

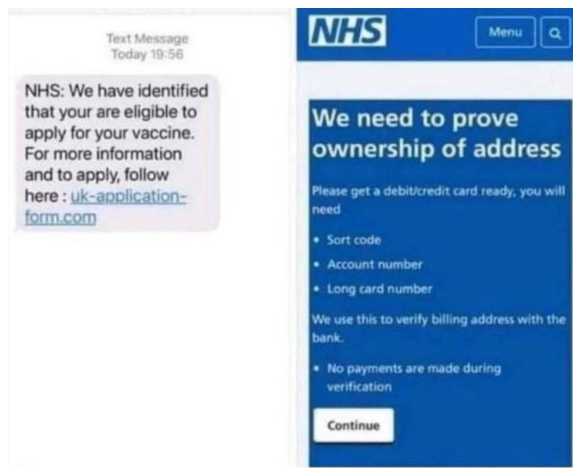


Fraud Alert

Fake NHS COVID-19 Vaccination Alert

tiaa

The Chartered Trading Standards Institute (CTSI) has issued a warning regarding fraudulent text messages being sent to the public informing them that the COVID-19 vaccine is available to them. Here is an example of the scam text. The link takes you to a bogus website that does appear to look like a genuine NHS site which asks for your banking details.



CTSI state that “this is the latest in a series of scams themed around the pandemic in circulation since last March. With the UK vaccine rollout underway, scammers have modified their scam to consider this new development”.

Full details can be found at: <https://www.tradingstandards.uk/news-policy/news-room/2021/fake-nhs-covid-19-vaccination-messages-target-vulnerable-public>

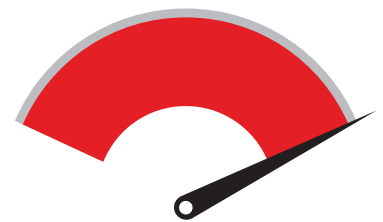


How to protect yourself from scams

- Stop and think before replying or clicking on a link
- Never give out personal or financial details in response to emails, text or phonecalls.
- Block numbers that you suspect may be from spammers.

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.



Status: Action Required

The alert provides information and advice to 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 you may have lost money, contact your bank immediately.

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

Melanie Alflatt, Director of Fraud & Security ■ Email: covidfraud@tiaa.co.uk

www.tiaa.co.uk

0845 300 3333