home during lockdown, Action Fraud are urging people to be wary of cold calls or unsolicited emails offering you help with your device or to fix a problem. Action Fraud has issued some advice on how to protect yourself and what to do if you become a victim, found here.
- Scam HMRC texts asking for passport numbers, NI and credit card numbers: Cifas has highlighted a scam text message purporting to be from HMRC informing recipients they are due a tax refund which can be applied for online via an official looking site that uses HMRC branding and is entitled "Coronavirus (COVID-19) guidance and support." The bogus site asks for several pieces of the user's sensitive information including government gateway login credentials before requesting their passport number or national insurance number as 'verification' – in some cases the scam further asks recipients to enter credit card details. An article by Info Security Magazine this week covers the scam, with over 80 London based self-employed workers reporting the scam. Read the article here
- Fraudsters posing as Amazon workers have stolen £70,000 from victims across the Midlands in just 24 hours. They netted £25,000 from Worcestershire residents and another £45,000 in Shropshire. The scam involves con artists cold calling and saying the recipient is entitled to an Amazon refund. The victim is given instructions from the scammer, who accesses their bank details and steals their money. Read article here

Social media and other messaging platforms

- As previous report romance scams are on the rise, with 517 victims in May 2020. This is 11% increase from the same time last year.

Cifas' Amber Burridge said: “More people have been moving online during lockdown and dating sites have been one of the few ways to interact with new people. Fraudsters are exploiting people’s loneliness.” Read the article in the Telegraph ‘I sent my lover £17k when he was dying of Covid – then found out he was a scammer’, here.

Online Retailers / Counterfeit goods

- Following the report in last week’s alert regarding holiday scams, Action Fraud have published a further article. Click here to read the Action Fraud publication. The publication highlights the increase of holiday scams during the COVID-19 pandemic. The scams include fake caravan and motorhome listings, along with refund and travel deal scams, as fraudsters target those who have had holidays cancelled and those looking to holiday in the UK. Spoof calls and emails continue to target those awaiting holiday cancellation refunds. In addition Good Housekeeping have also issued consumer guidance on how to avoid holiday scams. Read the Good Housekeeping guidance here.
- EMSOU has reported that organised criminals are continuing to exploit loneliness during lockdown to target isolated victims that use online sites to befriend others and look for romantic interests. BBC researchers have discovered that in one region romance scam victims were groomed, then tricked out of an average of £47,000. Romance Fraud is already one of the top five most commonly reported scams to Action Fraud and cost the UK 27 million last year according to the latest stats from the City of London Police’s National Fraud Intelligence Bureau (NFIB) and Get Safe Online.