NHS Greater Glasgow and Clyde

Core brief

Daily update
(1 July 2024, 11.30am)

Topics in this Core Brief:

- Data Security Spotlight – Password security
- Cyber Crime: Recognising the signs
- Hospital discharge and telecare
- Insulin Safety Week, 1 – 7 July 2024

Data Security Spotlight – Password security

Strong passwords and password security are essential to protect the integrity of our systems and our data. Always follow our guidance here on creating strong passwords and never share your password with anyone else.

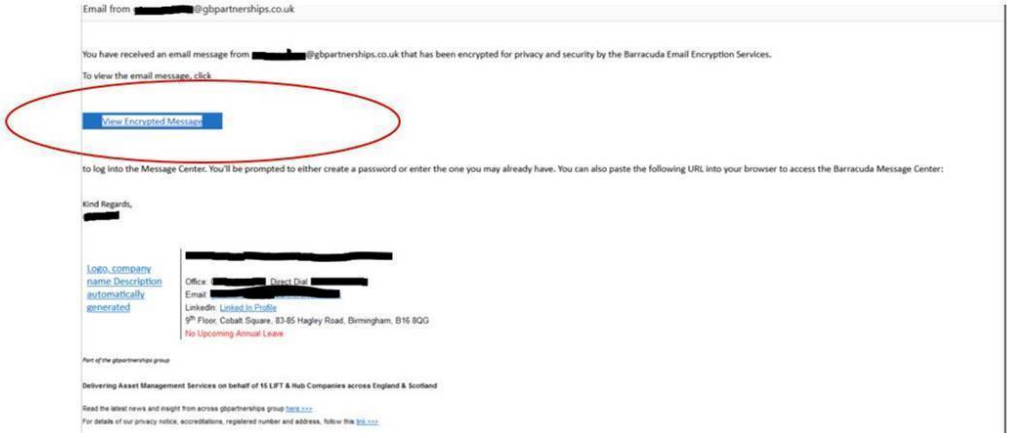
Cyber Crime: Recognising the signs

It's easy to assume the messages arriving via your mailbox are legitimate, however, this is the most frequent way of compromising data.

What is A Microsoft 365 - Adversary in the Middle attack (AiTM)?
This attack is a phishing attack via a malicious link or attachment which directs you to a fake website which requires you to enter your credentials, if you enter your account details your account may be compromised.

What to look out for
Beware of any links or attachments within emails asking you to enter your MS365 username and password or redirecting you to any sites where you have to enter your credentials to access a file.

External organisations can be compromised and in turn lead to phishing emails entering the Board, below is a recent example of a phishing email
entering the board.



Email from [redacted]@gbpartnerships.co.uk

You have received an email message from [redacted]@gbpartnerships.co.uk that has been encrypted for privacy and security by the Barracuda Email Encryption Services.

To view the email message, click

View Encrypted Message

to log into the Message Center. You'll be prompted to either create a password or enter the one you may already have. You can also paste the following URL into your browser to access the Barracuda Message Center:

Kind Regards,
[redacted]

Logo, company name Description automatically generated

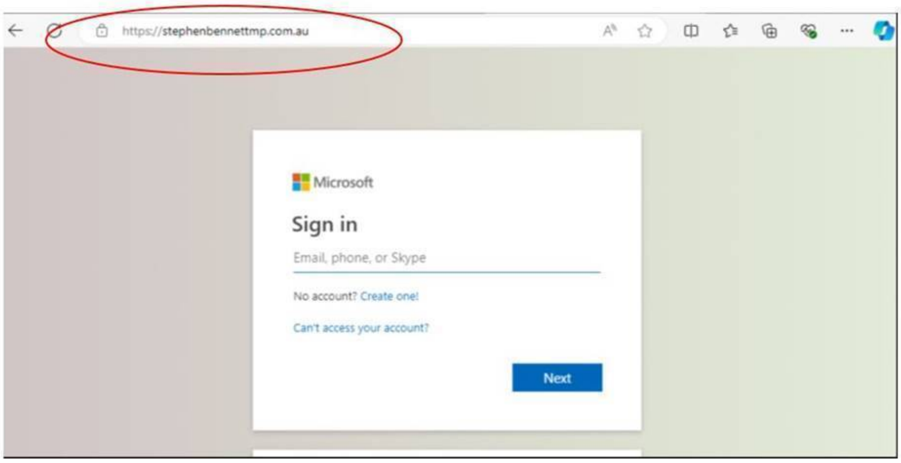
[redacted]
Office: [redacted] Direct Dial [redacted]
Email: [redacted]
LinkedIn: Linked In Profile
9th Floor, Cobalt Square, 83-85 Hagley Road, Birmingham, B16 8QG
No Upcoming Annual Leave

