In order to stop the increasingly frequent email attacks, the ICT Division has decided to implement a **multifactor authentication** system (MFA).

What is multifactor authentication?

Multifactor authentication is a system that provides stronger security measures to access one's email or Microsoft 365 account. In addition to their username and password, users are required to take a further step for authentication. This step can be customised by each user.

How does multifactor authentication work?

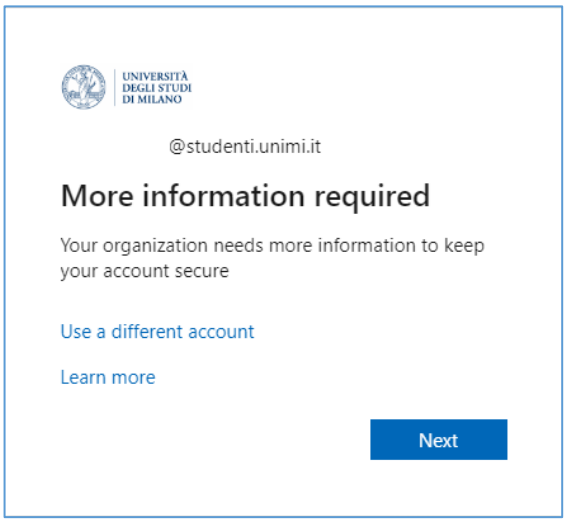
To access Microsoft services with MFA, users receive a **temporary code** on their smartphone, to be entered after their username and password.

To receive the code, you can use:

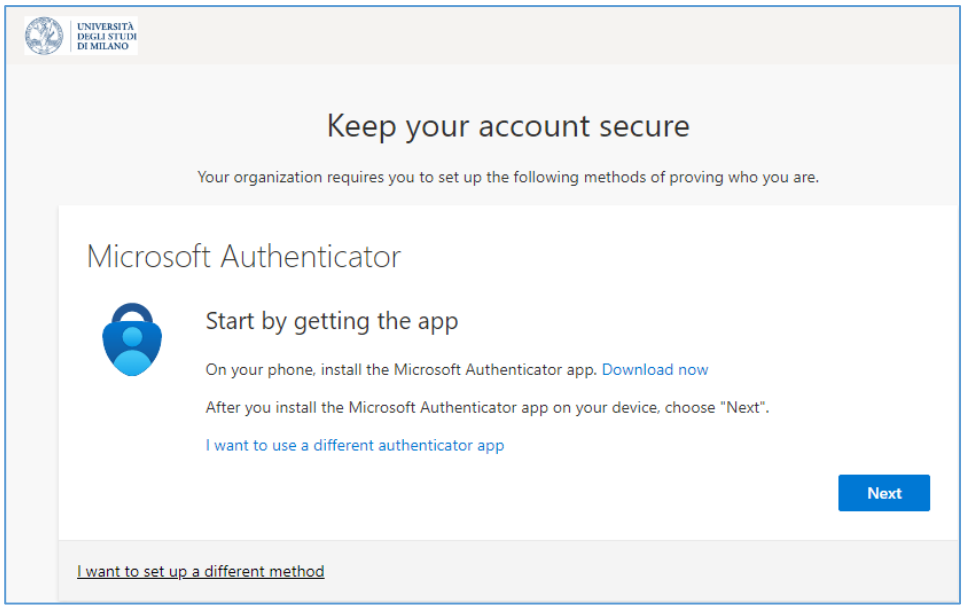
- The **Microsoft Authenticator app**, available for free download for iOS and Android devices;
- **Third-party authentication apps**, e.g. Google Authenticator;
- The **SMS** service, if you cannot or don't want to install apps on your mobile phone.

What should I do to set up the MFA system?

