

Introducing MFA (Multi-factor authentication) and password reset for Post-Graduate SAS students

The first time you log in with your university credentials, you'll be prompted to use multi-factor authentication (MFA). This will happen 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, in addition to your password, a secondary authentication method, i.e. a code that's sent via text message or via an app. The University have introduced it as a form of securing our environment, including Microsoft 365 (Outlook, Word, Excel, PowerPoint etc.), 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. To learn more about why MFA is crucial for our security and how to setup MFA, [watch these videos](#).



Register MFA via Microsoft Authenticator

Step 1:

Before you start, make sure you have **Microsoft Authenticator** installed on your mobile phone.

You can search for **Microsoft Authenticator** on the App Store or Play Store, or scan the QR code on the right to download the app.

Android



iOS



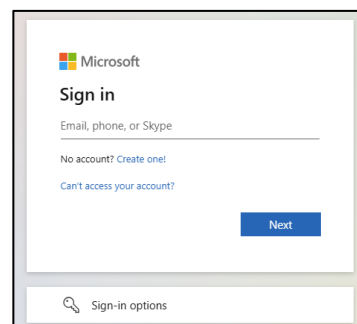
Step 2:

Log in to your account via
<https://login.microsoftonline.com>

Input your account name, e.g. `firstname.lastname@london.ac.uk`

*From **12 December 2024**, SAS student accounts and email addresses will be changing from **firstname.lastname@postgrad.sas.ac.uk** to **firstname.lastname@london.ac.uk**.*

From that date, you will need to use your new account to access many University of London services.





Step 3:

You will be redirected to the University of London login page and asked to enter your password.

Once you have entered your password, click on the blue Sign In button.

Step 4:

If you haven't set up MFA yet, you will see the setup screen. Follow the on-screen instructions to secure your account.

Click **Next** to Start

Step 5:

Click **Next** to confirm that you have installed the Microsoft Authenticator app on your smartphone and are enrolling in MFA with Microsoft Authenticator.

Step 6:

On your mobile phone:

Launch **Microsoft Authenticator**. Make sure you choose to allow to receive notifications when prompted to do so.

On your computer:

Click **Next**

UNIVERSITY OF LONDON

← test.sas4@london.ac.uk

Enter password

Password

[Forgotten my password](#)

Sign in

If you are a UoL Enquiry Hub visitor, in need of assistance, please tell the Virtual Agent "I can't log in" and you will be given further instructions.

If you are UoL staff, and need help with re-setting your password, please contact the IT Service Desk.

Microsoft

More information required

Your organisation needs more information to keep your account secure

[Use a different account](#)

[Learn more](#)

Next

If you are a UoL Student and want to reset the password, please visit [Student Portal](#)

Keep your account secure

Microsoft Authenticator

Start by getting the app

On your phone, install the Microsoft Authenticator app. [Download now](#)

After you install the Microsoft Authenticator app on your device, choose "Next".

Next

[Learn to set up a different method](#)

Keep your account secure

Microsoft Authenticator

Set up your account

If prompted, allow notifications. Then add an account, and select "Work or school".

Back **Next**

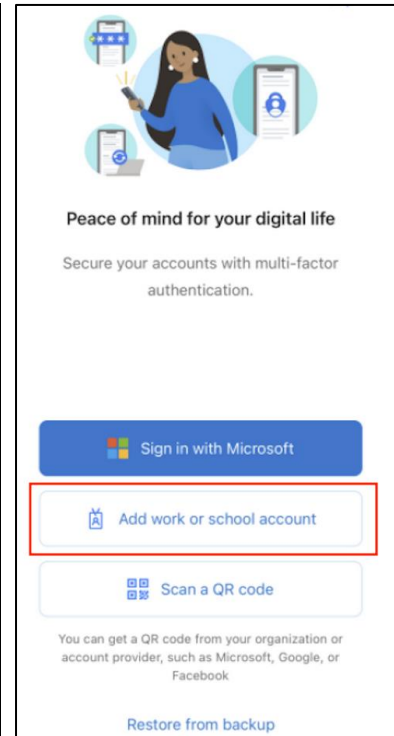
[Learn to set up a different method](#)



Step 7:

On your mobile phone:

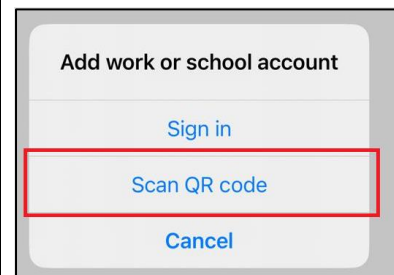
Select **Work or school account**



Step 8:

On your mobile phone:

Click **Scan QR code** on the pop-up

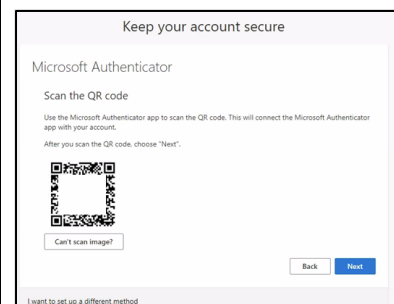


Step 9:

On your mobile phone:

Scan the QR Code presented on your computer screen.

