Last Updated: 4th November 2022

Multi-Factor Authentication (MFA) for SGUL Staff and Students

Introduction

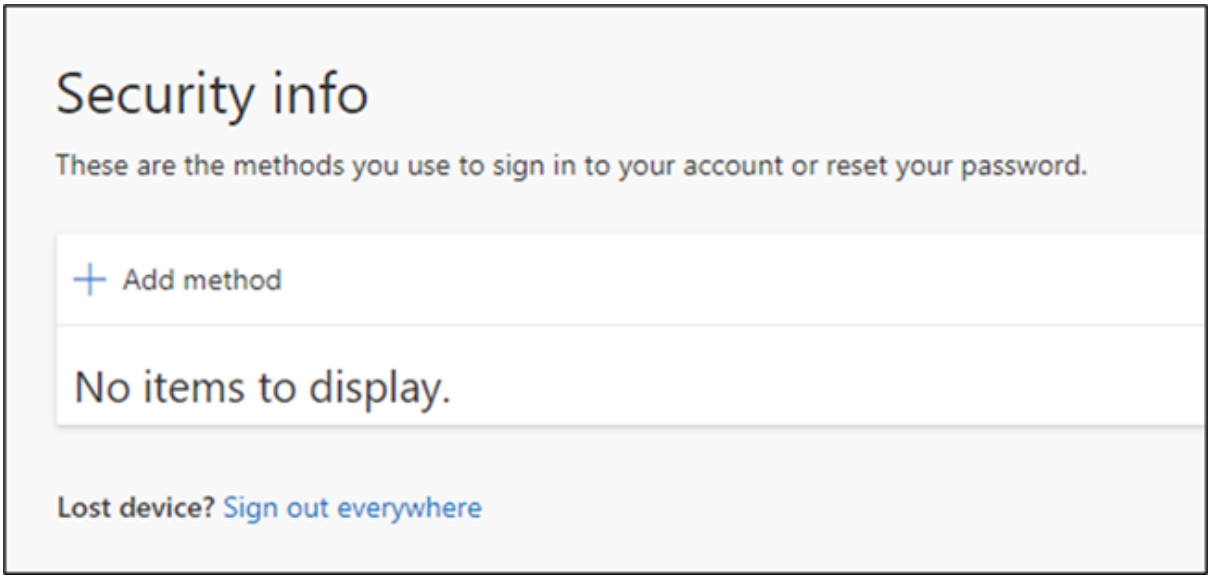
Multi-factor authentication (MFA) adds an extra layer of security when using online services. It requires users to provide more verification factors to gain access. This is often set up for online services that need extra security such as accessing your personal email or online banking.

At St. George's, MFA will be required when accessing any Office365 app for the first time on a particular computer or device, such as Teams. Please note that once you have successfully signed in with MFA on a device, it will remember that device so you will not be prompted to sign in with MFA every time you want to use an Office365 app. You will only be prompted for MFA when you are logging into Office365 apps from a new location or device.

How to set up MFA

You will be able to set up your Office365 additional sign-in methods prior to the IT department enforcing MFA on your Office365 account.

- Visit mysignins.microsoft.com/security-info and log in with your full email address and password.
- Select Add method.



You can then select an additional sign-in method from the following:

- Authenticator App
- Phone
- Office Phone
- Security Key

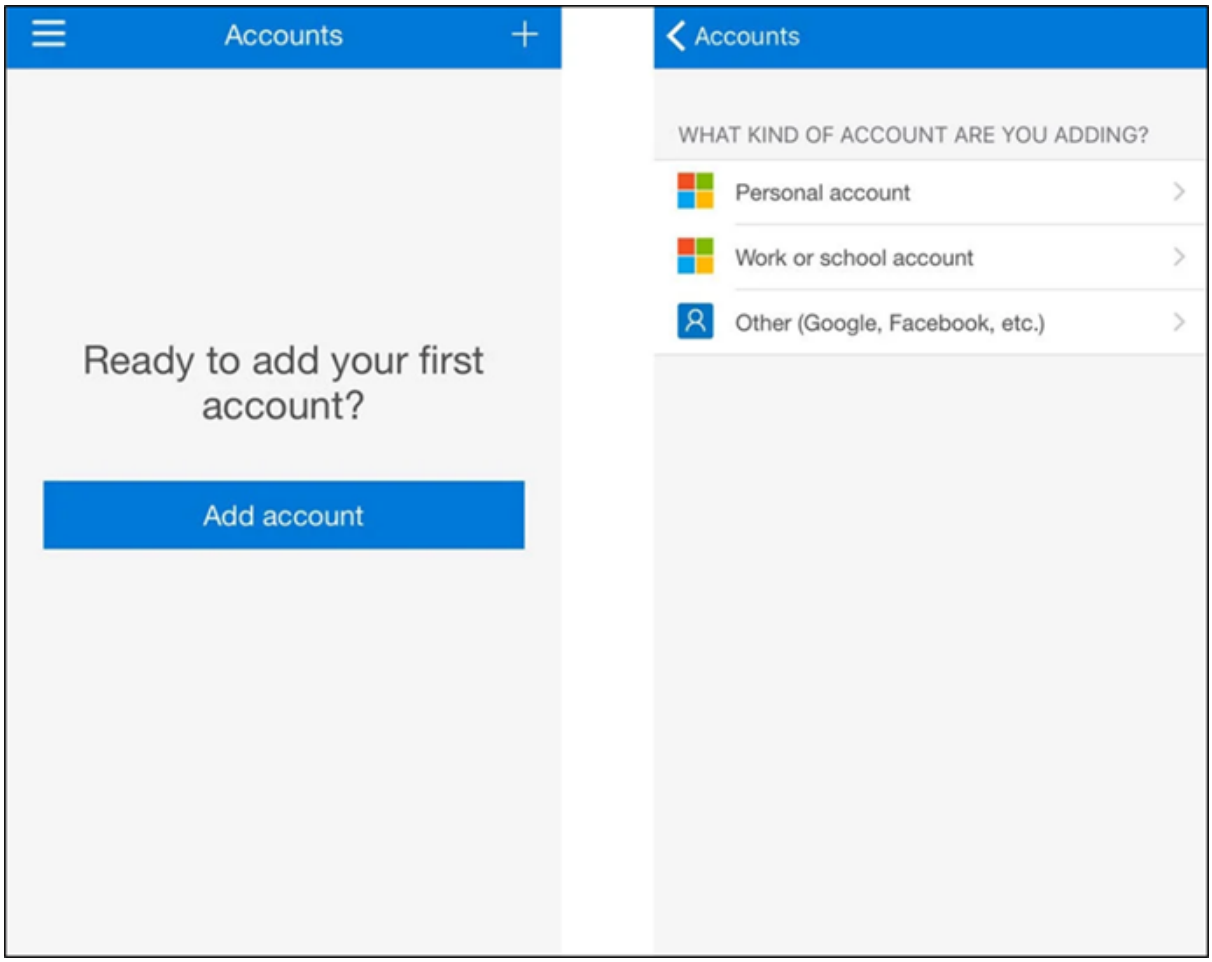
The additional sign-in methods on this page below are ordered from our most preferred to least preferred. Therefore, we recommend the Microsoft Authenticator App as your primary additional sign-in method.

