Multi-Factor Authentication – Guide

## What is Multi-Factor Authentication (MFA)?

MFA is the process of using two or more independent factors to verify your identity when logging into a BCU account - similar to what you may use with online banking or social media.

* The first factor is something known only to you - your BCU password.
* The second factor is a single use code sent to your personal device (mobile phone or tablet) OR a message sent asking for confirmation that you are attempting to log in.

## What are the benefits of MFA?

1. MFA gives you the ability to reset or change your BCU password yourself, from home.
2. MFA protects your personal data, BCU data and keeps the University secure against cyber-attacks.

Each year, cyber-attacks are becoming more sophisticated, and safeguarding our data has become more **crucial** than ever. Multi Factor Authentication is just one of the vital security measures in place as a solution to this.

Always remember that, as a member of the BCU community, you have a responsibility to **keep data secure** and be on guard against possible breaches and theft. See our tips for avoiding the common pitfalls on the [IT Security iCity page](https://icity.bcu.ac.uk/IT/Students/IT-Security).

## **Step-by-step Guides**

[First time signing in - Setting up MFA. 2](#_Toc127348902)

[Using the Microsoft Authenticator App 3](#_Toc127348903)

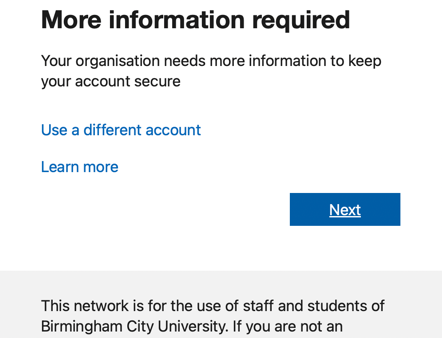
[IMPORTANT: Adding a secondary MFA option. 4](#_Toc127348904)

[How to change or add MFA methods. 4](#_Toc127348905)

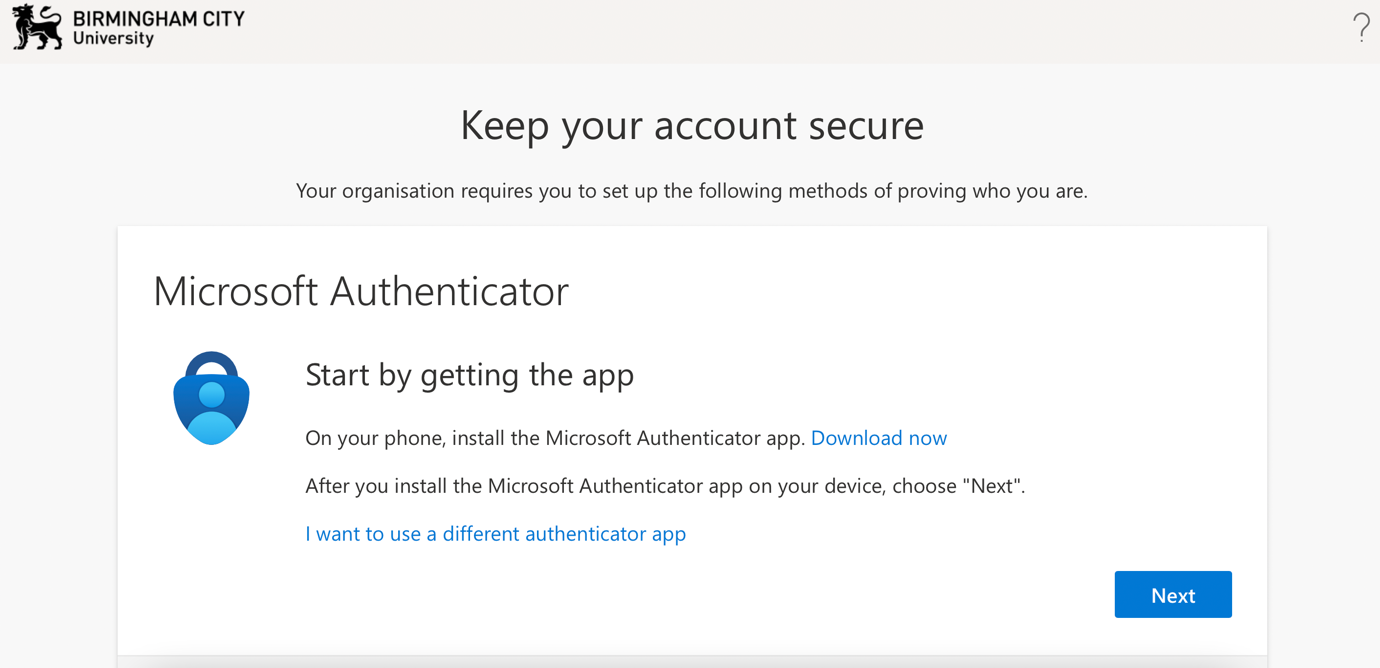
[Signing in after MFA registration 5](#_Toc127348906)

