Improving Account Security

Quick guide to Multi-Factor Authentication for accounts accessing Microsoft Office services online, including MyHub, Oracle Finance.

Contents

Introduction

Multi-factor authentication ('MFA') helps secure your University account and data from attackers. MFA adds an additional layer of security (something you have, e.g. a mobile phone) to your account to ensure that it is you using your account.

Initially, IT Services will just be implementing MFA on access to Office 365 and the Oracle Finance system. The system keeps a history of your usage so if you attempt to access these services from an unfamiliar location or device, you may be prompted for MFA or be asked to change your password, depending on the perceived risk. Whilst using a University device at work, you should not be prompted for MFA, as IT Services have enhanced the security of these devices.

The details entered are also use with Self Service Password Reset (SSPR). If you have already set this up, you may already see your mobile phone and personal email address configured.

MFA works best by using a mobile phone as this is something most people normally carry with them. Please consider using your personal and desk phone when setting up MFA on your account if the event of your primary method of access is unavailable. If none of these options are suitable, IT Services can provide physical tokens (like credit cards / key fob).

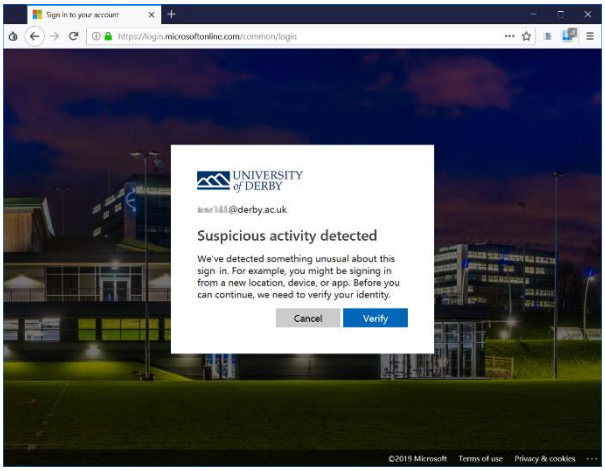
Physical tokens

Even with MFA enabled, please check addresses of web sites used to enter your account details. Malicious people are making copies for website that look very familiar to try and dupe people.

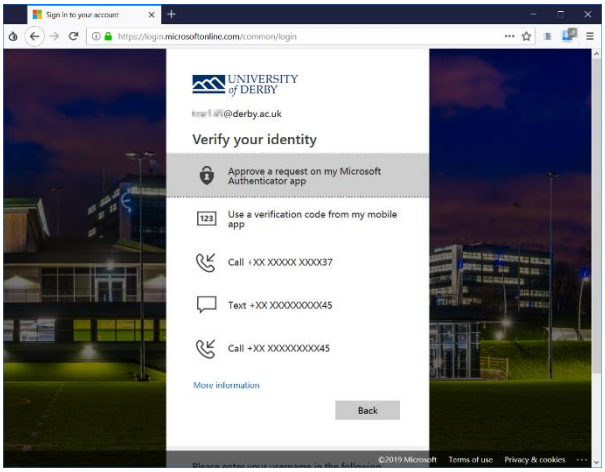
Remember that we will never send an email containing a link asking you to alter or verify your personal details so if you receive one please take advice before doing anything with it. Contact the sender (not by email), or get in touch with IT Services: ring +44 (0)1332 591234, email itservicecentre@derby.ac.uk or "Request IT Help" via StaffID: https://staff.derby.ac.uk/ | Professional Services | IT Services

What changes will I see?

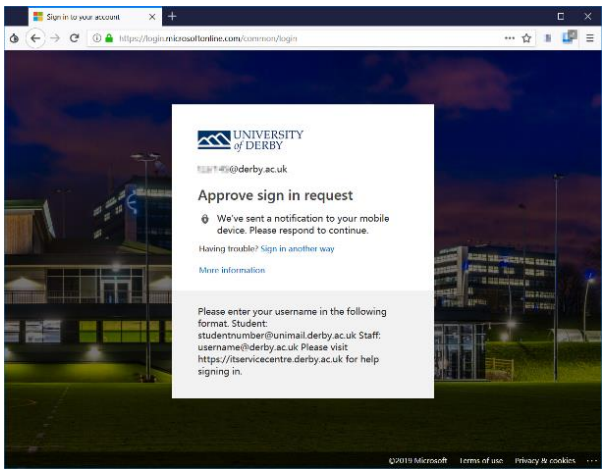
When visiting a website secured by your University ID, you may get message to verify your account after you have entered your password.