Part of the gbpartnerships group

Delivering Asset Management Services on behalf of 15 LIFT & Hub Companies across England & Scotland

Read the latest news and insight from across gbpartnerships group here >>>
For details of our privacy notice, accreditations, registered number and address, follow this link >>>

Clicking on the link in the email above would have resulted in you being directed to the following site.

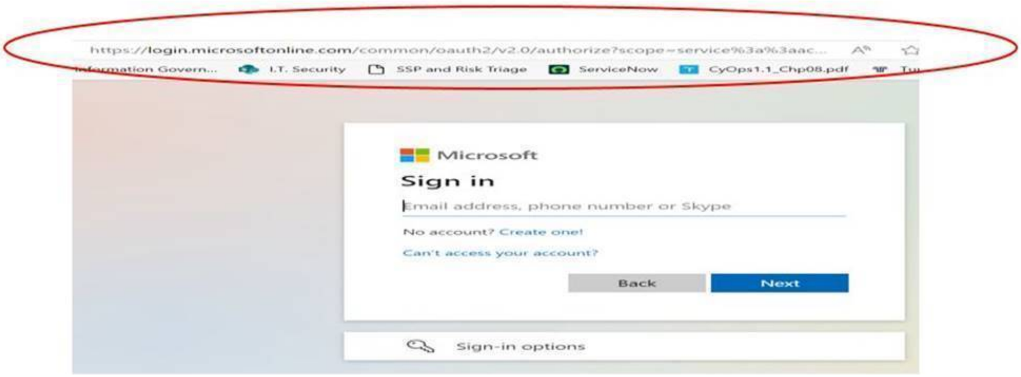


https://stephenbennettmp.com.au

Entering your details in this site would have resulted in your account being compromised by a Threat Actor.

Please pay attention to the https link in the capture above as this is an easy way to tell it is not genuine.

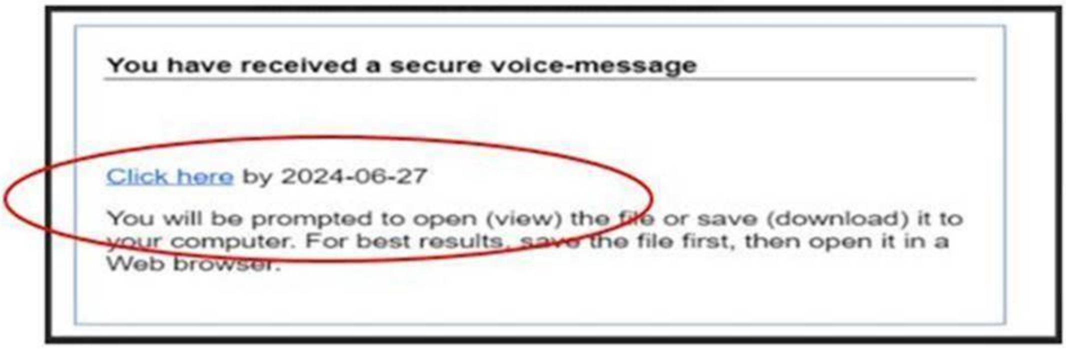
A genuine login for Microsoft 365 is shown below.



https://login.microsoftonline.com/common/oauth2/v2.0/authorize?scope=service%3a%3aac...

Once an account is compromised in the Board it can be used as a mechanism to generate further and different phishing emails, these will then present as being sent from internal colleagues. Below is a recent example of email content generated from a compromised account and sent from a NHSGGC account to other NHSGGC users.

