

MESSAGE FROM LINCS ALERT

We have been made aware of fake NHS text messages circulating, informing the public that they're eligible for a Covid-19 vaccine.

The scam message reads "We have identified that you are eligible to apply for your vaccine" which prompts you to click on a link to find out more and to "apply" for the vaccine.

The link directs you to a convincing fake NHS website, where fraudsters can coerce you to divulge personal or financial details.

Any texts or emails containing URLs should always be treated with caution and we'd urge for members of the public to avoid clicking links in unsolicited texts or emails.

Texts or emails that ask you to provide information such as your name, date of birth or financial details are scams and if you're ever unsure about these types of messages, ignore or delete them.

Cold calls that ask you to provide personal or financial details or ask you to pay over the phone to access the vaccine have also been reported. If you receive one of these calls, hang up immediately.

How to protect yourself from scams

Scams are becoming more and more sophisticated and they also come in many forms, making it difficult to distinguish real messages from fake ones. Below are some useful tips to avoid falling victim to any scam:

- If you receive a text or email containing attachments or links from unknown senders, do not open them. Move emails to your Spam inbox, delete the text messages and block the number if you can.
- If possible, use 2-factor authentication to provide extra protection to your online accounts. Visit the National Cyber Security Centre for more information.
- Never give out your personal information or financial details in response to emails, texts or phone calls. Always verify who you are speaking with.
- Look out for fake websites and if you're unsure, check the domain name.
- Check for errors in spelling. Messages or emails riddled with spelling mistakes are normally linked to phishing attacks.

If you think you have been a victim of a scam or know of someone who has fallen victim to an online fraud:

Contact your bank immediately to tell them what's happened.

Report it to Action Fraud on 0300 123 2040 or online.

Please share this warning with friends, families, neighbours and colleagues so we can prevent anyone from falling victim to scams.

Message Sent By

Gillian Fleet (Police, Preventing financial fraud officer, Lincolnshire)