Once completed, click **Next**





Step 10:

Your setup should be complete at this point. To ensure MFA is working, follow the screen instructions to complete the test.

On your desktop:

You will see a number on the screen (e.g., 21).

On your mobile phone:

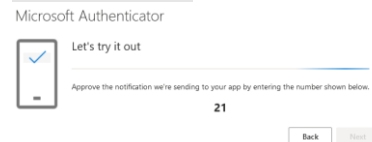
Your Microsoft Authenticator app will show a dialog asking you to sign in.

Enter the same number displayed on your desktop (e.g. **21**) to sign in.

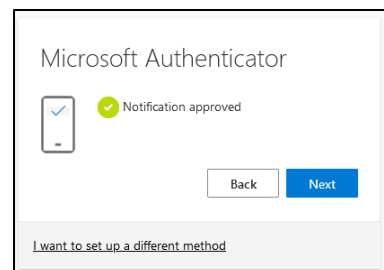
Step 11:

If the code matches, your MFA setup is now complete and ready to use.

On computer:



On phone:

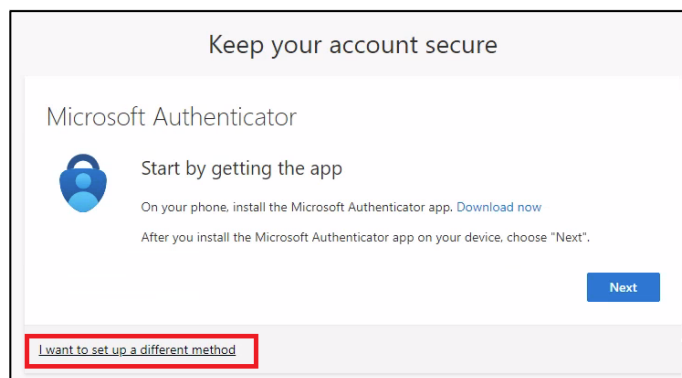


Register MFA via SMS / Phone Call

If you can't download or use Microsoft Authenticator, you can set up MFA using SMS or Phone Call. Follow these steps to set it up:

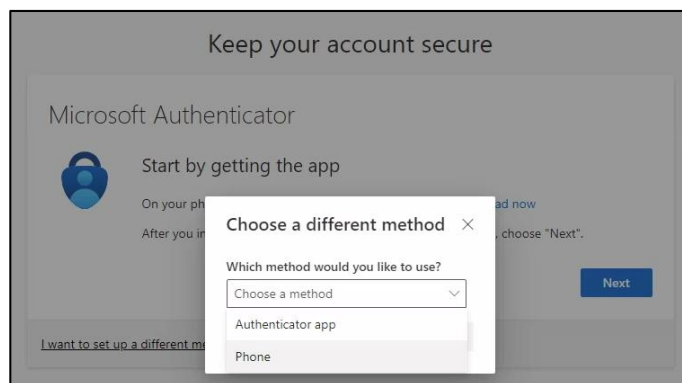
Step 5a:

Follow steps 1-4 as above, and then click **I want to set up a different method**



Step 6a:

On the next pop-up, choose **Phone** as your verification method, then click **Confirm**





Step 7a:

Select your phone number's **country code**, then enter your **Phone Number**.

There are 2 ways to receive your sign-in code:

Choose **Receive a code** if you want to receive a code via text message

or

Choose **Call me** if you want to receive a code via a phone call

Step 8a:

If you choose SMS: -

A one-time password will be sent to your phone number.

If you choose a phone call: -

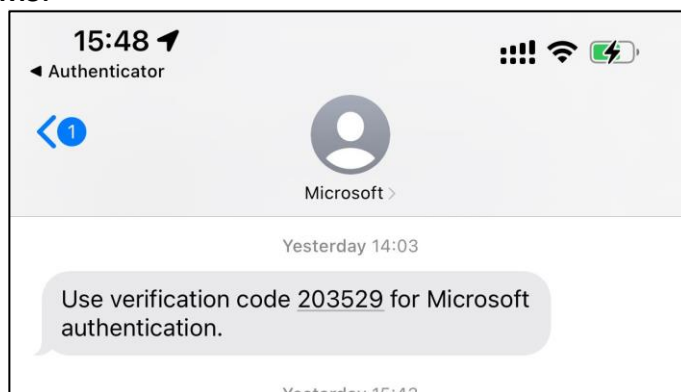
You will receive an automated call shortly, with the one-time password read to you.

Follow the instructions provided to complete the verification process.

