How to set up Multi Factor Authentication (MFA) for Office 365

To make sure our information is secure when you access Outlook, Teams and other Office 365 apps from personal devices, you need to set up multi factor authentication (MFA). This will help you to make sure that only you can access your information.

To set up multi factor authentication you'll need to:

- have both an up to date work or personal computer, and a smart phone (option one) or landline (option 2)
- follow the steps - **please read this guide carefully – take time to follow each step.**

We know there are a number of things that will affect how this process works for you including what type of computer or phone you have, the browser you're using and how many people may be trying to use the app at the same time. It's not possible to take account of every situation.

Contents

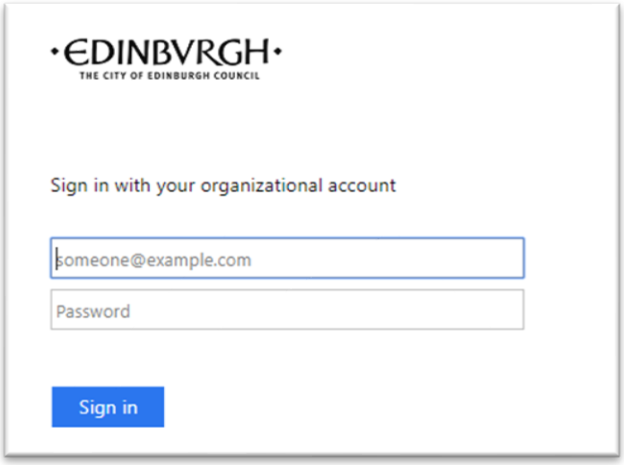
Option one – setting up multi factor authentication using your smart phone

Step 1 - sign into Office 365 on your computer or laptop

1. On your personal or work computer (not your phone) open Chrome or Edge internet browser.

2. Go to https://aka.ms/mfasetup

3. In the **Sign in** box, add your email address using the employee number instead of your name such as 1234567@edinburgh.gov.uk instead of joe.bloggs@edinburgh.gov.uk.

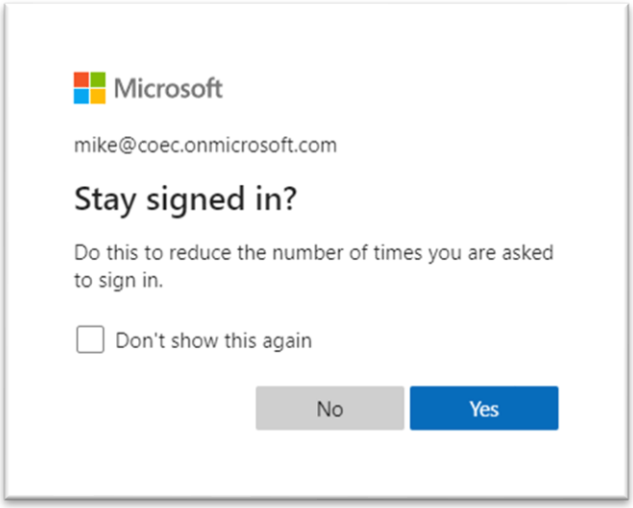


4. Click **Next** and enter the usual password you use to sign on to your work computer.

5. Click **Sign In**.

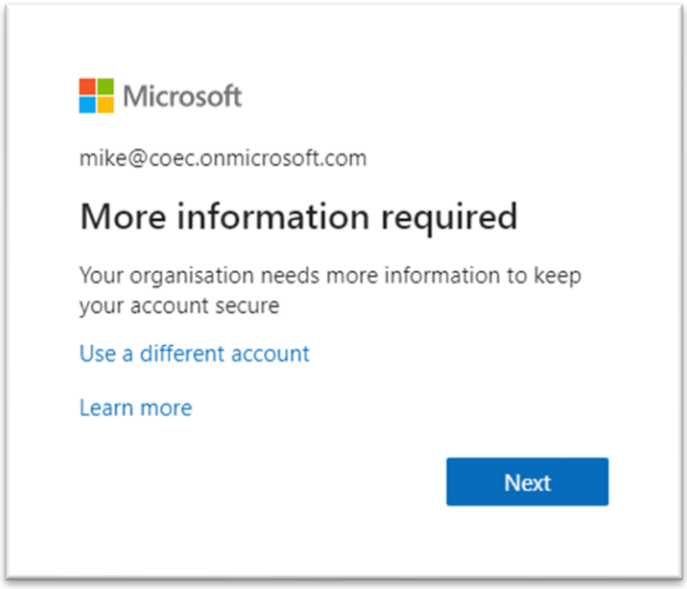
6. You may be asked to stay signed in.

