NHS Greater Glasgow and Clyde Core brief

Thursday 9 August 2018

Introduction

This issue of Core Brief brings you news of the biggest cyber threat – Phishing!

Message from eHealth

The email threat today – Phishing!

The biggest cyber threat to you today is from emails. NHSGGC mail has sophisticated mail filters in place which are updated as new threats are identified but there is a risk that malicious mail will arrive in your mail box. Motivations change but cybercriminals are always hunting for personal information, your name, address, date of birth, financial details, medical records etc.

One of the most common attack methods is Phishing which is a way of tricking you, often referred to as social engineering, to do 'the wrong thing', such as disclosing information or clicking a bad link or attachment.

What to look out for

- Check the actual email address of the sender. The name can be easily forged (spoofed) to say anything.
- Has the email originated internally or externally? Emails from outside NHSGGC will have the [ExternaltoGGC] tag on the subject line. Be more cautious about external emails.
- Am I being asked to click? Everything can change with one click. So check, think and recheck before you click, especially if it is an email from outside your organisation or someone you don't know or not expecting. Never click on links or attachments in an email, if you don't know/trust the sender.
- Common indicators of phishing are emails offering something too good to be true, email from HMRC advising about a refund, email from someone asking for personal details, email from the bank asking to transfer money to a different account urgently (Sense of Urgency) or a sudden email from senior manager or HR asking for some information (Sense of Authority).
- **VERIFY** the legitimacy of any requests via email by contacting the sender through official channels

eHealth is continually implementing technology and plans to remove/block these emails and want to make you more aware of Phishing. An NHSGGC phishing campaign is now underway and will run through 2019/20. If you are vulnerable to phishing and click within the simulated phish this will generate a learning experience designed to improve your awareness. Organisational percentage response will inform future awareness campaigns.

On 9 April 2019, an email came from sender name "HR Department" and with subject line "Next to Kin". The email has not been send by the NHSGGC HR Department but it is actually a Phishing exercise carried out by the eHealth Compliance Team to understand the user awareness when it comes to email phishing.

As we become aware of Phishing we are publishing the details on the Be Cyber Safe page on StaffNet. Please check the site if you are unsure of a mail's status. Please visit for more details about this phishing exercise and other information about how to stay cyber safe.

REPORT any suspected spam by forwarding the email to eHealth at spam@ggc.scot.nhs.uk

Are your contact details up-to-date? Click here to check