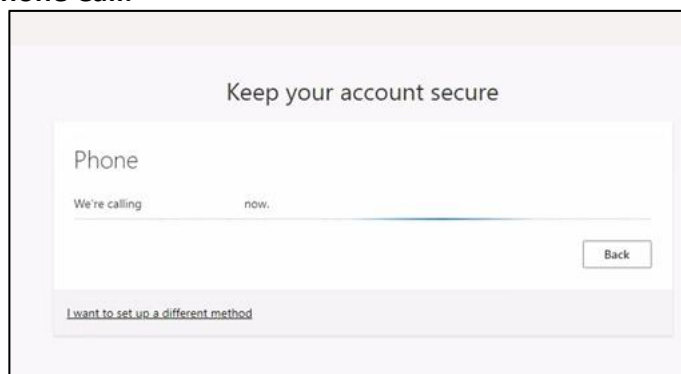
Please note that your mobile provider may charge you to receive SMS / Phone Call. Refer to your provider for details.

The screenshot shows the 'Keep your account secure' screen. Under the 'Phone' section, it says 'You can prove who you are by answering a call on your phone or receiving a code on your phone.' and 'What phone number would you like to use?'. There is a dropdown menu for 'United States (+1)' and a text field for 'Enter phone number'. Below these, there are two radio button options: 'Receive a code' (which is selected and highlighted with a red box) and 'Call me'. At the bottom, there is a 'Next' button and a link that says 'I want to set up a different method'.

SMS:



Phone Call:





Step 9a:

Read or listen to the verification code sent to you and input it on the screen presented. This step will verify your registration and ensure your phone number is correct.

Keep your account secure

Phone

We just sent a 6 digit code to +44 . Enter the code below.

203529

[Resend code](#)

[Back](#) [Next](#)

Step 10a:

If the inputted code is correct, your registration is complete.

Keep your account secure

Phone

✓ Verification complete. Your phone has been registered.

[Next](#)

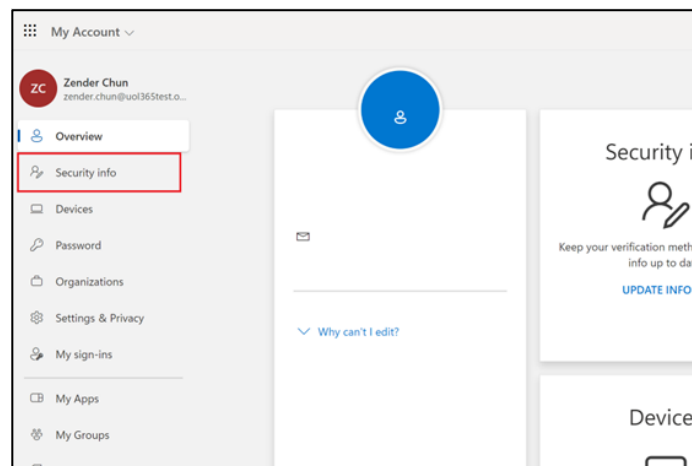


Register for alternative MFA options

You could lose access to your account if you lose or break the device used for MFA, or if you forget to back up the Microsoft Authenticator app when getting a new phone. This could impact your studies. To minimize the chances of this happening, we strongly encourage you to set up multiple MFA options.

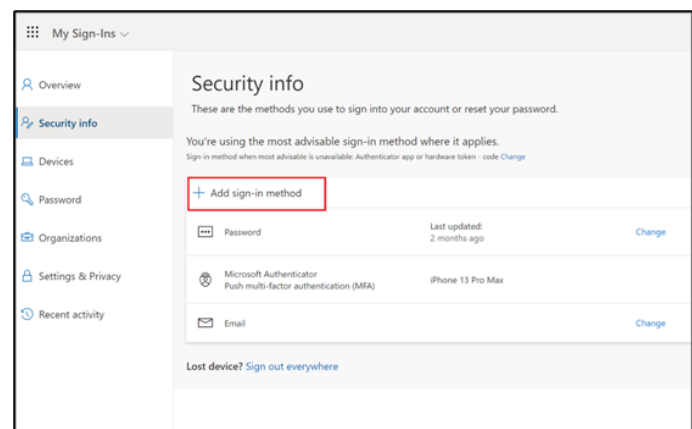
Step 1:

Visit [Microsoft My Account](#) page, and navigate to **Security Info**



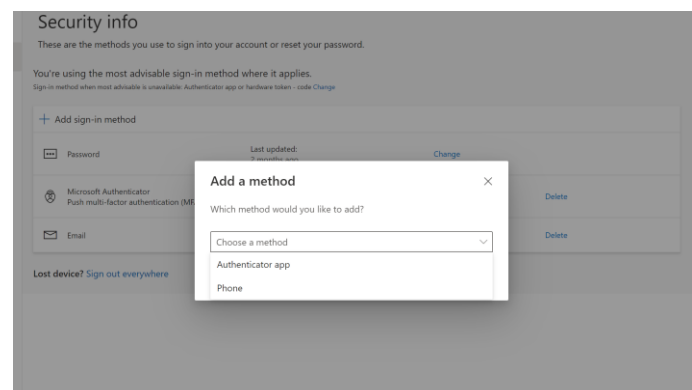
Step 2:

Click **Add sign-in method**



Step 3:

Select the option you wish to add.



