**From:** Evans, Marc - Corporate Services
**Sent:** 30 December 2020 12:45
**Subject:** Media release: Scammers target residents with promise of coronavirusvaccine

**Scammers target residents with promise of coronavirus vaccine**

**Read the story on the Oxfordshire County Council website** [**here**](https://news.oxfordshire.gov.uk/scammers-target-residents-with-promise-of-covid-vaccine/) **or below:**

Residents are urged to be on their guard against scammers using the promise of a coronavirus vaccine to con them out of money.

Criminals across the country are contacting people out of the blue with offers of a coronavirus vaccination. These approaches have been made by text or from a recorded voice message on the telephone.

In each case the recipient is required to respond by clicking a link in the text message or by pressing 1 when receiving the call. They are then asked to give personal information, as well as financial details to book their vaccination. However, these are scams, with criminals exploiting the pandemic to attempt to steal personal details and people’s money.

The NHS is currently offering the COVID-19 vaccine free of charge to people most at risk from coronavirus. These people will be contacted by the NHS.

**Jody Kerman, Oxfordshire County Council’s head of trading standards, said:** “Unfortunately, scammers will use any high-profile situation to try to commit their crimes and the coronavirus pandemic has given them a new opportunity. Scammers will often use fear tactics, or claims of big rewards or access to restricted goods and services – trying to rush their victims and taking away their time to think.”

Other warning signs to watch out for include:

* Scammers who try to get you to pay them money for ‘early access’ to the vaccine.
* Scammers who ask for private information such as bank account details or your NHS number.
* Scammers knocking on your door claiming they can get you early access to the COVID-19 vaccine.
* Vaccine-themed phishing campaigns from suspicious email addresses with hyperlinks that contain misspelled domain names.
* Highly emotive language designed to manipulate you; do not supply login credentials or personal information in response to an email.

People are urged to:

* Monitor key financial accounts regularly.
* Keep software and apps updated.
* If you get a suspicious text asking you to click on a link this could be a scam. Do not click on the link.
* If you receive a recorded voice message on your phone and are asked to press a number, this could be a scam. Do not press any buttons and do not call the number back.
* Report all scams to us via Citizens Advice Consumer Service on 0808 223 1133.

There has been a surge worldwide of vaccine-related ‘phishing’ email scams, and this is expected to increase in these in the coming days. Previous phishing emails have contained malicious files that installed malware, or links to bogus websites to obtain the victim's information.

Scams cost the UK economy £5-£10 billion a year and there is a scam out there for everybody. Before clicking on a link or providing your personal details, stop and ‘take five’. Never be afraid to delete the text, put the phone down or close the door.

To find out more about how scams work, the harm they cause and how you can help to protect people in your community, consider becoming a Friend Against Scams at [www.friendsagainstscams.org.uk](https://www.friendsagainstscams.org.uk/)

For more details on the ‘Take 5’ campaign, go to <https://takefive-stopfraud.org.uk/>

**Ends**

**For more information about this release contact the Oxfordshire County Council and Cherwell District Council communications team on 01865 323870 or email** press.office@oxfordshire.gov.uk

Marc Evans

Communications and Media Officer

Oxfordshire County Council