# First time signing in - Setting up MFA.

When you first sign into your University account, you will be presented with the following dialogue box asking you to set up MFA.



You will be instructed to use the BCU-recommended Microsoft Authenticator app, [available from the Google Play Store and the App Store](https://www.microsoft.com/en-us/security/mobile-authenticator-app#primaryR3). This is the most secure MFA method.



Click **Next**. You will now see a QR code on screen.

# Using the Microsoft Authenticator App

Download and install the Microsoft Authenticator App from the Google Play Store, App Store, or Windows Store onto your phone/tablet.



When you have opened the app on your phone/tablet, press the + button in the top right to add your BCU account.

Select **Work or school account**.

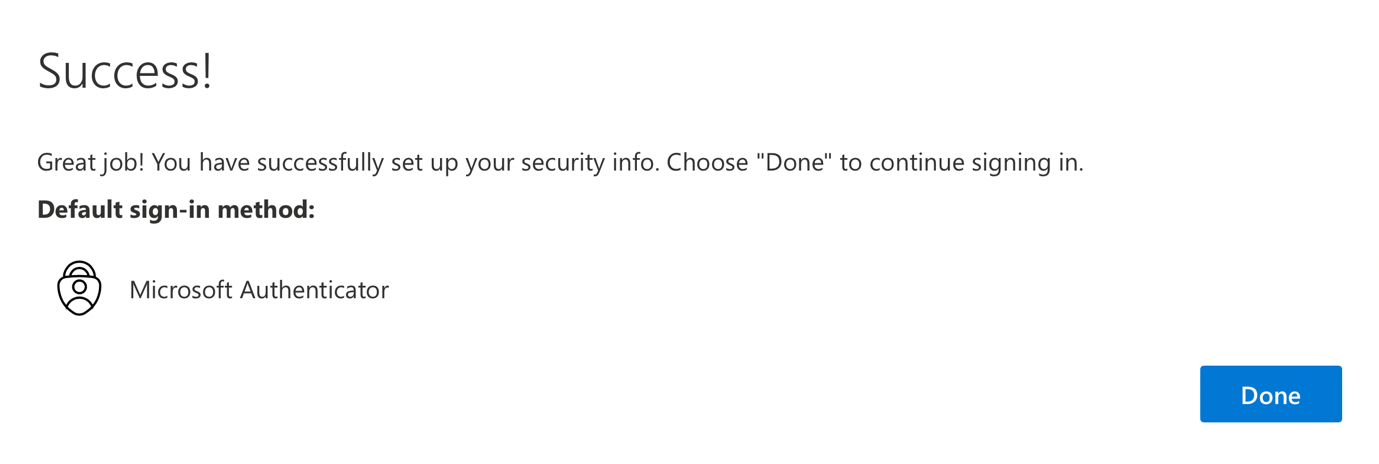
Select **Scan a QR code**.

Graphical user interface, text, application

Description automatically generated

The app will ask for permission to use your camera. Select **allow**.

Use your device’s camera to scan the QR code on your computer. This will link your Authenticator app to your BCU account, so that you can use it for MFA. You may also need to approve a notification on your Authenticator App.



Congratulations, you have successfully set up MFA.