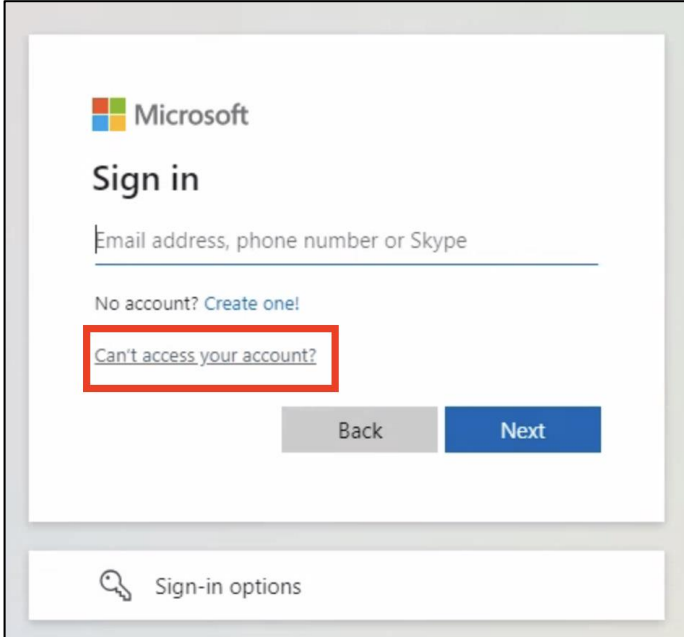


Forgotten Password?

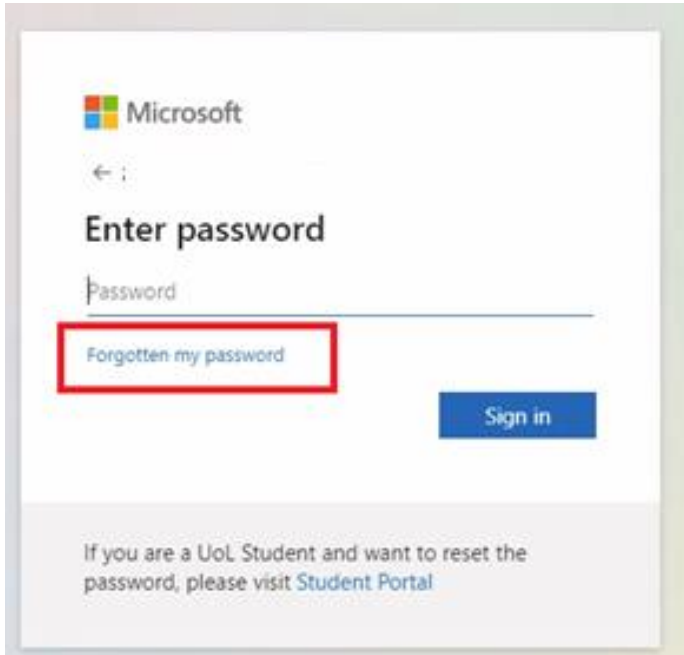
Follow these steps to reset your password independently using the self-service option provided by Microsoft. This guide will walk you through the process of securely changing your password in case you forget it or cannot access your account.

Step 1:

From the Microsoft sign-in screen at <https://login.microsoftonline.com>, Click **Forgotten Password** or **Cannot Access Your Account**



The screenshot shows the Microsoft 'Sign in' page. At the top is the Microsoft logo. Below it is the heading 'Sign in'. There is a text input field labeled 'Email address, phone number or Skype'. Below the input field, there are two links: 'No account? Create one!' and 'Can't access your account?'. The 'Can't access your account?' link is highlighted with a red rectangular box. At the bottom right of the main content area are two buttons: 'Back' (grey) and 'Next' (blue). Below the main content area is a section titled 'Sign-in options' with a key icon.

