



MFA for Guest Microsoft 365 users

Contents

Background.....	1
What is the process for guests?	1
Setting up MFA as a Guest	2
Authentication methods	3
‘Additional security verification’ screen.....	4
‘Keep your account secure’ screen	8
Help and support.....	10

This user guide is for guest users to set up Multi-Factor Authentication which will be required to access the UK University of Nottingham Microsoft 365 services.

Background

Multi-Factor Authentication (MFA) is an extra layer of protection. To ensure the data and information shared within the Microsoft 365 service is secure, the University of Nottingham requires all users (including guests) to provide secondary authentication to gain access.

Who is a guest?

A guest is anyone outside of the UK University of Nottingham network, e.g. a user without an @nottingham.ac.uk email address.

What is the process for guests?

When a member of the university shares a file, folder or invite to a Teams / SharePoint site with a guest, they are asked by Microsoft to verify their identity.

Guests will be asked to set up MFA for enhanced security and data protection.

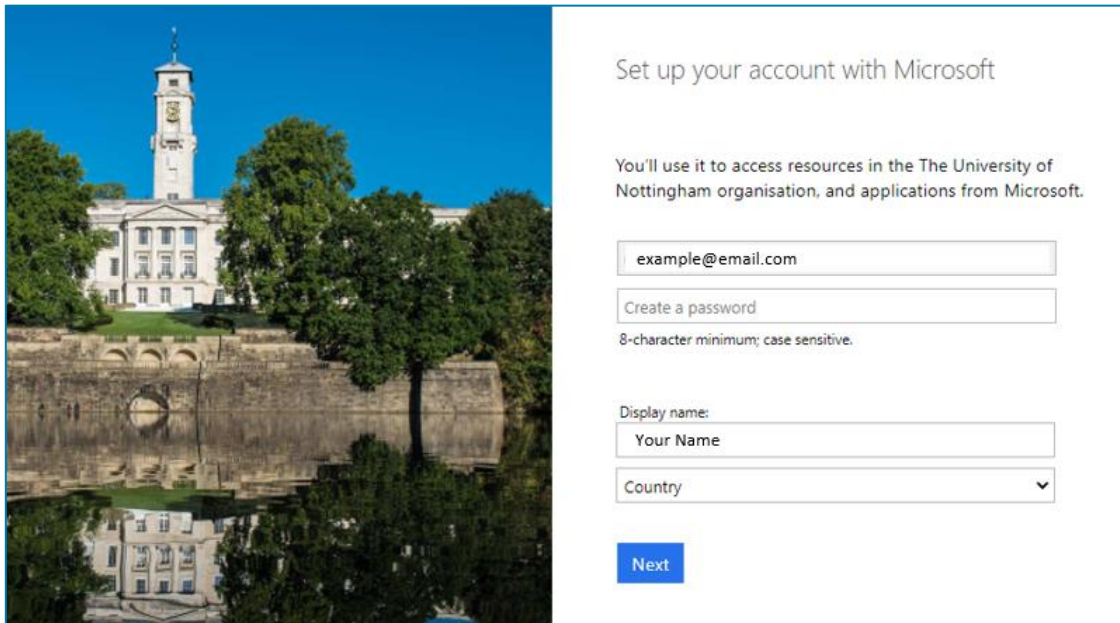
Please use the instructions in this guide to help you set up MFA when prompted.

Setting up MFA as a Guest

To start the process of setting up MFA, click on a link shared with you by someone within the University of Nottingham.

As a “Guest”, if your account is already a Microsoft 365 account, you will be first asked to review permissions as shown in point 1. below.

If you **don't** have a Microsoft account, you will be asked to set up your external account with Microsoft. Create a password and enter your display name, then click Next.



Set up your account with Microsoft

You'll use it to access resources in the The University of Nottingham organisation, and applications from Microsoft.

example@email.com

Create a password

8-character minimum; case sensitive.

