

COVID-19



Fraud Alert

Fake Omicron Email Scam

tiaa

TIAA has been alerted to a new phishing email that is circulating. The email is sent from contact@nhs-pcr.uk and the email content is as follows. Note the spelling and grammar errors which are commonly found in a phishing email.

Get Your Free Omicron PCR today to avoid restrictions

NHS scientists have warned that the new Covid variant Omicron spreads rapidly, can be transmitted between fully vaccinated people, and makes jabs less effective. However, as the new covid variant (Omicron) has quickly become apparent, we have had to make new test kits as the new variant appears dormant in the original test kits.

What happen if you decline a COVID-19 Omicron test?

In this situation, we warned that testing is in the best interests of themselves, friends, and family. People who do not consent or cannot agree to a COVID-19 test and refuse to undergo a swab must be isolated.

How to request a Free Omicron PCR test?

You can order your Omicron pcr test via NHS portal by clicking the link below: nhs-order-pcr/COVID-10-omicron-research/

What happen if you are positive?

If positive, they must isolate for 10 days and should be reported to Public Health England.

Status: Action Required

The alert provides information and advice about fraud and economic crime, and the risks associated with it.

If you have fallen victim to fraud you should report it to Action Fraud by calling 0300 123 2040, or visit: <https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime>

If you have given your bank details and think you may have lost money, contact your bank immediately.



How to protect yourself from fraud

- Stop and think before clicking on a link, as this may install malware, such as viruses, spyware or ransomware on your device, and data or sensitive information could be stolen.
- Delete any phishing email immediately.
- Never give out personal or financial information about yourself unless you are absolutely sure the source is genuine.
- Further prevention advice can be found on the National Cyber Security Centre website for both individuals and organisations.

Disclaimer: This document is provided for guidance and awareness purposes only. This summarising article is not a full record of the key matters and is not intended as a definitive and legally binding statement of the position. While every effort is made to ensure the accuracy of information contained, it is provided in good faith on the basis that TIAA Limited accept no responsibility for the veracity or accuracy of the information provided. Should you or your organisation hold information, which corroborates, enhances, contradicts or casts doubt upon any content published in this document, please contact the Fraud Intelligence Team.

Handling & Distribution: This document must not be circulated outside of your organisation, on public facing websites or shared with third parties without written consent. Onward disclosure without prior authority may be unlawful under the Data Protection Act 2018.

For further discussion and support, including fraud awareness training services, contact:

Melanie Alflatt, Director of Anti-Crime Services ■ Email: fraud@tiaa.co.uk

www.tiaa.co.uk
0845 300 3333