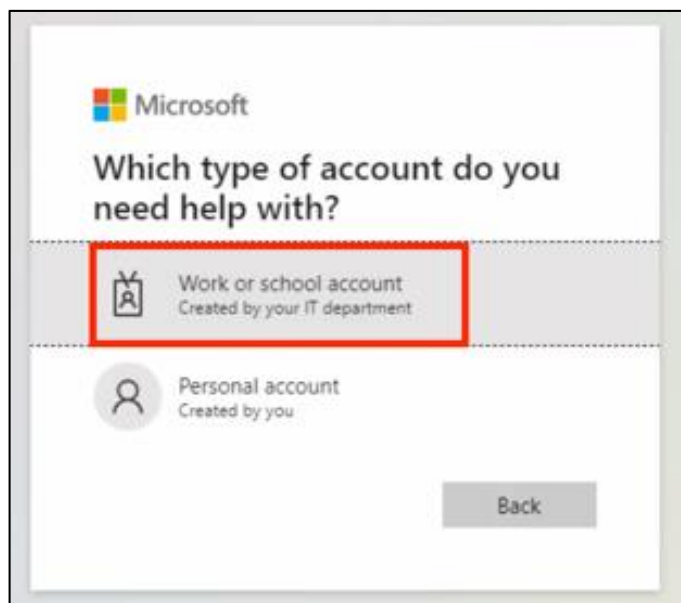


The screenshot shows the Microsoft 'Enter password' page. At the top is the Microsoft logo. Below it is a back arrow icon and the heading 'Enter password'. There is a text input field labeled 'Password'. Below the input field, there is a link 'Forgotten my password' which is highlighted with a red rectangular box. At the bottom right is a blue 'Sign in' button. At the bottom of the page, there is a grey box with the text: 'If you are a UoL Student and want to reset the password, please visit [Student Portal](#)'.



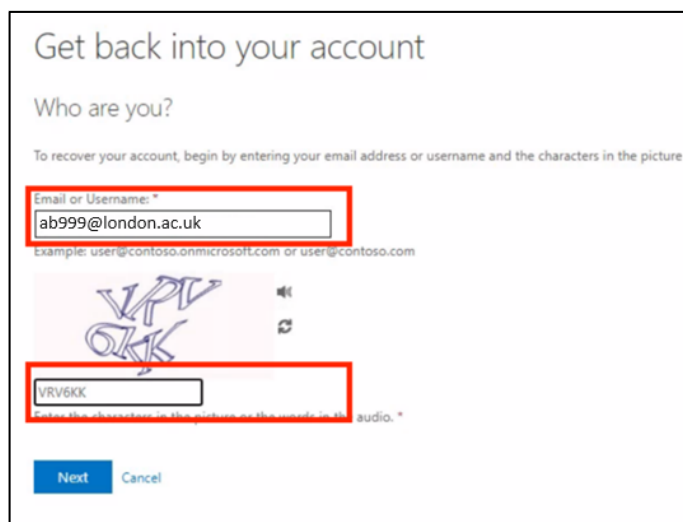
Step 2:

Click **“Work or School Account”**



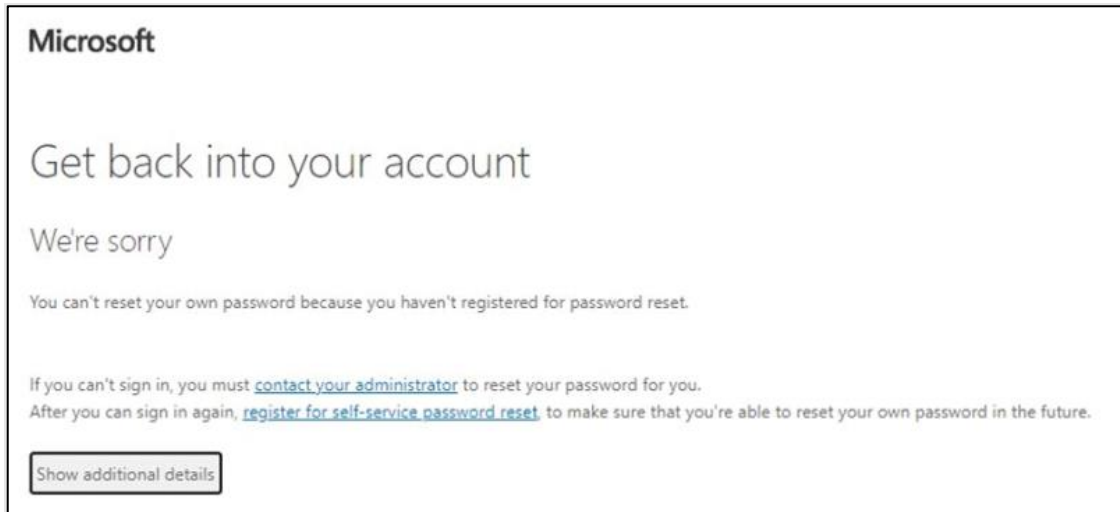
Step 3:

Enter your login name (e.g., `firstname.lastname@london.ac.uk`) in the username field, and complete the captcha security verification code.