Note: You should add more than one multi-factor authentication method in the event your initial method is unavailable.

Method 1: Microsoft Authenticator App

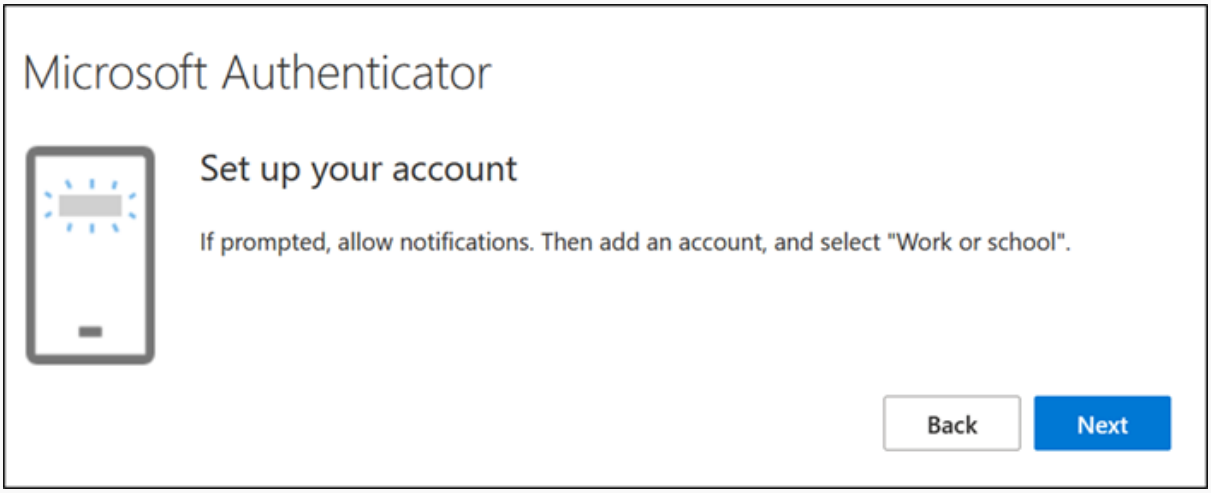
- Install the Microsoft Authenticator App on your phone.
  - Scan the QR code below to take you directly to the app, or search for Microsoft Authenticator in the Play Store (Android) / App store (iPhone).

Once the app is installed, select Add Account then Work or school account, then select Scan a QR Code. Enable Camera Permissions if needed.

