Coronavirus scams

Be wary of coronavirus scams.

Unfortunately, fraudsters commonly try to take advantage of situations and news which attract much public attention. Since these are front of mind, it's easy to fall for them. These scams work by exploiting existing fear and uncertainty.

Here are four ways scams like this might affect you and how you can protect yourself.

1. Phishing/email scams
Fraudsters may impersonate health organisations such as the WHO, NHS and US CDC due to their authority. Emails may ask victims to open dangerous links, download files promising important safety information or infection maps.

Promises of access to equipment such as medical masks or even COVID-19 cures have also been used. Criminals could also send emails soliciting charitable donations for COVID-19-related causes.

Other phishing attacks have involved investment scams claiming that coronavirus has created unique financial opportunities and inviting you to get involved.

2. Phone scams
The UK Government has introduced several economic measures to help the public and businesses get through this challenging situation likely to arise due to COVID-19. The measures can be complicated, and fraudsters are likely to use the potential confusion.

Fraudsters could phone in pretending to be HMRC or a bank offering tax refunds, interest-free loans or other benefits (likely asking for some payment to be made first). It's especially likely that these calls would come to landline numbers, but could also be on mobile.

3. Misinformation
False COVID-19-related information is currently being spread on social media and in messages. The WHO has referred to this as an "infodemic". Some of this information may simply be wrong, but it could also be used to cause panic or give harmful advice.

4. Sale of fraudulent goods
Many fraudulent sites have popped up claiming to offer discounted face masks, vaccines and other equipment. Even if the products are legitimate, there is no guarantee that they exist or will be sent if you pay for them.