Edinburgh Napier UNIVERSITY | Information Services

Multi-Factor Authentication (MFA)

Smartphone first time setup guide

This document explains how to set up **Multi-Factor Authentication** (**MFA**), allowing access to **Office 365** services (including **email, calendar** and **OneDrive**) from outside the University Network.

Please consult the Troubleshooting section at the end of this document if you require assistance.

What do I need to set up MFA?

An internet connected smartphone or tablet.

This is the device you will install the **Microsoft Authenticator** app on allowing you to perform MFA. Please have it with you when you wish to access Office 365 out with the University on it or any other device.

What if I don't have a smartphone or tablet?

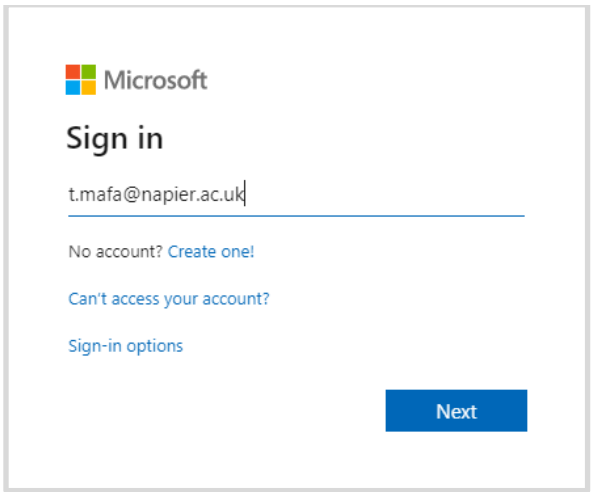
Step 1

On your smartphone

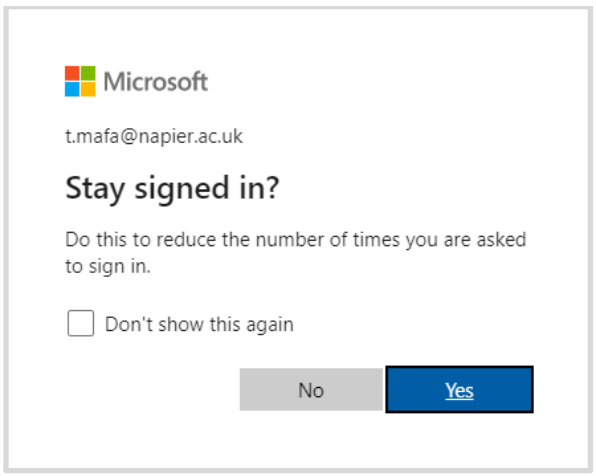
Navigate to https://aka.ms/mfasetup.

Sign in with your University **email address** and password.

Staff must not use their 4xxxxxxx number.

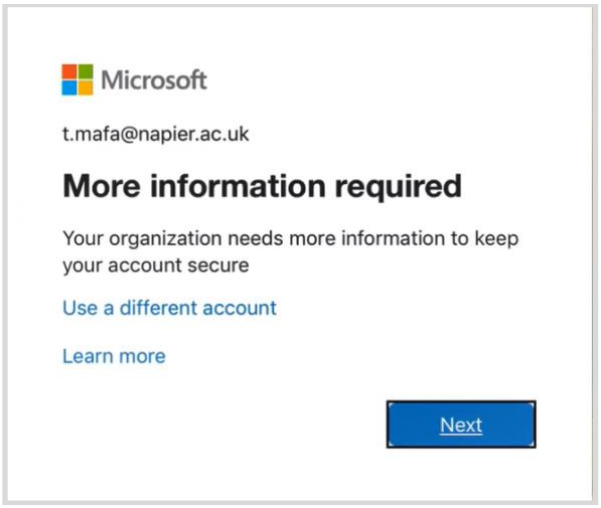


If prompted to stay signed in, select **Yes** if you trust the computer you are using.