This will give you a range of options to verify your identity:



The system will confirm it has sent a request:

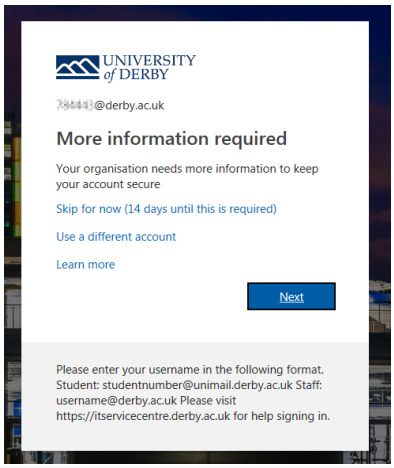


MFA Setup

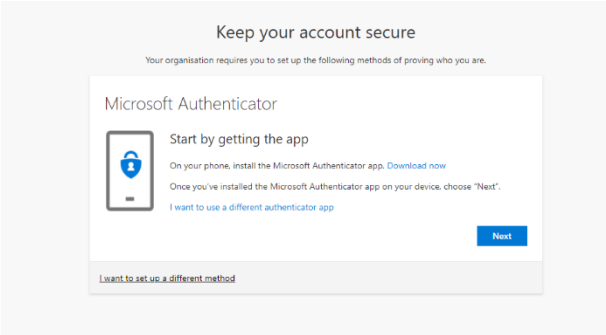
1. Upon MFA being enabled on your account, you will see this message when visiting the links at the top of Staff iD (Office 365, One Drive, Mail, Profile), the Finance or HR systems or by directly going to sites such as office.com.

   You can skip this request for 14 days, after which your account will be locked if you have not enabled MFA.

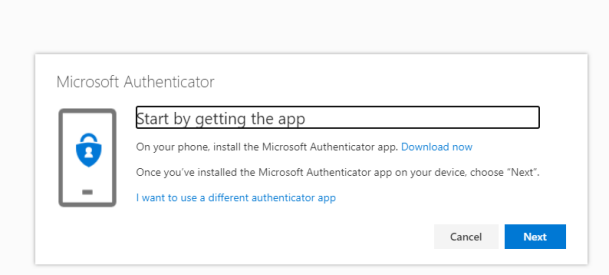
   Click Next to continue.



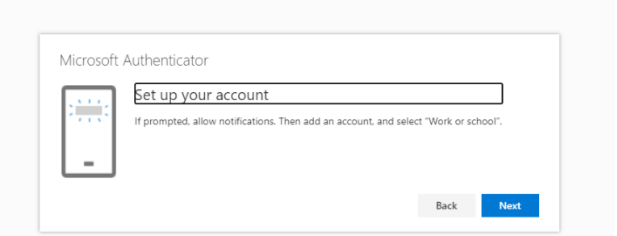
2. The easiest and most secure way to setup MFA is with Microsoft Authenticator, an app for your smartphone. However, if you wish to use a text message, click “I want to set up a different method” and follow the guide in the Appendix.

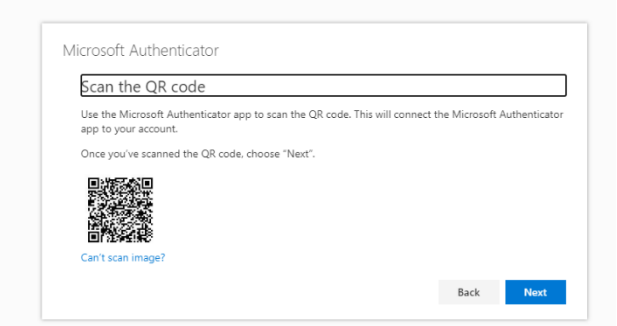


3. To do this, you will need to download the app from the Apple App Store or Google Play Store. Make sure you allow access to the camera and allow notifications.

