Coronavirus Special Edition

Information Alert 6

MIAA Anti-Fraud & Cyber Security Teams

29 June 2020

Coronavirus scams update

This is the sixth issue of MIAA's dedicated, regular series of fraud, scam 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.

It is encouraging to note that there have been fewer reports of new NHS-targeted scams resulting from the COVID-19 emergency; however, that does not mean the threat no longer exists. This alert includes a reminder of some of the most prevalent frauds that have targeted the NHS in recent months, to help maintain awareness.

As of the 14/06/20, Action Fraud have received 2,450 reports of COVID-19 related fraud, amounting to £7,396,111 of losses, and 12,323 reports of COVID-19 related phishing.

NHS Tracing App

On the 18/06/20, it was reported by BBC News that the UK government is changing the way its current coronavirus-tracing app works and moving to a model based on technology provided by Apple and Google.

The Apple-Google design has been promoted as being more privacy-focused, however it may not involve contact tracing when it is initially launched, instead enabling users to report their symptoms and order a test.

The government now intends to launch an app in autumn and, as such, there will be no official tracing app in the UK until this app is launched. There are continued reports of fake apps and any claiming to be available before the official launch will be fake, and potentially result in the download of malicious malware to your device.

Action(s) to take: Do not download any mobile app that claims to trace COVID-19 in the UK until the official government one is launched.

Google launches Scamspotter website

To help people avoid online scams (including COVID-19 scams)

Google and the Cybercrime Support Network have joined forces and launched the website scamspotter. The website assists in showing specific COVID-19 scams, plus more general scams locally and globally, and is especially geared at educating seniors, who disproportionality lose more money due to scams than other demographics.

ACTION REQUIRED

MIAA recommends this alert is distributed to:

NHS STAFF for ACTION & AWARENESS

For further information or to report NHS Fraud contact:

Ruth Barker
Anti-Fraud Specialist
07584 774 763
Ruth.Barker@miaa.nhs.uk
Ruth.Barker12@nhs.net

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

Action(s) to take: Scamspotter's three golden rules relating to COVID-19 scams:

1. Slow down – trust doctors over peddlers – treatments for COVID-19 require intense scrutiny. Information about safe and effective medical advancements will come from professionals, not salespeople.

2. Spot check – consult government sources – refer to relevant .gov.uk websites and the CDC (Centres for Disease Control and Prevention) for the most up-to-date information about governmental and medical developments.

3. Stop! Don't send – don't pay for government benefits, unemployment payments, etc, never require you to pay upfront to apply for or receive them.

Key NHS-Targeted Frauds Reported During the COVID-19 Emergency:

- **Testing Scams**

Members of the public, in particular the elderly and those in vulnerable groups, are strongly advised not to open the door to bogus 'healthcare', council or charity workers, claiming to be offering 'home testing' for the COVID-19 coronavirus.

Action(s) to take: Health organisations and individuals should not endorse use of any home testing kits or paid testing services. 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.

- **HR and payroll bank mandate fraud incidents**

Phishing attacks have been used by criminals targeting changes to bank accounts that staff members have their salaries paid into, by impersonating employees in emails to HR and Payroll.

Further NHS payroll phishing attacks have invited employees to click on a link to verify their details and ensure they receive payment. NHS employers will not request your personal details this way.

Action(s) to take: Organisations should undertake checks to ensure staff are aware and authorise any requested changes to their bank details before those changes are made.

Staff should follow the phishing guidance detailed below to ensure that they deal with scam emails appropriately and don't become a victim of fraud.

- **Fake companies offering medical supplies and equipment for sale**

Fraudsters are trying to take advantage of the increase in demand across the NHS for medical supplies and equipment in light of the COVID-19 emergency. NHS staff members are receiving emails from fake companies offering to sell them medical supplies and equipment, such as facemasks, thermometers, protective clothing and hand sanitizer.

Action(s) to take: Be wary of unsolicited and unexpected emails received from unknown sources and companies offering for sale medical supplies and equipment. NHS organisations have established procurement processes and procedures in place, with appropriate due diligence checks, to minimise the risk of losses, including fraud. Do not pay unsolicited invoices that cannot be traced back to actual orders.