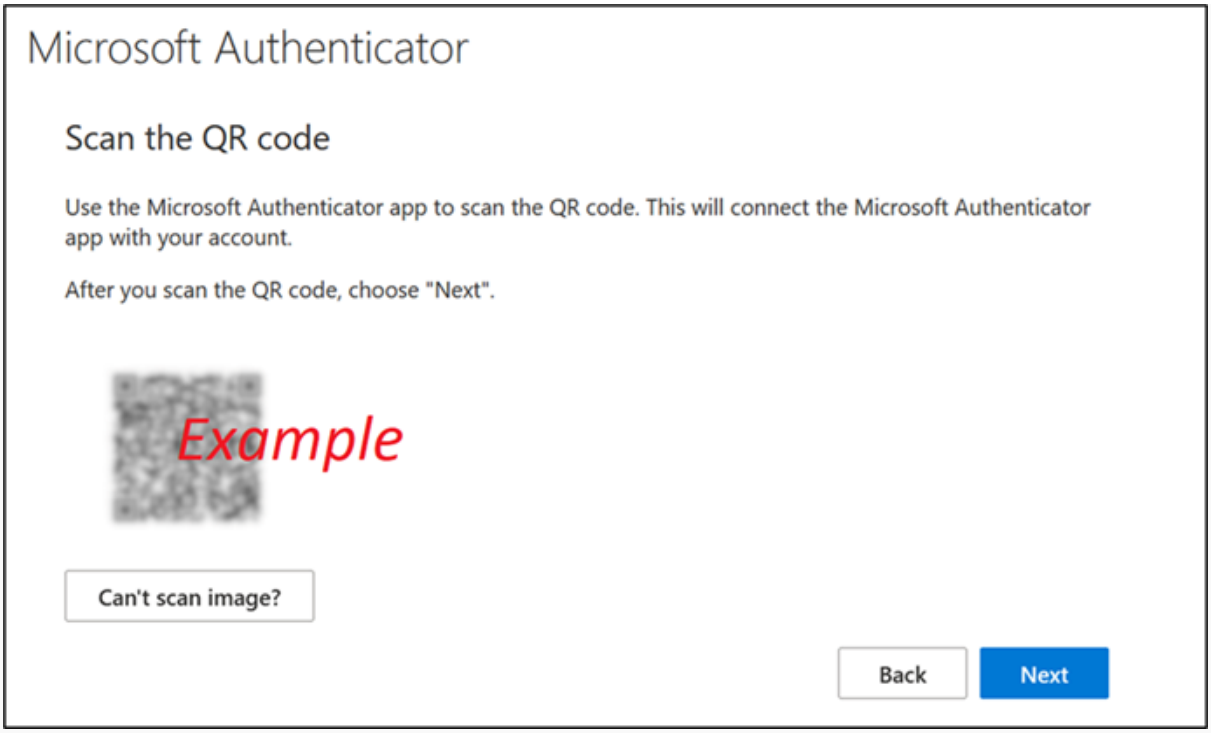


- Switch to your browser then click Next.

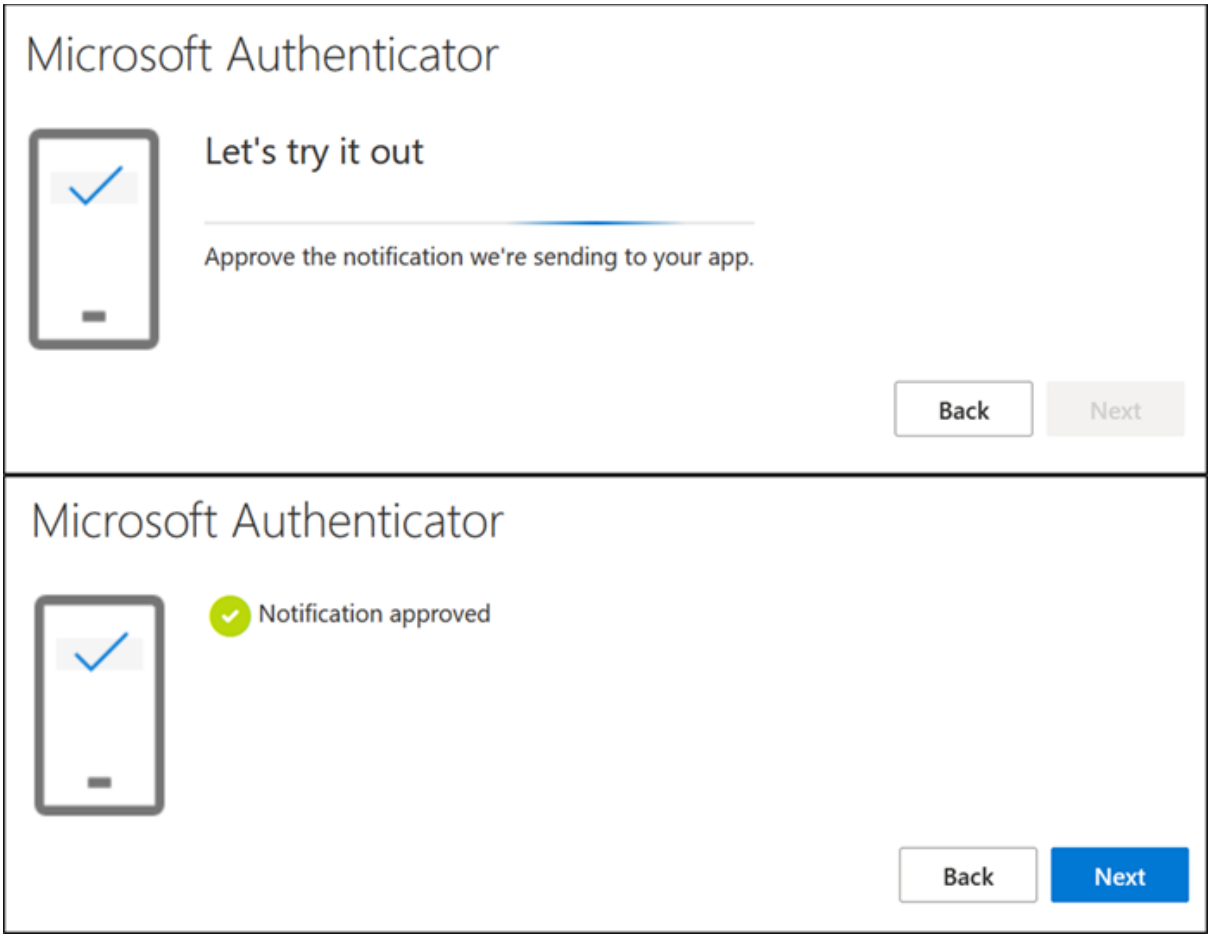
Click Next.



- A QR code prompt will appear in your browser. Use the Authenticator App to scan the code. After scanning, click Next.

