Making exceptional service the standard

NHS
Informatics Merseyside

Beware of COVID-19 cyber crime

IT Security Update
Issue 1 | April 2020

NHS Informatics Merseyside is urging all healthcare professionals to be cyber savvy following a rise in coronavirus-related cyber scams. Here are just some of the scams you should watch out for.

COVID-19 phishing e-mail scams

NHS staff are being targeted with multiple variations of phishing e-mails 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** 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.

If you receive a suspicious looking e-mail:

- 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 e-mail 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

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

Fake delivery e-mails

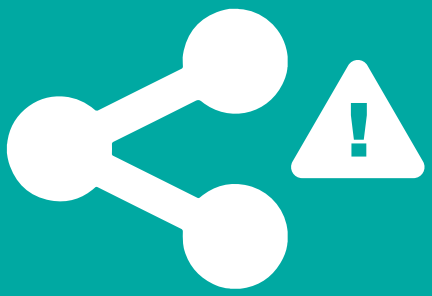
With most shops closed and online ordering at an all-time high, it can be easy to lose track of what you have ordered online. Cybercriminals know this, and send out e-mails that purport to come from legitimate courier companies. These e-mails ask recipients to click on a link, which might take you to a scam website or download malicious code onto your device.

Tip: Check the sender's address to ensure it is a legitimate company and go to the company's own website to track your order rather than through the e-mail you have received.

Social media scams

Cybercriminals use social media to tempt people to open and share content relating to coronavirus (COVID-19). Cybercriminals may even assume the identity of a 'friend' to help share content more successfully, without your real friend even knowing.

Tip: Please remain vigilant at all times and do not open any suspicious links or attachments.



Charity phishing

Cybercriminals know that many people feel charitable at this time and may look to exploit your good will. They may send e-mails from a bogus charity or ones that purport to come from a legitimate charity. Beware - they may contain a link to a scam site.

Tip: Should you choose to donate money to charity, please ensure that any donations are sent directly through the legitimate website for the charity of your choice.

CYBER SAVVY

Further information

For further information and guidance, please **watch our video** on the different cyber security scams taking place and what you should look out for.

Remain vigilant at all times, do not open any suspicious links or attachments and report anything unusual to **spam@imerseyside.nhs.uk** or contact **your IT Service Desk**.