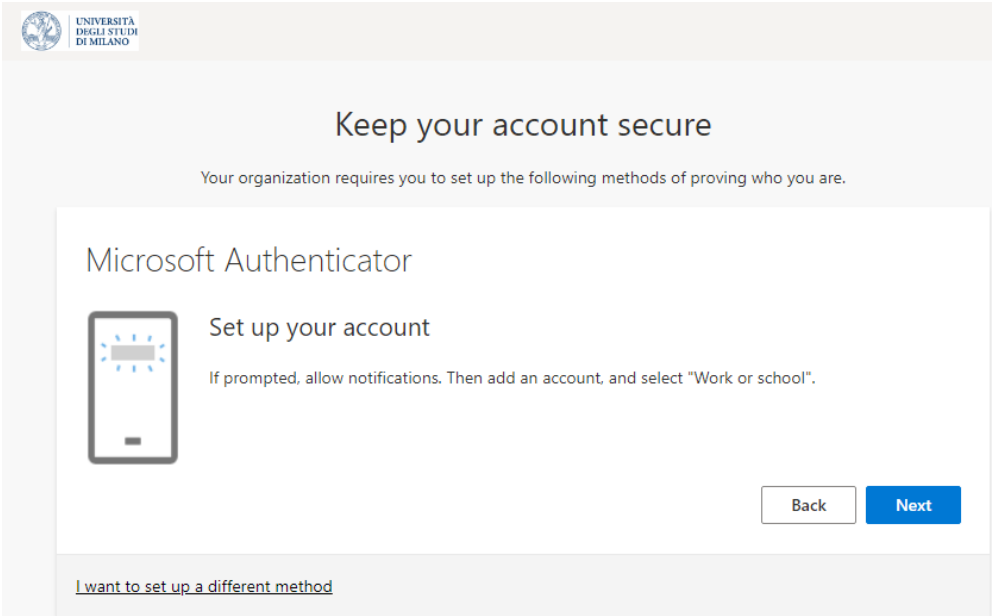
1. Go to https://aka.ms/MFASetup
2. Log in with your University user id and password
3. You will see the message "More information required": click on Next



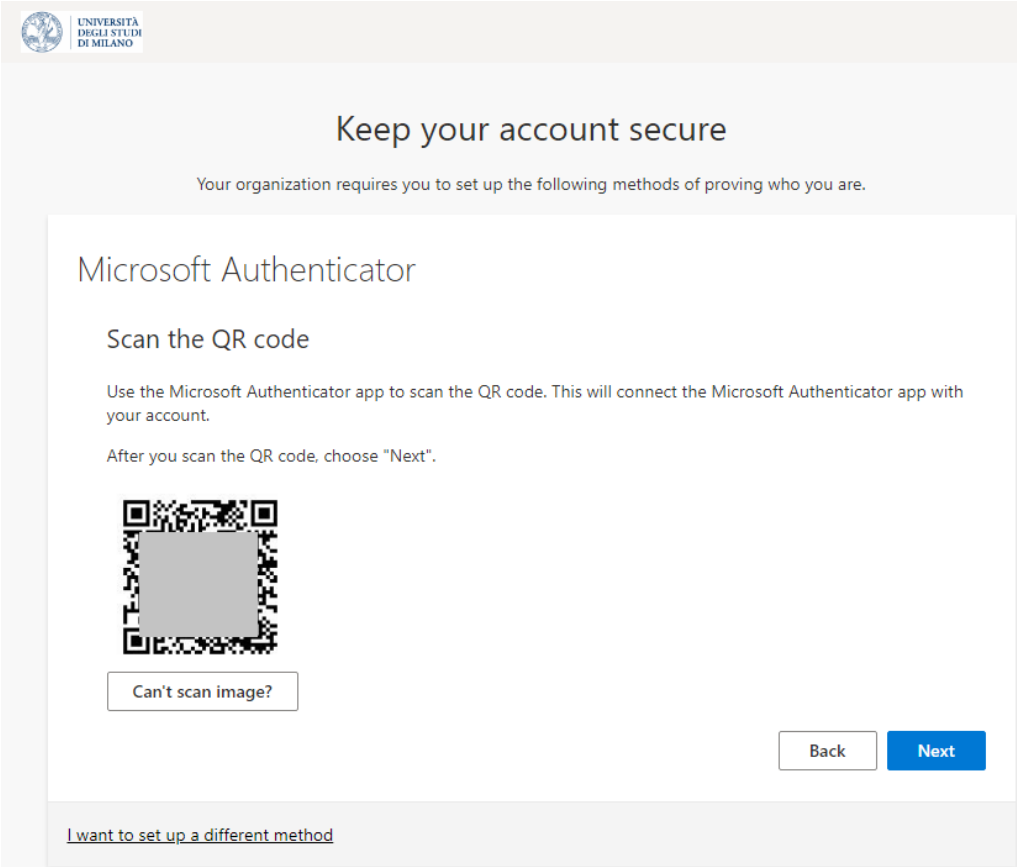
4. Download the Microsoft Authenticator app on your mobile and click on Next (**if you don't want to download the app, you can use the SMS service. Skip to step 9**).



