Warning – watch out for coronavirus scams

Lowlife scammers are taking advantage of coronavirus to try to defraud people, especially the elderly and vulnerable.

Action Fraud has already identified over 1,200 reports of fraud relating to coronavirus since February, with victims' losses totalling more than £2.7 million. Many of these are online shopping scams where victims have tried to buy products such as protective face masks and hand sanitiser from fraudsters. There have also been over 4,400 reports of coronavirus-themed phishing emails designed to trick people into opening malicious attachments or revealing sensitive information.

A common tactic used by scammers is to send messages purporting to be from research groups linked with the Centres for Disease Control and Prevention in the US, or the World Health Organisation. Some claim to be able to provide a list of people infected with Covid-19, which links to a malicious website or asks the victim to make a payment in Bitcoin.

Other common phishing emails include those pretending to be from the Government, sending articles about the coronavirus outbreak with links to fake company websites, or sending details of investment schemes which encourage people to take advantage of the coronavirus downturn.

Received a suspicious email? The National Cyber Security Centre (part of GCHQ) has launched its new Suspicious Email Reporting Service to take phishing scams down – all you have to do is forward suspect emails to its report@phishing.gov.uk email address.

Tips to protect yourself against scams

Action Fraud says you can do the following to minimise your chances of being tricked:

- **Be vigilant for scam messages.** This includes not clicking on any links or attachments if you receive a suspicious message, and not responding to any unsolicited messages or calls that ask for personal or financial details.
- **Take care when shopping online.** You should always do your research if buying from a company or person you don't know and trust, and possibly ask a friend or family member for advice first. If you do go ahead with an online purchase, you should use a credit card if possible for extra protection (see our Section 75 guide).
- **Protect your devices from threats.** This includes always installing the latest software and app updates to protect your devices from new threats.

Also see MSE Katie's 19+ coronavirus scams to watch out for blog for more of the known coronavirus-related scams out there and tips to protect yourself from fraudsters.

Have you been scammed?

If you've lost money to fraudsters, you should do the following:

1. Immediately end all communication with them.
2. Contact your bank to tell them you've been scammed, and cancel any recurring payments.
3. Report the scam to the police through the Action Fraud website. You can also call it on 0300 123 2040, but be aware it has a reduced phone service at the moment, so waiting times may be longer than usual.
4. If you want one-on-one help, you can contact Citizens Advice Scams Action by phone or online chat.