COVID-19 scams identified include:

Doorstep crime

- Criminals targeting older people on their doorstep and offering to do their shopping. Thieves take the money and do not return.

- Doorstep cleansing services that offer to clean drives and doorways to kill bacteria and help prevent the spread of the virus.

Online scams

- Email scams that trick people into opening malicious attachments, which put people at risk of identity theft with personal information, passwords, contacts and bank details at risk. Some of these emails have lured people to click on attachments by offering information about people in the local area who are affected by coronavirus.
- Fake online resources – such as false Coronavirus Maps – that deliver malware such as AZORult Trojan, an information stealing program which can infiltrate a variety of sensitive data. A prominent example that has deployed malware is '*corona-virus-map[dot]com'*.

Refund scams

- Companies offering fake holiday refunds for individuals who have been forced to cancel their trips. People seeking refunds should also be wary of fake websites set up to claim holiday refunds.

Counterfeit goods

- Fake sanitisers, face masks and Covid19 swabbing kits sold online and door-to-door. These products can often be dangerous and unsafe. There are reports of some potentially harmful hand sanitiser containing glutaral (or glutaraldehyde), which was banned for human use in 2014.

Telephone scams

- As more people self-isolate at home there is an increasing risk that telephone scams will also rise, including criminals claiming to be your bank, mortgage lender or utility company.

Donation scams

- There have been reports of thieves extorting money from consumers by claiming they are collecting donations for a COVID-19 ‘vaccine’.

Loan sharks

Illegal money lenders are expected to prey on people’s financial hardship, lending money before charging extortionate interest rates and fees through threats and violence