Coronavirus Special Edition

Information Alert 1

MIAA Anti-Fraud & Cyber Security Teams

March 2020

Coronavirus scams update

Welcome to the first 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.

There are many different types of Coronavirus scams currently being perpetrated by fraudsters. Some of the scams are targeted specifically at individuals, the elderly and vulnerable in particular, and some are targeted more at organisations such as the NHS.

The scams are perpetrated for a number of reasons: for the purpose of immediate financial gain; in order to steal victims' personal information and/or login credentials for their own use or selling on; and in order to infect victims' computer with malicious software, for whatever reason.

There are many different methods of scam in operation too. These include:

- **Doorstep** scams where fraudsters come to the doors of victims to try and scam them out of money or gain access to their property;
- **Phishing** scams where fraudsters send fake emails and/or create bogus web pages with the malicious intention of obtaining a victim's online bank, credit card, or other login information;
- **Smishing** scams where fraudsters send fake SMS messages and/or create bogus web pages with the malicious intention of obtaining a victim's online bank, credit card, or other login information; and
- **False invoicing**, **procurement** and **payment diversion** scams in order to get critical money out of the NHS when fraudsters believe the usual checks and controls in place may be stretched or not working.

Three scams currently in circulation are:

1. COVID-19 'home testing' scam

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 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

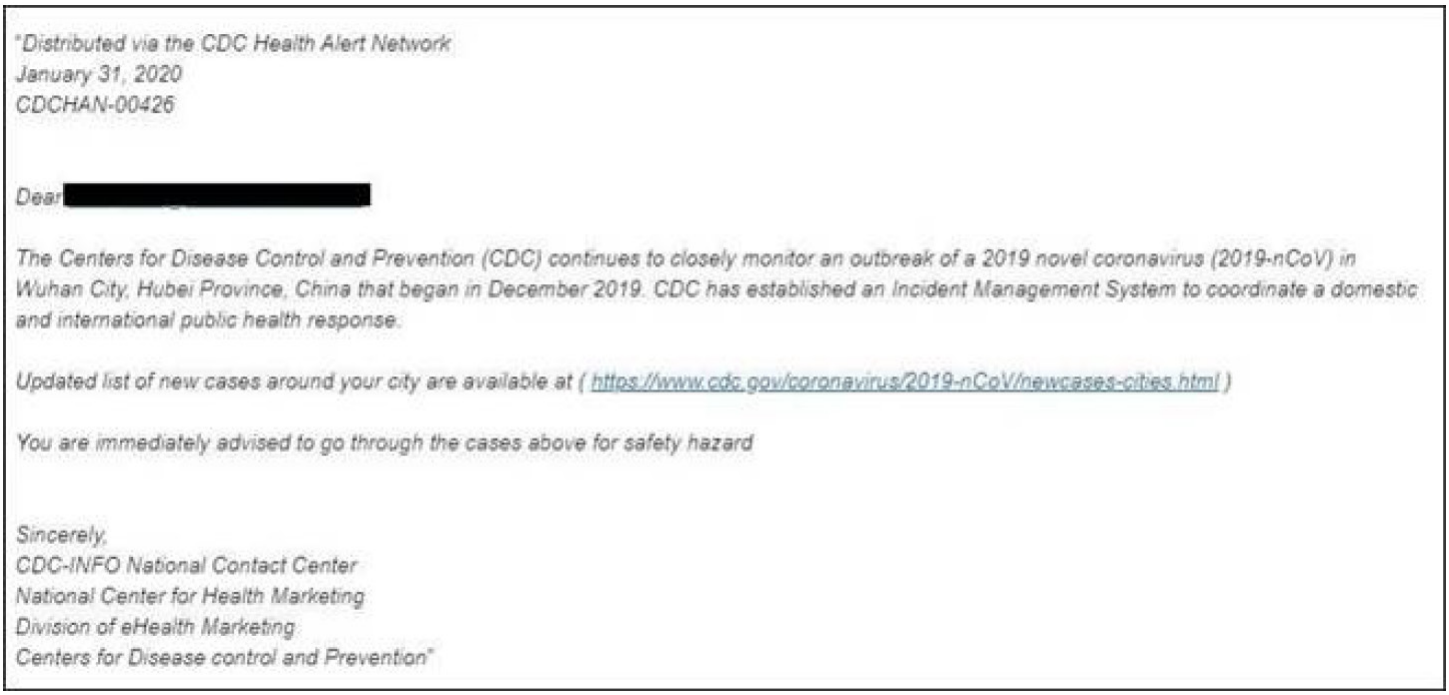
If you are concerned that you are a victim of a cyber-crime or want to know how to improve your organisation's cyber resilience, contact:
Tony Cobain
Assistant Director (Informatics)
07770 971 006
Tony.Cobain@miaa.nhs.uk

MIAA ASSURANCE

Suspicious callers are said to be knocking on doors of intended victims saying that they are local council officers or health officials (in some cases from the Red Cross) doing door-to-door testing, with the aim of gaining entry to the property to steal (or de-fraud) money (or possessions) from them, or worse. People who open the door and allow strangers into their home are placed at greater risk of catching Coronavirus.