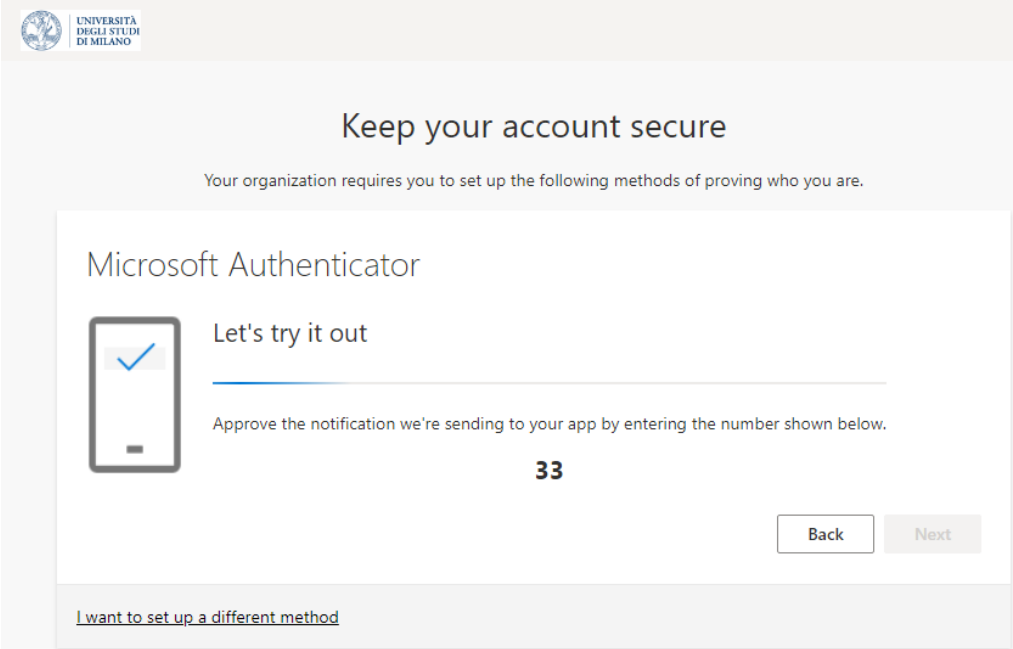
5. Follow the instructions on the following page and click on Next.



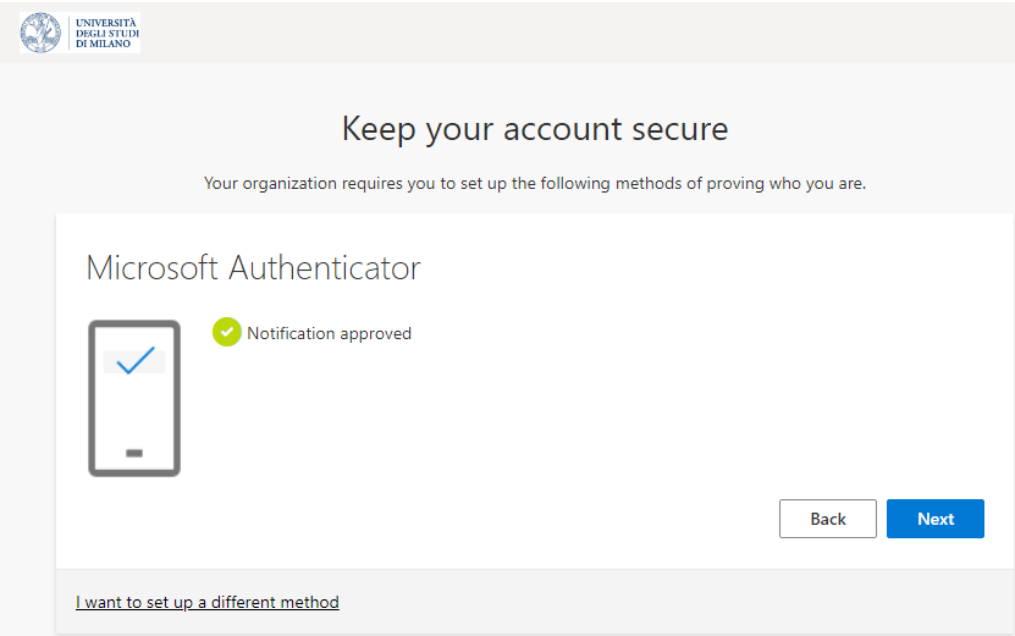
6. On the Microsoft Authenticator app, click on + to add an account, then select “Work or school”. Scan the QR code and click on Next.



