



Coronavirus Special Edition

Information Alert 3

MIAA Anti-Fraud & Cyber Security Teams

23 April 2020

Coronavirus scams update

This is the third 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.

In the four weeks to the 12 April, overall crime figures dropped by 28%, with some crimes dropping nationally by over 50%. One area where the figures are actually increasing, however, is [fraud](#).

Illegal/Fake COVID-19 Tests

On 15 April, [BBC News](#) reported that two people have been arrested on suspicion of selling illegal tests. No home tests have yet been certified under European safety standards, and the use of home testing kits is also not advised by Public Health England. It is illegal to sell them.



One individual arrested, a pharmacist, is suspected of making false and misleading claims about the capability of coronavirus testing kits he had allegedly tried to sell, according to the National Crime Agency (NCA). This is particularly concerning due to the position of trust that a pharmacist holds in relation to medical care and treatments, making an illegal test appear to be reputable. The second individual was

allegedly targeting construction workers; however, offers of illegal testing kits could be directed at anyone regardless of sector, including individuals in their homes.

We're also aware of some scam **text messages** starting to circulate indicating the recipient has been in contact with someone with Covid-19 and they need to click on a link for more information. These are scam texts – no such system is currently in place for tracking Covid-19 and notifying the public on an individual level.

Action(s) to take: Health organisations and individuals should not purchase or endorse home testing kits until it has been formally certified for use. 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.

Phishing Emails/Cyber Security Alerts

● COVID-19 phishing emails

On 17 April, [BBC News](#) reported a huge increase in malicious phishing emails, particularly where COVID-19 is the subject. Google has published that 18 million COVID-19 phishing emails have been blocked on their email service every day, amounting to almost a fifth of all phishing emails identified and blocked, a trend supported by cyber-security companies.

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

Blocked emails were reported to imitate emails from genuine authorities, such as the World Health Organization (WHO) and the Centre for Disease Control and Prevention (CDC), as well as some high profile individuals. Whilst email providers are able to block a majority of these emails, some are still getting through to email inboxes, which could have an impact on both individuals and organisations.

- **NHS-targeted phishing emails**

NHS scam emails continue to circulate during the crisis, looking to exploit relaxed checks and controls. The NHS has again recently been targeted with a payroll phishing scam, inviting employees to click on a link to verify their details and ensure they receive payment.

Your employer will not request personal details in this way. Any details you provide will not be sent to your employer and instead be accessed by a fraudster, who may use it to defraud you. An example image of one such recent email is below.

Subject: RE: COVID-19 & APRIL PAYROLL BENEFIT.

All staff & employee are expected to verify their email account for new payroll directory and adjustment for the month of April benefit payment. Please kindly Click [APRIL-BENEFIT](#) and complete the required directive to avoid omission of your benefit payment for April 2020.

Thank you,

Payroll Admin Department.

© 2020 All rights reserved.

- **General phishing emails targeted at the public**

Everyone is being targeted by scam emails at home, not just work. We can't cover all the variations that these are taking but be on the lookout for some of the more prominent and persistent ones relating to the DVLA, energy supplier bill payments, PayPal and mobile phone accounts and HMRC. Between Saturday 11 April and Tuesday 14 April 2020, Action Fraud received 23 reports of phishing emails that purported to be sent from HMRC. The emails stated that the recipient was eligible to receive a tax refund of up to £775.80.

We're also aware of an increase in threats relating to ransomware and requesting payments in bitcoins or personal accounts and computers will be locked. These are pretty obvious and crude in nature, but no-one should feel pressured by these emails or respond to them. We also hear that some more audacious fraudsters are actually resorting to **phone calls** too, particularly relating to HMRC and account suspension scams.

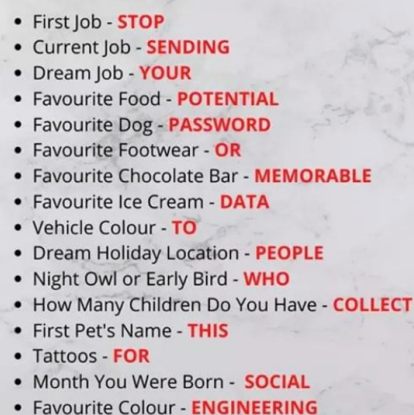
Action(s) to take: Individuals should remain vigilant to the potential for receiving malicious phishing emails, both in work and to personal email accounts, and report them appropriately to Action Fraud and via the NHS Spam reporting mechanism (see details at end of alert). Do not click on links, open attachments or download software where the email is not expected or the sender is unknown, and be wary of urgent tones used in emails inviting you to click those links or open attachments. If you receive any suspicious phone calls, hang up. If the call sounds like it might be genuine but you're not sure – hang up and call the organisation whom the caller states they represent via official, established contact numbers which are available on genuine documentation or via internet searches,

If you don't already have it, consider purchasing/upgrading Internet Security and Anti-Virus software from reputable providers on your personal PCs and mobile devices.