7. Select **Yes**.



8. You will now see a **More information required** screen.

9. Click **Next**.

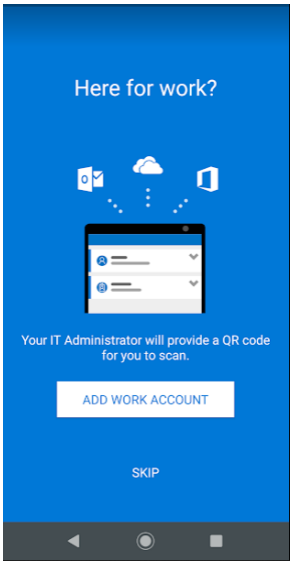


10. The page (right) will open asking you to install the Microsoft Authenticator app on your mobile phone.

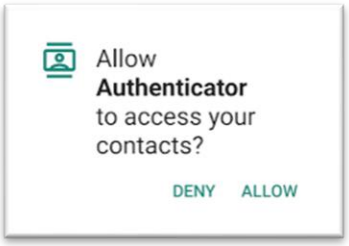
Step 2 - installing the authenticator app on your mobile phone

If you don't have a smart phone or have issues using the authenticator app, please see Option 2 below.

11. On your mobile phone, go to the App Store (for iPhones/iPads) or Play Store (for Android), search for and install the Microsoft Authenticator app.
12. Open this app.
13. If there are questions about data privacy, please press **OK**.
14. If you're asked to **ADD PERSONAL ACCOUNT** press SKIP.
15. If you're asked to **ADD NON-MICROSOFT ACCOUNT** press **SKIP**
16. When you see the screen '**Here for work?**', press **ADD WORK ACCOUNT**

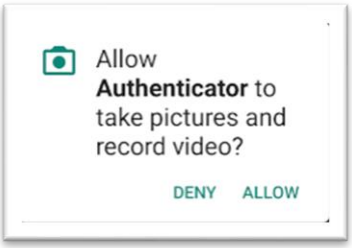


17. You'll then be asked to **Allow Authenticator to access your contacts**.
18. The authenticator app will not use your contacts, however to allow the app to work you have to press **ALLOW**.

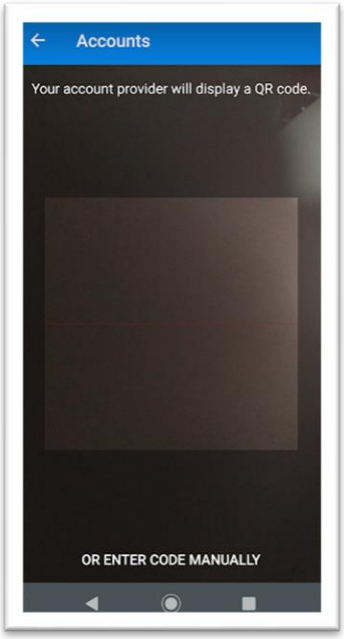


The app needs this permission so it can search for existing work or school Microsoft accounts on your phone and add them to the app. This helps to make sure your account works properly. This permission also helps save you time while adding your personal Microsoft accounts, by automatically filling in some of the information for you, like your first and last name.

19. Press **ALLOW** for **Allow Authenticator to take pictures and record video** – you need this to scan a QR code in the next step.