Display name:

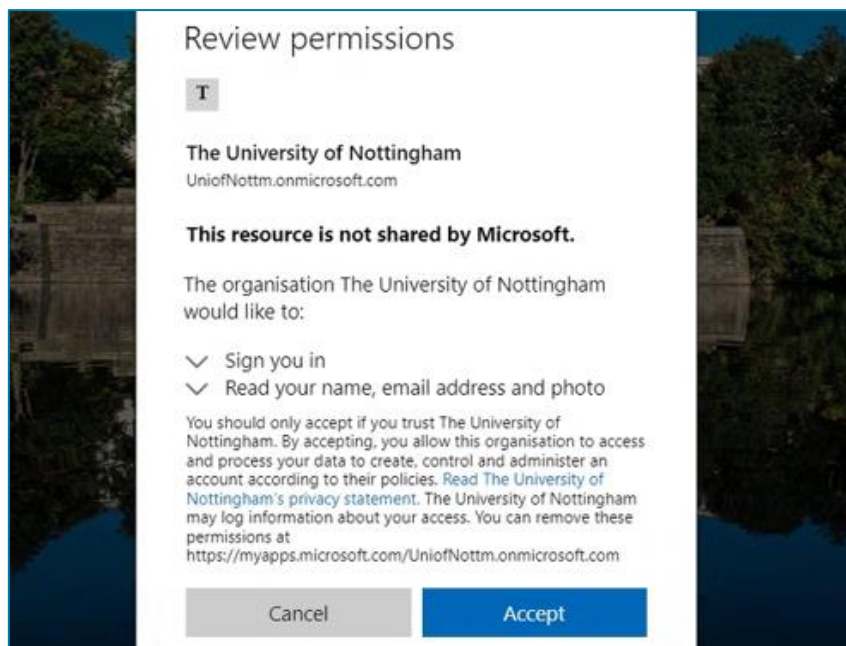
Your Name

Country

Next

Now that your account is linked to Microsoft, you can proceed to point 1. below.

1. After you click the link shared with you, you will be asked to 'Review permissions', click **Accept**



Review permissions

T

The University of Nottingham
UniofNottm.onmicrosoft.com

This resource is not shared by Microsoft.

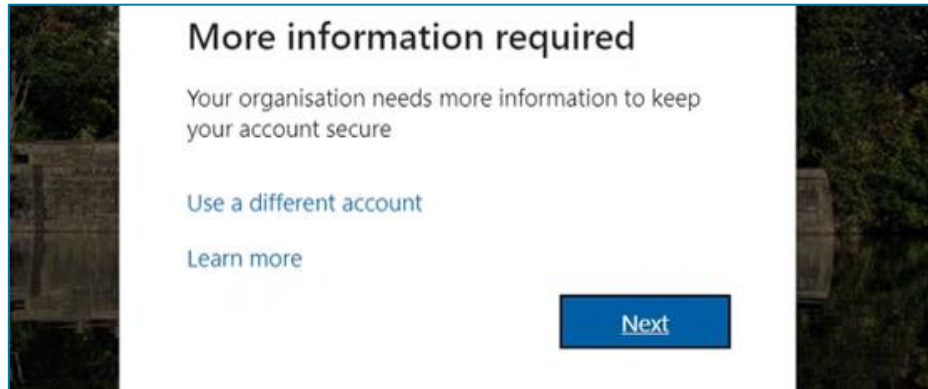
The organisation The University of Nottingham would like to:

- ✓ Sign you in
- ✓ Read your name, email address and photo

You should only accept if you trust The University of Nottingham. By accepting, you allow this organisation to access and process your data to create, control and administer an account according to their policies. [Read The University of Nottingham's privacy statement.](#) The University of Nottingham may log information about your access. You can remove these permissions at <https://myapps.microsoft.com/UniofNottm.onmicrosoft.com>

Cancel Accept

2. You may be asked which app you wish to open in, e.g., Word, Teams or web app etc., select your preferred option when asked.
3. If your organisation uses Microsoft 365, you will be redirected to your own organisations log in page. Log in with your appropriate username and password. Otherwise, log in with the Microsoft password linked to your external account.
4. Now you will be asked for more information to secure your account, click **Next**



5. Depending on your account type, you will be directed to either the '**Additional security verification**' screen or the '**Keep your account secure**' screen.

Follow the relevant guidance below depending on which set up screen you are directed to:

- [Additional security verification](#)
- [Keep your account secure](#)

Authentication methods

When setting up MFA, there are a variety of ways to approve authentication. This will depend on the device you have and your preferred method, as listed below:

Method	Description
Microsoft Authenticator app	This is the recommended method as it offers the best experience if using a smartphone. It can be used for push notifications or verification code.
Verification code	This method can be used with the Microsoft app or other alternate third-party verification apps.
Text message	This is a simple method; however, it does require mobile phone signal to receive an SMS text.

