Coronavirus Special Edition

Information Alert 5

MIAA Anti-Fraud & Cyber Security Teams

5 June 2020

Coronavirus scams update

This is the fifth 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 the 24/05/20, the National Fraud Intelligence Bureau reported that Action Fraud had received 1,992 reports of COVID-19 related fraud, amounting to £4,552,661 of losses, and 10,920 reports of COVID-19 related phishing (Source: National Economic Crime Centre).

COVID-19 Testing *UPDATE*

The UK Government has announced that all NHS and care staff in England will be offered an anti-body test, with patients and care residents eligible at their clinician's request. UK Government official guidance on its national anti-body testing programme was published on the 22/05/20.

The anti-body test is a blood test that looks for antibodies in the blood to see whether a person has had the virus, and differs from the swab test, which tests if a person currently has the virus.

MIAA has become aware of a number of private companies offering anti-body tests for sale online, some falsely advertising accreditation and approval from Public Health England. Public Health England has not approved any anti-body test for use at home.

NHS England has warned against using commercially sold tests. Professor Stephen Powis, NHS England's Medical Director, said on the 20/05/20: 'I would caution against using any tests that might be made available without knowing quite how good those tests are... I would caution people against being tempted to have those tests' (Source: BBC News).

On the 27/03/20, it was reported by the Guardian that retailers in England selling anti-body tests have been instructed to stop sending them out, while the regulatory body examines how well they work. The Medicines and Healthcare Products Regulatory Body has contacted all the private providers and the labs they use to tell them to halt the tests while they assess their accuracy.

Professor John Newton, from Public Health England, said: '*We wouldn't recommend at the moment that people rely on the tests that are becoming widely available. My advice would be to wait until we have better tests which will be available in a similar form very soon, though they are still under evaluation at the moment'.*

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

In addition to the concerns around the accuracy and reliability of such tests, there is also the risk to individuals being scammed by disreputable companies into purchasing goods online that they subsequently do not receive. Action Fraud previously reported in March that the majority of reports of coronavirus-related fraud that they had received were concerned with online shopping scams where people had ordered products online, which had then never arrived.

Action(s) to take: Individuals should not purchase any anti-body testing other than through the official route described in the link above. Anyone who believes they have been the victim of online shopping fraud should report the matter to Action Fraud. People should remain alert to the heightened risk of all forms of online scams at this time.

NHS Test and Trace (Track and Trace)

The UK Government has announced the launch of the NHS test and trace service. UK Government official guidance on the new initiative was published on the 27/05/20. Individuals who test positive for coronavirus will now be contacted by NHS test and trace to identify all people that they have been in close contact with, so they can be advised to self-isolate for 14 days.

The initiative is in its infancy and therefore MIAA is not aware of any specific concerns. However, one of the key questions that has been raised since the announcement was made has been how someone contacted can tell the difference between a genuine contact tracer and a potential scammer.

Action(s) to take: The following measures help provide assurance that the contact is genuine:

- The NHS test and trace service will make contact with people via text message, email or phone.
- All texts or emails will ask you to sign into the NHS test and trace contact tracing website.
- If NHS test and trace texts you, the sender of the text message will show as **'NHS'.**
- If NHS test and trace calls you by telephone, the service will be using a single telephone number: **0300 013 5000.**
- The contact tracer **will** ask for your full name and date of birth to confirm your identity, and postcode to offer support while self-isolating.
- The contact tracer **will** ask about the coronavirus symptoms you have been experiencing.
- The contact tracer **will** ask you to provide the name and contact details of anyone you have had close contact with in the two days prior to your symptoms starting.
- The contact tracer **will** ask if anyone you have been in contact with is under 18 or lives outside of England.
- The contact tracer **will** ask if you have family members or other household members living with you.
- The contact tracer **will** ask if you work in, or have recently visited, a setting with other people (for example, a GP surgery, a school or a workplace).
- **The contact tracer will never ask you to dial a premium rate number to speak to them (for example, those starting 09 or 087).**
- **The contact tracer will never ask you to make any form of payment or purchase a product or any kind.**
- **The contact tracer will never ask for any details about your bank account.**
- **The contact tracer will never ask for your social media identities or login details, or those of your contacts.**
- **The contact tracer will never ask you for any passwords or PINs, or ask you to set up any passwords or PINs over the phone.**
- **The contact tracer will never provide medical advice on the treatment of any potential coronavirus symptoms.**
- **The contact tracer will never ask you to download any software to your PC or ask you to hand over control of your PC, smartphone or tablet to anyone else.**
- **The contact tracer will never ask you to access any website that does not belong to the government or NHS.**