20. Your QR code scanner will now appear on your mobile phone.



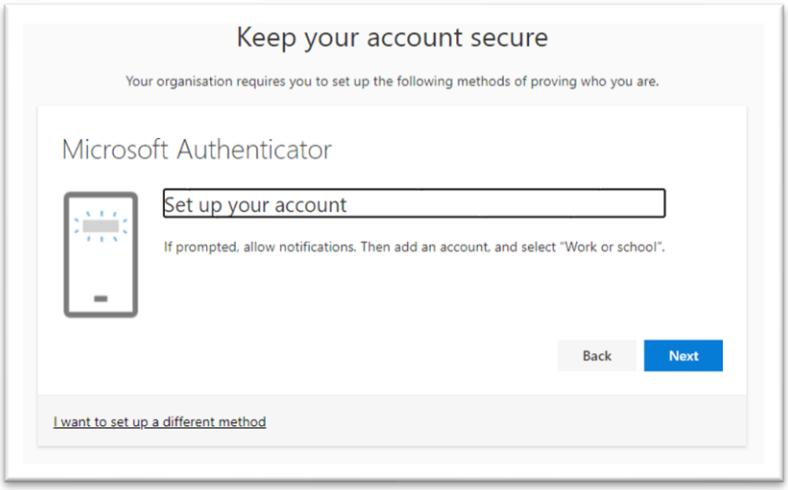
Step 3 - return to your personal or work computer

21. Go back to the browser on your computer and the **Keep your account secure page**.

22. Click on **Next**.

23. The page on the right will appear.

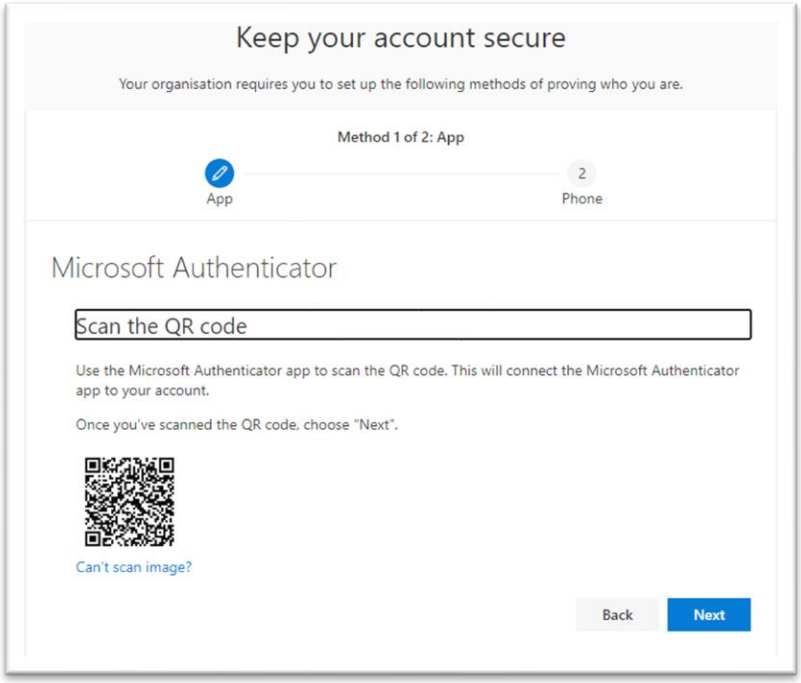
24. Click on **Next**.



If a message appears saying **We're sorry, we ran into a problem**, please start the process again.

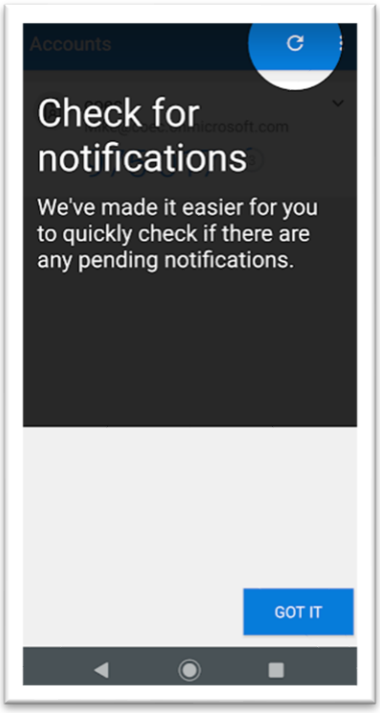
Step 4 - using your mobile phone to scan the QR code