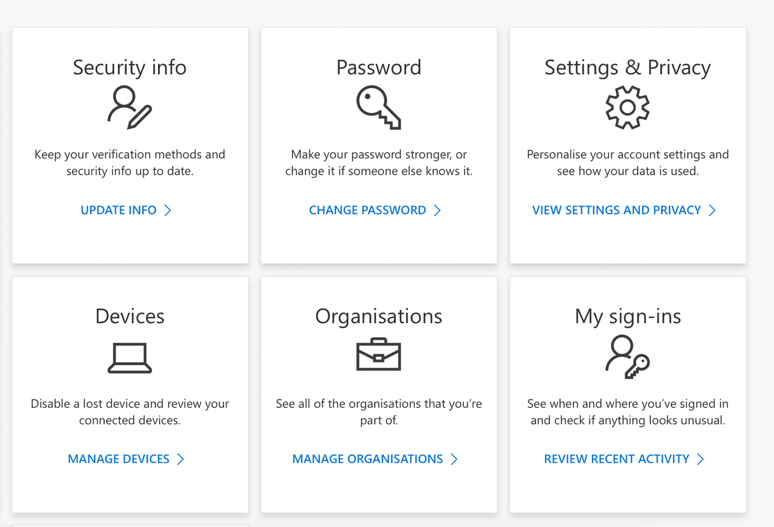
# IMPORTANT: Adding a secondary MFA option.

You can also add a secondary option. This is important in situations where you may not have access to your primary method. A secondary method can be a text or a call to a phone number of your choosing.

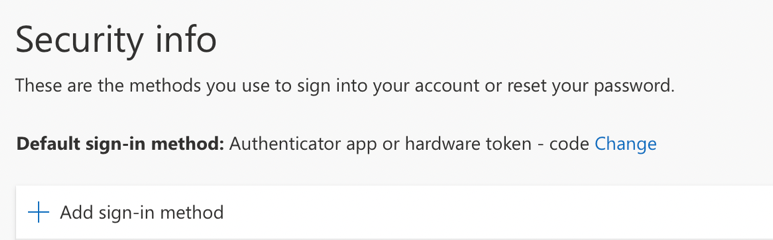
# How to change or add MFA methods.

At any time after completing MFA registration, you can follow these instructions to change, add, or update your MFA options.

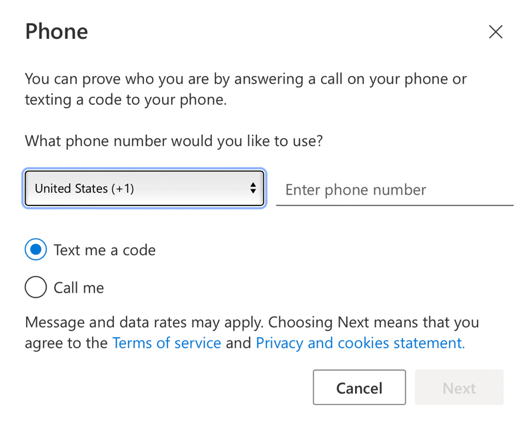
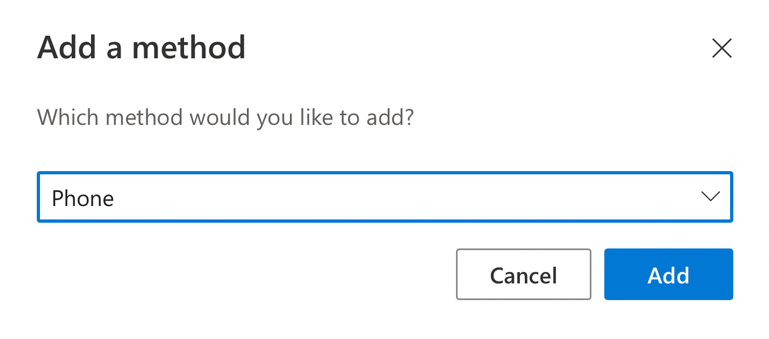
Go to <https://myprofile.microsoft.com>, and sign in if prompted.



Click **UPDATE INFO** under **Security info.**

****

You will now see a list of your verification methods. Click **Add sign-in method**.