Set up instructions

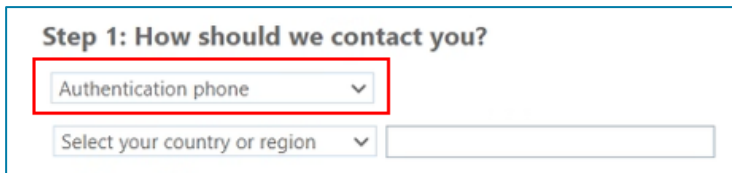
'Additional security verification' screen

Setting up Microsoft Authenticator app

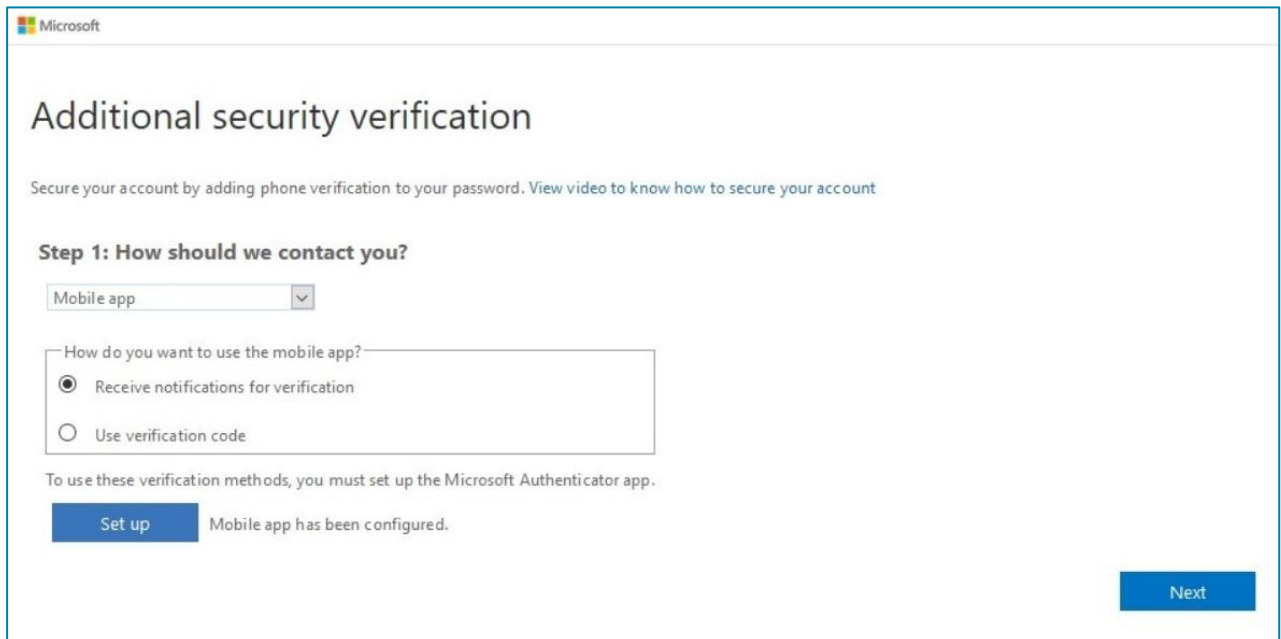
Our recommendation is for Guests to use the Microsoft Authentication app because it is the only authenticator app that supports push notifications.



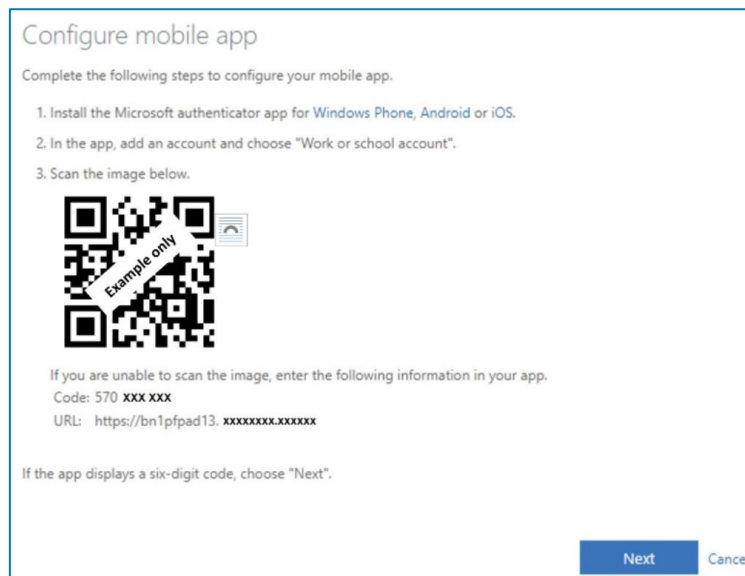
1. Firstly, download the Microsoft Authenticator app from your smartphones App Store
2. Once installed, on the 'Additional security verification' screen on your computer, under Step 1, select the 'Authentication phone' drop-down menu and choose the **'Mobile app'** option.

