SCAM and FRAUD ALERT

From Hampshire and IOW Neighbourhood Watch

Coronavirus Phishing

The worldwide spread of the Coronavirus is being used by scammers to scare people into clicking on links, open malicious attachments, or give out confidential information.

The World Health Organisation (WHO) has sent out an alert about rising Coronavirus (COVID-19)-themed 'phishing' whereby messages appearing to come from WHO officials ask the recipients to share sensitive info like usernames and passwords, redirect them to a phishing webpage via malicious links embedded in the emails, or ask them to open malicious attachments containing malware payloads.

Be careful with anything related to the Coronavirus: emails, attachments, any social media, texts on your phone, anything.
Look out for topics like:

- 'Check updated Coronavirus map in your city'
- 'Coronavirus Infection warning from local school district'
- 'CDC or World Health Organisation emails or social media Coronavirus messaging'
- 'Keeping your children safe from Coronavirus'
- You might even get a scam phone call to raise funds for "victims".

How to keep safe from this type of fraud

There will likely be a number of scams using COVID-19 as bait, so please be cautious:

1. Do not open or download attachments to unexpected emails eg if you see "*go through the attached document on safety measures regarding the spreading of coronavirus*", ignore it.

2. Do not click on any buttons in unexpected emails eg if invited to click on a "*Safety Measures*" button to see more information, ignore it.

3. Ignore any pop-up that appears on your computer asking you to verify your information eg email username and password.

4. If you are contacted by a person or organisation that appears to be from WHO, verify their authenticity before responding.