Coronavirus Special Edition

Information Alert 4

MIAA Anti-Fraud & Cyber Security Teams

13 May 2020

Coronavirus scams update

This is the fourth issue of MIAA's dedicated, regular series of frauds, scams and cyber-crime alerts related to the COVID-19 emergency. Please read this alert carefully and share it as widely as possible. This special alert series is intended to provide up-to-date information on scams and fraud threats, in whatever form, currently in circulation to help prevent NHS staff and organisations from falling victim.

As at 3rd May, the National Fraud Investigation Bureau (NFIB) reported that Action Fraud had received 1,390 reports of fraud, amounting to £2,853,827 of losses, and 5,670 reports of phishing.

Fake COVID-19 Tracking Apps

There are currently a number of apps circulating online that claim to provide live information on the spread of COVID-19, such as tracking movements and alerting the individual if they have been in contact with another individual that later developed symptoms or tested positive for the virus.

The fake tracking apps could be used to infect your mobile device with malware and steal your financial or personal data, if downloaded. Whilst such apps have commenced use in some countries, the UK Government has not yet approved an official app to track the spread of COVID-19. At the time of this alert, UK app testing has been commenced on the Isle of Wight.

When an app is approved by the UK Government, this will be widely publicised through official sources and it will be possible to verify the app as genuine.

Action(s) to take: Do not click on links or download apps claiming to track the spread of COVID-19, without first verifying that such an app exists in the UK and is approved for use by the UK Government. If you are asked to take part in an app trial and wish to participate, ensure you check official sources before doing so. Always check what permissions an app requires before downloading it. If the permissions seem unreasonable for the type of app, then do not download it.

COVID-19 Testing

Testing for COVID-19 has now become available through Public Health England for individuals meeting certain criteria, based on their employment, age category and those living with individuals meeting the other criteria. Details of the criteria and how to arrange for testing can be found here. This is the only approved means of getting a test for COVID-19 outside of an NHS or social care setting. All other tests, including home testing kits, are not certified under European safety standards, and not advised by Public Health England. It is illegal to sell them

Action(s) to take: Health organisations and individuals should not endorse any testing other than through the official route described in the link above.

ACTION REQUIRED

MIAA recommends this alert is distributed to:

NHS STAFF for ACTION & AWARENESS

For further information or to report NHS Fraud contact:
Darrell Davies
Assistant Director (Anti-Fraud)
0151 285 4520
07785 286381
darrell.davies@miaa.nhs.uk

If you are concerned that you are a victim of a cyber-crime or want to know how to improve your organisation's cyber resilience, contact:
Tony Cobain
Assistant Director (Informatics)
07770 971 006
Tony.Cobain@miaa.nhs.uk

MIAA ASSURANCE

Anyone with knowledge or suspicions of illegal testing kits being offered for sale should report this to Action Fraud initially or their local police if the sellers' details are available.

Theft of Patient Property

MIAA has noticed a recent increase in reports of theft of property in hospitals, particularly patient property. Thefts have included physical property as well as cash. This comes at a time when there are less visitors to hospital sites and staff are busy, focusing on the current crisis.

Action(s) to take: All staff should remain vigilant to anyone on site that does not have a reason to be, and any patients that are expected to be on site but are found in the wrong ward or staff areas. Anyone attending hospital, other than in an emergency situation, should be advised not to bring unnecessary items of value or significant amounts of cash. Report any suspicious behaviour or concerns to security, or contact the police on 101.

Phishing, Smishing and Vishing

Fraudsters may contact their victims by various means and, as such, it is important to stay vigilant to all methods to ensure you can protect yourself, your family and your organisation. It has been widely reported that whilst most crimes have reduced during the COVID-19 crisis, fraud has increased significantly.

All methods seek to gain financial or personal details from their victims, such as bank details, credit card, or other login information, or download malicious content such as malware to their device. Usually, fraudsters will impersonate an official body, such as Government agency or utility provider, with the aim of gaining the victim's trust.