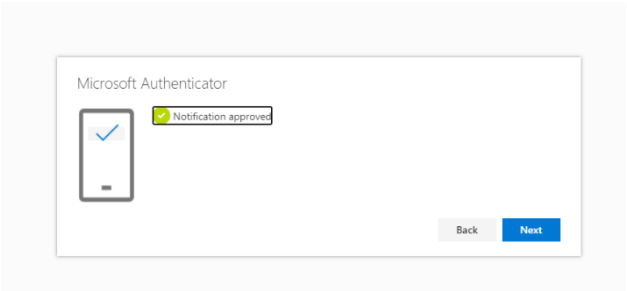


4. Follow the prompts to add a “Work or School” account.



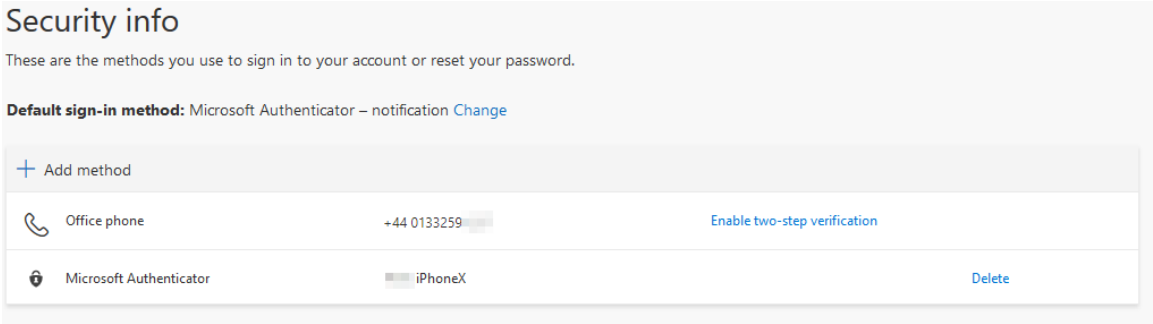


5. After a few seconds, the notification will be approved.



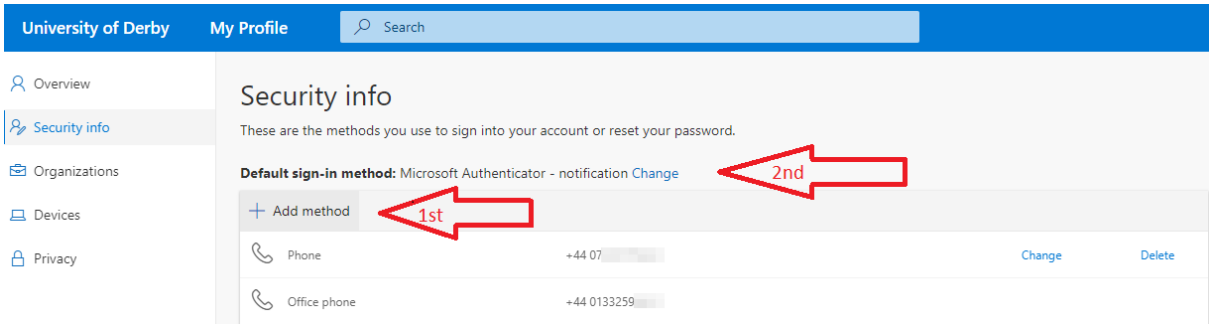
6. You will then be taken to a page were you can confirm your default sign-in method and add more methods. We recommend that you add as many methods as you can.

   To do this, first click on 'add method' and then add as many as you can, step by step guides are in the Appendix. Once setup following the steps below, choose the default sign-in method.



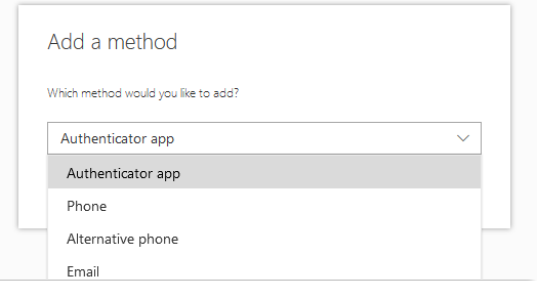
Appendix

To setup additional authentication methods, visit https://myprofile.microsoft.com click on Security info. Select 'Add method' (1st arrow) to add a new method of verification. To change your default sign-in method, select 'Change' (2nd arrow).