A screenshot of the "Step 1: How should we contact you?" screen. It features a dropdown menu with "Authentication phone" selected, which is highlighted by a red rectangular box. Below it is another dropdown menu labeled "Select your country or region" followed by an empty text input field.

If you do wish to set up text message as the authentication method, skip to page 7.

A screenshot of the "Additional security verification" screen. The title "Additional security verification" is at the top. Below it is a sub-header "Step 1: How should we contact you?". A dropdown menu shows "Mobile app" selected. Below that is a section titled "How do you want to use the mobile app?" with two radio button options: "Receive notifications for verification" (which is selected) and "Use verification code". At the bottom, there is a blue "Set up" button and a message "Mobile app has been configured." A "Next" button is located in the bottom right corner.

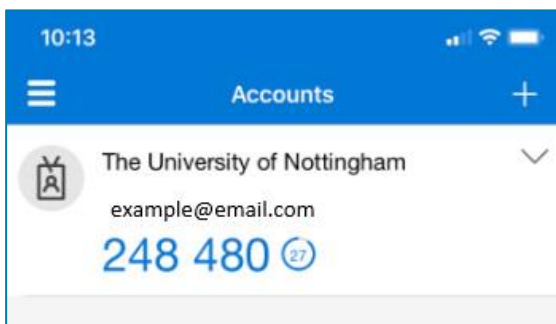
- To use the Microsoft Authenticator app, leave the option **'Receive notifications for verification'** selected for push notifications.
 - Select 'Use verification code' if you wish to use an alternative authenticator.
3. Click the **'Set up'** button. The 'Configure mobile app' screen will appear with a QR code for you to scan with the Microsoft Authenticator app on your mobile device.



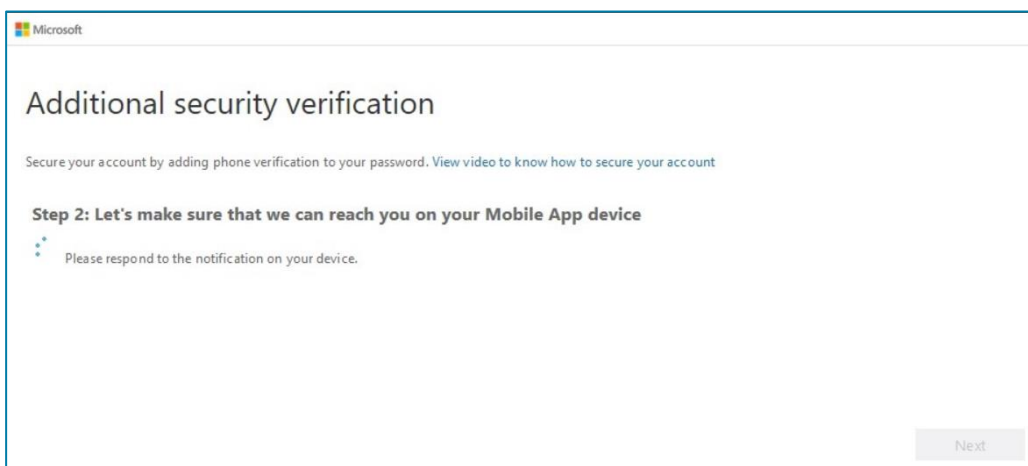
4. Open the Microsoft Authenticator app on your mobile, select **Add account** on the Accounts screen and then select **Work or school account**. Now use the mobile device's camera to scan the code displayed on your computer.

Note: if the camera wasn't working properly, the on-screen Code and URL can be entered manually.

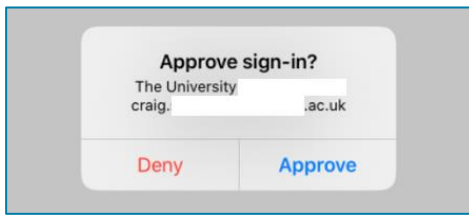
5. The Accounts screen of the app shows the account name and a six-digit verification code. For additional security, the verification code changes every 30 seconds preventing you from using the same code twice.