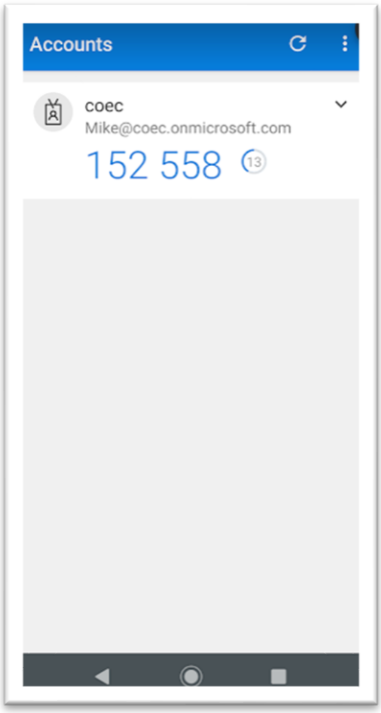
25. Using your mobile phone again, use the QR code scanner to scan the QR code that appears on your computer screen.



26. If you're asked to accept notifications on your mobile phone, press **GOT IT**.

27. Your Council Office 365 account should now be added to the Authenticator app and look similar to the screen on the right, below

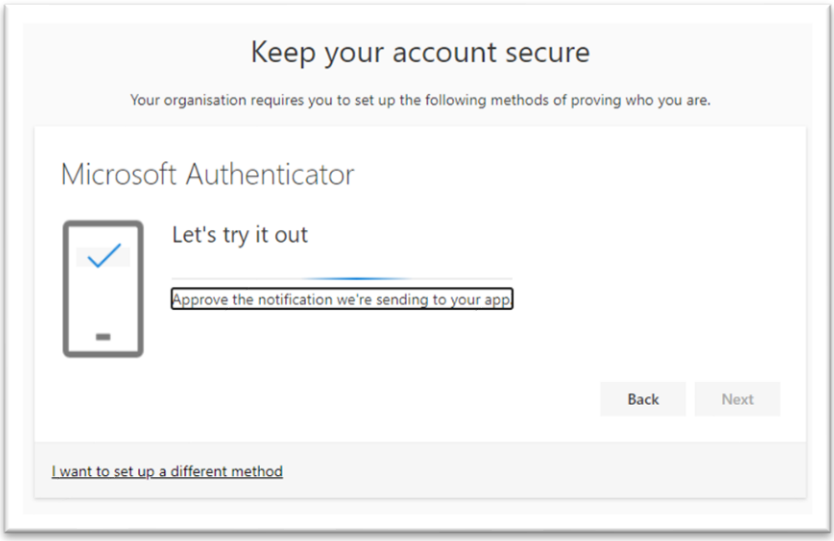




Step 5 - testing the authentication is working on your computer

28. Go back to your computer and the QR code screen and click **NEXT**.

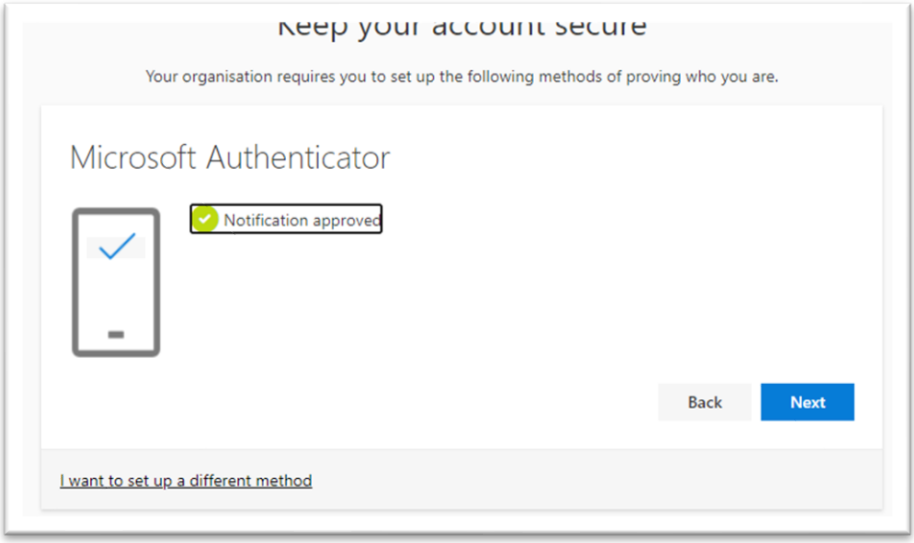
29. The next step tests the authentication is working. Click **Next**.