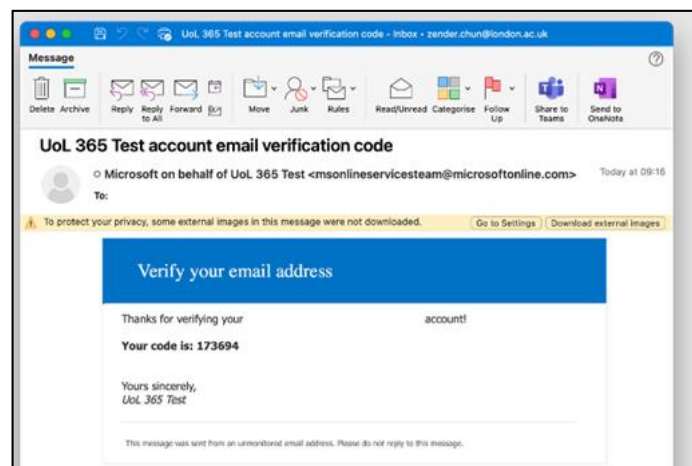
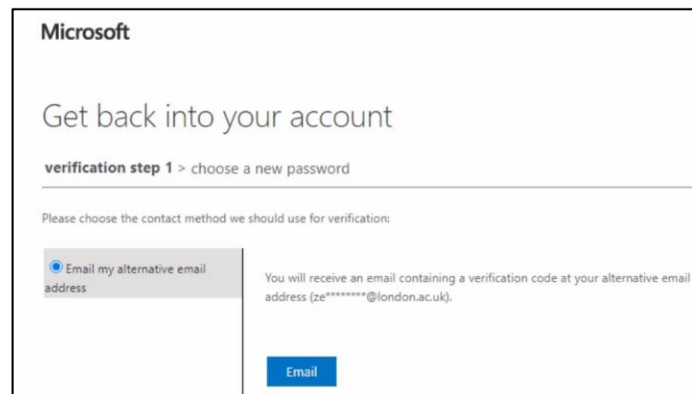
Note:

If the following screen appears, it means you are not registered for self-service password reset. Please visit the [Student IT Support Page](#) for support options, a team member will assist you in resetting your password.



Step 4:

To verify your identity, you will receive an email from Microsoft with a verification code sent to your password recovery email address.





Step 5:

Enter the verification code.

The screenshot shows the Microsoft account recovery interface. At the top, it says 'Microsoft' and 'Get back into your account'. Below this, it indicates 'verification step 1 > choose a new password'. A section titled 'Please choose the contact method we should use for verification:' has a radio button selected for 'Email my alternative email address'. To the right, it says 'We've sent an email message containing a verification code to your inbox.' Below this, there is a text input field containing the code '173694'. At the bottom, there is a blue 'Next' button and a link that says 'Are you having any issues?'.

Step 6:

If the verification code is correct, you will be given the opportunity to change your password.

Please note your password should: -

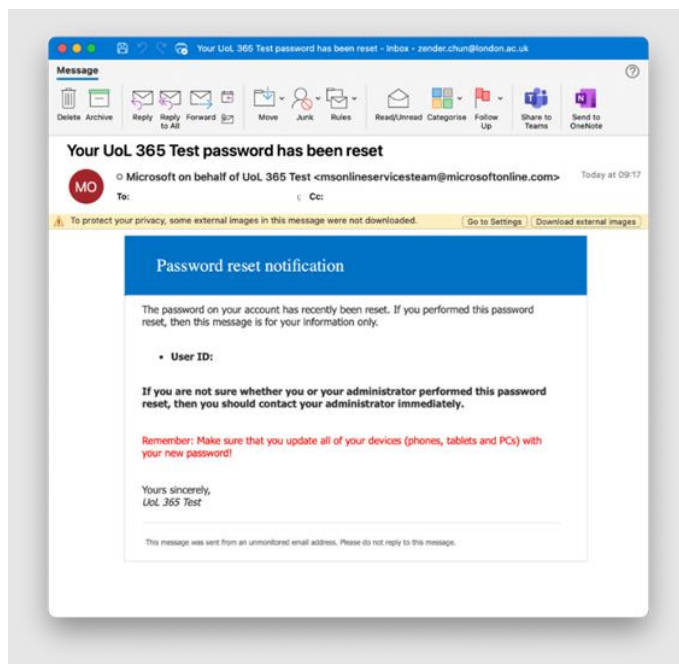
- NOT contain your name or username.
- Contain at least 3 of these character types:
 - o Lowercase characters (a-z)
 - o Uppercase characters (A-Z)
 - o Numeric characters (0-9)
 - o Special characters
- Passwords can only be changed once every 24 hours.
- You cannot reuse the last 10 passwords.
- You may be required to change your password annually.

The screenshot shows the Microsoft account recovery interface for Step 6. It says 'Microsoft' and 'Get back into your account'. Below this, it indicates 'verification step 1 ✓ > choose a new password'. There are two password input fields. The first is labeled '* Enter new password:' and the second is labeled '* Confirm new password:'. Both fields show masked characters with dots. At the bottom, there are two buttons: a blue 'Finish' button and a grey 'Cancel' button.



Step 7:

Once you successfully change the password, you will receive a notification email.



Getting a new Device?