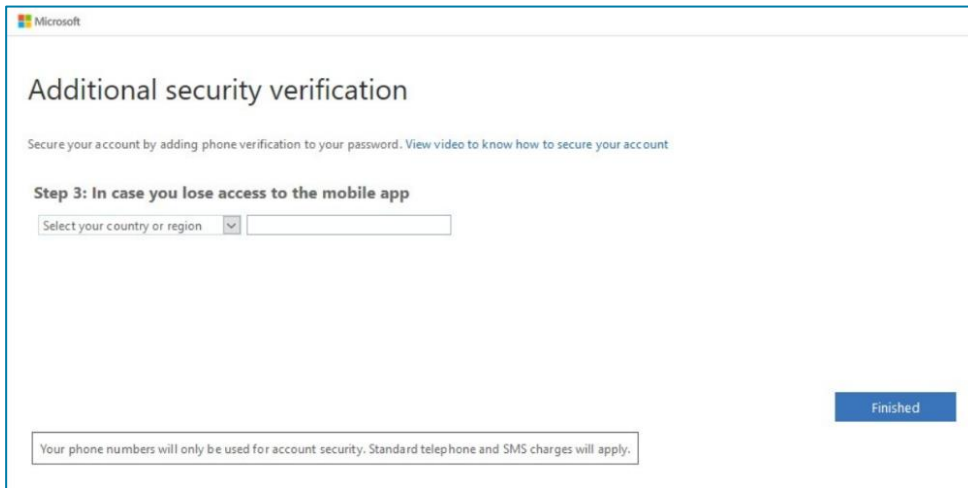
6. On the computer, click **Next** on the 'Configure mobile app' screen, and **Next** again on the 'Additional security verification screen'



7. A notification will be sent to the app on your mobile device, tap '**Approve**'



8. Once approved, you will be prompted on your computer to enter a mobile phone number. This is in case you lose access to the mobile app.



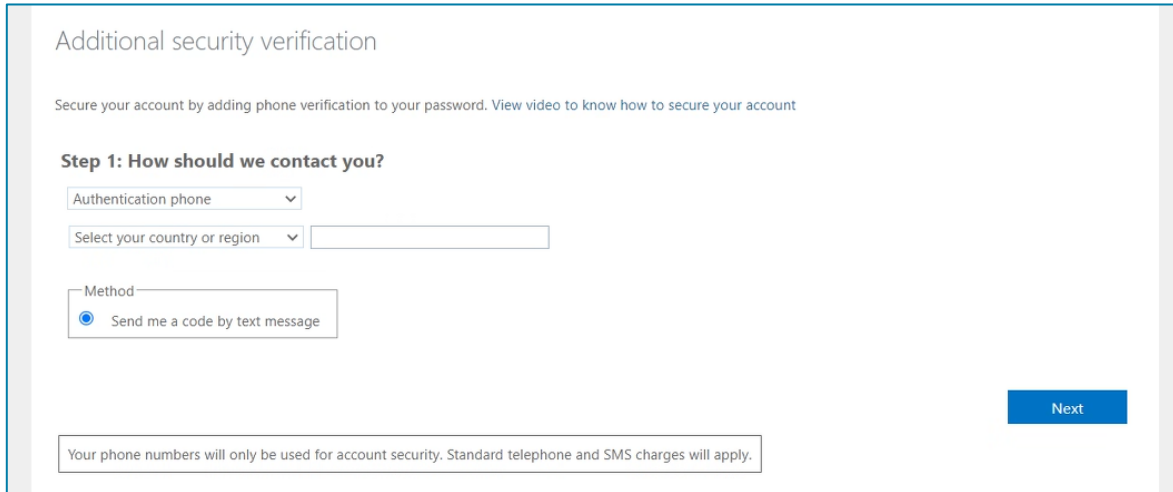
9. Click **Finished**

All the steps above are part of the initial set up and once this has been completed, you won't be asked again.

Setting up SMS text message

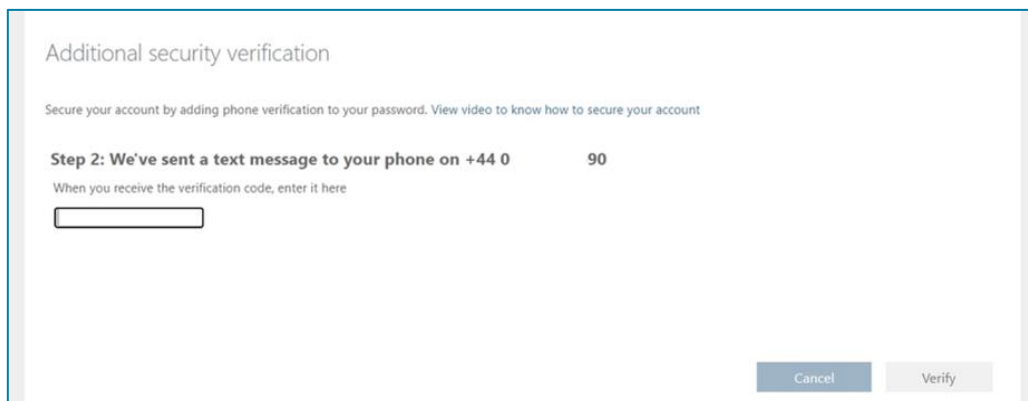
You can approve access by entering a code sent to your phone from Microsoft.