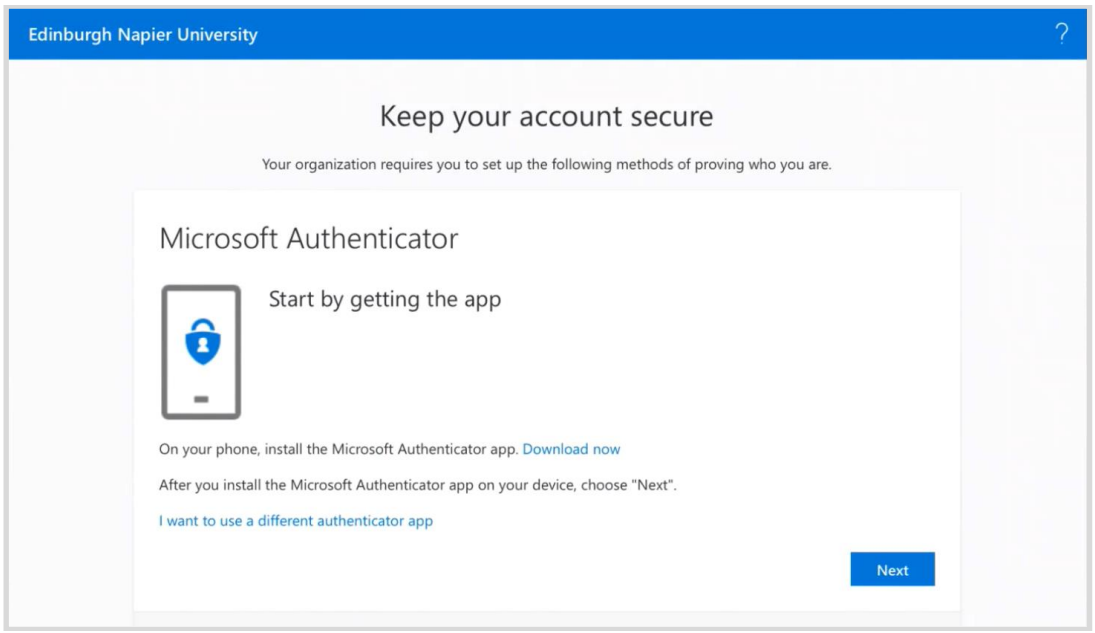
You will be prompted to provide additional information.

Select **Next** to continue.



Step 2

The following page will display.



Install and open the **Microsoft Authenticator** app, available on the App or Play store.

Allow the app to send you notifications if asked.

Skip all other initial messages.

What is the Microsoft Authenticator?

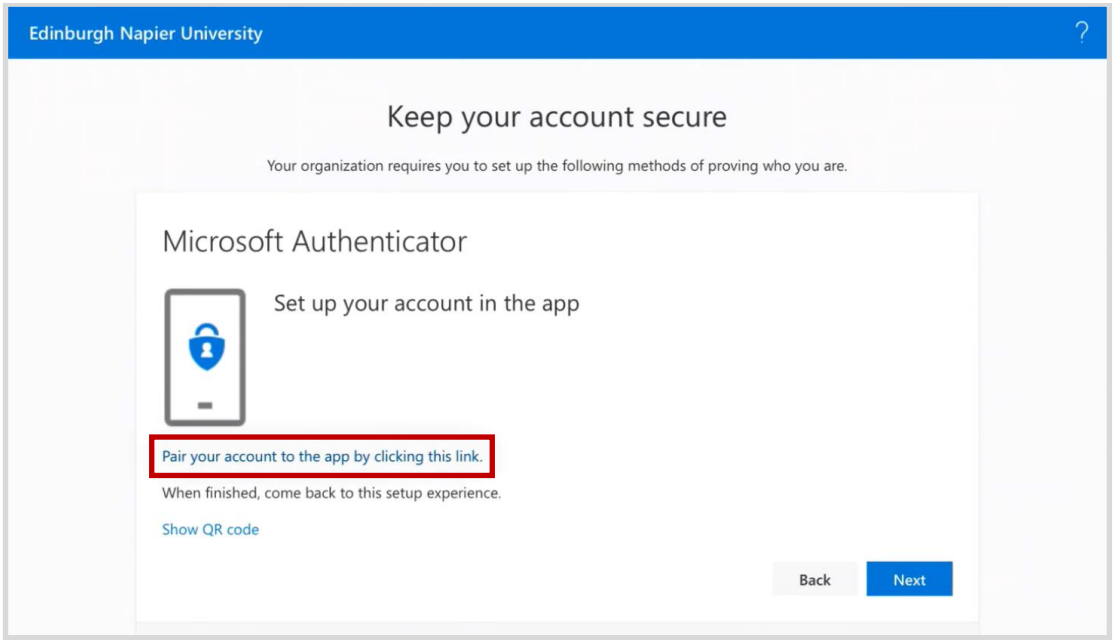
Once you have installed the app, return to the website and select **Next** to continue.

