

## Residents at risk of being scammed over COVID-19 vaccine.

Dyfed Powys Police Economic Crime Team has become aware that criminals have been sending texts and emails attempting to lure people to apply for the COVID-19 vaccine.

DC Gareth Jordan, from the Cyber Crime Unit, said: “The text is made to look like it comes from the NHS and states ‘we have identified that you are eligible to apply for your vaccine’ and advises you to follow a link to get more information and ‘apply’.”

“If you follow the link, you are taken to a convincing looking, but fake NHS website that asks for your personal details.

“After entering your details, it then requests bank/card details to ‘check your identity’.”

“But as with all scams, if you look a little closer, you will see it is not real. In this instance, note the URL is not [www.nhs.uk/](http://www.nhs.uk/)

The image displays two screenshots of a fraudulent NHS website. The left screenshot shows a browser window with the URL [uk-application-form.com/Appf](http://uk-application-form.com/Appf). The page features the NHS logo and a 'Menu' button. The main heading is 'Coronavirus (COVID-19) vaccine' with a sub-heading 'Application at foot of page'. A yellow box contains the text: 'Read before applying. Please take the necessary time to read over our information on the vaccine. It is important your choice is informed as some parties may not be recommended to take the vaccine currently.' Below this, it states: 'The coronavirus (COVID-19) vaccine is safe and effective. It gives you the best protection against coronavirus.' The right screenshot shows a 'We will now ask some questions' screen. It lists the information requested: Name, Date of birth, Address, A payment card (to check billing), and Proof of address. It also explains: 'We ask this so we can: Get the right mix of different people taking the vaccine, Confirm identity, Confirm ownership of address'. A 'Continue' button is visible at the bottom, along with a security notice: 'NHS Digital will keep your answers secure. Find'.

“As multiple vaccines are now being approved for use in the UK, these types of fraud attempts will continue as criminals look to take advantage of the vaccine roll out.

“It’s not only texts, beware of cold calls and emails regarding the vaccine as scammers are also asking people to pay for it over the phone. Remember – the vaccine is free of charge and there is no way to jump the queue by paying for a ‘priority slot’.

“If you receive one of these calls, hang up and block the number.

“If you have received an email, which you are not quite sure about, forward it to the Suspicious Email Reporting Service (SERS) at [report@phishing.gov.uk](mailto:report@phishing.gov.uk)

“Suspicious text messages should be forwarded to **7726**. This free-of-charge short code enables your provider to investigate the origin of the text and take action, if found to be malicious.”

**Always:**

**Stop:** Take a moment to think before parting with your money or information - it could keep you safe.

**Challenge:** Could it be fake? It’s OK to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

**Protect:** Contact your bank immediately if you think you’ve fallen victim to a scam and report it to the Police.

**Remember** – The NHS, the police, or your bank, will never ask you to withdraw money or transfer it to a different account. They will also never ask you to reveal your full banking password or PIN.

Do not click on links or attachments in unexpected or suspicious texts or emails. Confirm requests are genuine by using a known number or email address to contact organisations directly.

**Always check the URL of a website.**

**Scammers are trying to trick people regarding the Covid-19 Vaccine**

**The NHS don’t need your bank details and won’t ask for them in an email or text.**

# NHS

There is no charge for the vaccine  
The NHS don't need your bank details  
Do not pay 'to see your place in the  
vaccine queue' - it's a scam

**Report it:**

**Emails:** [report@phishing.gov.uk](mailto:report@phishing.gov.uk)

**Texts:** Forward text to 7726

**Phone:** Hang up on & block the number

**Tell:** Tell others about this scam

