How to setup Multi-Factor Authentication

Multi-Factor Authentication (MFA) uses a mobile app verification message, an SMS (text message), or an email to verify who you are for extra identity security.

YOU ONLY NEED TO DO THIS ONCE.

You can choose the method you prefer, however we recommend using the Microsoft Authenticator App on your mobile phone.

Follow these steps (or watch the video below):

1. Login as normal to your Office365 tools/apps. You may need to repeat this step for different apps and devices.
2. Follow the on-screen instructions when extra information is requested.
3. Select how you want to verify your identity (App recommended)
4. Download the MS Authenticator App (or follow the options for SMS/email)
5. Link the downloaded App to your University profile
6. Approve the access request within the App
7. Add your mobile telephone number for additional security verification
8. You should be automatically logged back in

There will be an option to 'don't ask me again for 60 days' if you want to stay authenticated for a longer period of time.

What is Multi-Factor Authentication?

Simply put, it's a secondary method of proving you are who you say you are at the point of logging in and this extra security step significantly increase the level of data and identity security.

Read more about MFA and watch a video: What is MFA?

MFA sign in will be required to access your University account including Teams, SharePoint, OneDrive, and all Office 365 applications.

MFA uses a secondary method to prove you are who you say you are.

Setting up your MFA for the first time:

This video goes through the first-time user steps explained above for using the Microsoft Authenticator App. You only need to do this once.

Setting up MFA using the MS Authenticator App

Changing your verification method:

Watch this video on how to access and change your verification settings (eg from SMS to using the MS Authenticator App).

Changing you authentication method for MFA

MFA Frequently asked questions:

Q: Why do I need to sign up to MFA?

A: MFA is being implemented to help protect your identity and your work. MFA provides an additional layer of security through the provision of a user authentication process when signing in to your University account when you are off campus.

Q: How do I reset my password?

To use the University's Self Service Password Reset:

1. Go to your **Office 365 Home Page**
2. From your Profile, select **My Account**
3. You will see a Security Information Tile
4. Select **Set Up Self Service Password Reset**
5. Follow the onscreen instructions to either CHANGE or RESET your password

Q: Who needs to use MFA?

A: For the Exeter IT Pilot, only Exeter IT staff will need MFA. Once the pilot is successfully completed other users will be informed and via timely and targeted emails.

Q: Why is the University doing this?

A: To improve security for individual identities and university systems and to reduce the risk of hacking and data breaches.

Q: I am experiencing problems logging in, what should I do?

A: Check that you have entered your password correctly. Check your cookies setting. If this still doesn't work call the IT Helpdesk.

Q: I signed up to receive passcodes by text message. How do I now change this to App or Email?

A: Follow the instructions in your Office 365 My Account Security Settings to change your verification numbers/methods or watch this video: Changing your MFA verification options

Q: Access to Stream denied after using MFA Application?

A: Clear your computer's cache (Shift+F5) and browsing history (Ctrl-Shift-*Delete)* and try accessing Stream again.

Q: Is there a recommended way to receive passcodes?

A: Download the Microsoft Authenticator App to your smartphone.

Q: The remember my settings for 60 days option is greyed out?

A: You should see this option next time you use MFA.

Q: What is the impact for Associate users?

A: Anyone who uses their own device has to MFA each app/tool therefore may have to sign in multiple times each day. This can be overcome by selecting 'dont ask me again for 60 days' at sign in.

Q: SSPR - Do I need to do anything before using MFA, if so, what and when?

A: No you do not need to sign up for SSPR before signing up for MFA.

Q: Is there a difference between Windows 7 and Windows 10 for MFA?

A: No.

Q: Will I be charged for receiving MFA SMS messages?

A: Please check with your network provider.

Q: If working remotely, who do I contact if I am unable to log in?

A: Telephone the IT Helpdesk (01392 724724).

Q: How long are the six digit passcodes valid for?

A: 60 seconds. If you don't use it then you can generate another one.

Q: How many times should I see MFA prompts on initial set up?

A: Several times during initial setup when accessing Outlook and Office 365. Select 'remember for 60 days' to avoid this.

Q: How will MFA affect me if I am using my own computer?

A: You may be required to undertake separate MFA when accessing each application/system.

Q: What happens if I lose or break my phone and need to sign in?

A: Telephone the IT Helpdesk (01392 724724).

Q: I have a new device and need to set this up for MFA, how do I do that?

A: This can be done by going to https://account.activedirectory.windowsazure.com/proofup.aspx where you can see your old device (that you can delete) and set up a new one which will give you the QR code to scan. The link can be reached by logging into Office 365, clicking on your name (top right), clicking view account, and selecting "Additional Security Verification" under "Security Info".