LINCS ALERT messaging

FAKE NHS COVID-19 VACCINATION TEXTS

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

The scam message reads "We have identified that you are eligible to apply for your vaccine" and 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 into divulging personal or financial details.

Any text messages or e-mails containing URLs (links) should always be treated with caution. We urge members of the public to avoid clicking on links in unsolicited texts or e-mails. Texts or e-mails that ask you to provide information such as your name, date of birth or financial details are **SCAMS**. If you are ever unsure about these types of messages, ignore and 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. Here are some useful tips to avoid falling victim to any scam:

- If you receive a text or e-mail from an unknown sender containing attachments or links, do not open attachments and do not click on links. Delete the text message and block the number if you can. Move e-mails to your *spam* folder.
- If possible, use two-factor authentication to provide protection to your online accounts. Visit the *National Cyber Security Centre* for more information.
- Never give out any personal information or financial details in response to e-mails, texts or phone calls. Always verify who is speaking to you on the phone.
- Be aware of fake website and if you are unsure, check the domain name.
- Check for spelling and grammatical errors. Messages or e-mails riddled with mistakes are normally linked to phishing attacks.

If you think you have been a victim of a scam, or if you know of someone who has fallen victim to an online fraud, report it to Action Fraud on 0300 123 2040 or online. If you have given out bank, credit card or debit card details, contact your bank immediately and tell them what has happened.

Please share this warning with friends and family members, neighbours and colleagues, so that we can prevent people from falling victim to scams.

Message sent by: **Gillian Fleet**
Police, Preventing financial fraud officer, Lincolnshire