1. On the 'Additional security verification' screen on your computer, under Step 1, check that the 'Authentication phone' option is selected. Click **Next**



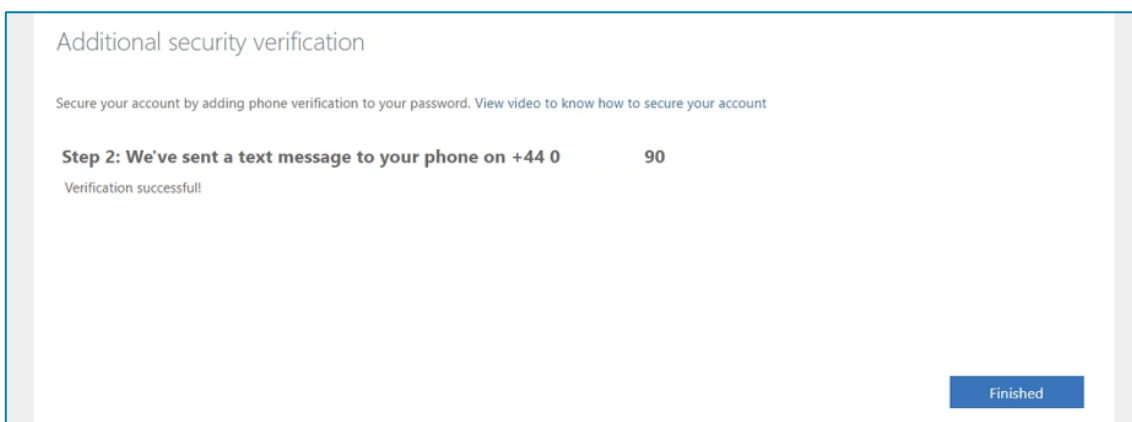
The screenshot shows the 'Additional security verification' screen. At the top, it says 'Additional security verification' and 'Secure your account by adding phone verification to your password. View video to know how to secure your account'. Below this is 'Step 1: How should we contact you?'. There are three main sections: 'Authentication phone' with a dropdown menu, 'Select your country or region' with a dropdown and an input field, and 'Method' with a radio button selected for 'Send me a code by text message'. A blue 'Next' button is in the bottom right. A disclaimer at the bottom states: 'Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.'

2. A code will be sent to your phone, enter the code on-screen and click **Verify**



The screenshot shows the 'Additional security verification' screen at Step 2. It says 'Step 2: We've sent a text message to your phone on +44 0 90'. Below this, it says 'When you receive the verification code, enter it here' and there is an empty input field. At the bottom right, there are 'Cancel' and 'Verify' buttons.

3. The next message should confirm verification is successful. Click **Finished**.



The screenshot shows the 'Additional security verification' screen at Step 2. It says 'Step 2: We've sent a text message to your phone on +44 0 90'. Below this, it says 'Verification successful!'. At the bottom right, there is a blue 'Finished' button.