Select **Phone** from the drop-down list.

Select your area code, input your phone number, and click **Next**.

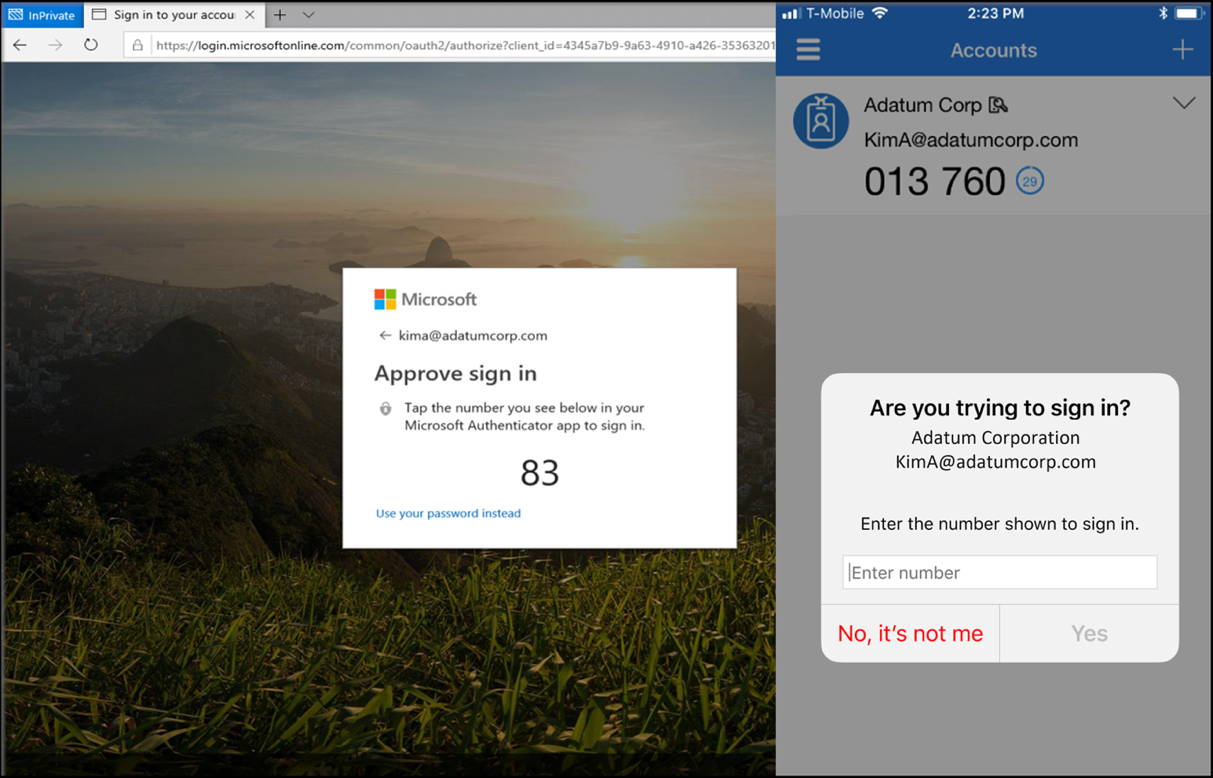
Microsoft will then text a code to your phone number. Enter the code on your screen and click **Next**. Your change is complete.

# Signing in after MFA registration

Microsoft has introduced **number-matching** to make MFA more secure and protect against ‘notification fatigue’ cyberattacks.

**If you are using the Authenticator app (recommended) the process is:**

1. Go to BCU service (iCity, Moodle etc)
2. Enter your BCU credentials (email address and password)
3. A 2-digit code will appear on the screen



Computer screenshot and phone screenshot

1. Enter the 2-digit code into your mobile device's Authenticator and click **YES**. You will also see the service that you are trying to sign in to (making it easier to notice if the activity is from someone else attempting to access on your behalf)

You will then be signed into the service.

**If you have any further difficulties with this process, please contact** [**ITHelp@BCU.ac.uk**](mailto:ITHelp@BCU.ac.uk?subject=Multi%20Factor%20Authentication)