

How to set up Multi-Factor Authentication

Over the 2019-20 academic year the LSE will be rolling out Multi-Factor Authentication (MFA) for all LSE users (staff and students).

This means that when you log into Microsoft 365 – for instance your Outlook email – you will be required not only to log in with your username and password, but also with an additional method of authentication too.

The School are introducing MFA as an extra layer of security - to help protect accounts from being exploited by hackers.

Before you request to enable MFA for your account, we highly recommend you print the instructions on this page and print out the instructions from the LSE at <https://info.lse.ac.uk/staff/divisions/dts/help/guides-faqs/mfa>, so you have these to hand.

We also recommend you have a backup non-LSE email, e.g. gmail, yahoo, hotmail, so that the LSE can send you a confirmation message and MFA instructions, in case you temporarily lose your connection to your LSE email account.

Read ALL the instructions below carefully first.

You will need your **computer and your smartphone** nearby.

Setting up MFA

1. On your computer open your browser and go to <https://info.lse.ac.uk/staff/divisions/dts/help/guides-faqs/mfa>
2. Click on the link for Enable or request to reset your MFA settings and fill in the simple form for your account:
 - Make sure you check "Enable MFA".
 - Check "Send me an email receipt of my responses."

The image shows a screenshot of a web form titled "LSE Multi-Factor Authentication". The form is set against a dark background with a red LSE logo. The main heading is "Multi-Factor Authentication". Below the heading, there is a sub-heading "Update your Multi-Factor Authentication status." and a URL "https://lse.ac.uk/mfa". A personalized message reads "Hi Anita, when you submit this form, the owner will be able to see your name and email address." A red asterisk indicates a required field. The first section is "1. Please Choose an action to perform" with a note "You will receive automated email informing you when your request has been processed." There are two radio button options: "Enable MFA" and "Request MFA Reset". Below these is a checkbox option "Send me an email receipt of my responses". A dark "Submit" button is located at the bottom of the form. At the very bottom, there is a footer with the text "This content is created by the owner of the form. The data you submit will be sent to the form owner. Never give out your password." and "Powered by Microsoft Forms | Privacy and cookies | Terms of use".

3. A second text box will appear in the form. Under "(Optional) Alternative email address", type your back up email address e.g. your gmail, yahoo or hotmail email.

This is useful because if you are locked out of your LSE email account during the MFA set up process you can access instructions from your backup email.

LSE Multi-Factor Authentication

Update your Multi-Factor Authentication status.

<https://lse.ac.uk/mfa>

Hi Anita, when you submit this form, the owner will be able to see your name and email address.

* Required

1. Please Choose an action to perform
You will receive automated email informing you when your request has been processed.

Enable MFA

Request MFA Reset

2. (Optional) Alternative email address
Access to your LSE office 365 account will be changed, you can specify an alternative email address for us to send a guide on how to set-up MFA.

Enter your answer

Send me an email receipt of my responses

Submit

This content is created by the owner of the form. The data you submit will be sent to the form owner. Never give out your password.

Powered by Microsoft Forms | [Privacy and cookies](#) | [Terms of use](#)

4. Make a note of the time you have done this. Then click Submit.
5. Once you have completed the form, you will have to wait approximately 1 - 2 hours before you can start using MFA.

- The School recommends that you use the Microsoft Authenticator App (for your mobile device) as your first method of authentication, and phone (for a text message or voice call) as your next (backup) method of verification.

In our next steps we will download the Microsoft Authenticator App on your phone first, and configure that as your default method of authentication.

- Download the App from your device App store, but do NOT click Open when it has downloaded. Instead close your App store.