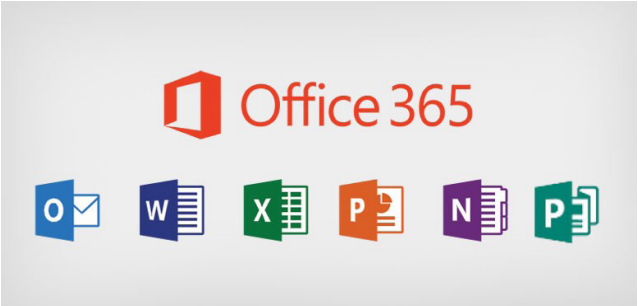
Emerging Phishing Scams:

- **Multi-Platform Phishing Attacks**

MIAA have received recent reports of a sophisticated cyber-attack involving phishing emails. Fraudsters use a combination of contact and approach methods to target an individual, such as using a phone call to support a phishing email, both claiming to be from the same apparently genuine individual. This dual approach is intended to validate the phishing email, to make it appear genuine and trick their victim.

- **Remote Workers Targeted Through Office 365**

Emails purporting to be from an organisation's IT department have been used to target remote workers in a recent phishing attack. The emails request users update the VPN configuration used to access the organisation's network while working from home, by clicking a link. The link directs the user to a spoof webpage, which looks like a legitimate Office 365 login page, and requests their log-in credentials, ultimately giving fraudsters their details and access to their Office 365 account.



The National Cyber Security Centre has published advice for organisations and staff around home working, which can be found here.

- **Ransomware**

Phishing emails are being used to spread ransomware, which can affect entire computer networks and have a massive impact at a hospital that is under strain from the virus.

These emails use a subject that may seem genuine or interesting to the recipient, often claiming to be from an official organisation or individual, and seek to persuade the reader to download an attachment or click on a link. Doing so will download malware to the user's computer or wider network, stealing personal information, spreading banking Trojans and even enabling criminals to carry out financial transactions and take over computer systems.

On 11/06/20 BBC News reported on the huge increase in cyber-attacks, including ransomware, during the COVID-19 emergency, with the health sector among the primary targets. Cyber criminals are taking advantage of increased home working, which may result in reduced security arrangements.

- **Health and Safety Executive (HSE) Violations Emails**

It is reported that emails have been sent to a number of organisations, purporting to be from the HSE, and claiming that their business has committed health and safety violations. The HSE has confirmed that it has not sent out such emails, confirming that these bogus emails are sent from @hse.online email addresses. A statement to this effect has been published by the HSE on their website.

- **Spoofed Websites**

Fake websites have been used to target shoppers of UK supermarkets and retail businesses, including Tesco, Asda and Amazon. Cyber criminals have abused the increased demand for online shopping during the pandemic by creating numerous fake websites for each supermarket, using similar domain names to the original. The websites are designed to look like the legitimate site, so that users will enter their credentials, allowing fraudsters to obtain their personal and financial information.

Fraudsters are also using internet search engines to target individuals wanting to access their online banking service (including corporate banking), through maliciously targeted advertisements that lead to a spoofed banking website. This follows reports of emails purporting to be from banks (one example is Deutsche Bank) offering one-year interest free loans. The emails offer the loans of between £5,000 and £100,000 without credit checks with a 2-day approval.

- **DocuSign scam**

Many organisations have been finding alternative methods of authorising documents during lockdown. In some cases this has been through use of DocuSign, a service that facilitates sending and signing electronic copies of contracts.

Cyber criminals have used this increased demand for electronic documents to send emails impersonating a DocuSign email and request the recipient follows a link to review the document. Upon clicking the link, they are directed to a spoof website, which then takes their log-in credentials.

- **Amazon Prime renewal scam**

Amazon Prime renewal scams have been reported as circulating, impersonating Amazon Prime, and advising victims their subscription will be 'renewed' for £39.99. The scam is designed to persuade Amazon Prime customers into sharing their personal and financial data.

A further Amazon phishing email has been sent directly to NHS staff email addresses at one North West Trust. The email advises the recipient that their payment card is no longer valid, and requests an attachment is downloaded.

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