

# Coronavirus vaccine scam warning

Action Fraud is warning the public to remain vigilant as criminals begin to take advantage of the roll out of the COVID-19 vaccine to commit fraud.

As of 7 January 2021, Action Fraud, the national reporting centre for fraud and cyber-crime, had received 57 reports in relation to the COVID-19 vaccine.

Pauline Smith, Head of Action Fraud, said:

“The vaccine is a crucial tool in fighting the coronavirus and keeping people safe. Thankfully, the number of reports into Action Fraud are relatively low but we have seen an increase in the last two months, particularly around scam text messages. 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.”

Action Fraud has received 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 the vaccine. 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.

## How to protect yourself:

In the UK, coronavirus vaccines 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 GP surgery or pharmacy local to you, to receive your vaccine. Remember, the vaccine is free of charge. At no point will you be asked to pay.

- The NHS will never ask you for your bank account or card details.
- The NHS will never ask you for your PIN or banking password.
- The NHS will never arrive unannounced at your home to administer the vaccine.
- The NHS will never ask you to prove your identity by sending copies of personal documents such as your passport, driving licence, bills or pay slips.

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](mailto: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](http://www.actionfraud.police.uk).

This information is taken directly from an article on the Action Fraud website at the following link: <https://www.actionfraud.police.uk/vaccine>