Microsoft Authenticator 4+

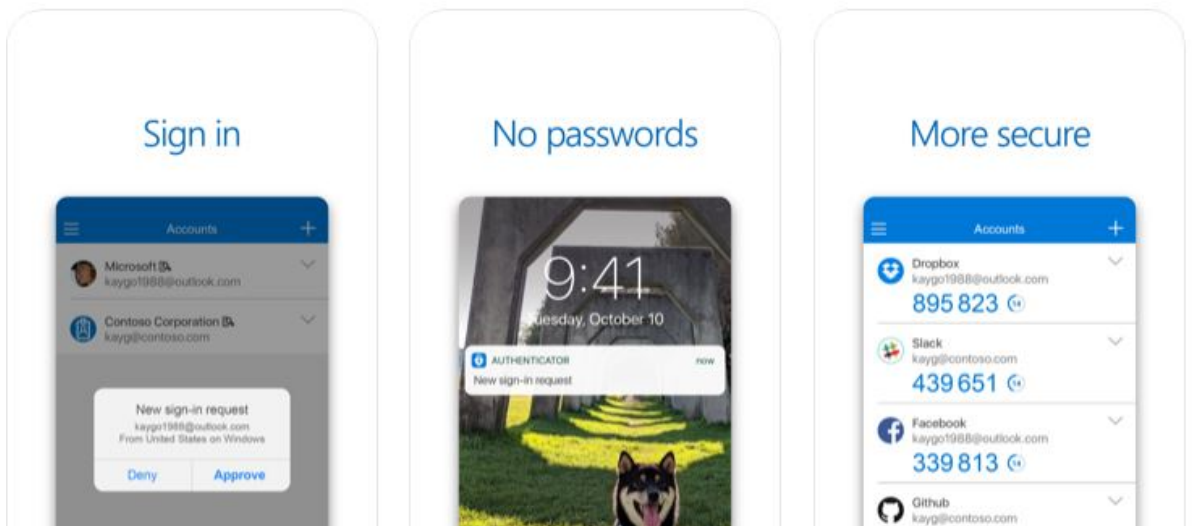
Microsoft Corporation

#6 in Productivity

★★★★★ 4.7, 9.4K Ratings

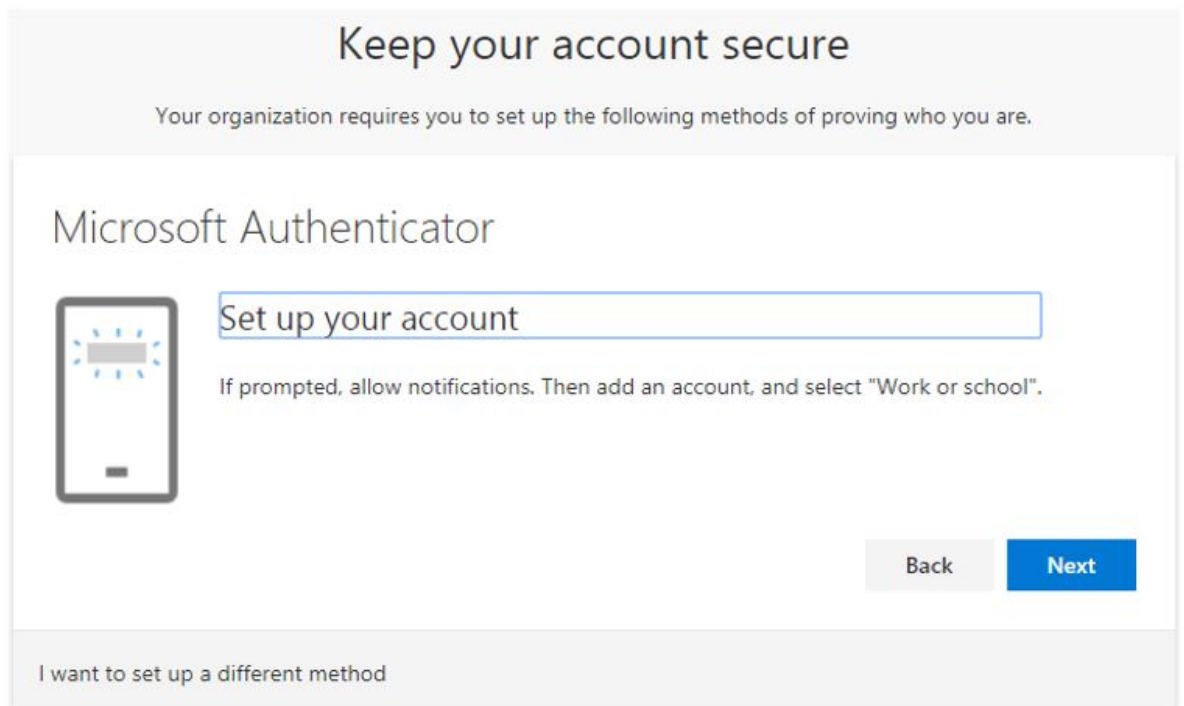
Free

Screenshots [iPhone](#) [iPad](#) [Apple Watch](#)