30. An ‘approve sign-in request’ screen with a number will appear on your computer then an ‘**Approve sign-in?**’ notification will appear on your mobile phone. Enter the number into the mobile screen and press ‘YES’. You may then be prompted for your mobile PIN or fingerprint – please do this.

31. The page on your computer should update to state that the notification has been approved.

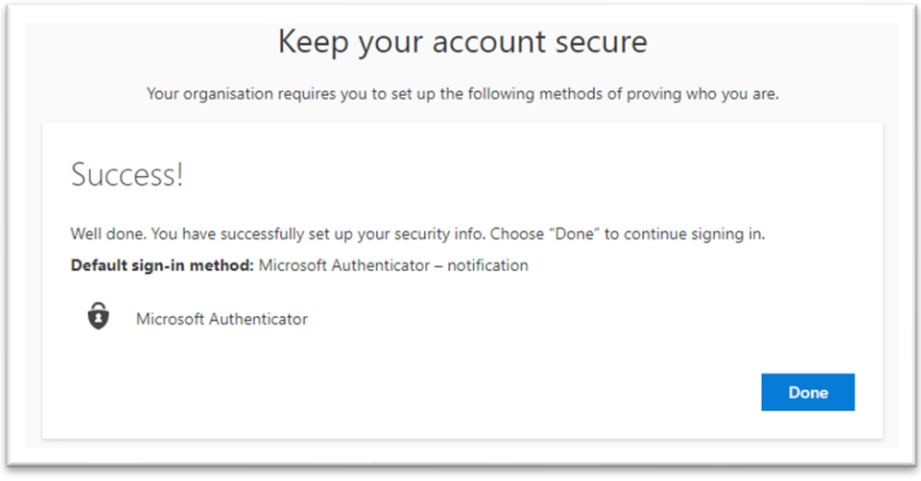
32. Press **NEXT**.



33. A **Success!** message should now appear.

34. Click **Done**.

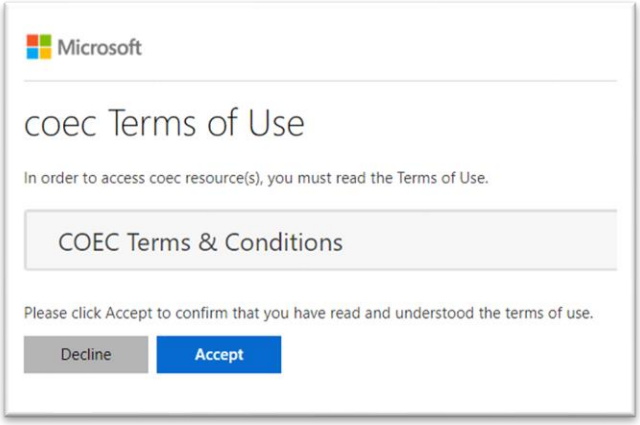
35. You should now be directed to a page where you can manage your sign-ins.



Logging into Outlook for the web or Teams web app

Now that you've set up multi factor authentication, you can access Outlook for the Web on any device by going to http://outlook.office.com or for Teams go to http://teams.microsoft.com. Please save this web address in your bookmarks so you can access it easily.