Tip: On iPhones and iPads, double tapping the home button will allow you to switch between the Microsoft Authenticator app, and your web browser.

Step 3

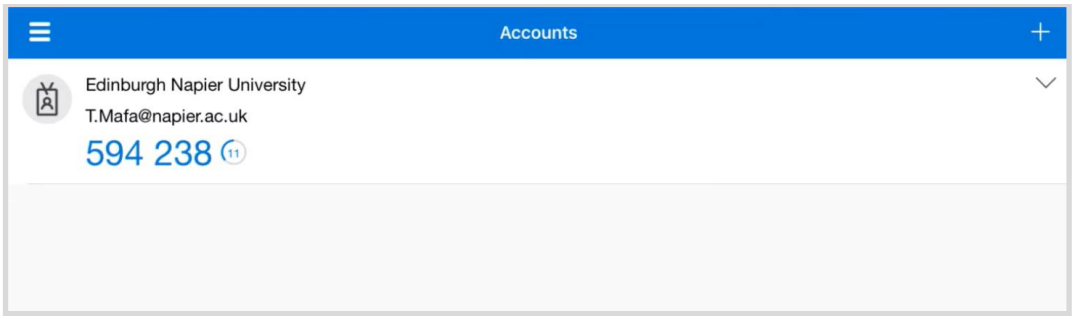
Select **Pair your account to the app by clicking this link.**

This will open the **Microsoft Authenticator** app.



Step 4

In the **Microsoft Authenticator** app, your account should appear.

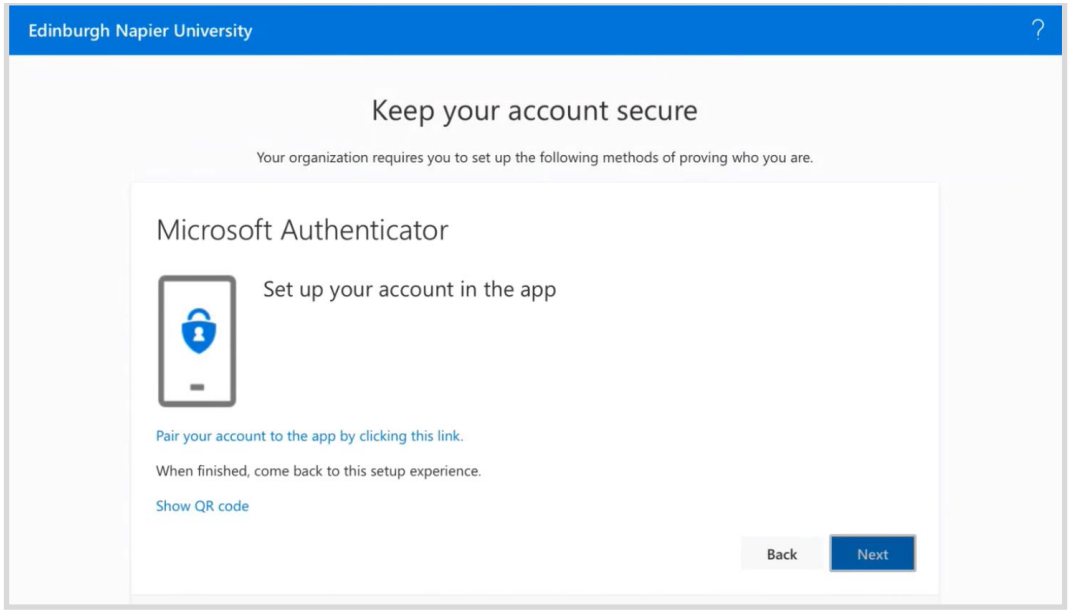


Step 5

Minimise or close the Microsoft Authenticator app.

Return to your web browser and the MFA website, then select **Next**.

