Coronavirus Related Scams

Please pass this information on to relatives, friends and neighbours. Fraudsters are exploiting the spread of the coronavirus (COVID-19) to facilitate various types of fraud and cyber crime.

Since February 2020 the National Fraud Intelligence Bureau (NFIB) has identified 21 reports of fraud where Coronavirus was mentioned, with victim losses totalling over £800,000. Ten of these reports were made by victims that attempted to purchase protective face masks from fraudulent sellers.

Fraudsters are also sending out coronavirus-themed phishing emails in an attempt to trick people into opening malicious attachments or revealing sensitive personal and financial details.

Some of the other tactics that NFIB has identified from victim reports include:

Fraudsters purporting to be from research organisation's affiliated with the Centers for Disease Control and Prevention (CDC) and the World Health Organisation (WHO) contact potential victims over email. They claim to be able to provide the recipient with a list of coronavirus infected people in their area. In order to access this information, the victim needs to click on a link, which leads to a malicious website, or is asked to make a payment in Bitcoin.

Watch out for scam messages:
Don't click on the links or attachments in suspicious emails, and never respond to unsolicited messages and calls that ask for your personal or financial details.

Shopping online:
If you're making a purchase from a company or person you don't know and trust, carry out some research first, and ask a friend or family member for advice before completing the purchase. If you decide to go ahead with the purchase, use a credit card if you have one, as most major credit card providers insure online purchases.

For more information on how to shop online safely, please visit:
https://www.actionfraud.police.uk/shoponlinesafely

Protect your devices from the latest threats:
Always install the latest software and app updates to protect your devices from the latest threats.
For information on how to update your devices, please visit:
https://www.ncsc.gov.uk/guidance/securing-your-devices