36. When logging in for the first time, you must read the Terms of Use. Click on **COEC Terms & Conditions** to view the policy.
37. Click **Accept**.
38. It may ask you if you want to download the Outlook app, please decline this by clicking on the X.
39. You may also be asked to use the authenticator app every time you need to log in.
40. You'll need to select the language and timezone.
41. Click **Save**
42. Your emails will now show.

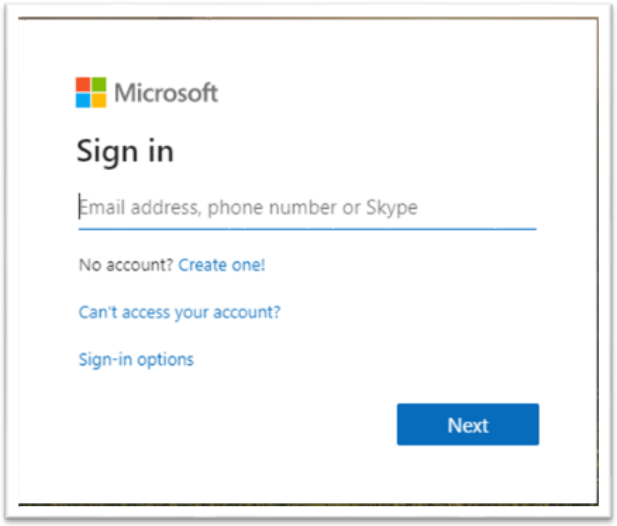


Option two – setting up multi factor authentication if you don't have a smart phone or you're having issues with the authenticator app

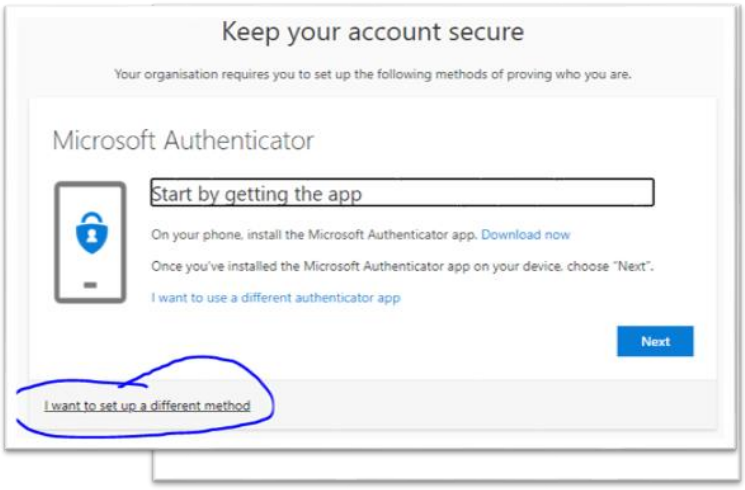
If you can't install the Microsoft Authenticator or don't have a smart phone, you can use the phone or 'call me' method of multi factor authentication.

43. To set this up, go to http://aka.ms/mfasetup in your browser on a personal or work computer.

44. You'll be asked for your email address (use your employee ID number and not your name such as 1234567@edinburgh.gov.uk).