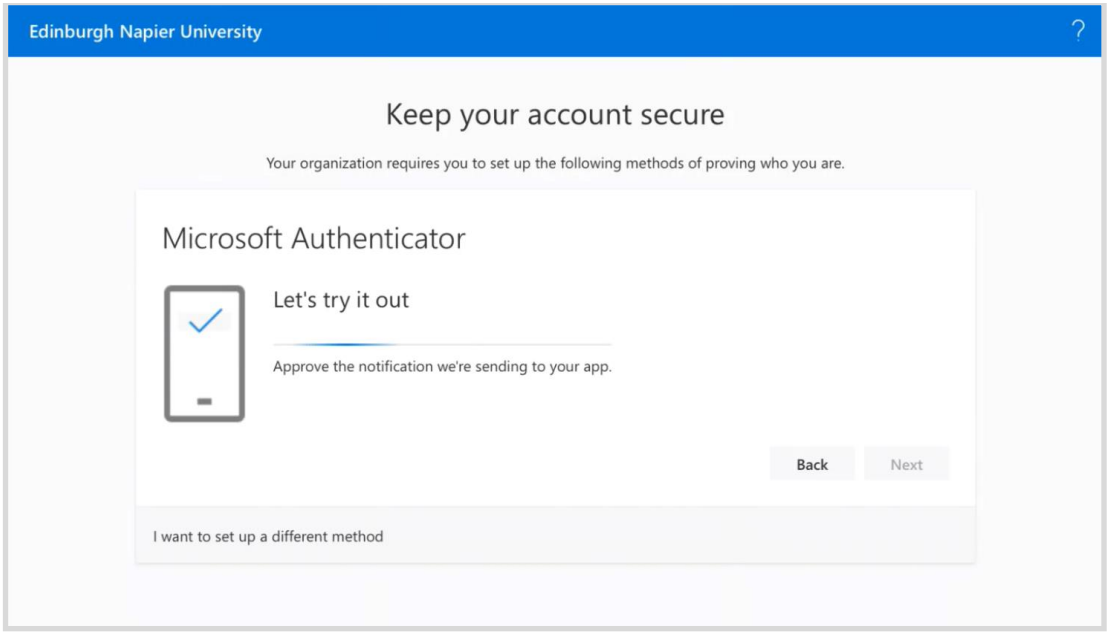
It may pause for a moment. If an error appears select **back** to return to **Step 3** and try again.

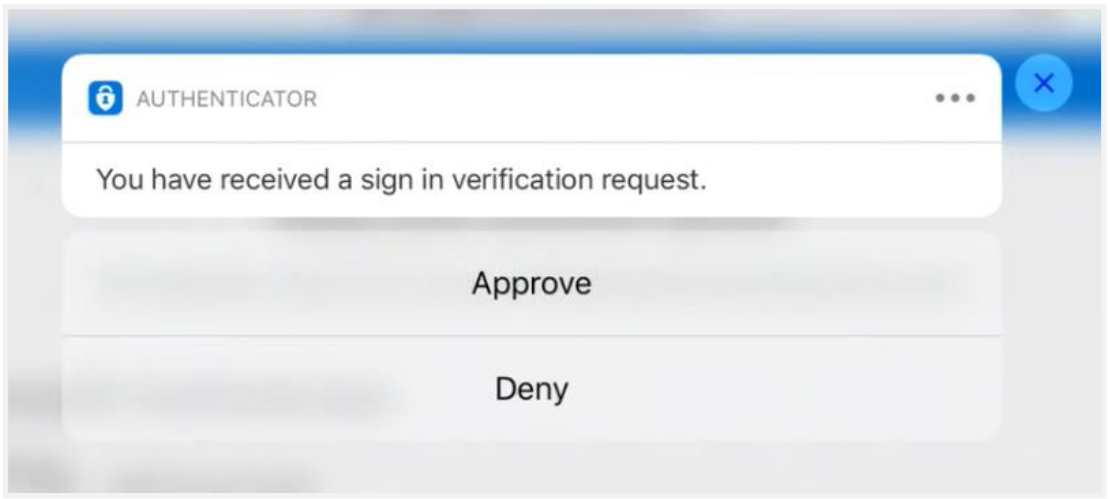


Step 6

A notification will be sent to the **Microsoft Authenticator** app. Approve it.

If a notification does not appear, ensure the app has been given permission to send notifications by checking in your phone's settings. The notification times out if there is no response, but you are given the option to try again.





Stay safe in the future! You will only ever receive a notification like this when you have manually triggered its generation and are expecting one.