National Shielding Helpline concerns about possible scam telephone calls

Since the beginning of April, 1.3 million people considered to be at highest clinical risk from coronavirus have been written to by the NHS to inform that they should be 'shielding' – staying at home at all times and avoiding all face-to-face to contact for a period of at least 12 weeks. Some of the people at home 'shielding' may be contacted by a government support service (by letter, email or telephone) to assist with food and wellbeing support needs. MIAA has been made aware of some concerns around whether phone calls that people have received have been genuine or are scams. As it turned out, they were all genuine calls.

Action(s) to take: The following measures help provide assurance that the call is genuine:

- The caller will identify themselves with their name and identify themselves as a representative of the National Shielding Helpline.
- The telephone number that they are calling on will register on your phone as **0333 3050466.** This is the correct number for genuine calls.
- It is not a live telephone line, but if you call it you will get the following recorded message: 'You were called today by the Shielding Helpline sorry that we missed you, there is no need to call us back as we will try again soon. Thank you goodbye'.
- Early on in the call, agents from this service will ask you to confirm some details, for example your name and NHS number, to make sure they are speaking to the right person.
- They will **NEVER** ask you for information like your National Insurance number or bank details.

Police impersonation scam

Members of staff and the public are warned to be alert to the potential threat of fraudsters impersonating the Police. Thankfully, this is rare, but there have been a small number of incidents reported where fraudsters have attempted to impersonate the Police. On the 22/05/20, an incident was reported in Scotland where a fraudster pretending to be a police officer telephoned a member of the public to issue them with a fine for an alleged breach of lockdown regulations. The intended victim became suspicious and ended the call. (Source GlasgowLive).

An arguably more frightening incident occurred in Yorkshire on the 27/03/20, when a female member of the public was stopped whilst driving in her car by fraudsters impersonating the Police. The two men, who were wearing black hoodies and earpieces and carrying walkie talkies, attempted to 'fine' the woman £60 on-the-spot for unnecessary travel during the COVID-19 lockdown. After the intended victim refused, the fraudsters drove off. (Source: Somerset.Live)

Action(s) to take: Individuals are warned to be vigilant to the threat of fraudsters pretending to impersonate the Police (or any other official). If you receive a suspicious telephone call, do not give out any personal or financial information, including that you live alone or are older or vulnerable (if this is the case). Phone the genuine Police non-emergency number 101 to check that the telephone call you received was legitimate. If you are face-to-face with somebody representing themselves as the Police, always ask for their identification and badge number. If you are concerned for your safety or in danger, remove yourself from the scene as quickly and safely as possible and/or shout for assistance and immediately call 999 when safe to do so. The Police have confirmed that they would never instruct immediate payment of an 'on-the-spot' fine for breach of the lockdown regulations; a fixed penalty notice would be issued to the individual with instructions on how to pay within a certain period of time.

SMISHING - Text Based Scams

Fraudster prosecuted for 'smishing' campaign

Mohammed Khan, 20, from London, appeared before Westminster Magistrates' Court on the 15/05/20 and pleaded Guilty to two counts of fraud (one charge of fraud by false representation and one of possession of articles for use in fraud) related to the sending of scam COVID-19 text messages.