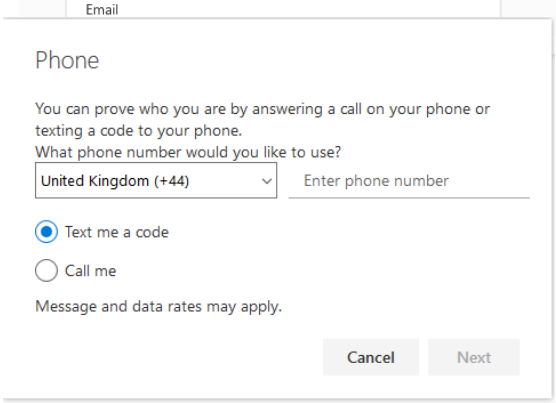


Setting up a mobile phone

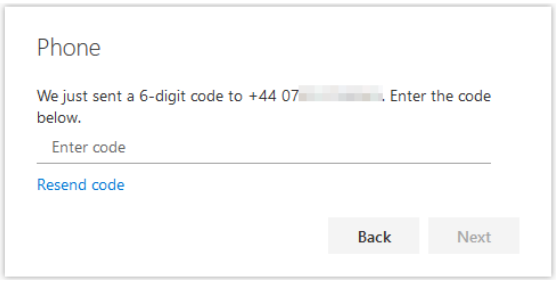
1. Select 'Add method' and select Phone and 'Add'.



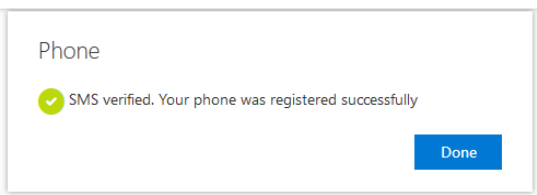
2. Add your mobile phone number, selecting United Kingdom (+44) if your phone is based in the UK.



3. If text code is selected, you will be sent a 6 digit number to enter. If this has not arrived within 30 seconds, try resending the code.

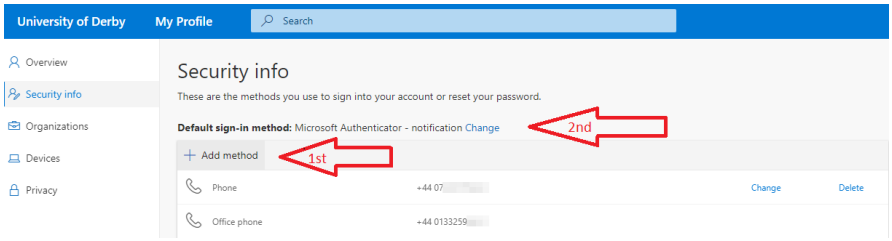


4. The system will confirm the code has been verified correctly.

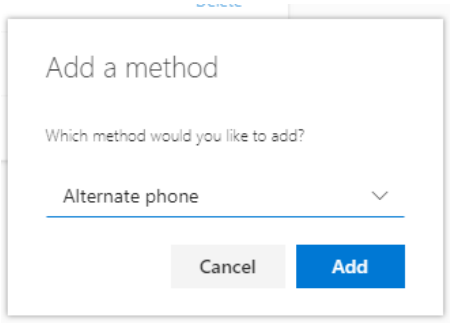


Setting up an Alternate phone

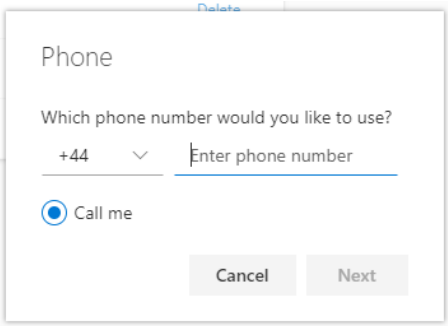
1. Visit https://myprofile.microsoft.com select Security info and then 'Add method' (first arrow in the image). Don't forget to change your 'Default sign-in method' at the end.



