Multi-factor Authentication (MFA) setup

MFA Setup will take around 5-10 minutes to complete, and you'll need a computer and smartphone to make things simple.

1. On your phone, download **Microsoft Authenticator** from the App or Play store. Make sure to **Allow notifications** when prompted.
2. On your computer, browse to https://aka.ms/mfasetup and log in with your UWA account:
    - For students, use ***studentID*@student.uwa.edu.au**
    - For staff, use ***staffID*@uwa.edu.au**
    - For visitors and guests, use ***visitorID*@ext.uwa.edu.au**
3. Navigate to the **Security info** tab on the left.
4. click **+Add method**, choose **Authenticator app** and click **Add**, then click **Next** until a QR code is displayed – leave this page open.
5. On your phone, open the Microsoft Authenticator app, tap **Add account**, then **Work or school account,** and choose **Scan a QR code.**
6. Use your phone to scan the QR code on the browser window you left open in step #4.
7. On your computer, click **Next**.
8. On your phone, tap **Approve** – your authenticator app is now set up.
9. Back on your computer, click **Next** to close the dialog box, then navigate to the **Security info** tab as in step #3, click **+Add method** as before, and choose **Phone.**
10. Enter in your phone number, choose whether you'd like a call or text prompt, and click **Next**.
11. You'll be sent a code by text (or call) to the number you specified. Enter the code on your browser and click **Next** – your phone number is now set up as a backup MFA method.

Your phone is now set up to use the authenticator app for MFA, and your phone number can be used as a backup – handy if you upgrade to a new phone handset, or if you uninstall your authenticator app by mistake.

Additional support resources and contacts are available via the UWA MFA website.