Following an investigation conducted by the Police, it was found that Khan had been involved in a large-scale 'smishing' campaign, sending out fraudulent text messages to take advantage of genuine financial concerns around coronavirus to de-fraud members of the public. The scam messages that were discovered included ones that claimed to be from the UK Government and offering a tax refund as a result of the pandemic (which MIAA warned about in COVID-19 Scam Alert 1).

The ultimate aim of the fake messaging was to dupe intended victims into accessing a link to a bogus webpage to provide their personal and financial information that could then later be used to commit fraud. Khan has been remanded in custody and is awaiting a court sentencing date. (Source: Action Fraud)

NHS Charities Together text scam

MIAA has been made aware of a smishing scam whereby intended victims are receiving a fraudulent text message encouraging them to make a donation to the NHS Charities Together fund in return for a free home testing kit. The text message reads: 'Donate to the NHS Charities Together Covid19 Fund and receive a home testing kit free of charge'. The sender of the text message is 'NHSFund'. The text message contains a malicious link, which, if accessed, leads to a bogus webpage.

Cervical screening scam

A number of health organisations have been alerted by Public Health England to reports of a potential cervical screening text message scam. It has been reported that a number of women have received a text message, claiming to be from the call and recall service, to advise that they are overdue for screening. The text message asks them to call a mobile telephone number and provide personal details. Public Health England's Screening Quality Assurance Service (SQAS) has confirmed that the text messages have NOT been sent from the NHS Cervical Screening Programme. The official government guidance on the cervical screening programme confirms that invitations for screening are sent by mail not text message.

Action(s) to take: Individuals should remain vigilant to the threat of receiving malicious text messages and treat with extreme caution any unexpected messages received. Do not respond or go through links on text messages that ask for personal or financial information. Individuals should not respond to any text message received claiming to be from the call and recall service. Do not call the mobile number provided and do not disclose personal details.

Free e-learning to stay safe online

The National Cyber Security Centre (NCSC) has made available free online training to help improve staff knowledge and understanding of cyber security – particularly important with so many people now working from home and also with the increase in online shopping. The 30 minute e-learning package includes a short quiz and links to further reading, and has been designed for people who may have a limited knowledge of cyber security. It covers the following areas:

- Why cyber security is important
- How cyber-attacks happen
- Defending yourself against phishing
- Using strong passwords
- Securing your devices; and
- Reporting incidents

Actions(s): Individuals can directly access the training via the following link, which goes through to the NCSC website – no login is required. Health organisations who wish to integrate the package into their own organisation's training package can download the following zip file, which contains the package as a SCORM-compliant file. The content is covered by the Open Government Licence. The core messages from the training have been summarised in an infographic, which is also free to download, print and share. (Source: NCSC)

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 received in to your NHS email account 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 - where you have acted on a suspicious email and now believe you have been the victim of a fraud as a result - 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:

- Mersey Internal Audit Agency (MIAA)
- NHS Counter Fraud Authority (NHSCFA)
- Government Counter Fraud Function
- National Cyber Security Centre (NCSC)
- Action Fraud (National Fraud Intelligence Bureau)
- Metropolitan Police
- Financial Conduct Authority (FCA)
- Chartered Institute of Public Finance and Accountancy (CIPFA)
- Chartered Trading Standards Institute (CTSI)

- Citizens Advice Bureau (CAB)
- Take Five

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

- Metropolitan Police: The Little Book of Big Scams - Fifth edition of the Metropolitan Police fraud prevention advice publication - https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/fraud/met/the-little-book-of-big-scams.pdf

- Metropolitan Police: The Little Book of Cyber Scams 2.0 - Latest update from the Metropolitan Police on cyber crime - https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/fraud/met/little-book-of-cyber-scams-2.0.pdf

- Metropolitan Police: Little Booklet of Phone Scams - Guidance from the Metropolitan Police on phone scams - https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/fraud/met/little-booklet-of-phone-scams.pdf