It is also possible that once a mailbox is compromised you may receive a phone call from the Threat Actor pretending to be Microsoft, you will **never** receive a call from Microsoft asking you to undertake actions, should you receive a call like this, please terminate it immediately and inform IT Security.

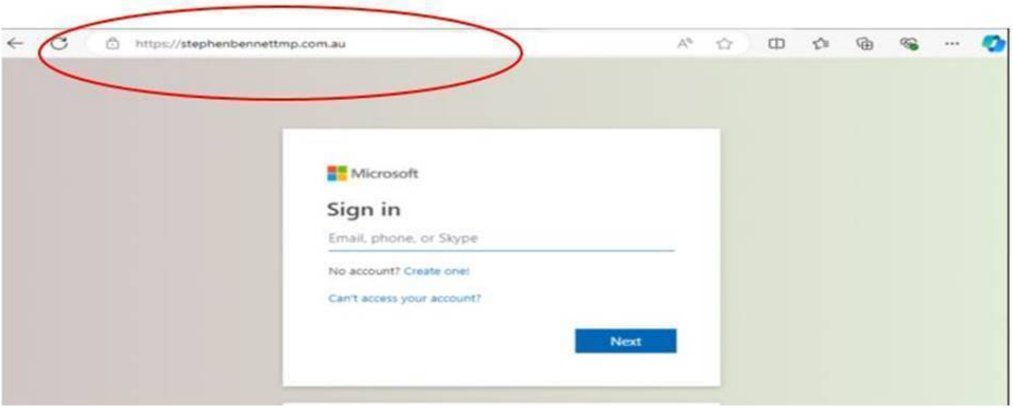


You have received a secure voice-message

Click here by 2024-06-27

You will be prompted to open (view) the file or save (download) it to your computer. For best results, save the file first, then open it in a Web browser.

Clicking on the link in the example above would have taken you to the same credential harvesting site.

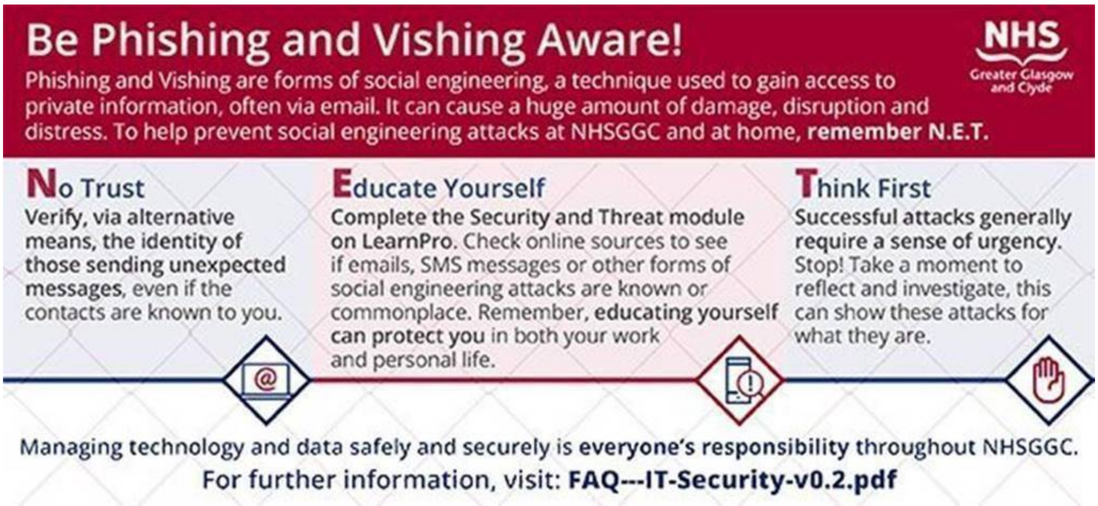


https://stephenbennettmp.com.au

What can I do to minimise the risk?

1. Look for the **External** sender Markers, if the email advises that you do not often receive emails from the person then treat with **caution**
2. Never click on links which are advising you to change password or ask for username and password unless you are sure they are genuine and come from eHealth
3. Look at the **https domain** if redirected to any site asking you to enter username and password details
4. Avoid downloading or accessing attachments, particularly if you do not recognise the source or asked for the information

5. If you suspect you have received suspicious emails you can report it to: itsecurity@ggc.scot.nhs.uk
6. Follow the guidance in the graphic below – remember N.E.T



Be Phishing and Vishing Aware!