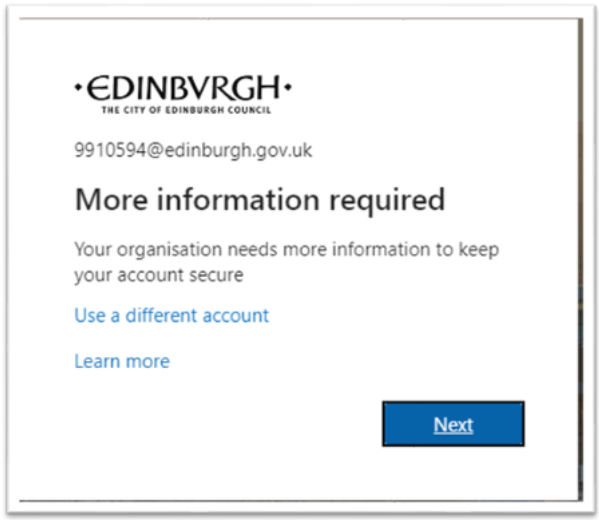


45. Use your normal work login password and click **Sign in**



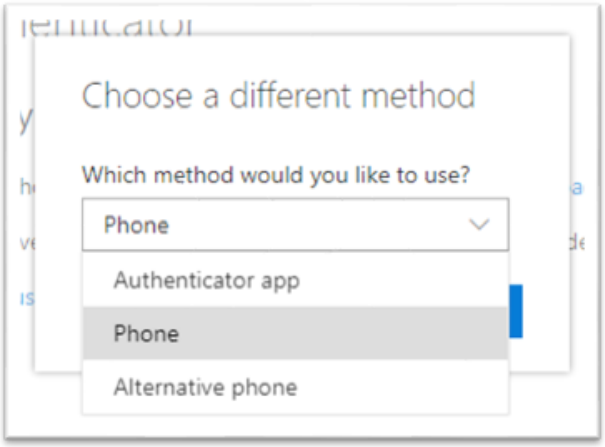
46. If you're asked to stay signed in, select **Yes**

