

Protect your tech

Scams and threats to avoid, plus new security tools

WATCH OUT FOR...

Fake NHS Coronavirus website

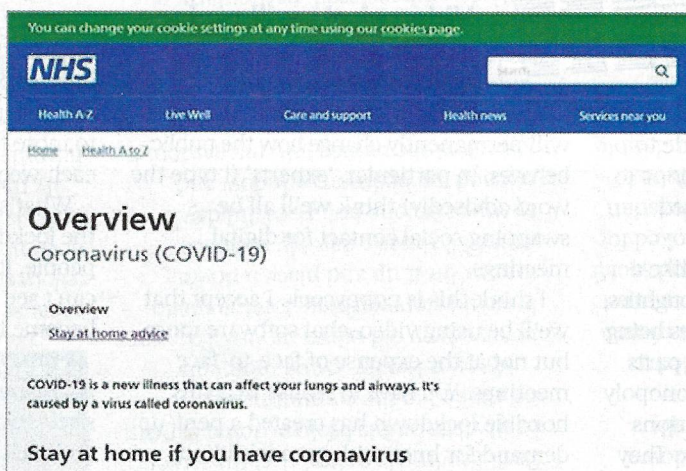
Criminals have hidden malware in a fake version of the NHS website (see screenshot) to exploit public interest in the Coronavirus pandemic.

The malware, which is a **Trojan**, is installed on your computer if you click one of three links on the site: 'Advice about staying at home', 'Use the 111 Coronavirus service' and 'How to avoid infection'.

If you click any of these you'll see a message asking whether you want to save a file called 'COVID19'. By installing this file you're giving the scammers access to your passwords and payment-card details from browsers, files and other data stored on your computer.

Kaspersky, which discovered the fake website, said the global lockdown

hasn't affected criminals' ability to target people. Scammers are used to working from home, it said, adding that their circumstances haven't changed drastically. This has been demonstrated by the bewildering range of Coronavirus-related scams targeting the public since the outbreak began.



How can you stay safe?

As our screenshot shows, the fake site looks convincing, with the correct NHS logo and sections along the top, from left to right: Health A-Z, Live Well, 'Care and support', 'Health news', 'Services near you'. It even has a link at the top to change the site's **cookie** settings.

However, it's unlikely you'll stumble upon the fake site by searching for the NHS online.

Type **NHS Coronavirus** on Google, for example, and the official site (www.nhs.uk/conditions/coronavirus-covid-19) should always be the top result. Bookmark this to make sure you always go to it. It's much more likely you'll end up on the bogus site by clicking a link on a blog or on a social-media site, so be especially cautious when browsing these.