2. Enter your phone number, e.g. personal mobile phone. This will only be used for authentication to your account. The system will ring you.

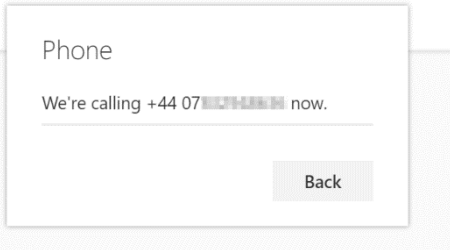


3. Enter your phone number, with the UK country code of +44:

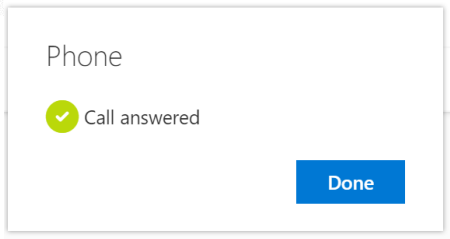


4. When the phone rings, an automated message will ask you to press the hash / pound button:

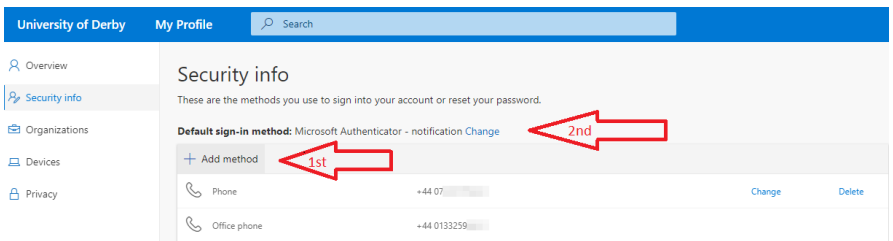
   #



5. Your computer will confirm the call has been answered.

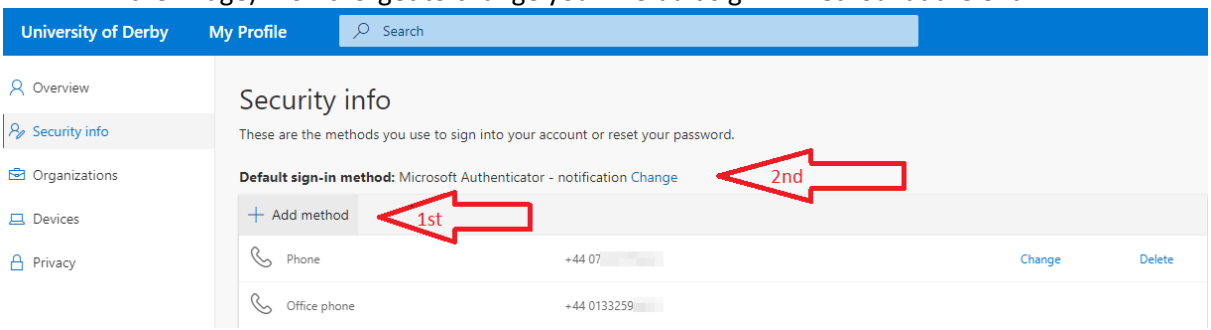


6. Once setup, you can change the Authenticator app to be the 'Default sign-in method', which allows authorisation with a click of a button, 2nd arrow below.

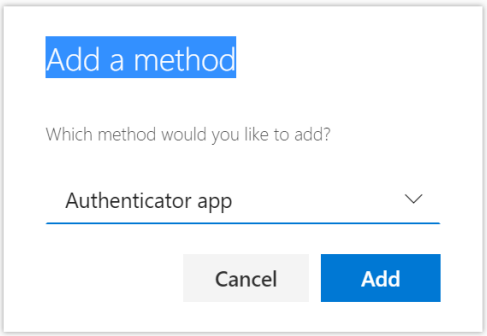


Setting up the Authenticator App

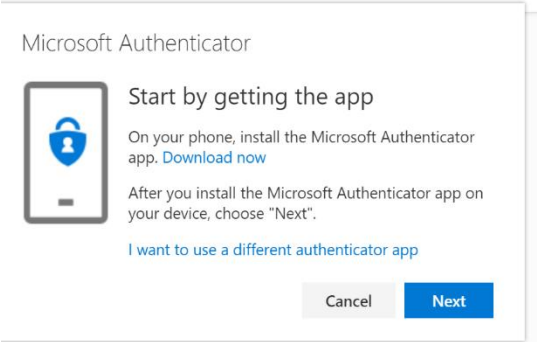
1. Visit https://myprofile.microsoft.com select Security info and then 'Add method' (first arrow in the image). Don't forget to change your 'Default sign-in method' at the end.