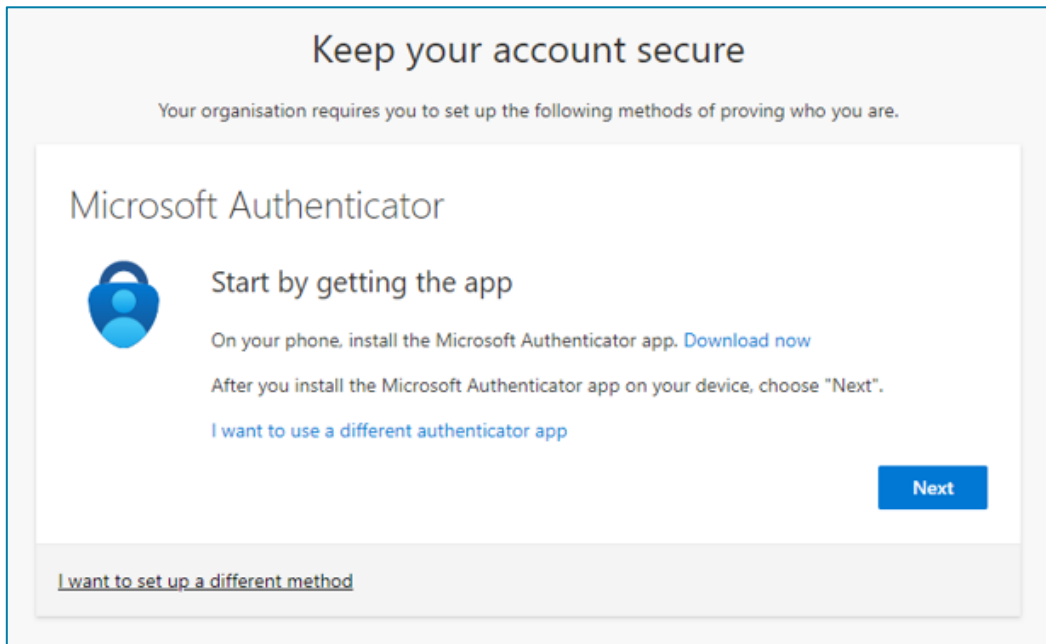
All the steps above are part of the initial set up and once this has been completed, you won't be asked again.

'Keep your account secure' screen

If you are directed to the 'Keep your account secure screen' on the mysignins.microsoft.com website, follow the onscreen instructions by clicking **Next** to set up the Microsoft Authenticator app (recommended).

You can also click 'I want to use a different authenticator app' if you already use an alternative third-party app.

You may also have the option 'I want to set up a different method', if available, you can use this to set up SMS text message authentication.

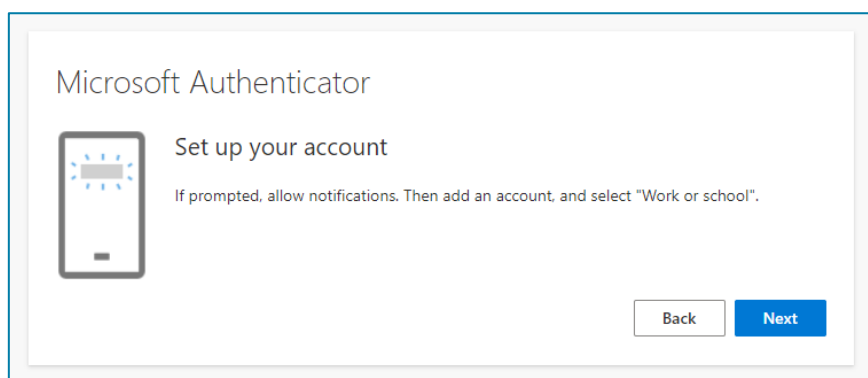


Our recommendation is for Guests to use the Microsoft Authentication app because it is the only authenticator app that supports push notifications.

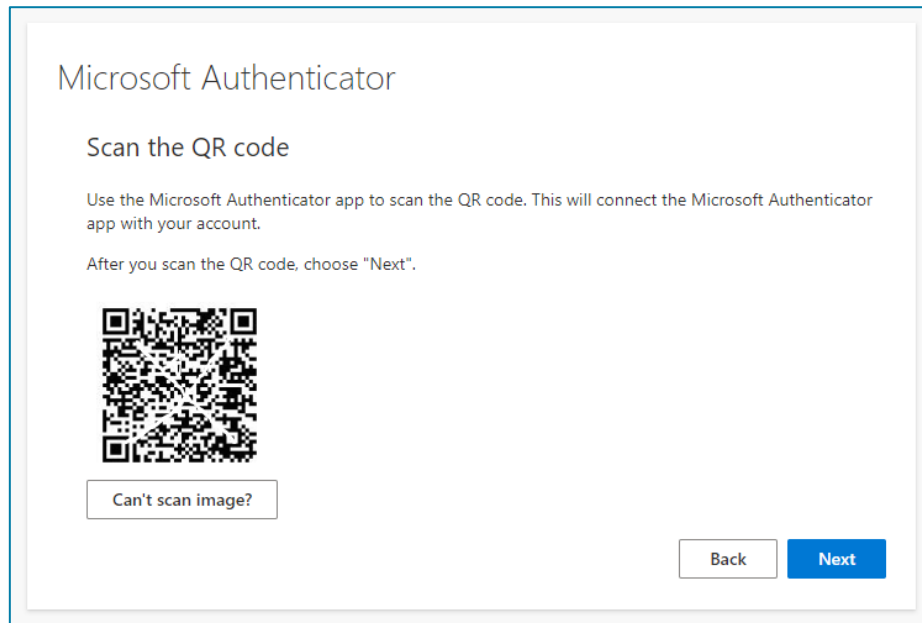
If you wish to use an alternate authentication app or method, follow the on-screen steps provided by Microsoft.

