NHS Greater Glasgow and Clyde

Core brief

Daily update
(9 May 2024, 10.55am)

Topics in this Core Brief:

- Cyber Crime: Recognising the signs
- GGC Medicines Update
- Hospital Broadcasting Service
- Roadworks and transport news

Remember, for all your latest news stories, visit our new Staffnet Hub:
GGC-Staffnet Hub - Home (sharepoint.com)

Cyber Crime: Recognising the signs

Cyber-crime and the Threat Actors who deploy it, continue to use ever more elaborate ways of stealing both your personal and your organisation's information. Here we look at two of the most widely used means used by scammers – Phishing and Vishing.

What is Phishing?

Phishing is a form of social engineering where a scammer impersonates a well-known figure or organisation, most commonly via email, to defraud the target into forwarding sensitive information. Some common goals of a phishing attack are:

- get access into your network
- inject malware
- gain access to confidential information
- transfer money or anything of value.

What is Vishing?

This is a phone-based cyberattack where Threat Actors exploit the phone as a tool for their attacks. During a vishing phone call, a Threat Actor may try to get you to share personal information and financial details, such as bank account numbers and passwords. Typical examples of Vishing would be **Bank scams, Internet Provider scams, Solar and Green Energy scams,** and others.

What can I do?
It's easy to assume the messages arriving in your inbox or calls you receive are legitimate, but be wary - phishing emails often look safe and genuine. To avoid being fooled, slow down and examine hyperlinks and senders' email addresses for clues such as spelling mistakes, especially before clicking on any reply in the body of the message.

Take your Time - Successful Social Engineering attacks generally require a sense of urgency, take your time, Threat Actors hope you will not think too hard about what is going on. Take a moment to reflect and investigate: this can show these attacks for what they are.

Educate yourself - This can be the best form of defence, check online sources to see if emails, SMS messages or other forms of Social Engineering attacks are known and commonplace.

No Trust - Verify - Adopt a position of verifying - via alternative means - the identity of those sending unexpected messages even if the contacts are known to you.

Top Things to look out for;

- Emails with bad grammar and spelling mistakes
- Emails with an unfamiliar greeting or salutation
- Inconsistencies in email addresses, links and domain names
- Suspicious attachments
- Emails or calls requesting **login credentials**, **payment information, invoices** or **sensitive data**
- Unsolicited phone calls.

Reporting suspicious content
It's important to remember never to click on any links or open any emails which look even remotely suspicious.

If you suspect you have received anything to your work email address containing malicious content you can report it to: **spam@ggc.scot.nhs.uk**

GGC Medicines Update

NHS Greater Glasgow and Clyde

GGC Medicines Update is a series of blogs with important medicines related messages relevant to all healthcare professionals across NHSGGC. Please see below for new blogs and relevant updates.

New blogs

Click on the following links to access the recently published Medicines Update blogs.

- **Adrenal Insufficiency and Provision of Steroid Emergency Cards**
- **Opioid Induced Adrenal Insufficiency (OIAI)**
- **Fluoroquinolone safety – GGC position following updated restrictions**

Updated blog

Click on the following link to access the recently updated Medicines Update blog.

- **Safe disposal of sharps waste in primary care**

Updates

- **Guideline News March 2024**
- **Formulary Update (March 2024)**
- **MHRA Drug Safety Update March 2024**

All our blogs can be found on http://www.ggcmedicines.org.uk and anyone can join our mailing list by contacting us at: Medicines.Update@ggc.scot.nhs.uk

We're also on social media, follow us on: X/Twitter @NHSGGCMeds

Hospital Broadcasting Service

We are thrilled to introduce the Hospital Broadcasting Service (HBS), a vital radio station delivering therapeutic programming to hospital patients across Glasgow and Paisley. As one of the UK's premier radio stations of its kind, HBS offers nightly request shows, specialist music, and informative programs to uplift spirits.

While patients in the QEUH can listen on channel 7 of the bedside entertainment system, everywhere else programmes can be heard on-line via the radio station's website www.hbs.org.uk. There are currently over 32 hours a week of programmes dedicated to playing music requests for patients and staff with the most popular ways of requesting songs being by email to studio@hbs.org.uk or by text to 07756 434 225.

Our dedicated team of over 70 volunteers ensures seamless operations, from collecting requests to curating playlists. With broadcasts available 24/7, patients can access our service not only in local hospitals but worldwide via the internet.

What's more, many of today's beloved broadcasters, like Ken Bruce, George Bowie, and Linda Sinclair, kick started their careers right here at HBS. For them, as

for us, it's more than just a hobby – it's about making a meaningful difference in the lives of others.

Join us in making a difference through the power of music and communication. Tune in, support us, and together, let's brighten the hospital journey for all.

To listen online scan the QR code opposite or visit: www.hbs.org.uk

For a request: Call: 0141 221 4043, text: 07756 434 225 or email: studio@hbs.org.uk.

Roadworks and transport news

Overnight roadworks/road closures continue to take place on the Kingston Bridge and surrounding approach roads of the M8 motorway. Information on the current work, and other planned major roadworks, is available from Roadworks & Transport News pages.

Staff are reminded to make sure their personal contact details are up to date on eESS.

It is important to share Core Brief with colleagues who do not have access to a computer.
A full archive of printable PDFs are available on website