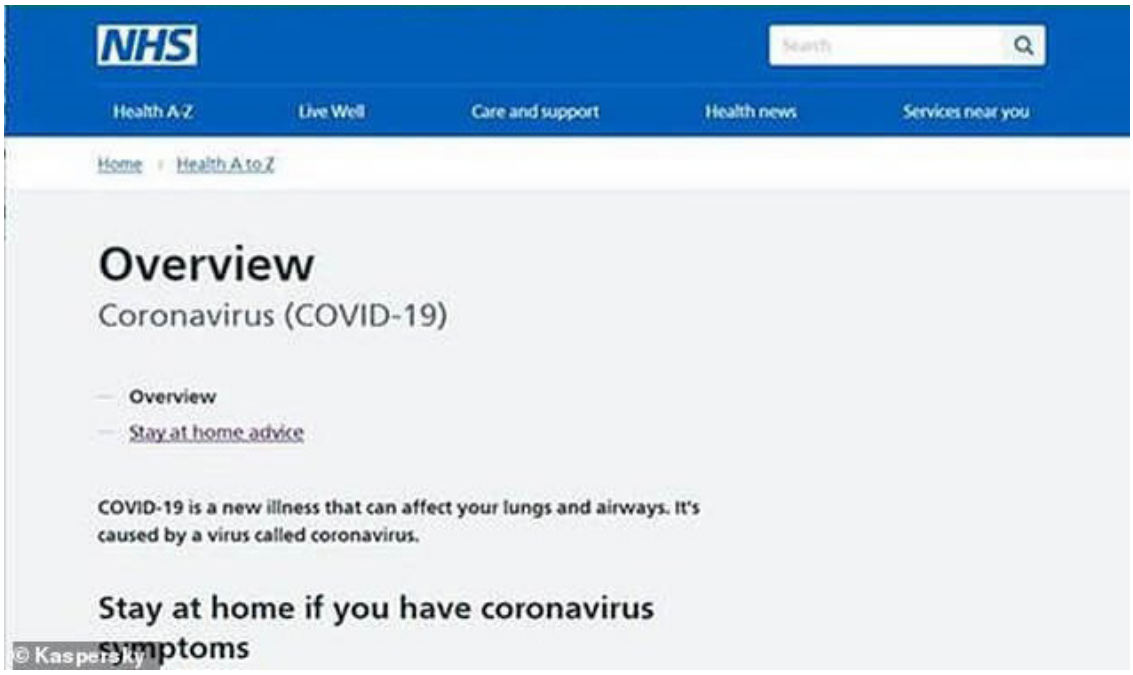
Three common methods are as follows, with some recent examples of each scam:

- **Phishing**

Scams are where fraudsters send emails and/or create bogus web pages, which encourage the recipient to click on a link or download an attachment.

◆On 5th May, the BBC reported that **cyber-criminals have been targeting healthcare bodies,** particularly those involved in coronavirus response, saying "Cyber-security agencies in the UK and US have issued a joint warning to healthcare and medical research staff, urging them to improve their password security, after cyber-criminals have been targeting healthcare bodies, particularly those involved in coronavirus response."

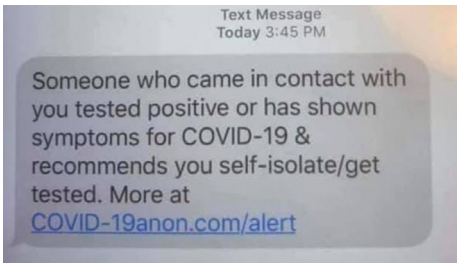
◆ A **hoax copy of the NHS website** has been reported, which includes harmful links luring people who are searching for COVID-19-related health tips. Once a link is clicked, a pop-up box appears asking if you want to save a file called 'COVID19'. If saved, your device is infected with malware which can steal passwords, credit card data, cookies from popular browsers, crypto wallet files and screenshots. A screenshot of the fake website is below.



◆ The BBC reported figures from the UK's National Cyber Security Centre (NCSC) of over 2000 online coronavirus scams last month, including 472 fake online shops, 900 advance-fee fraud schemes, where a large sum of money is promised in return for a one-off payment, and numerous malware and phishing sites.

◆Supermarkets such as Tesco have been impersonated in emails, offering recipients free vouchers if they register. This gives fraudsters an opportunity to steal email logins, passwords and personal details.

● **Smishing**
Scams are where fraudsters seek to obtain financial or personal details of their victim by SMS text messages. As with phishing, they usually encourage clicking on a link. Recent examples include:



◆ Reports of scam text messages claiming to track individuals that have been in contact with an individual that later tested positive for COVID-19 or developed symptoms. There is currently no officially sanctioned system in the UK to track individuals and alert them by text message. Right is a screenshot of one such text message.

● **Vishing**
Scams are where fraudsters seek to obtain financial or personal details of their victim by telephone. Some recent examples include:

◆ Targeting those working from home, fraudsters have impersonated **utilities and internet providers**, requiring payment by telephone or the service will be cut off. Victims have provided bank details for payment to fraudsters. Fraudsters have also impersonated **IT services** in order to gain access to computer systems and commit computer software service fraud.