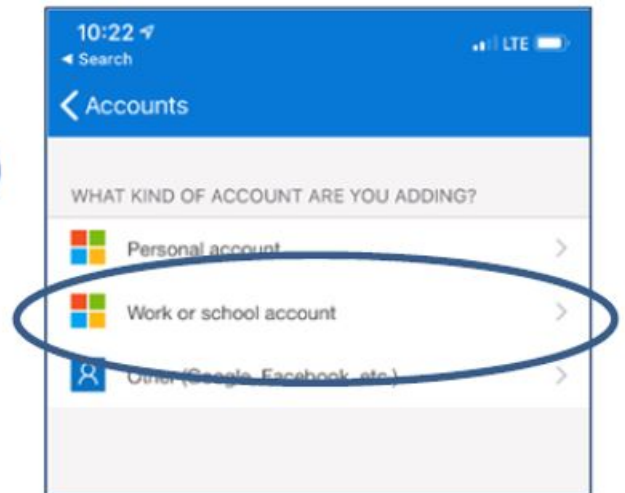
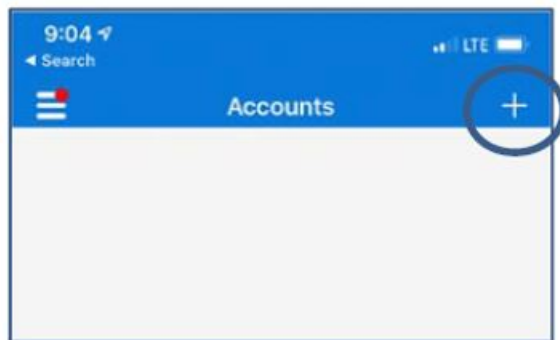


- You will NOT be notified when MFA is ready. Instead, after an hour has passed, open Outlook on your computer or go to Microsoft 365 on your browser.

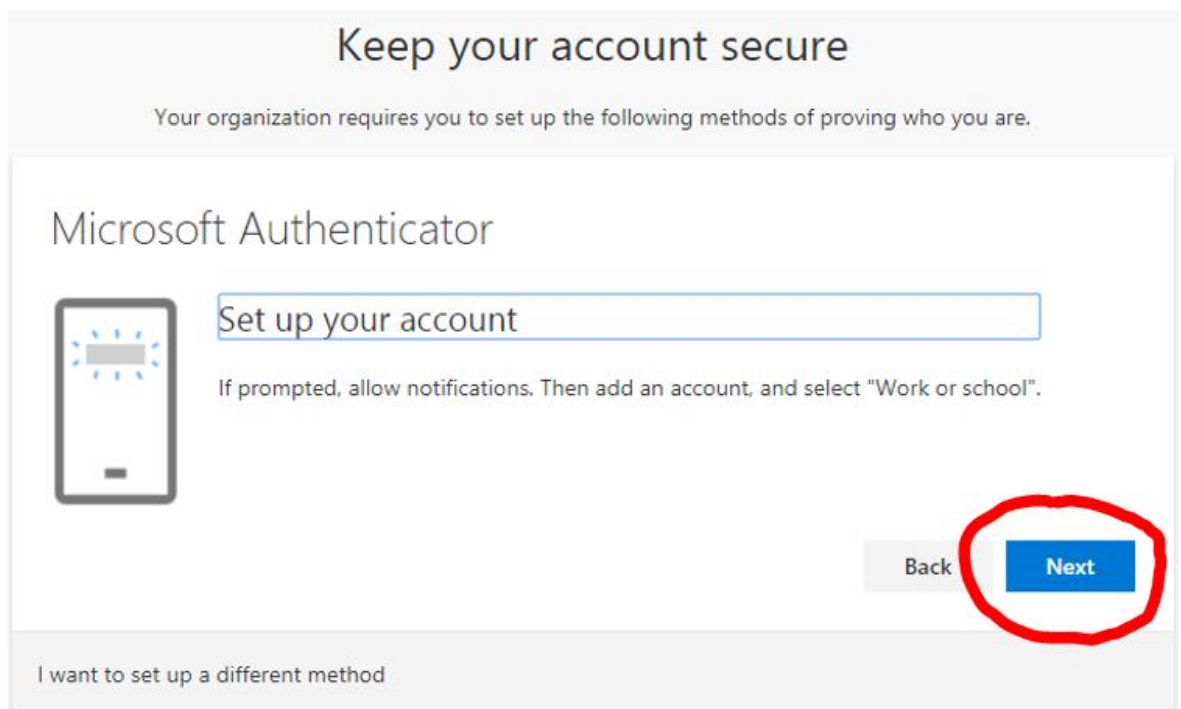
9. You may be prompted to log in with your LSE email address. If not, you will see a dialog box showing your email address and prompting you to "Enter Password". Type in your LSE password and click Sign In.
10. You will see a Microsoft Authenticator dialog box, prompting you to download the App if you have not done so already. Click on Next.
11. You will see a "Set up your account" dialog box. At this point, go to your phone.