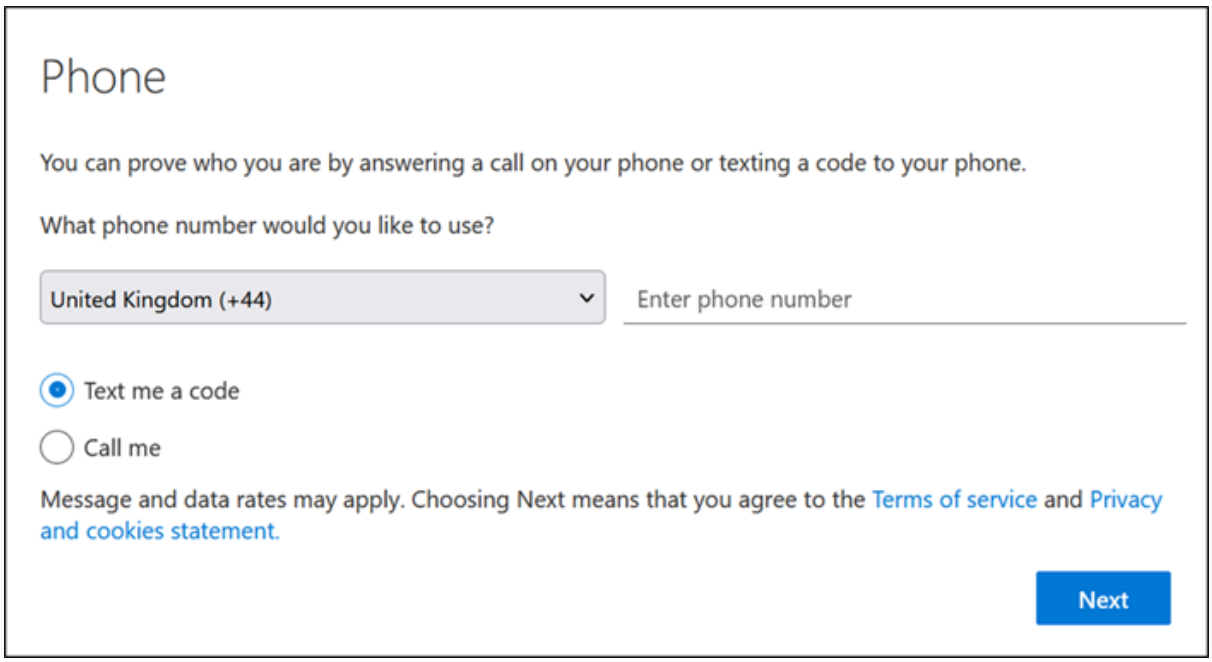


- Afterwards, you will receive a test notification. Press Approve on your phone then click Next on your browser.



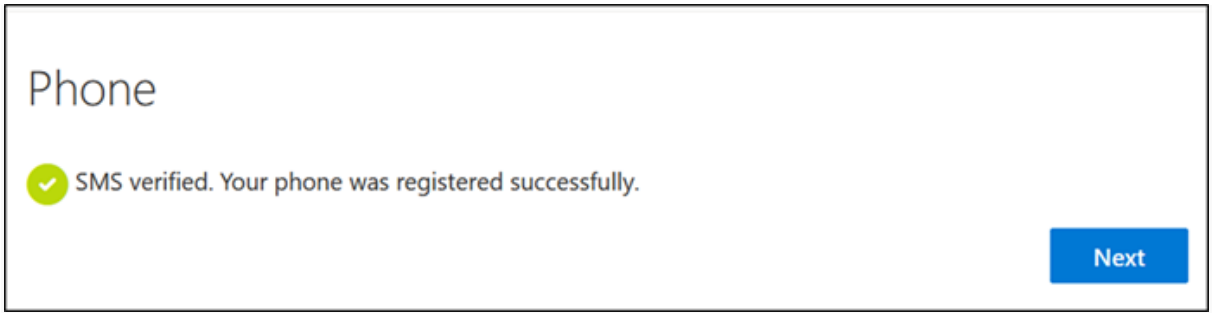
Method 2: SMS

- Select your phone's Country code and enter your mobile phone number, then select Text me a code.



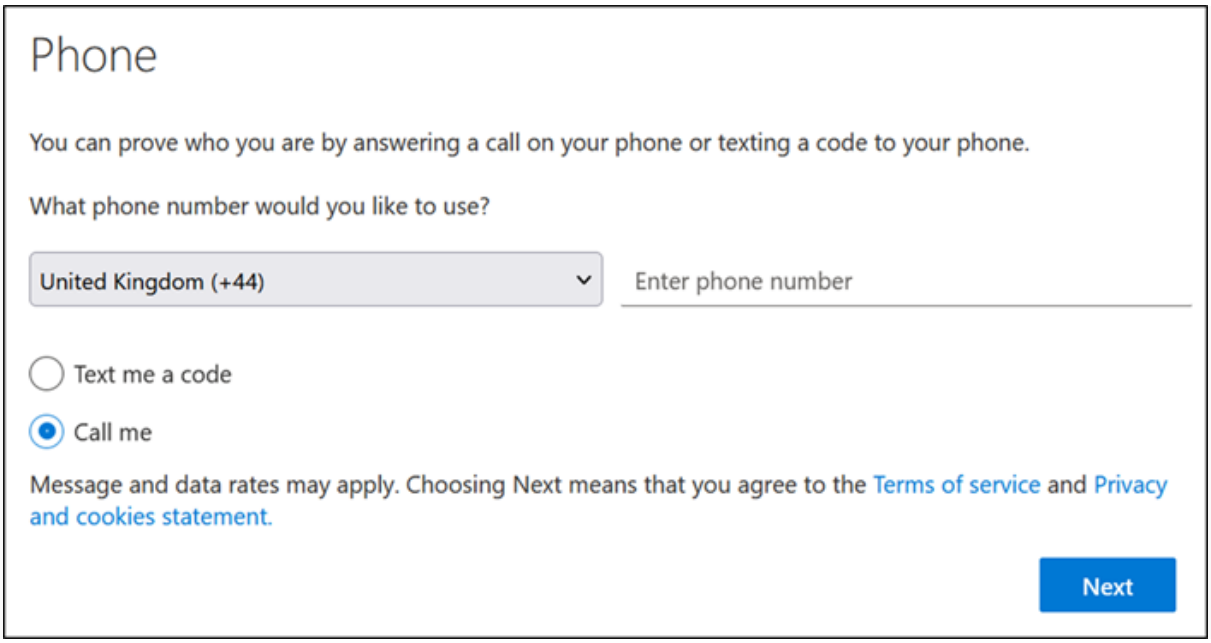
- Click Next, you will receive a 6-digit code via text from Microsoft. Enter the code given via text and click Next.

