

COVID-19



Fraud Alert

tiaa

Fake Emails Sent to NHS Staff Promoting COVID-19 Support Fund

A member of staff at one of TIAA's clients, an NHS Trust, has been targeted by fraudsters. The email appeared to be sent from a genuine nhs.net email address, which is likely to have been hacked, and will almost certainly be circulated to a large number of NHS staff. The text in the email is as follows:

In response to the current hardship in the community due to the COVID-19 pandemic, NHS England has decided to support workers, Faculty/Staff and Students to get through these hard times.

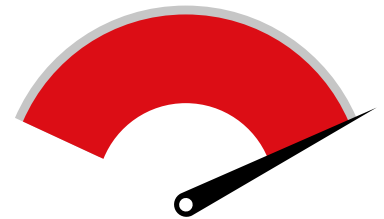
NHS England will award GBP £2,920.00 COVID-19 support to all eligible NHS Workers, Faculties, Staffs and Students, starting from, Tuesday, 16 November 2021. Visit NHS England Covid-19 support registration page and register with your information to be eligible for this support fund payout.

Note: If you do not submit all the information requested, your application will not be processed.

Sincerely,
COVID-19 Support Team



NHS England,
PO Box 16738, Redditch, B97 9PT



Status: Action Required

This alert provides information and advice to NHS employees about fraud and economic crime, and the risks associated with it.

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

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

The member of staff advised that if you click on the link you are asked for bank details and a photo of your staff ID badge.



How to protect yourself from fraud

Stop and think before replying to an email, clicking on a link, or phoning a number given in an email. Never give out personal or financial information about yourself unless you are sure the source is genuine.

Remember if it looks too good to be true - it probably is!

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