12. On your phone open the Microsoft Authenticator App. The App will ask if you want to be sent notifications. Click Allow.
13. In the App select "+" or Add account option. Then select "Work or school account". If you do not see "Work or school account" close your App and reopen it. You should then see the option.



14. Now return to your computer, to the "Set up your account" dialog box, and click Next.




15. On your computer, you will now be shown a QR code to scan with your phone (which will link the Microsoft Authenticator App with your account).

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.



Configure app without notifications

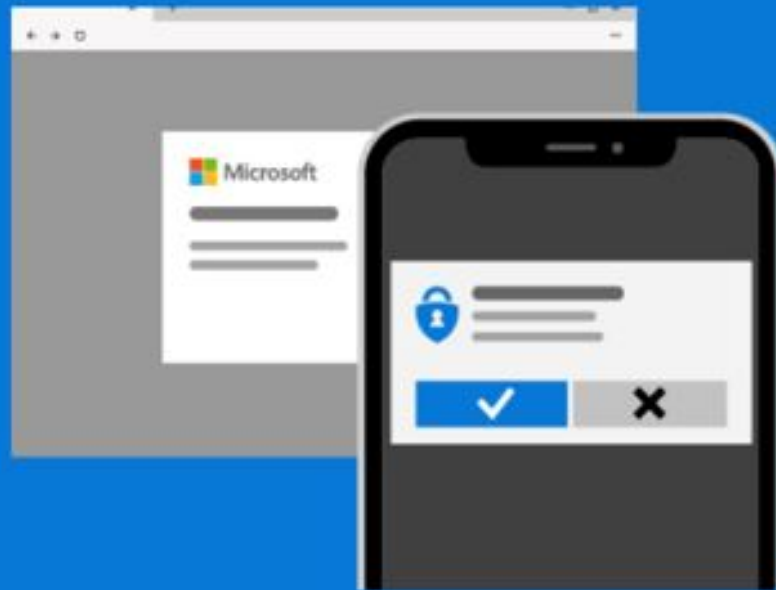
If you are unable to scan the image, enter the following information in your app.
Code: 857 634 999
Url: <https://co1pfpad16.phonefactor.net/pad/648069390>

If the app displays a six-digit code, you are done!

Next cancel

16. The first time you set up the Microsoft Authenticator App on your phone, you might receive a prompt asking whether to allow the app to access your camera (iOS) or to allow the app to take pictures and record video (Android). You must select **Allow**.

With your phone click "Scan QR code" ...