If you are getting a new device, make sure to back up your Microsoft Authenticator app before erasing your old device. Without a backup, you will lose access to MFA. If this happens, please visit the [Student IT Support Page](#) for support options. We will assist you in deregistering the old device and you can re-setup MFA on your new device.

Follow guidance from Microsoft to [back up](#) and [restore](#) your Microsoft Authenticator



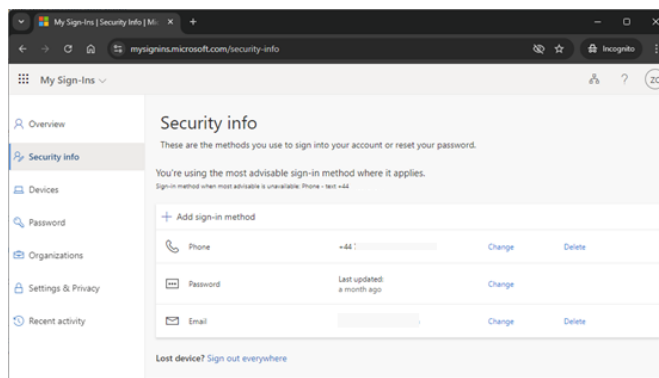
Change your Phone Number?

If you register MFA through by phone call or SMS and you have changed your phone number, you need to re-register your MFA. Follow below steps

Step 1:

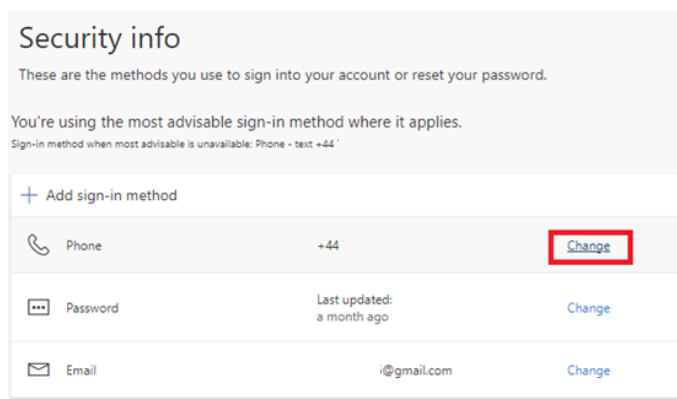
Go to the [Security info](#) page by Microsoft and sign-in your account.

Note: If you have already lost access to your previous phone number, please visit the [Student IT Support Page](#) for support options. We will help you deregister and allow you to re-setup MFA.



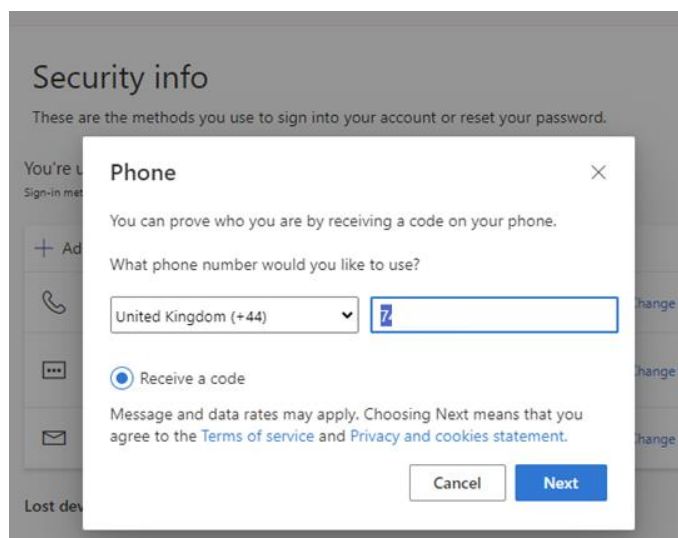
Step 2:

Under **Phone**, click **Change**



Step 3:

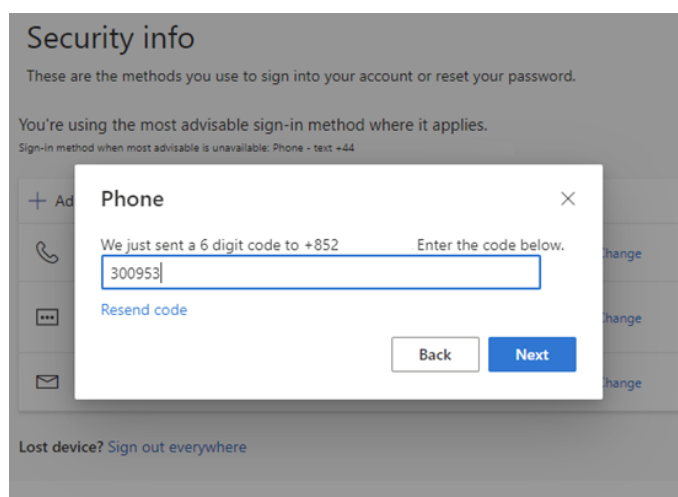
Enter your New **Phone Number**, and click **Next**



The screenshot shows the 'Security info' dialog box. The title is 'Phone'. The text says: 'You can prove who you are by receiving a code on your phone. What phone number would you like to use?'. There is a dropdown menu for the country code, currently set to 'United Kingdom (+44)'. To the right of the dropdown is a text input field containing the number '7'. Below this, there is a radio button labeled 'Receive a code' which is selected. A note below the radio button says: 'Message and data rates may apply. Choosing Next means that you agree to the [Terms of service](#) and [Privacy and cookies statement](#).' At the bottom right are two buttons: 'Cancel' and 'Next'.