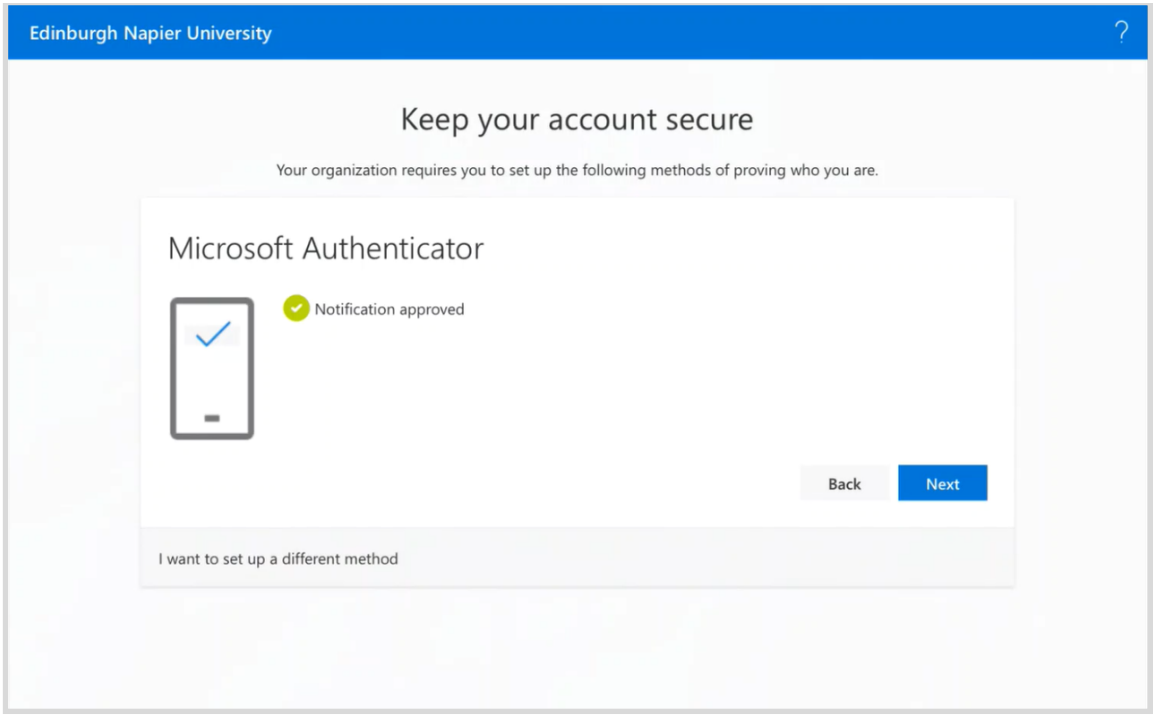
If you have received one out of the blue, it is an indication your account has been compromised! Contact the IS Service Desk immediately and request a **password reset.**

Step 7

Return to the MFA website.

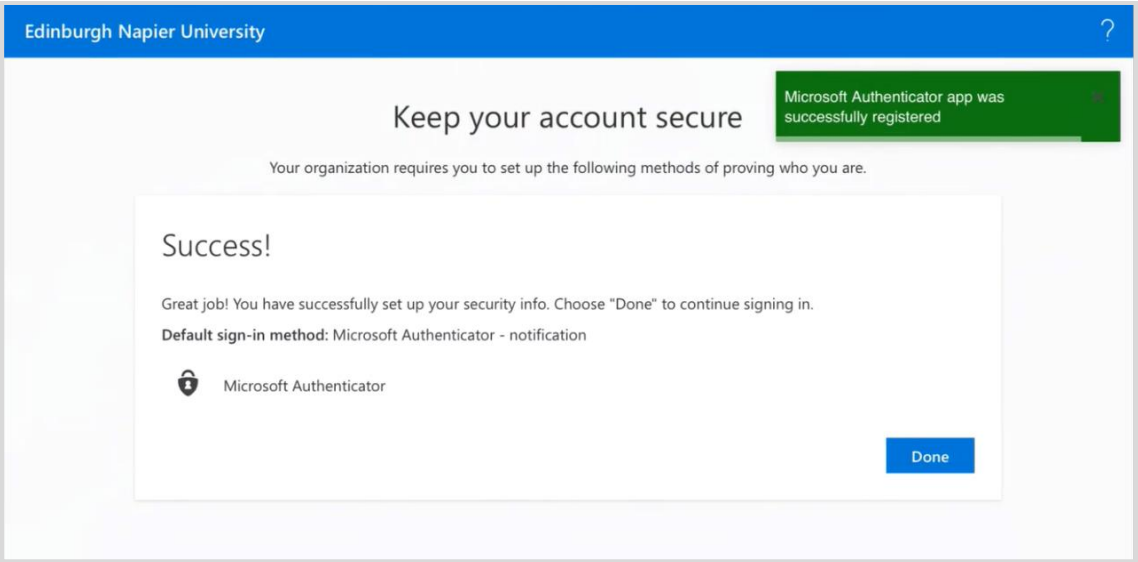
The website will update to confirm you have approved the notification.

