Phishing Scams
COVID-19

PHISHING ATTACKS
Cybercriminals are exploiting the public anxiety and interest in the pandemic in order to conduct phishing attacks. Generally these are emails containing links to malicious sites, malicious files and malicious attachments.

DESIGNED TO CONVINCE
These emails attempt to trick users into doing the wrong thing such as:
- clicking a link to a malicious website
- opening a malware infected attachment
- disclosing user IDs and passwords
- making financial transactions

BE VIGILANT
Be suspicious of:
- any unusual request from a known contact
- a request that is different from normal practice
- being pressured to take action quickly
- badly worded and poorly constructed emails
- hyperlinks that do not match the context of the email
- requests to provide, input or verify login details

NHS HIGHLAND

PASSWORDS
Never disclose personal or work related passwords to anyone including NHS Highland colleagues and IT support staff.

REPORT IT
Phishing emails can be very convincing and it is easy to be fooled. If this happens do not be worried about reporting it. The sooner we know, the sooner we can take action.

eHealth Service Desk 01463 704999

FURTHER INFORMATION
For further support contact the Information Assurance & IT Security team by emailing high-uhb.informationsecurity@nhs.net

Advice and guidance is also published on the NHS Highland Intranet **Cyber Security Page**