47. Click **Next** when you're asked for more information

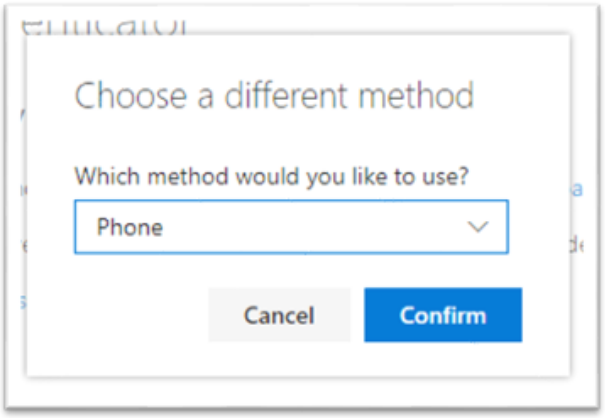


48. On the bottom right, click **I want to set up a different method**

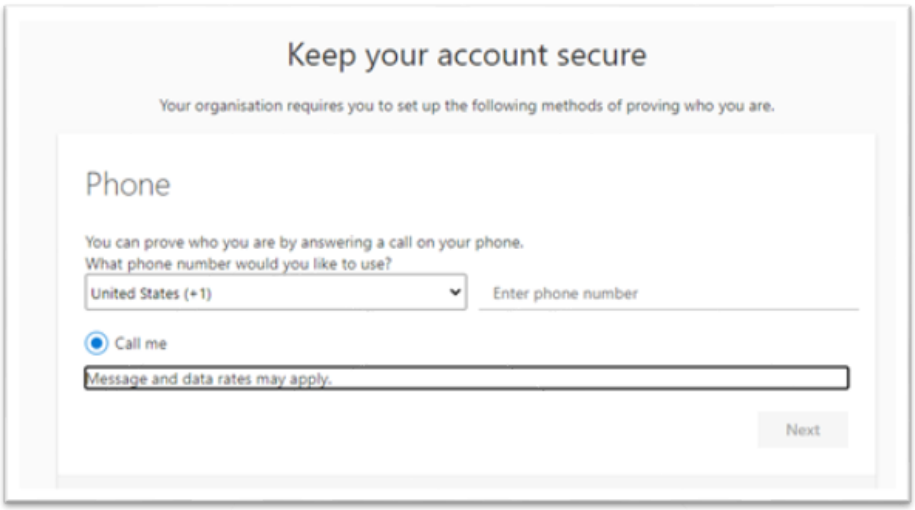
49. Select **Phone**



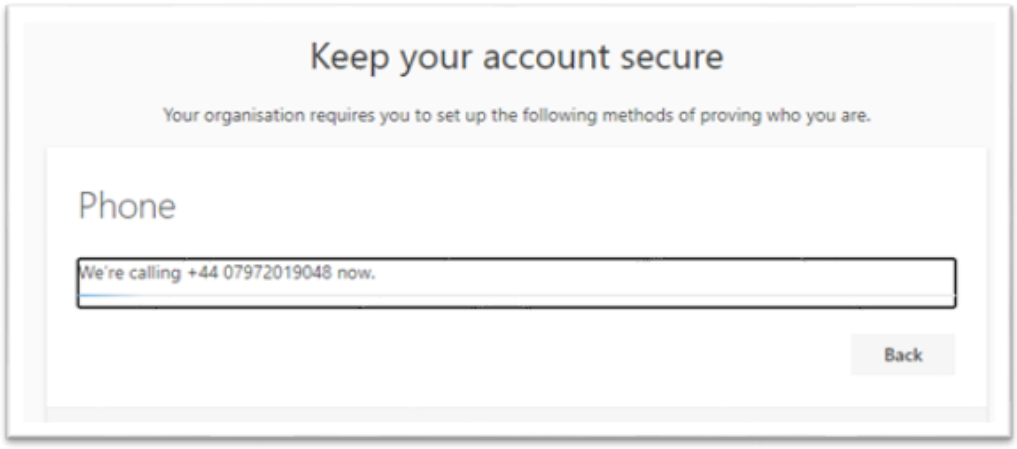
50. Then click **Confirm**.



51. Provide your preferred phone number (mobile or landline that you'll have regular access to) and click **Next**.



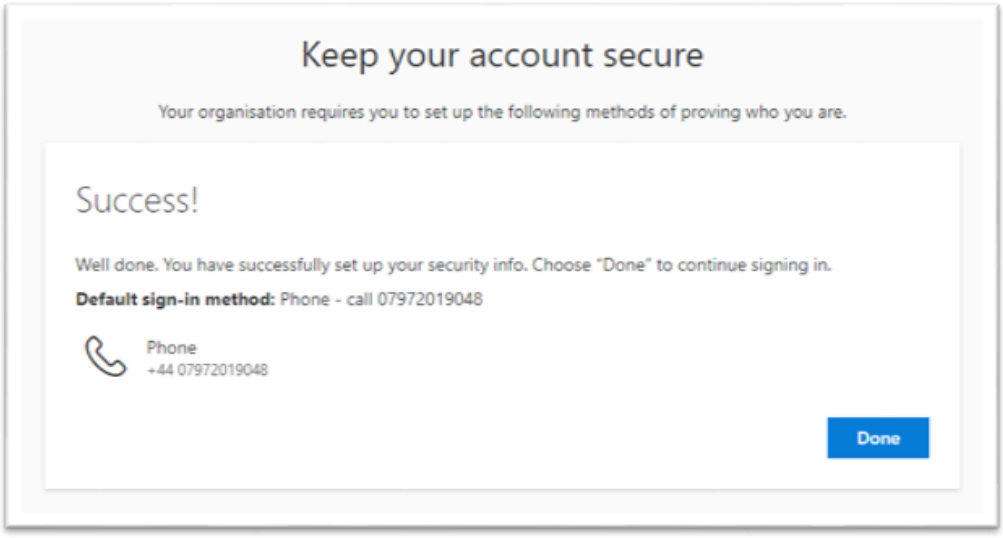
52. You will now be called on the number you provided. Answer the call. You will be asked to press the hash key on your phone – do this.



53. You should now get the following message:

54. Click **Next**.

55. The **Success!** page will now appear. You have set up the phone or 'call me' method of MFA



56. Click **Done** and in your browser, go to http://outlook.office.com for Outlook on the web and http://teams.microsoft.com for Teams web app.

57. You'll get the following message:

58. Your phone should ring.

59. Answer it and press the hash key on your phone.

60. You should now see your Outlook email account.

61. You should be able to log in to Outlook on any compatible device but you'll need access to your phone to login.

Managing your account

When you've set up your work email account on your personal device(s), please check each time to make sure you're sending your email from the correct account. This is to protect you, and the Council.

Further support

You can also:

- view short training videos on how to use Outlook on the web
- read guides on how to get started on the Outlook on the web.
- view and read Teams training

Reporting issues

If you have any issues with setting up multi factor authorisation or Outlook web access, please call the CGI helpdesk on 0800 085 7232.