Step 4:

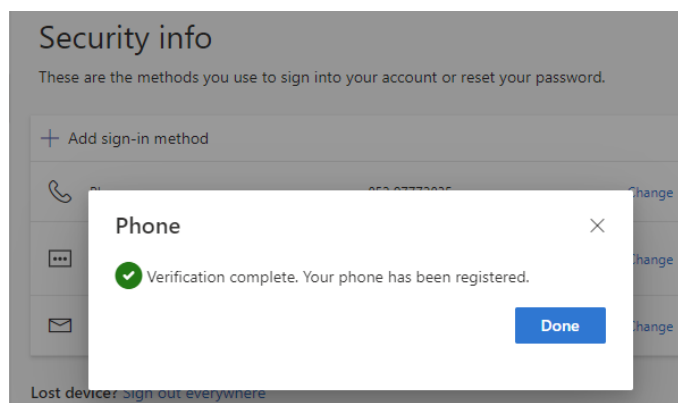
Enter the verification code sent to your phone, and click **Next**



The screenshot shows the 'Security info' dialog box. The title is 'Phone'. The text says: 'We just sent a 6 digit code to +852 Enter the code below.' Below this is a text input field containing the code '300953'. To the left of the input field is a link that says 'Resend code'. At the bottom right are two buttons: 'Back' and 'Next'.

Step 5:

Your MFA number has now been changed.



The screenshot shows the 'Security info' dialog box. The title is 'Phone'. The text says: 'Verification complete. Your phone has been registered.' There is a green checkmark icon to the left of the text. At the bottom right is a button labeled 'Done'.



Frequently Asked Questions:

1. What is Multi-Factor Authentication (MFA)?

MFA is a security system that requires multiple forms of identification before granting access to an account. It combines something you know (password) with something you have (mobile device).

2. How does MFA work?

MFA works by adding an extra layer of security to the login process. After entering your password, you'll be prompted to verify your identity through a secondary method, such as inputting a code on your Microsoft Authenticator app, or input a code sent to your or mobile.

3. Why is MFA important?

MFA significantly enhances account security by making it much harder for unauthorized users to access your accounts. Even if someone obtains your password, they will still need the secondary authentication factor to gain access.

4. How do I set up MFA on my account?

To set up MFA, follow the instructions provided above. You will require a smart phone with Microsoft Authenticator installed. Alternatively, you could also choose to setup with SMS.

5. What MFA methods do you provide?

- Microsoft Authenticator
- SMS
- Phone call

6. What should I do if I replace my phone?

If you setup your MFA by Microsoft Authenticator, make sure you follow the steps on [Getting a new Device?](#) This is essential to transfer your MFA to your new phone.

7. What should I do if I get a new phone number?

If you get a new phone number and register MFA by SMS / Phone Call, update your MFA settings as soon as by following the steps on [Change your Phone Number?](#)

8. What should I do if I lost my device?

If you lose your device or no longer have access to the previous phone number, please visit the [Student IT Support Page](#) for support options. We will help you disable MFA on the lost device and set it up on a new one to ensure your account remains secure.



9. What should I do if I'm not receiving the MFA code?

If you are using **Microsoft Authenticator** and you are not receiving notification during sign-in. Please make sure you have stable internet connection on your phone, and you have turn on Notification. You could check by following steps:

On your Android Device:

- Tap **Settings** and then tap **Notifications**.
- Tap **App settings**.
- Select **Authenticator** and make sure **notifications** are **ON**.

On your iOS device:

- Tap **Settings** then tap **Notifications**.
- Tap **Authenticator** and make sure the "**Allow Notifications**" is **ON**, and notification delivery is select as **Immediate Delivery**.
- Also, make sure [Do Not Disturb](#) mode is **OFF** which will block notification.

If you are using **SMS/Phone Call**, make sure your have stable phone signal. You should expect the SMS with authentication code arrives within 3-5 minutes. Occasionally, the SMS may take longer to deliver.

10. Can I use MFA while traveling internationally?

Yes, you can use MFA while traveling internationally. However, ensure you have access to the internet or mobile network to receive authentication codes. Consider using Microsoft Authenticator as it doesn't rely on SMS if you expect limited connectivity.