Setting up multi-factor authentication (MFA)

You'll be prompted to use multi-factor authentication (MFA) the first time you log in with your University credentials, when logging into University systems from each new device, and periodically from the same device.

This document outlines what it is, why we need it and how you can set it up.

What is MFA?

Muti-Factor Authentication (MFA) is a method of logging in that uses, on top of your password, a secondary authentication method, i.e. a code that's sent via text message or an app. The University have introduced it as a form of securing our environment, including Office365, to protect the content of the University and our students.

Why do we need MFA?

MFA is one of the most powerful tools we have to mitigate the threat presented by phishing and similar types of cyber-attack. Using MFA makes it extremely difficult for anyone who has stolen or guessed your password to use that password to log in to your account. If you want to learn more about why MFA is crucial for our security, you can watch this.

How do I set it up?

To set it up in five easy steps, you can read the instructions below or watch this video.

Depending on whether you have an Android (Google Play) or Apple device (App Store), please head to the appropriate store for your device and download the **Microsoft Authenticator App**:

1) Login to your Microsoft account using the link below:
https://login.microsoftonline.com
Enter your credentials – email address and password. Once you
have entered these, you will be presented with the following
screen. Click on Next.

UNIVERSITY
OF LONDON

More information required

Your organization needs more information to keep
your account secure

Use a different account

Learn more

Next

You will then be presented with this screen:

UNIVERSITY
OF LONDON

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 1: How should we contact you?

Authentication phone

Select your country or region

Method
● Send me a code by text message

Next

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

2) Click on the first drop-down box, under Step 1: How should we contact you? And choose 'Mobile app'.

At this point you can choose to:
- Receive notifications for verification; this will display a notification on your mobile device, and you will have to open this notification and approve it
  OR
- Use verification code; this means each time you are prompted for additional verification to access your account, you will need to open the Microsoft Authenticator app and type in the code displayed under your account.

After choosing the type of way in which you want to use the app, you can then click on the blue Set Up button.

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 1: How should we contact you?

Mobile app

How do you want to use the mobile app?

○ Receive notifications for verification

○ Use verification code

To use these verification methods, you must set up the Microsoft Authenticator app.

Set up   Please configure the mobile app.

Next

You will then see the following screen:

3) Please follow the instructions around configuring the mobile app contained within the box.

Configure mobile app

Complete the following steps to configure your mobile app.

1. Install the Microsoft authenticator app for Windows Phone, Android or iOS.

2. In the app, add an account and choose "Work or school account".

3. Scan the image below.

If you are unable to scan the image, enter the following information in your app.
Code: 222 668 081
Url: https://mobileappcommunicator.auth.microsoft.com/mac/MobileAppCommunicator.svc/201192467

If the app displays a six-digit code, choose "Next".

Next   cancel

4) Once you have scanned the QR code it should automatically continue and display the following screen:

Simply click on the blue Next button in the bottom right-hand corner.

UNIVERSITY OF LONDON

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 1: How should we contact you?

Mobile app

─How do you want to use the mobile app?─
◉ Receive notifications for verification
○ Use verification code

To use these verification methods, you must set up the Microsoft Authenticator app.

Set up   Mobile app has been configured for notifications and verification codes.

Next

UNIVERSITY OF LONDON

5) The app will then send a test to your mobile device which you can respond to accordingly:

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 2: Let's make sure that we can reach you on your Mobile App device

Please respond to the notification on your device.

Next

As a fail-safe to ensure you do not lose access to your account, then please choose your country or region from the first drop-down box, then enter your mobile phone number. In the event of losing access to the app, you can choose to be sent a text message as an option when accessing your account. Once you have completed both fields, please click on the blue Done button.

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 3: In case you lose access to the mobile app

Select your country or region ▼

Done

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

Your account is now configured to use the Microsoft Authenticator app, and this will be required to access your account moving forward.