- You will see a confirmation that you are SMS verified. Click Next.



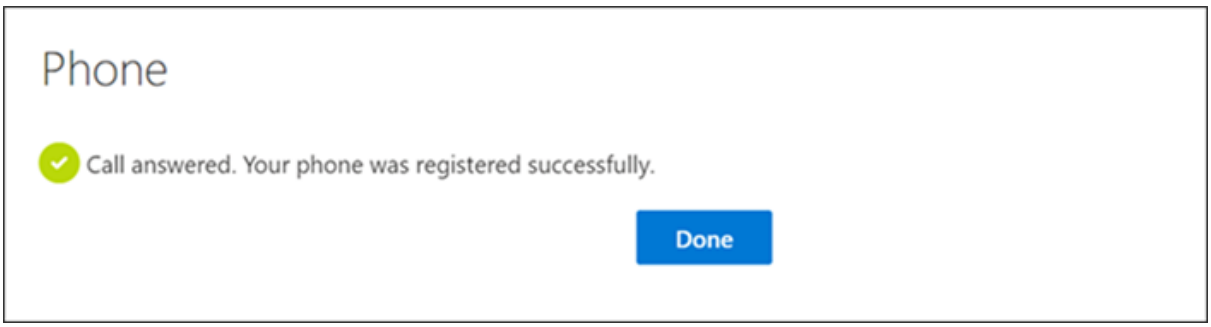
Method 3: Phone Call

- Select your phone's Country code and enter your mobile phone number, then select Call me and Next.



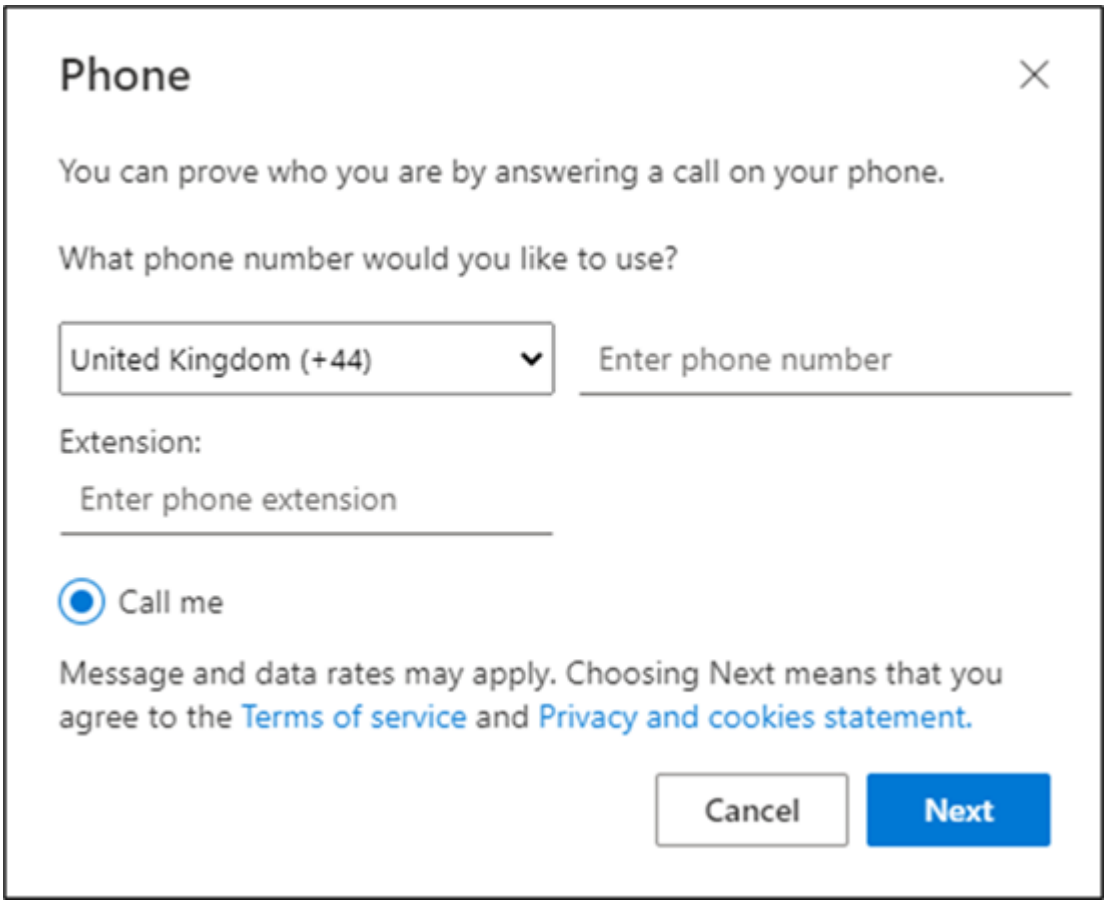
- Shortly, you will receive an incoming call asking you to enter the Hash key. This is also known as the Pound key.