Select **Next** to continue.



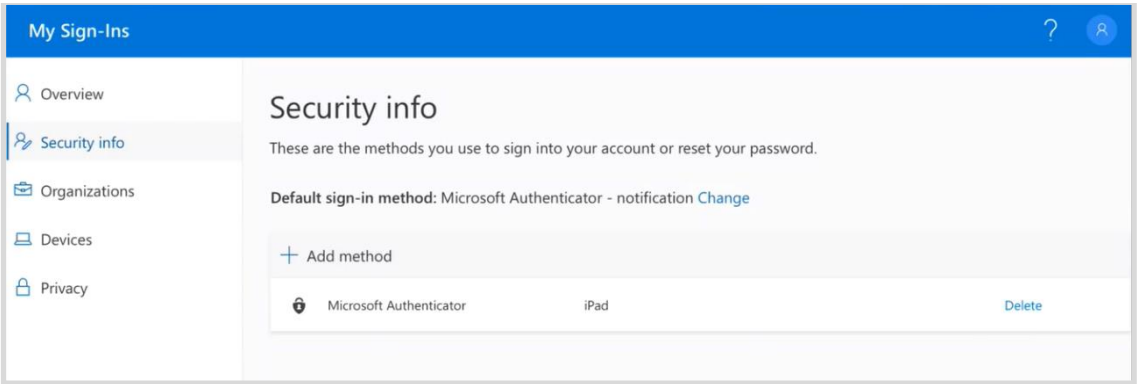
Step 8

You have successfully set up MFA with your smartphone or tablet, ensure you have it with you wherever you want to access the University Office 365 service. Select **Done** to finish.



Step 9

You will be taken to your **Security info** page. Here you can manage your MFA settings. You can access this in the future by returning to https://aka.ms/mfasetup.

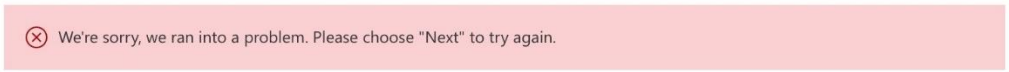


Troubleshooting

What if I don't have a smartphone or tablet?
MFA can also be performed with an SMS code. You will need a mobile phone capable of receiving SMS messages. No charges are incurred. A guide to first time setup can be found here.

I haven't been sent a notification?
Make sure that the Microsoft Authenticator app is allowed to send you notifications in your phone's settings. If you do not approve the notification MFA hasn't been setup.

It says I ran into a problem?



This can appear if the process isn't completed quickly enough (it times out for security reasons). It's best to start the process again from scratch. Close down the browser tab and go back to **Step 2**. Alternatively you can setup MFA using the QR code method - guidance can be found here.

When I click 'Pair your account to the app by clicking this link' it gives me a code to copy.
If this happens, Information Services recommends using the QR code method instead to setup MFA – guidance can be found here.

How do I know if MFA is set up and working?
If you have received and approved the notification sent to the authenticator app then MFA is functioning correctly.

At Step 9 it says an unexpected error has occurred?
This is due to a conflict between your browser remembering a sign in using your 4xxxxxxx@napier.ac.uk and your email address. It doesn't indicate that MFA isn't working. You must sign out of the website from the top right dropdown, then clear your browser data. When you return to https://aka.ms/mfasetup it should display correctly.

Alternatively use a different browser to access this page in the future.

I've lost my device!
Contact the IS Service Desk. They are able to reset your MFA settings so that you can set up MFA on a new device.

I do not wish to use a personal device for MFA, what can I do?
Please use a corporate smartphone or tablet to perform MFA if you have been provided with one. Otherwise, please use the Virtual Desktop Service or Virtual Private Network service to access Office 365. These services are temporarily exempt from MFA.

If you are still having difficulty, please phone the **IS Service Desk** on **0131 455 3000**.