Other doorstep scams currently in operation include fraudsters knocking on doors pretending to be: NHS employees offering a **COVID-19 vaccine;** and helpful 'neighbours' offering to **run errands,** such as collecting prescriptions or doing shopping, in exchange for cash upfront or a credit card with its PIN.

2. Fake alerts from the Centers for Disease Control and Prevention (CDC)



"Distributed via the CDC Health Alert Network
January 31, 2020
CDCHAN-00426

Dear [redacted]

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

You are immediately advised to go through the cases above for safety hazard

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention"

Intended victims receive an email purportedly from the CDC Health Alert Network with a list of active infection cases in their surrounding area.

In order to access the 'list' to see if there are any outbreaks of the virus in their vicinity, the intended victim must click on a link that seems to go through to the official CDC portal but, in reality, redirects them to a malicious domain that is intended to steal their Outlook login credentials or place malicious software on their computer/network.

The phishing email imitates the genuine ones sent out by the CDC Health Alert Network. The logo and everything else look consistent with the authority allegedly sending out this warning.

Other impersonation email scams currently in circulation include fraudsters pretending to be **HMRC** offering a tax refund, the **World Health Organization (WHO)** offering advice on how to stay safe during the outbreak, and **Wuhan Medical Authorities** claiming to distribute advice for dealing with the virus.

3. 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 to fight coronavirus. NHS staff members are receiving emails from fake companies offering to sell them medical supplies and equipment to fight coronavirus. Examples of the types of medical supplies and equipment being offered for sale include facemasks, thermometers, protective clothing and hand sanitizer.

Sales.59@medical-supplies.com on behalf of bbiber@yahoo.com? [redacted]

Find something to do at home

Dear Customer,

How are you?

Lily hope you and your family are well.

Currently we are produce mask production line machine and offer the 3 Ply medical mask(BFE ≥99%) and and detection Kit (Colloidal Gold-Based). Which supply for China rescue team and sent it to Iran.

I will send you the catalog if you need it.

You might have learned that the virus spreads through droplets mainly, Tips below which have been proven to reduce the risk of infection COVID-19 effectively from our experience:

1. Please wear a mask whenever you go outside.
2. Try your best to stay away from the public, stay in the house instead.
3. When you are back from outside, do not touch your eyes, nose, and mouth before washing your hands first.
4. Please cook the meat as well-done instead of the medium or rare.
5. Ventilate the room at least three times per day.

Please feel free to call us in case you need any other help, we will do our best.

Regards from China.

Actions to take:

1. Be wary of all strangers who knock at the door. Do not open the door or allow them in to your home. The Local Government Association (LGA) advises anyone who is stuck without food or medical supplies, or lonely due to self-isolation, and who does not have any family or friends or neighbours that they know in the area, to contact their local council in the first instance.

2. Be wary of all unsolicited and unexpected emails and SMS messages from health organisations such as the WHO and the CDC, but also large trusted institutions like HMRC, DVLA, banks, BT, Sky, PayPal, Microsoft and the BBC. In particular, be suspicious of anything with an urgent tone that invites you to open an attachment or click on a link. Look out for poor grammar and spelling errors and emails that begin impersonally with 'Dear Sir' or 'Dear Customer'. If in any doubt, phone the genuine company or person via an established or known number to verify.
Above all, take your time and think before you click.

3. Be wary of all unsolicited and unexpected emails received from unknown and unfamiliar companies offering for sale medical supplies and equipment to protect against coronavirus. NHS organisations have established procurement processes and procedures in place, with appropriate due diligence checks, to ensure that they are adequately supplied with what is required. The same applies to unsolicited invoices that don't relate to actual orders.

4. 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.**

5. Security awareness – with the influx of additional personnel to the NHS, don't be afraid to challenge unfamiliar faces for their ID badges, particularly individuals in sensitive areas or around store rooms containing vital equipment, food or medical supplies. Challenging times can mean individuals may resort to desperate measures to get what they need.

To stay up-to-date on the latest coronavirus scams, please visit:

- 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