- You will see a confirmation message of your call answered. Click Done.



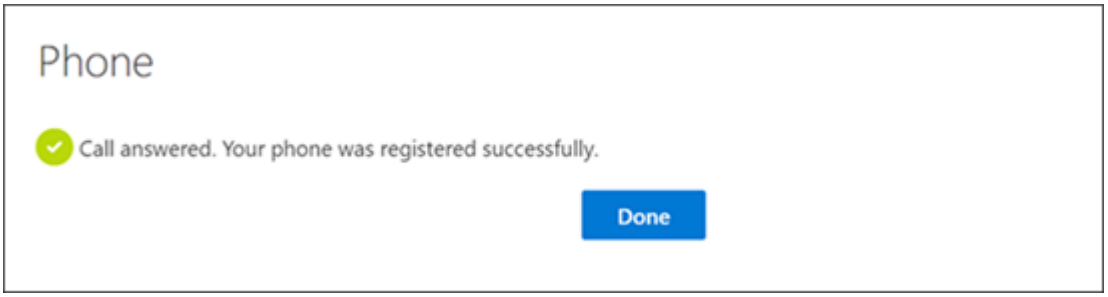
Method 4: Office Phone

- Select United Kingdom (+44) and enter your office landline number and your extension number.



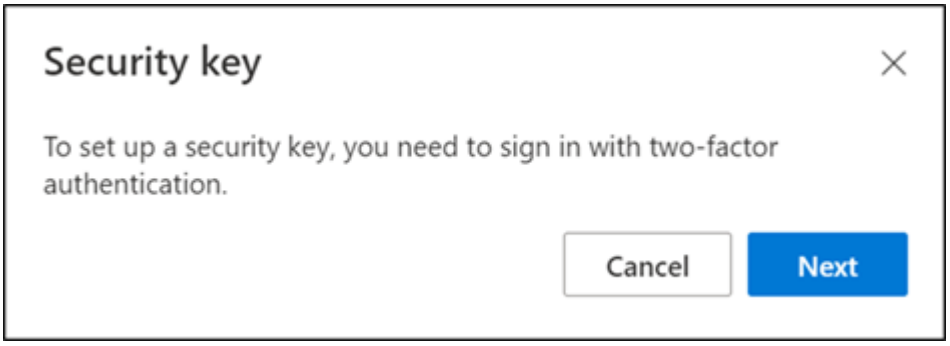
- Shortly, you will receive a call that begins with 4 clicks. You will then be prompted to press the Hash key to continue, followed by another prompt to press the hash key to verify the call.

- You will see a confirmation message of your call answered. Click Done.



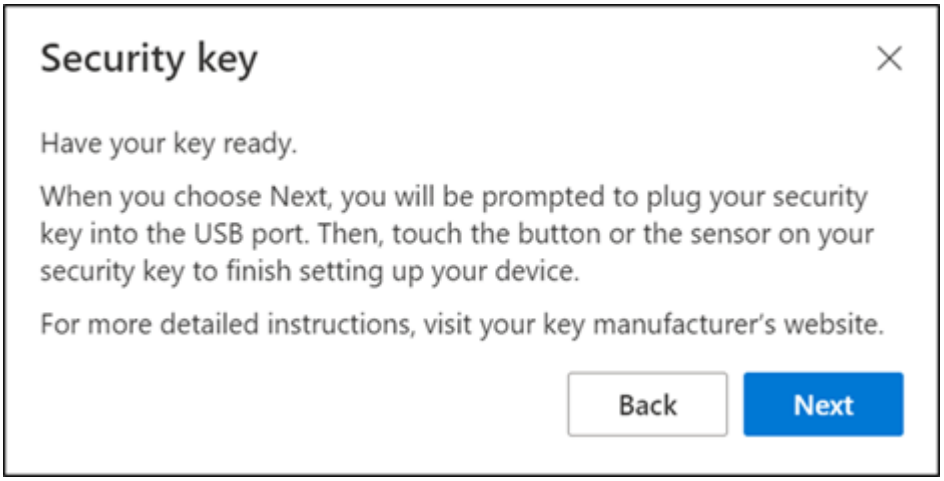
Method 5: Security Key

- Note: This additional sign-in method requires at least one other verification method set up beforehand. To use a security key for MFA, you will need to log a ticket with ITAV support to discuss how the other methods will not be sufficient as additional sign-in methods.
- Note: To register a Yubi key you must use a browser that supports FIDO2 security keys, such as Microsoft Edge.
- Sign in with a two-factor authentication.

