UIS Multi Factor Authentication

Introduction

In order to better secure University staff Raven accounts, UIS is turning on Multi Factor Authentication (MFA) to all Raven accounts by 1 October 2021. This means that when you go to use your Raven account for certain Microsoft applications you will need to confirm your log in using another device. Typically this is done by using the Microsoft Authenticator app on a mobile phone (note that there are other options if this doesn't work for you).

As a Medschl, SLCU or Zoology user you would be required to use MFA for both Teams and Exchange Online in the following instances:

- Initial log in to Teams and Exchange Online once you've set up MFA
- For each application after you change your password
- If you log in to a new device to use Teams or Exchange Online
- Add your Exchange Online email account to a new device
- Accessing a new SharePoint resource for the first time

This will NOT apply to your Medschl email as it is a separate system to Exchange Online.

If you are an SDHS user, this is not the same MFA or token that you use for SDHS access. You will continue to need to use both 2 different MFA tokens - one for SDHS and the other for Teams and Exchange Online (If you use that).

Information

Below are links to the UIS information created to date to help you with this process. Please see the Support section below if you need help.

Enabling MFA

Users are being contacted alphabetically by CRSID. You will be contacted by email inviting you to set it up. We strongly recommend you set it up BEFORE the date MFA is turned on for your account. If you wait until the date, you may be left without any access whilst it is set up. You can ask for it to be activated earlier or postpone it for a month using the MFA options form: http://www.uis.cam.ac.uk/mfa-options

Choosing your authentication method

There are several methods you can use to authenticate. And you should set up more than one so you've always got a backup.

Possibilities are:

Method	Notes
Microsoft Authenticator mobile app	Recommended method. Works on Android and Apple Smartphones
Codes sent via text to a mobile phone	
Code sent via landline (eg home or office phone)	You can set up any phone to receive a code. If you are working remotely, you can still access your office phones using Jabber. Here is a guide on setting up and using Jabber https://www.phone.cam.ac.uk/your-phone/UsingJabber
Code from hardware token	Not recommended as UIS have not yet determined how to provide the tokens
Twilio Authy	There is currently no UIS documentation about how this could be set up

Setting up your authentication methods

Please see this page for help on setting up your authentication methods: https://help.uis.cam.ac.uk/service/accounts-passwords/multi-factor-authentication/mfa-set-up

Setting up your email apps

This page shows how to set up your email apps: https://help.uis.cam.ac.uk/service/accounts-passwords/set-multi-factor-authentication-your-university-microsoft-account/set

Managing your authentication methods

https://help.uis.cam.ac.uk/service/accounts-passwords/multi-factor-authentication/managing-mfa

Support

As CSCS is not involved in the setup or maintenance of MFA, please contact the UIS' dedicated support desk for assistance staff and students with any MFA-related queries. You can reach them at **https://mfahelp.uis.cam.ac.uk** which will be available 24/7 during the initial rollout ending 1 October 2021.