





Covid19 Phishing Emails Reported To Action Fraud

A number of #COVID19 related phishing emails have been reported to Action Fraud. These emails attempt to trick you into opening malicious attachments which could lead to fraudsters stealing your personal information, logins, passwords, or banking details.

https://www.actionfraud.police.uk/alert/coronavirus-related-fraud-reports



(Click the image to see a larger version)

Protect yourself

1) 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.

2) 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

3) 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/quidance/securing-your-devices
For the latest health information and advice about COVID-19 please visit the NHS
website.

Message Sent By

Mike Douglas (VISAV, Administrator, National)

To reply or forward this email please use the buttons below or these links: Reply, Rate, Forward / Share.











To login to your account, click here, To report a fault, click here