Nottinghamshire Health Informatics Service
Transforming care through technology

CYBER SECURITY – WHAT YOU NEED TO KNOW…..

It is vitally important that you are aware that external organisations will use many methods to try and access some of your personal data to use for many reasons; this includes attempting to access NHS data through targeted and non-targeted attacks.

What is it?

Cyber security threats can take a number of forms, but essentially they are a way to introduce malicious software into a computer system or network by the use of attachments in emails or by concerted efforts to attempt to infiltrate the network.

- Phishing is a term used to describe a fraudulent attempt to acquire information such as usernames, passwords and credit card details by pretending to be a trustworthy source in an electronic communication.
- Phishing emails are designed to deceive the recipient. They may look as if they come from a trusted source such as a social network, auction, online payment or IT administrators.
- Phishing emails often contain links to websites that are infected with “malware” malicious software used to gather sensitive information such as passwords. Malware such as computer viruses can also be used by attackers to disrupt computer operation or gain access to private computer systems.
- If a user opens an attached document, a macro embedded in the document surreptitiously triggers a download of the malware.
- ‘Hacking’ is a more targeted way of attacking computer systems, either in order to exploit vulnerability, or gain information that can then be sold on, such as identity theft.
- Hackers can also exploit software bugs and find ways to infiltrate complex system utilities.
- Antivirus software can continuously scan the network for any cyber threats, but cannot prevent all attacks by malware as the threat is initiated by the user opening unsolicited emails.

- If you give away your password, you may give inadvertently give access to email and other services. Information such as personal data could then be used to commit theft and fraud using your identity.

However, if you stop to think, look carefully at the email text and images and check any links before clicking, you should be able to identify the spurious communications.

STOP!

- Don't react straight away!
- Take time to read the email
- Don't automatically click on links (URLs)
- Don’t automatically open attachments
- Don't automatically reply

THINK!

- Does the email look right? Are the logos or signatures correct
- Does the text make sense? Are there spelling mistakes or other obvious signs that it might not be genuine
- Are you being asked to click on a link and enter personal information
- Are you being asked to verify your details
- Are you being asked for your password or other data such as your date of birth

CHECK!

- Were you expecting this email?
- Use your mouse to hover over any links to check that it matches the URL (web address) that you were expecting
- Check the reply to email and address, does it match the from address

- If you suspect you have a computer virus or are unsure about any of the above, contact corporate governance or the IT Service Desk on extension 01623 410310 or ext. 4040 nhis.servicedesk@notts-his.nhs.uk