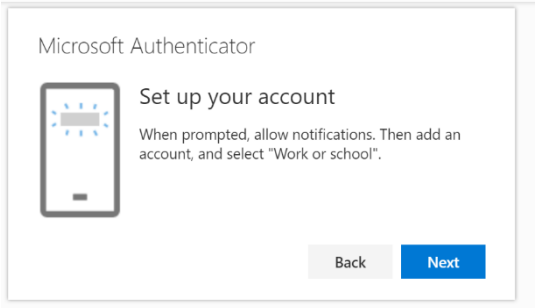
2. IT Services recommend using the Microsoft 'Authenticator app' on your mobile phone. This will work even if there is no phone signal and is a step towards removing the need to type your password. You can do this by adding the 'Authenticator app' method.



3. Although there are other authenticator apps available, the preferred option is the Microsoft 'Authenticator app'. For more information visit https://www.microsoft.com/en-us/account/authenticator

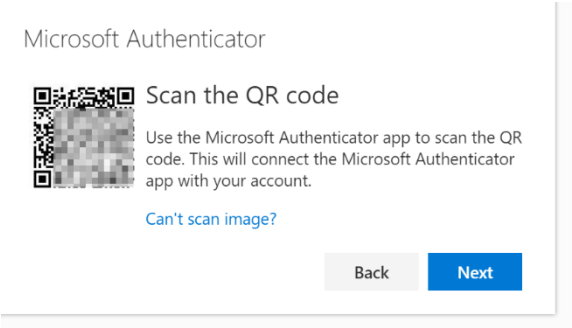


4. Once the 'Authenticator app' is on your phone, add your account followed by @derby.ac.uk and select 'Work or school'. If you already have your account setup, click the '+' symbol to continue.

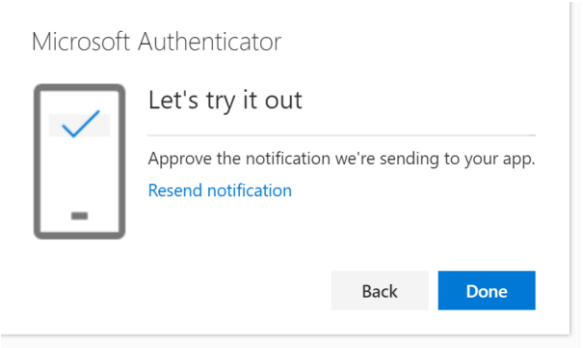


5. The app may ask your permission to use the camera to scan the QR code on the screen.

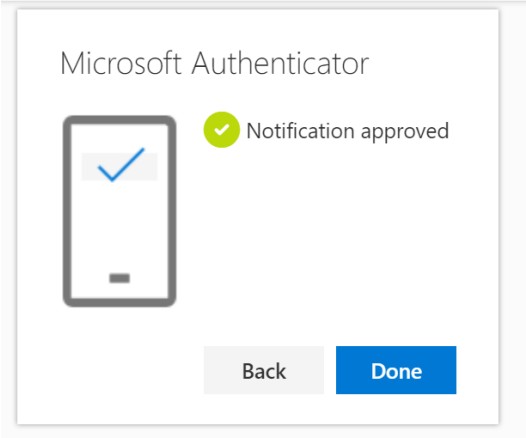
   If you have the Authenticator app already installed, please check that it has access to the camera. If not, it will ask for a code and website address accessed by clicking on 'Can't scan image?'



6. You will be asked to try it out. Your phone will receive a notification and you can select 'Approve'.



7. Your computer will confirm the notification has been approved.



8. Once setup, you can change the Authenticator app to be the 'Default sign-in method', which allows authorisation with a click of a button, 2nd arrow below.