Making exceptional
service the standard

NHS
Informatics Merseyside

COVID-19 Phishing Email Scams

NHS staff are being targeted with multiple variations of phishing emails which are pretending to deliver important coronavirus (COVID-19) updates and information.

These fake phishing emails contain different types of cyber-attacks, which include:

Links to fake OneDrive or Office365 logins aimed at staff working remotely to capture username and password credentials.

Links to malicious websites showing statistical coronavirus information whilst implanting malicious software on computers.

Malware infected attachments which appear to be information and guidance documentation to be opened and circulated.

NHS Informatics Merseyside has detected and blocked more than 45 different fake websites, emails and sender addresses, but it is known there are many more of these fake coronavirus phishing emails still in circulation. If you receive a suspicious looking email:

- Double-check the sender address – is it a known address? Does the address even look genuine/official?
- Does the information within the body of the email look authentic?
- If the email contains a link, hover the mouse cursor over the link and check the address, does the link look suspicious?

www.corvid-19.com.uk

If you are unsure or have any queries, please contact your IT Service Desk. Alternatively, you can also forward the details of any suspicious emails to: spam@imerseyside.nhs.uk