NHS Greater Glasgow and Clyde

Phishing and Vishing are forms of social engineering, a technique used to gain access to private information, often via email. It can cause a huge amount of damage, disruption and distress. To help prevent social engineering attacks at NHSGGC and at home, **remember N.E.T.**

No Trust
Verify, via alternative means, the identity of those sending unexpected messages, even if the contacts are known to you.

Educate Yourself
Complete the Security and Threat module on LearnPro. Check online sources to see if emails, SMS messages or other forms of social engineering attacks are known or commonplace. Remember, **educating yourself can protect you** in both your work and personal life.

Think First
Successful attacks generally require a sense of urgency. Stop! Take a moment to reflect and investigate, this can show these attacks for what they are.

Managing technology and data safely and securely is **everyone's responsibility** throughout NHSGGC.
For further information, visit: **FAQ---IT-Security-v0.2.pdf**

Hospital discharge and telecare

Telecare can play a contributory role in supporting a safe discharge from hospital. Glasgow's HSCP continues to prioritise referrals in these circumstances. The provision of telecare is going through a significant transition as its analogue telephone form of connection is being phased out and replaced by a digital one.

In this transitional phase telecare suppliers have had difficulties supplying enhanced peripheral devices such as property exit, bed and epilepsy sensors that are compatible with digital telecare base units. Requests for these devices can potentially delay discharges due to the lack of availability of this equipment. To improve the effectiveness and speed of telecare provision for patients coming home from hospital, the standard alarm unit and pendant only will be provided to support safe hospital discharge from today - **Monday 1 July**. This will provide guarantees of fast and efficient installation within prescribed discharge timescales.

The alarm call element that this provides is the core function of the telecare service in keeping people safe. If the patient has specific high risks, a follow up assessment in the community through Care Services' Reablement Team will be arranged to identify if further telecare equipment is required. If hospital staff feel this follow up home assessment would be beneficial, they can highlight this when they are submitting a referral for standard telecare.

Telecare Fall Detectors
Glasgow's Telecare Service is set to undergo a significant change as a result of the requirement to move from analogue to digital connectivity. The HSCP is required to replace current service users' telecare equipment over the next 18 months to

ensure that users can connect digitally when the analogue network is shut down at the end of January 2027.

In preparation for this we have been reviewing the performance of the existing equipment used which requires to be replaced as part of this project. The HSCP has carried out extensive analysis on the outcomes of fall detectors and have consistently found them to be inadequate in identifying genuine falls. The most recent analysis found under 2% of calls generated were sent as a result where the service user had fallen. This inefficiency of generating multiple false calls has had a negative impact on service users, their families and the service operators when responding to accidental activations.

In terms of usage, the alarm pendant remains the primary and most reliable means of contacting the service in the event of a fall. As the fall detector is an ineffective means of summoning assistance in these circumstances, service users' detectors will be replaced by pendants when digital equipment is installed and in general fall detectors will be no longer be available for new telecare referrals from **Monday 1 July**.

Insulin Safety Week, 1 – 7 July 2024

Are you aware that NHSGGC has an Instagram account that is packed with hints and tips relating to the management of people with diabetes in all inpatient areas of the hospital?

Created for NHSGGC staff and managed by the Diabetes Team at Glasgow Royal Infirmary, the @diabetes_education_gri Instagram account provides digestible information and is designed to increase knowledge and confidence amongst medical, nursing and pharmacy staff in managing diabetes patients in common scenarios.

The Instagram account also signposts followers to NHSGGC clinical guidelines and other verified resources. This will help staff to learn small knowledge points week to week and will also be a tool for them to refer back to.

This week, as part of Insulin Safety Week, we're asking staff to tell others in their team about the account so that they can follow. Scan the QR code, right, to follow.

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

Sexual Harassment -
Cut It Out
If you need help or support, visit: www.nhsggc.scot/sexualharassment

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