Set up passwordless sign-in for your personal Microsoft account



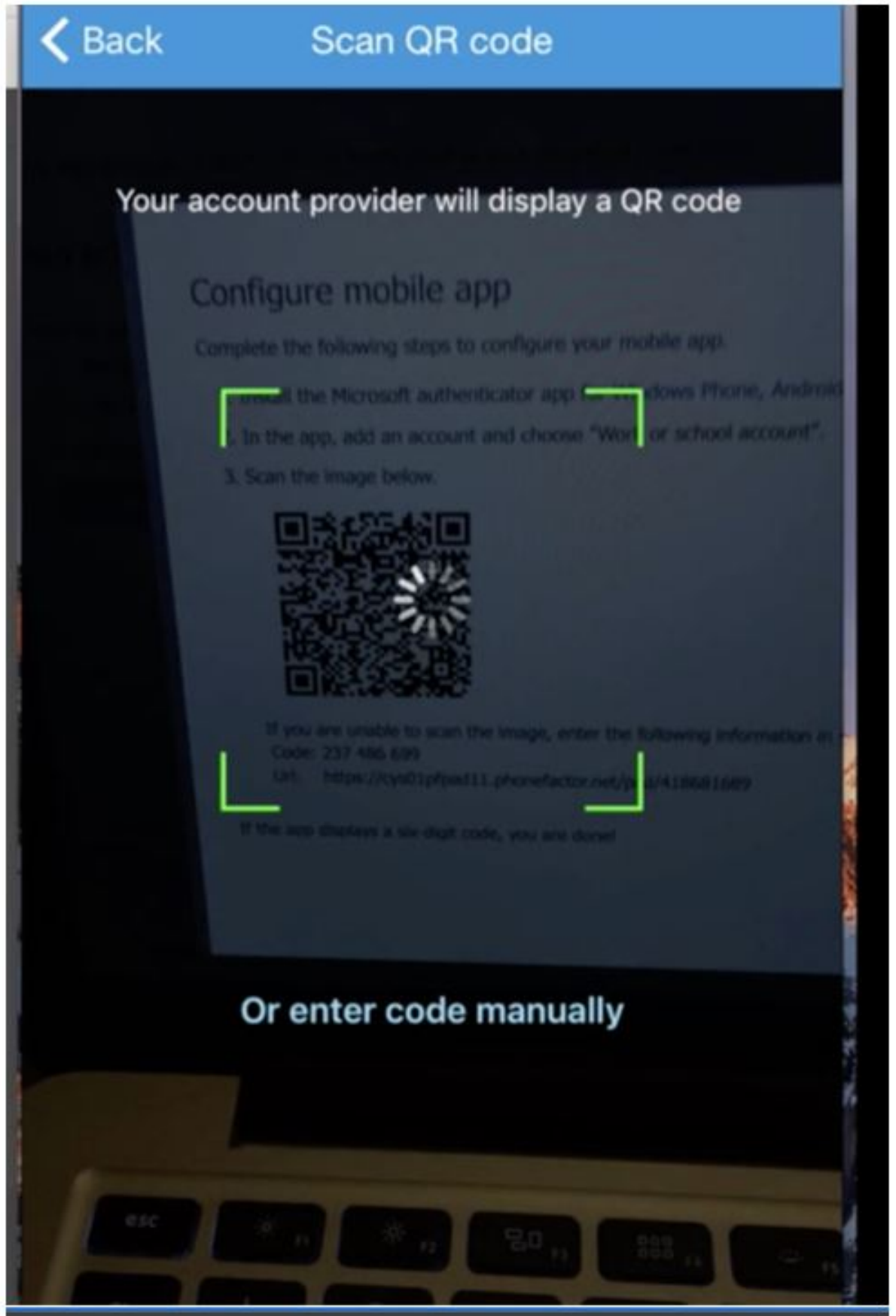
Add personal account



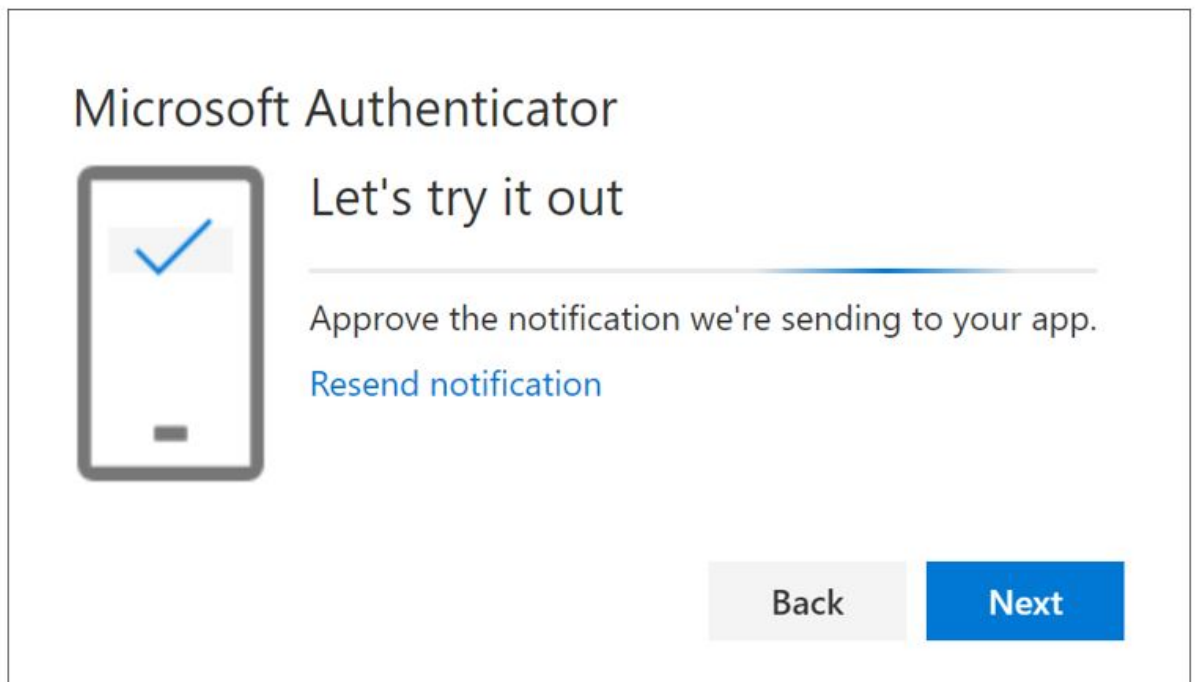
Scan QR code

Skip

...and scan the code on your computer screen:



17. After the QR code is accepted by the App, Microsoft will send a test authentication request to the App.



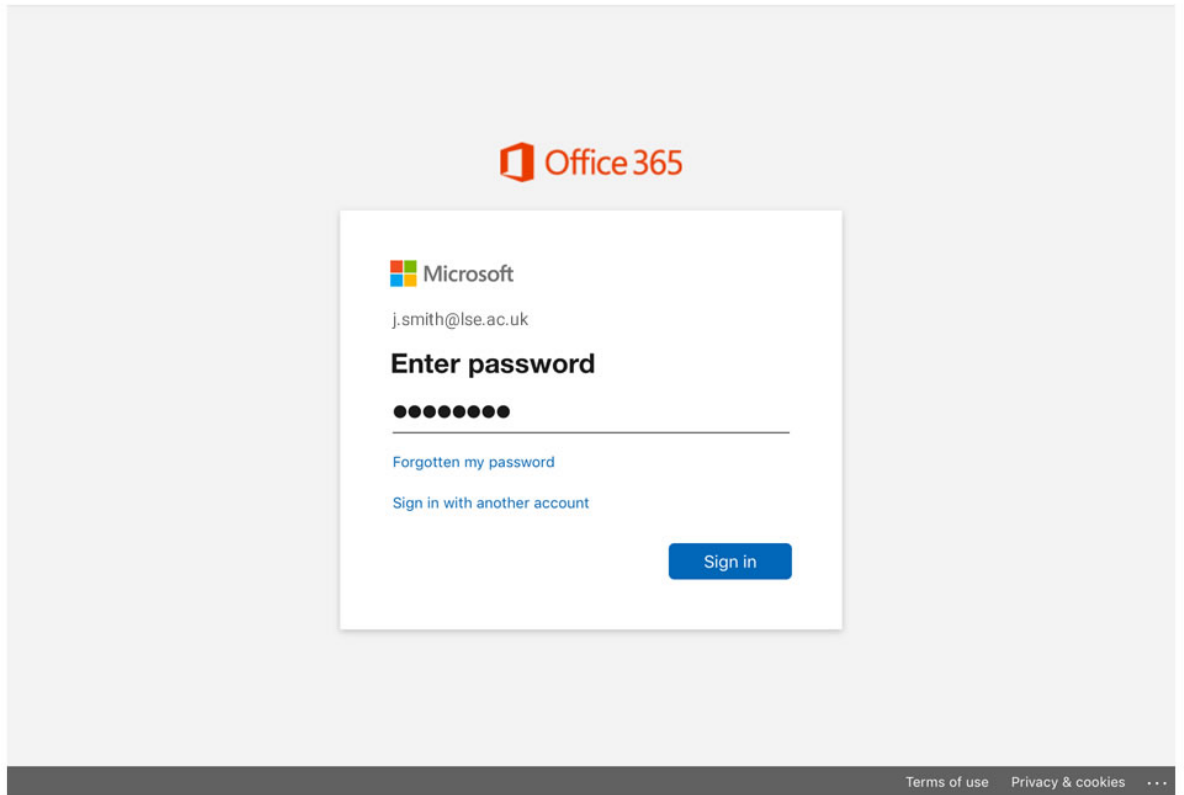
18. Click **Accept** in the App notification on your phone to complete the test and confirm successful setup.