Setting up Microsoft Authenticator

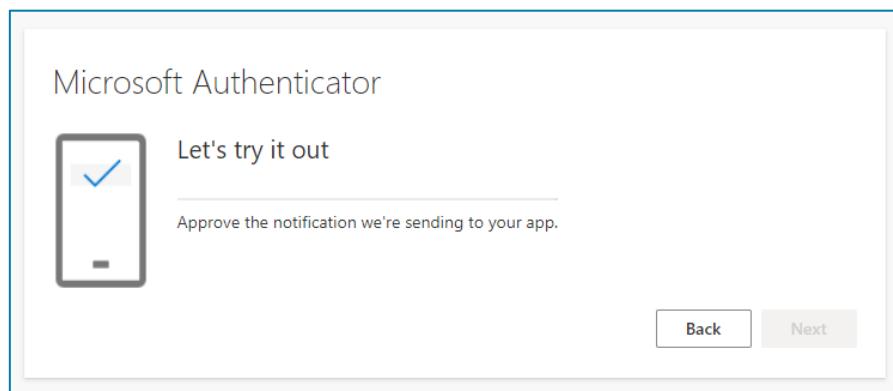
After clicking Next on the screen above, you will be asked to set up your account on the app.



1. Firstly, download the Microsoft Authenticator app from your smartphones App Store
2. On the app, add an account and select "Work or school" and then select the option 'Scan QR code'
3. On the next screen, scan the QR code displayed with your phone and click **Next**



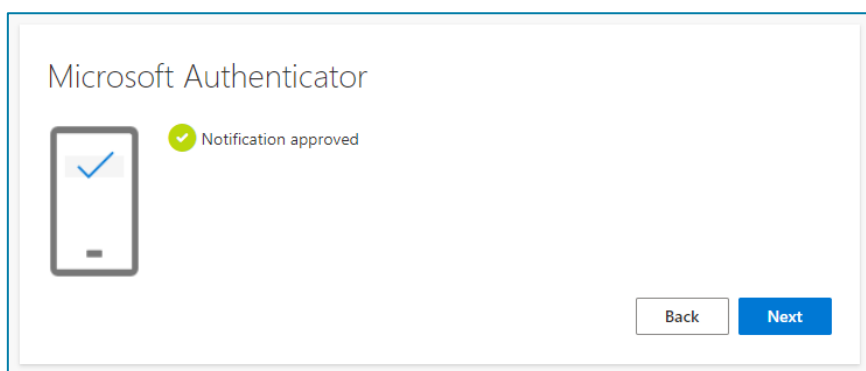
4. A notification will be sent to your app for approval



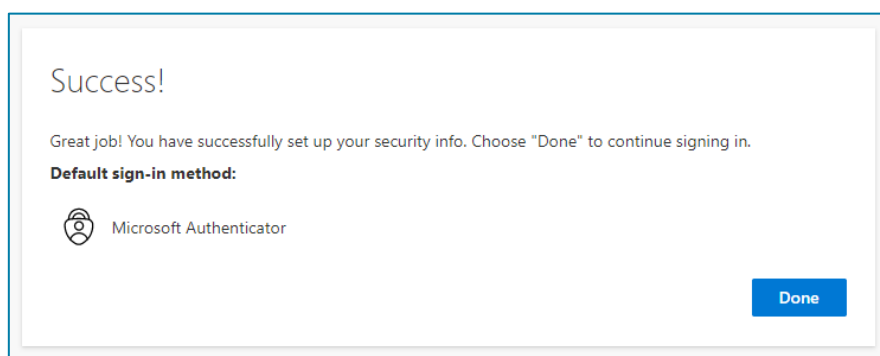
5. Tap **Approve** on your phone



6. Click **Next**



7. Click **Done** to finish the setup process.



If you wish to use an alternate authentication app or method, follow the initial on-screen steps provided by Microsoft.

Help and support

All staff and students at the University of Nottingham have been through the MFA set up process. In the first instance, please ask the person sharing information with you for support.

Secondly, many organisations and companies now use the same or similar two factor authentication methods, please ask your local IT team for support.

Thirdly, if you still require assistance, you can contact our [IT Service Desk](#) on +44 (0)115 95 16677, Monday to Friday 8am – 5pm. Please note that we can only provide limited support.