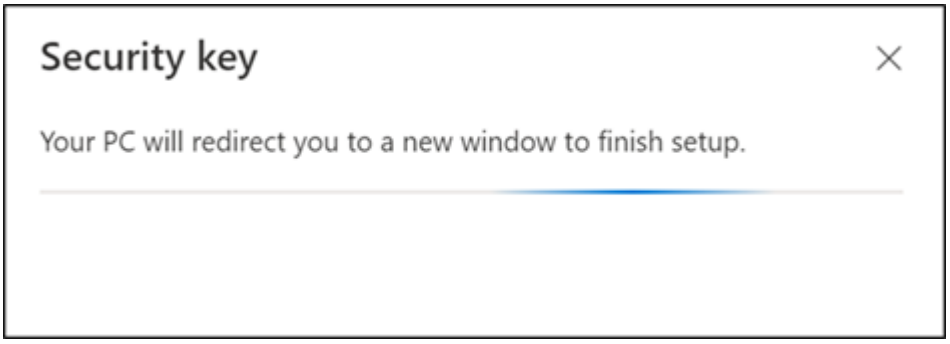


- Once logged in, select USB device.

- You will be prompted to have your key ready. Click Next.

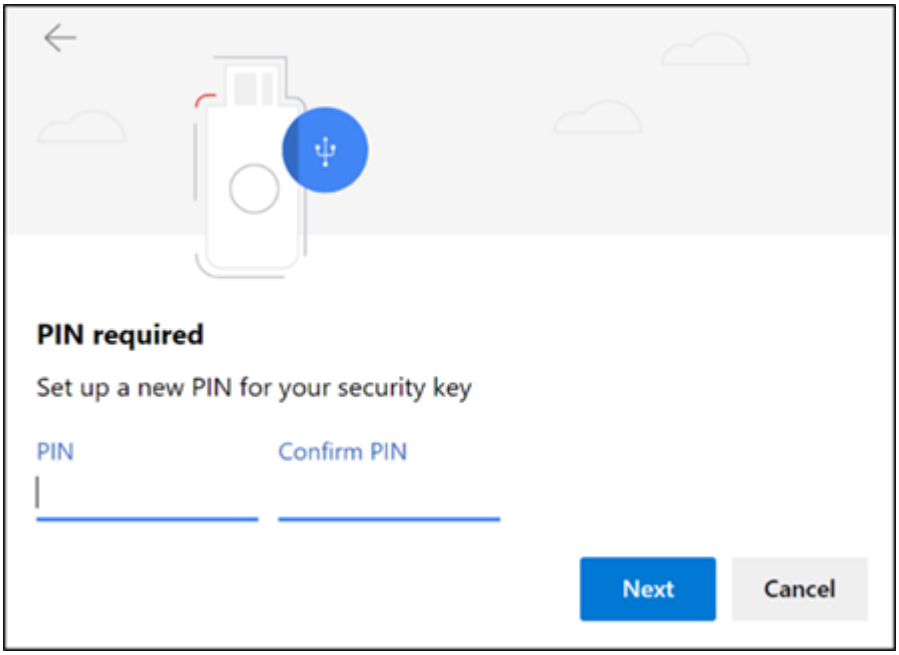


- Shortly, a new window will appear to set up your Yubi key.

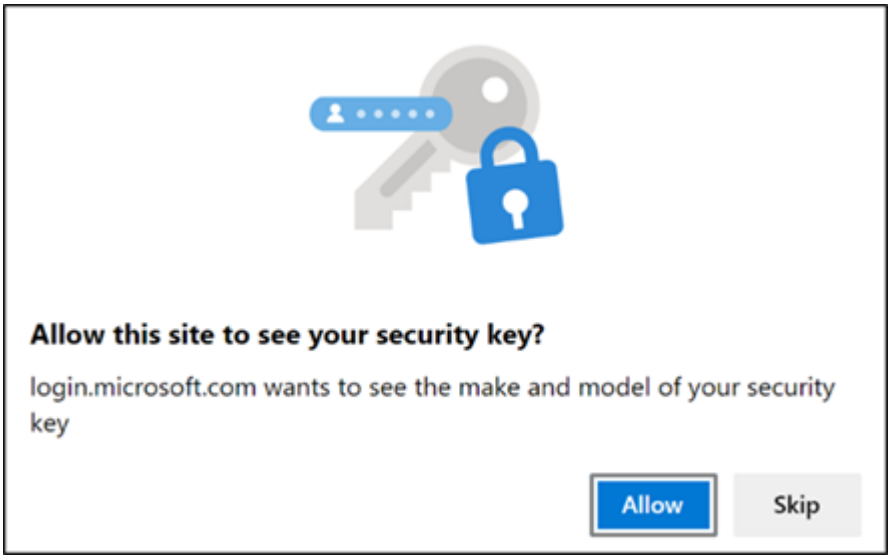


- Insert your Yubi key into an available USB slot and touch the gold circle.

- You will be asked to set up a new PIN for your Yubi key. Create a PIN then retype your PIN to confirm it. Click Next.

