



Alert - Coronavirus Vaccination Scams

As of 7 January 2021, Action Fraud had received 57 reports from members of the public who have been sent text messages claiming to be from the NHS, offering them the opportunity to sign up for coronavirus vaccinations. The texts ask the recipient to click on a link which takes them to an online form where they are prompted to input personal and financial details. In some cases the online form has looked very similar to the real NHS website.

Pauline Smith, Head of Action Fraud, said:

“Remember, the vaccine is only available on the NHS and is free of charge. The NHS will never ask you for details about your bank account or to pay for the vaccine. If you receive an email, text message or phone call purporting to be from the NHS and you are asked to provide financial details, this is a scam.”

How to protect yourself:

In the UK, coronavirus vaccinations will only be available via the National Health Services of England, Northern Ireland, Wales and Scotland. You can be contacted by the NHS, your employer, a local GP surgery or pharmacy, to receive your vaccination. **Remember, the vaccinations are free of charge and you will not be asked for a payment.**

The NHS will never:

- ask for your bank account or card details
- ask for your PIN or banking passwords
- arrive unannounced at your home to administer the vaccine
- ask for documentation to prove your identity, such as a passport or utility bills

If you receive a call you believe to be fraudulent, hang up. If you are suspicious about an email you have received, forward it to report@phishing.gov.uk. Suspicious text messages should be forwarded to the number 7726, which is free of charge.

If you believe you are the victim of a fraud, please report this to Action Fraud as soon as possible by calling 0300 123 2040 or visiting www.actionfraud.police.uk.

Please forward this email to any friends, family members, or colleagues that may find this information useful

Message Sent By

Action Fraud (Action Fraud, Administrator, National)

To reply or forward this email please use the buttons below or these links: [Reply](#), [Rate](#), [Forward / Share](#).



To login to your account, [click here](#), To report a fault, [click here](#)



You are receiving this message because you are registered on Action Fraud Alert. Various organisations are licenced to send messages via this system, we call these organisations "Information Providers".

Please note that this message was sent by Action Fraud (NFIB) and that Action Fraud (NFIB) does not necessarily represent the views of Action Fraud Alert or other Information Providers who may send you messages via this system.

You can instantly review the messages you receive and configure which Information Providers can see your information by clicking [here](#), or you can [unsubscribe](#) completely, (you can also review our terms and conditions and Privacy Policy from these links). You can also send unsubscription requests to unsubscribe@neighbourhoodalert.co.uk

This email communication makes use of a "Clear Image" (gif) to track results of the email campaign. If you wish to turn off this tracking for future emails, you can do so by not downloading the images in the e-mail itself.

VISAV Limited is the company which built and owns the Neighbourhood Alert platform that powers this system. VISAV's authorised staff can see your data and is registered with the Information Commissioner's Office as the national Data Controller for the entire database. VISAV needs to see your data in order to be able to manage the system and provide support; it cannot use it for commercial or promotional purposes unless you specifically opt-in to Membership benefits. [Review the website terms here](#).

