Fraud Alert

10 May 2022

Alert Ref: 003-CC-22/23

Issued to:

- DOFs /CFOs
- Counter Fraud Champion
- Comms teams

Action required:

- Circulate the contents of this alert to all staff
- Confirm by email return to your Counter Fraud Specialist that this alert has been actioned

If you wish to report any concerns regarding fraud, bribery or corruption, please contact a member of our team, contact your nominated Counter Fraud Specialist, email counterfraud.360@nhs.net, or contact the NHS Counter Fraud Authority Reporting Line on 0800 028 4060.

Disclaimer: This alert, prepared by 360 Assurance is for the sole use of 360 Assurance clients, and no responsibility is taken by 360 Assurance or the Anti-Crime Specialist to any director or officer in their individual capacity. No responsibility to any third party if accepted as the alert has not been prepare for, and it IS not intended for any other purpose and a person who is not a party to an agreement for the provision of anti-crime services with 360 Assurance shall not have any rights under the Contracts (Rights of Third Parties) Act 1999.

ACTION REQUIRED

Subject: False Covid text asking patient to order test kits.

360 Assurance have been notified of a sophisticated text scam that has been sent to individuals purporting to be from various sources including their GP practice and the NHS-NoReply service. The text could easily be mistaken as a legitimate notification as the recipient's mobile will show the text grouped with legitimate texts from their own GP practice and other NHS notifications.

The message advises them that they have been in close contact with someone who has tested positive for Omicron and that they must order a test kit using a link within the text. The link then asks for a payment for postage, to which the victim then adds details of their bank card, home address and telephone number.

This information is then used by the fraudster to call the victim with the pretence of being from the fraud team at their bank. During this call the fraudster advises that a number of suspicious transactions have been identified and are due to leave the victim's bank account, and then asks the victim to confirm much money they have in their account. The fraudster then asks the victim whether they have clicked on any links from companies such as PayPal and Amazon. They then ask about the ordering of PCR testing kits. When the victim then confirms they clicked on the link to order a test kit, they are told that their bank card will be cancelled and reissued as the link is likely to be a scam. When the victim questions the caller's identity, the fraudster tells the victim they can check their bank's website to confirm the legitimacy of the caller's telephone number, which appears to be correct. The fraudster then continues and asks the victim to confirm their banking username and password.

One victim later confirmed with their bank that no transactions had recently been blocked from leaving their account and no new card/pin had been recently issued. The bank also confirmed that fraudsters are cloning telephone numbers belonging to banks to make it look like they are legitimate. In one particular case, after having had contact with the fraudster, the victim's bank contacted them to advise them that a number of suspicious transactions had been blocked from leaving their account, as a result of clicking the link to purchase a Covid-19 test kit online.

This information should be shared with all staff. The NHS would not text individuals in this way seeking payment for test kits. Individuals should be vigilant to avoid providing personal information such as bank details to fraudsters. Anyone who suspects they may have fallen victim to this type of scam should contact their bank immediately and report the incident to Action Fraud by visiting https://www.actionfraud.police.uk/ or calling 0300 123 2040.