Any concern regarding a health organisation's cyber security provision should be referred to MIAA's Assistant Director (Informatics) – see page 1 for contact details.

Think twice before taking a quiz on Social Media

With so many people staying at home during the COVID-19 pandemic, it is tempting to turn to social media for distraction and entertainment. We are sharing this alert from Cumbria Trading Standards about quizzes circulating on social media. The information can give scammers the type of personal information that can be used to hack bank or shopping accounts.

- 
- First Job - **STOP**
 - Current Job - **SENDING**
 - Dream Job - **YOUR**
 - Favourite Food - **POTENTIAL**
 - Favourite Dog - **PASSWORD**
 - Favourite Footwear - **OR**
 - Favourite Chocolate Bar - **MEMORABLE**
 - Favourite Ice Cream - **DATA**
 - Vehicle Colour - **TO**
 - Dream Holiday Location - **PEOPLE**
 - Night Owl or Early Bird - **WHO**
 - How Many Children Do You Have - **COLLECT**
 - First Pet's Name - **THIS**
 - Tattoos - **FOR**
 - Month You Were Born - **SOCIAL**
 - Favourite Colour - **ENGINEERING**

Action(s) to take: Be aware that the information that is added to social media accounts can be used by fraudsters to target you. You can redact your accounts and/or adjust your privacy settings and please remain vigilant. Refrain from posting personal information on chain messages that may later be used by fraudsters for unscrupulous purposes.

Gifts, Donations and Fundraising

In light of the exceptional public support for the NHS and unprecedented offers of donations during the COVID-19 emergency, HFMA have released some [guidance](#) around gifts and hospitality for health organisations to consider.

Whilst most offers and donations have been low value consumable items and have been a huge benefit to many staff, this also presents an increased risk of individuals and criminal elements abusing this generosity.

Reports of such abuses have included solicitation of financial or higher value item donations on behalf of health organisations, by individuals with no connection to that organisation or the NHS, or who are not authorised to do so; as well as sites being set-up supposedly fund raising for NHS related initiatives/charities/organisations on public fundraising websites. Unfortunately, there are always some looking to exploit a crisis for their own ends. Any donations made for a health organisation that are not made directly or through an authorised channel may never reach the intended recipients.

Action(s) to take: NHS staff are reminded to check their own NHS employer's policy and any temporary guidance in relation to gifts, hospitality and donations in the first instance. Health bodies should be making clear to the public how they can donate directly, and warn against donations through alternative routes.

Staff should ensure they are compliant with the current gifts and hospitality guidance, and make declarations as required by that guidance.

Similarly, anyone who appears to be fundraising for a local NHS organisation should be notified to that organisation so that it can verify the fundraiser is genuine and that donations reach the intended recipients. Any scam fundraising campaigns with no NHS connection should be reported to the police or the Local Anti-Fraud Specialist for investigation – see page 1 for contact details.

Tax Scam Targeting Health Worker Returning to NHS



HMRC has warned health workers returning to the NHS in response to the Covid-19 outbreak that they could be heavily out of pocket if they fall prey to illegal tax scams. HMRC has issued an [alert](#) as tens of thousands of former NHS staff answered the call to return to work.

The scheme works by unscrupulous agencies or umbrella companies signing up returning staff by tempting them with arrangements that they claim to be legitimate, tax-efficient ways to allow the contractor to take home as much as 85% of their gross salary and reduce their paperwork, without explaining the risks

associated with the scheme. In reality, the companies that provide the schemes will attempt to disguise the true level of the individual's earnings which would ordinarily be the subject of income tax and NICs, while seeking to assure the user that the scheme is tax compliant.

HMRC is clamping down harder on tax avoidance throughout this year and it will be even keener to ensure fair play, given the massive sums the Government is investing to fight coronavirus.

Working Elsewhere Whilst Off Sick, or Self-Isolating

Staff undertaking other work whilst off sick is one of the most common staff related frauds in the NHS, with staff potentially receiving income in addition to their sickness pay during their absence. A number of reports have been received recently regarding staff undertaking other work whilst claiming to be self-isolating due to COVID-19. We're also receiving allegations of some individuals falsifying official 12 week 'shielding' and 'self-isolation' letters in order to avoid work. These are being actively investigated by our Anti-Fraud Specialists. This includes working in secondary employment or private practice, and also self-employment. Any such instances put additional pressure on those still working at a time when demand for frontline staff and health professionals is at a peak.

Action(s) to take: Anyone with suspicions that someone is working elsewhere whilst off sick or falsely claiming to self-isolate should report this to their Anti-Fraud Specialist for investigation – see page 1 for contact details. The matter will be dealt with sensitively, but thoroughly.

OTHER ACTIONS TO TAKE:

1. Report all suspicious 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. All successful phishing attempts should be reported to Action Fraud at <https://www.actionfraud.police.uk> or on **0300 123 2040**.
2. 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 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.emfiles4.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>

