Fraud Information Alert 6

MIAA Anti-Fraud Service

March 2020

Coronavirus email scams

Healthcare professionals should be warned that they are being targeted by cybercriminal gangs with phishing emails about coronavirus. It was recently reported in the national news that a number of healthcare organisations had received emails purporting to be from their internal IT team.

The email titled 'ALL STAFF: CORONA VIRUS AWARENESS', informs that a seminar is being organised for all staff to attend to discuss the coronavirus, and asking them to click on a link to register.

From: [redacted]
Sent: Wednesday, March 04, 2020 10:55 AM
To: [redacted]
Subject: ALL STAFF: CORONA VIRUS AWARENESS

Dear Employee/Staff,

There is an ongoing outbreak of a deadly virus called coronavirus (Covid-19). The virus is spreading like wide fire and the world health organization are doing everything possible to contain the current situation. The virus which originated from china has hit Europe, America, Asia and Africa. The government has hereby instructed all organization and institution to educate and enlightened their employee/staff about the virus in order to increase the awareness of the coronavirus (covid-19).

in view of this directives, the institution is currently organizing a seminar for all staff to talk about this deadly virus. All employee/staff are hereby ask to quickly participate in the quick survey to show your awareness about the coronavirus and also register for the seminar. The survey and seminar is compulsory in the battle to win the fight against this epidemic as all employee are Mandated to participate in the survey immediately you receive this notice. Disciplinary measure would be taken on staff that failed to carry out this instruction. Winning this battle is in our collective effort. Kindly follow the link SURVEY/SEMINAR to participate in the survey and register for the seminar.

Best Regards
IT-Service desk

The link, when clicked on, goes through to a third-party website disguised as an Outlook web app. Anyone who fills in the form contained on the link ends up giving their details to the hackers.

It is believed that scams intending to take advantage of COVID-19 have become increasingly common since the beginning of the outbreak.

Since February 2020, the National Fraud Intelligence Bureau (NFIB) has recorded 21 incidents of fraud involving coronavirus, with victim losses totalling in excess of £800k. Ten of the victims were attempting to purchase protective face masks from fraudulent sellers, with one victim in particular losing £15k.

ACTION REQUIRED

MIAA Anti-Fraud Service recommend this alert is distributed to:

NHS STAFF for ACTION & AWARENESS

MIAA IA 19/20 6

For further information on MIAA's Anti-Fraud Service visit miaa.nhs.uk

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

Another example are emails from fraudsters purporting to be from research organisation's affiliated with the Centers for Disease Control and Prevention (CDC) and the World Health Organisation (WHO) contacting potential victims by email in an attempt to trick people into either clicking on a link leading to a malicious website or making a payment in Bitcoin.

Recommended Actions

1. Don't click on the links or attachments in suspicious emails, and never respond to unsolicited messages and calls that ask for personal or financial details.
2. If making a purchase from a company or person that is unfamiliar or untrusted, carry out some research first, and ask a friend or family member for advice before completing the purchase.
3. Use a credit card where possible, as most major credit card providers insure online purchases.
4. Forward any suspicious or spam emails as an attachment to spamreports@nhs.net.
5. Report all successful phishing attempts to Action Fraud on 0300 123 2040 or at www.actionfraud.police.uk.
6. For further information or advice, contact the Local Counter Fraud Specialist.

How to Report Spam & Phishing Messages

1. Select the email from your inbox.
2. Click on the "New mail" icon in the top left of the screen
3. Drag and drop the spam email from the email list onto the body of the new blank email
4. Enter spamreports@nhs.net into the To: field
5. Enter an appropriate subject into the subject field. It's recommended that you use spam, phishing or malicious depending on the type of email you are reporting.
6. Click Send.

To view the latest National Fraud Intelligence Bureau alert, please visit: http://bit.ly/2TTMNMl

To view previous MIAA fraud alerts, please visit: https://www.miaa.nhs.uk/insights/fraud-alerts-news