◆ Targeting bereaved families, fraudsters have impersonated the Council's **bereavement service**, stating a payment for the deceased's funeral had been declined and as such, the family was required to make a card payment by telephone.

◆ Targeting older and vulnerable people, fraudsters have impersonated NHS and Careline employees to offer services such as **grocery shopping, prescription collection and COVID-19 detection devices**. Victims have provided bank details for these services and have not received goods.

◆ Targeting individuals and organisations with offers of protective **face masks, hand sanitiser, testing kits, medicine and other COVID-related supplies.** Victims have provided bank details for these services and have not received goods.

Action(s) to take: Spotting a phishing, smishing or vishing attempt is becoming increasingly difficult, and many scams will even trick experts utilising what are known as 'social engineering' techniques. However, there are some common signs to look out for:

● **Authority** - Is the sender claiming to be from someone official (such as your bank, doctor, a solicitor, government department)? Criminals often impersonate a source you're more likely to trust in order to trick you into doing what they want.

● **Urgency** - Are you pressured with a limited time to respond (such as 24 hours or immediately)? Criminals often threaten you with fines or other negative consequences.

● **Emotion** - Does the message make you panic, fearful, hopeful or curious? Criminals often use threatening language, make false claims of support, or tease you into wanting to find out more.

● **Scarcity** - Is the message offering something in short supply (such as a COVID-19 test or cure)? Fear of missing out on a good deal or opportunity can make you respond quickly.

● **Current events** - Are you expecting to receive a message like this? Criminals often exploit current news stories, big events or specific times of year (such as a global pandemic) to make their scam seem more relevant to you.

If you are approached unexpectedly by email, text message or telephone, remember to:

- **Stop** - Taking a moment to think before parting with your financial or personal information could keep you safe.

- **Challenge** - Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you. An official organisation will not try to stop you contacting the organisation directly through known contact details.

- **Protect** - Contact your bank immediately if you think you've fallen victim to a scam and report it in line with the actions below.

OTHER ACTIONS TO TAKE:

1. If you have received a suspicious email, forward it to the Suspicious Email Reporting Service (SERS) at report@phishing.gov.uk. Report all supicious and spam emails as an attachment to spamreports@nhs.net (click here for step-by-step instructions). Also, report any coronavirus-related attempted scams to your Anti-Fraud Specialist.

2. All successful phishing attempts should be reported to Action Fraud at https://www.actionfraud.police.uk or on **0300 123 2040.**

3. Report any suspicious texts by forwarding the original message to 7726, which spells SPAM on a phone keypad.

4. To report any concerns or suspicions of fraud, bribery or corruption, please contact your Anti-Fraud Specialist (see page 1 for contact details). You can also contact the national **NHS Fraud and Corruption Reporting Line** on **0800 028 40 60** or online at https://cfa.nhs.uk/reportfraud

OTHER USEFUL LINKS:

- MIAA - https://www.miaa.nhs.uk/insights/fraud-alerts-news

- Action Fraud (National Fraud Intelligence Bureau) - https://www.actionfraud.police.uk/news

- Chartered Trading Standards Institute (CTSI) - https://www.tradingstandards.uk/news-policy/news-room

- Other useful sources of online counter fraud advice can be found from Scamsmart, CIFAS, TakeFive, Citizens Advice, Trading Standards and the National Cyber Security Centre. There is bespoke advice about COVID-19 fraud on the Action Fraud website.

OTHER USEFUL DOCUMENTS:

- HFMA: Identifying malicious e-mails - Eight red flags to help identify malicious e-mails - https://www.hfma.org.uk/publications/details/identifying-malicious-emails

- ACCA: A warning be vigilant - coronavirus scams - Examples of scams and how to reduce your risk - https://i.emlfiles4.com/cmpdoc/2/5/6/6/2/files/660004_coronavirus-scams.pdf

- National Cyber Security Centre: Home working: preparing your organisation and staff - Advice on preparing for an increase in home working and spotting COVID-19 scam emails - https://www.ncsc.gov.uk/guidance/home-working

- HMRC: Current list of digital and other contacts issued from HMRC and guidance on recognising phishing emails - https://www.gov.uk/government/publications/genuine-hmrc-contact-and-recognising-phishing-emails/genuine-hmrc-contact-and-recognising-phishing-emails