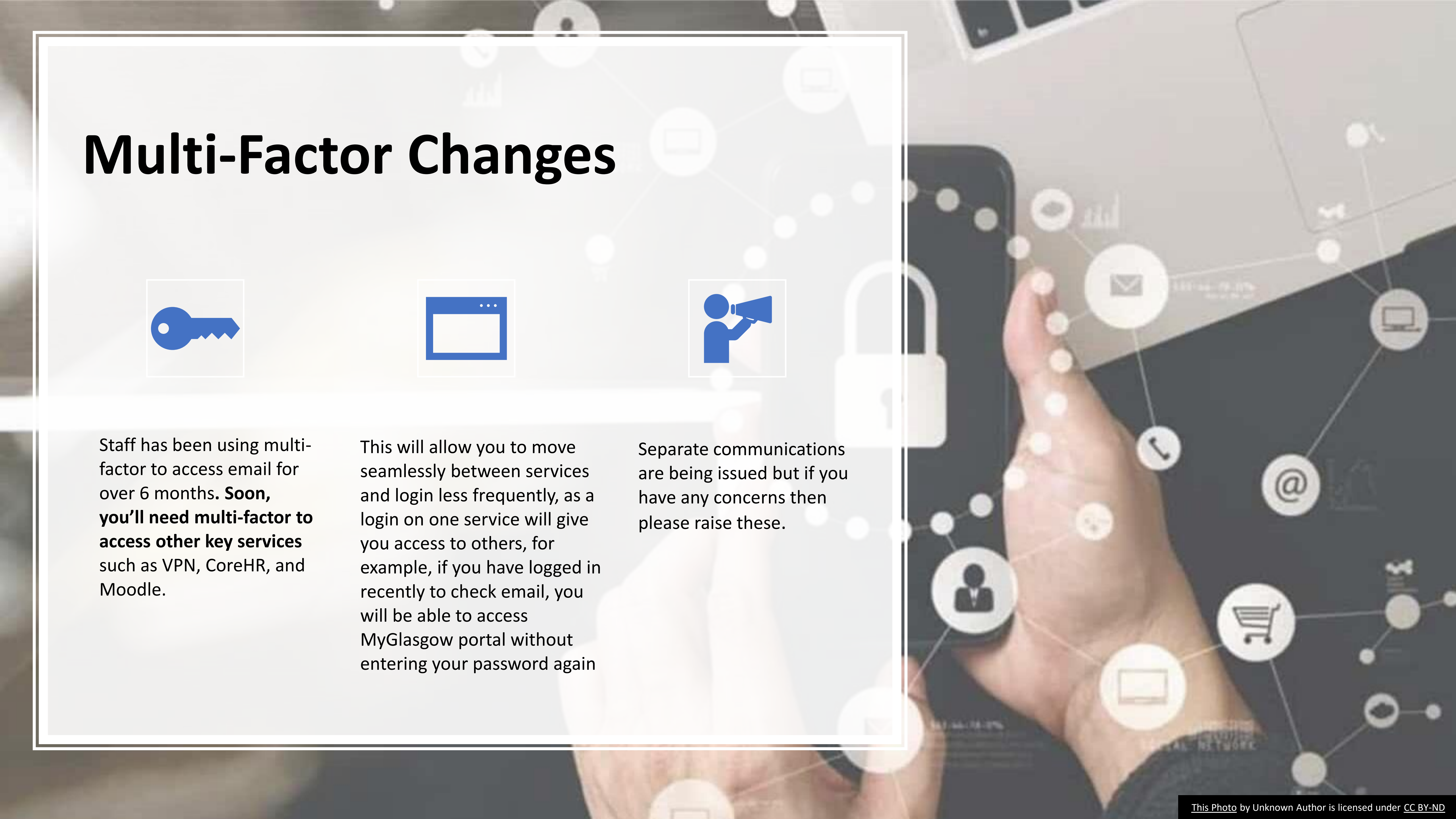
Cyber talk

Welcome to the first of our quarterly security talking points. We want to make our security at UofG as open and transparent as possible. To help you with discussions you may have with your team, individuals, or committees we’ve created these talking points to help ensure our awareness of security issues remain high.