Logging into Email, Teams, or Microsoft 365 with MFA enabled

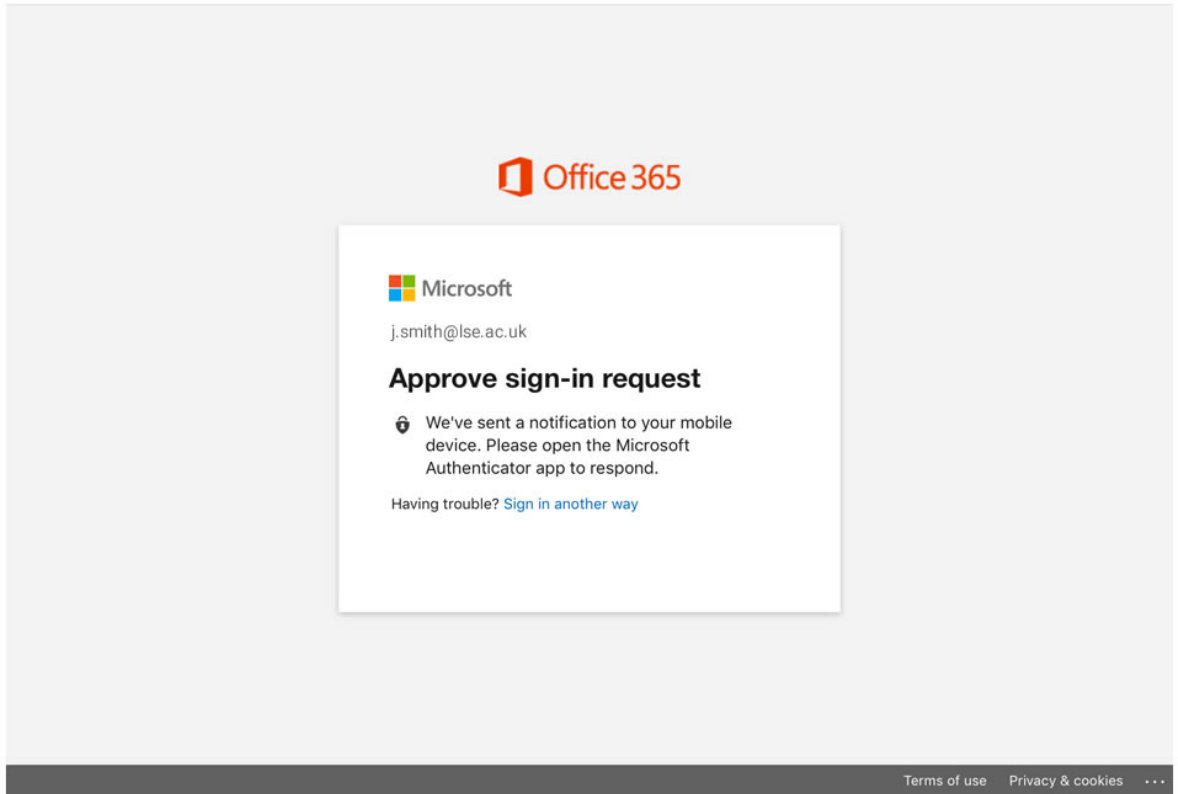
You will now have MFA enabled and your Microsoft Authenticator App set as your default method of authentication.

This means when you log in to email, or Teams, on a device, you will be prompted to sign in with your password and also verify your log in through your Authenticator App:

1. You will be prompted for your password.



2. You will be prompted to verify the log in using your Microsoft Authenticator App:



3. If you have notifications enabled for the Authenticator app, a popup will appear on your phone to allow you to "Approve" your sign-in.



4. If you **do not have notifications enabled or have no signal or Internet connection on your phone**, you can still complete a logon to Microsoft 365 by entering the 6-digit verification code displayed in the Authenticator app.

This code changes every 30 seconds so be sure to enter the code while it is still displayed in the app:



One-time password code
17 347 542

After enabling MFA and configuring the Microsoft Authenticator App it is advisable to **Set up a Phone call or sms text message as a second method of authentication.**

The LSE recommend you set-up both the "Microsoft Authenticator App" and "Phone" methods of verification to ensure you always have access to your account.