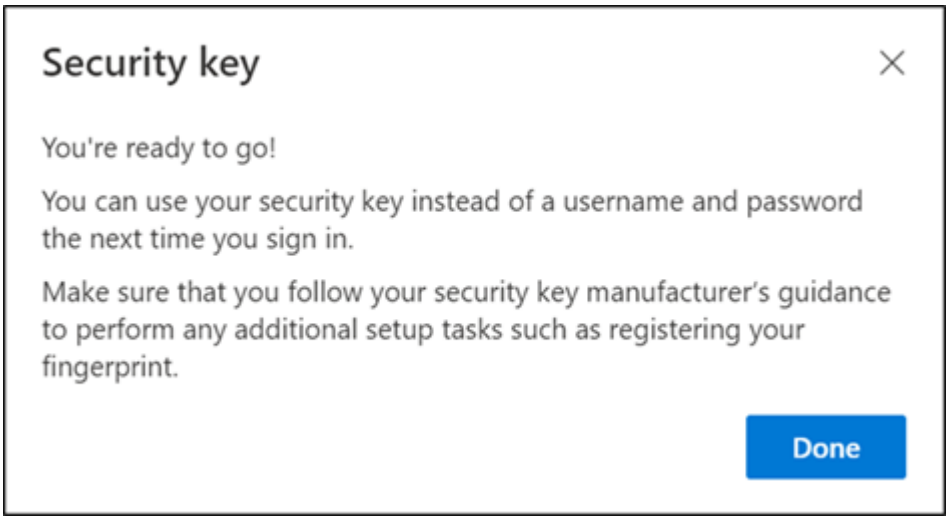


- Microsoft will ask to be allowed to see your Yubi key. Click Allow.



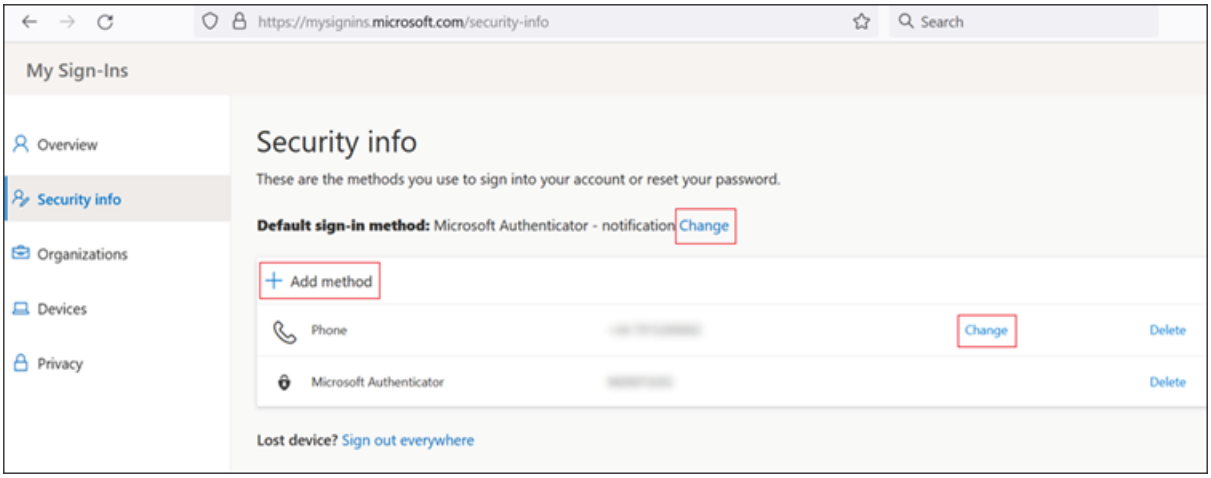
- Lastly, name your Yubi key. Click Next.

- You will see a confirmation message for setting up your Yubi key. Click Done.



Managing your MFA settings

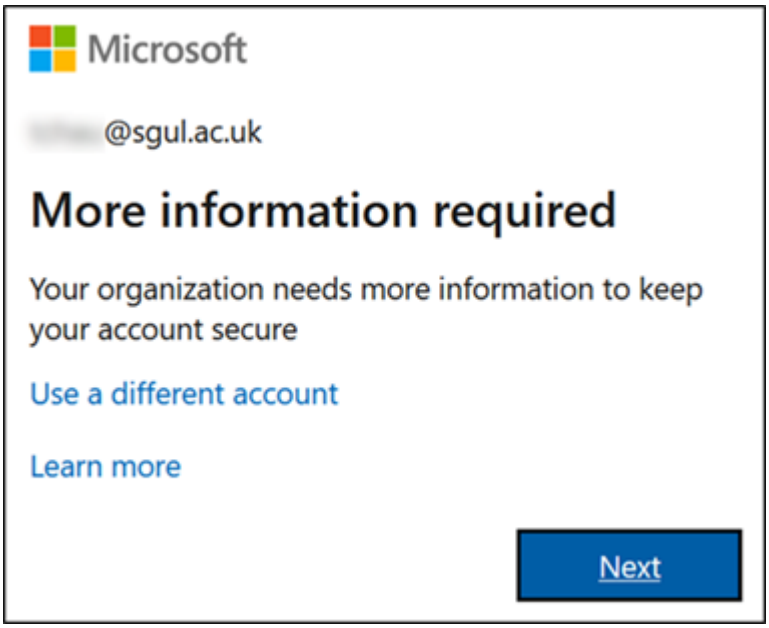
Once your multi factor authentication has been completed, you will not be prompted to authenticate again unless you are signing in on a new location or device. If you wish to add or change any of these authentication methods, for example changing a phone number, visit mysignins.microsoft.com/security-info. From the Security info page, you will be able to add, delete and change default sign-in methods.



Note: If you remove all MFA options whilst your account is enrolled into MFA, the next time you log in to Office 365 apps you will be prompted to add at least one additional verification method (see below).

What if I have already been enrolled into MFA without adding additional sign-in methods?

If your account has already been enrolled into multi-factor authentication without adding a second sign-in method, it will ask you for More information required the next time you log into an Office365 app. Click Next and enter your SGUL password to verify your login and continue. You can then choose how to set up your multi-factor authentication via a drop-down menu.



If you require further assistance with regards to Office365 MFA, please contact ITAV Support or visit our helpdesk at J0.27 on Monday - Friday between 12 and 2 pm.