Multi-Factor Changes

Staff has been using multi-factor to access email for over 6 months**. Soon, you'll need multi-factor to access other key services** such as VPN, CoreHR, and Moodle.

This will allow you to move seamlessly between services and login less frequently, as a login on one service will give you access to others, for example, if you have logged in recently to check email, you will be able to access MyGlasgow portal without entering your password again

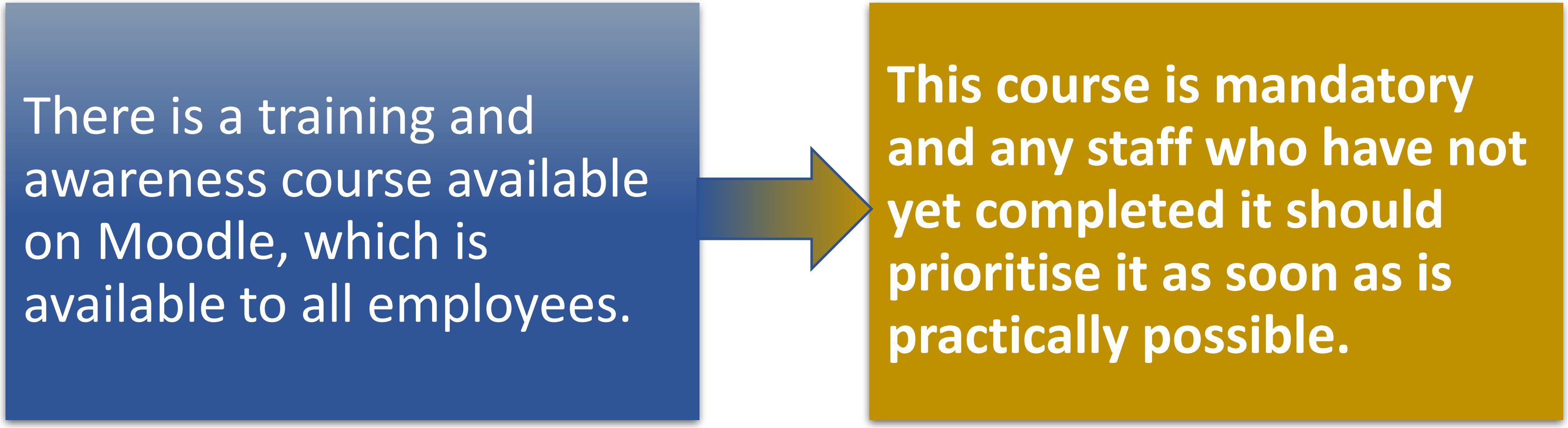
Separate communications are being issued but if you have any concerns then please raise these.

Annual password changes

Our passwords form part of our security controls and since the COVID lockdown restrictions forced us to think differently and the annual change was temporarily suspended. However, in 2023 the requirement for password change will return and all staff will need to do this at least **annually.**

Completion of mandatory training

It is important that we understand how security relates to our day to day working life and is important for us to be able to identify suspicious situations which should be reported.



There is a training and awareness course available on Moodle, which is available to all employees.

This course is mandatory and any staff who have not yet completed it should prioritise it as soon as is practically possible.

Deletion of old documents & data

It is easy for us to generate, share and retain documents – we do it every day. However, over time we can build-up old files and emails which we no longer need. These makes finding our important data more difficult and indirectly cause increased costs to the University to store files and could also mean we're storing data we're no longer supposed to be.
We would like all staff members to:

- Review their old files in OneDrive or elsewhere and delete ones they no longer need
- Consider whether old emails are still required or may be required in future
- Check if you have old Microsoft Teams / Sharepoint sites which are no longer required and can be deleted

It is important to remember that we should only keep information we need or may be legally required to retain.

We urge people to delete with caution, if you delete files accidentally then we may not be able to recover them

Contact us!

- As always, the Information Security team is available to provide advice and guidance on these and any other matters which you may need assistance with
- Details