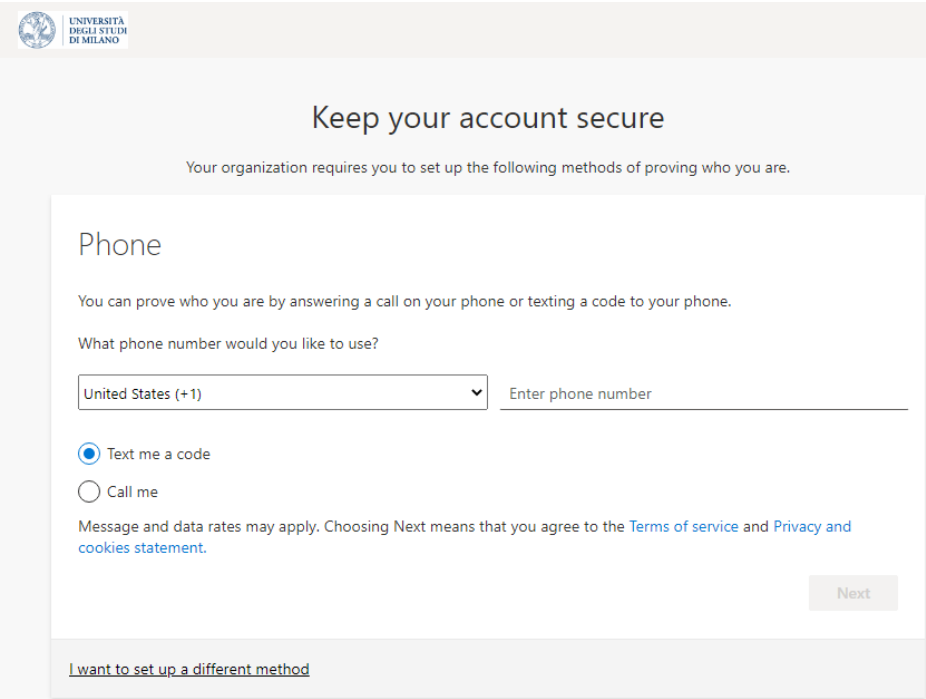
7. On the screen you will see a two-digit number to be entered into the Microsoft Authenticator app for verification.



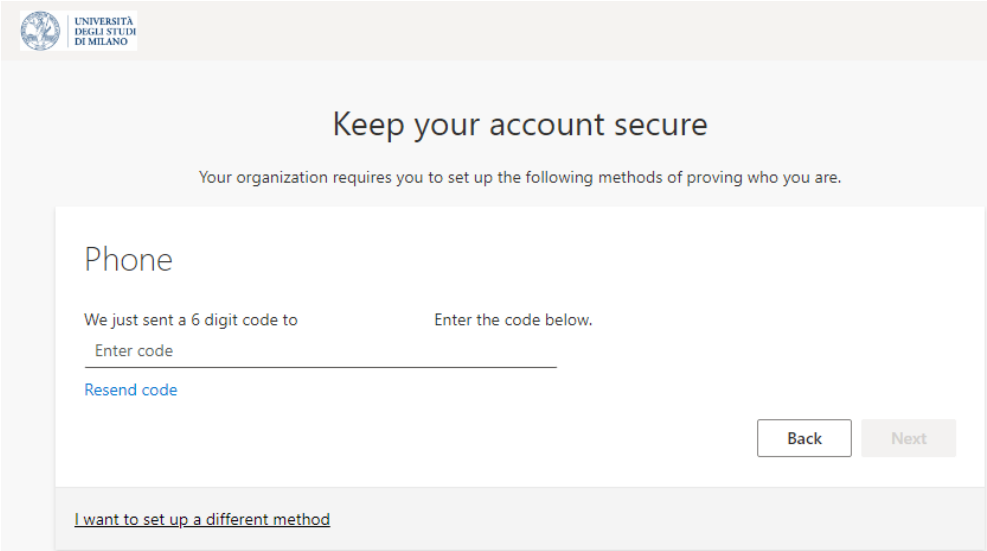
8. The authentication process has been completed.



9. If you do not want to use the Microsoft Authenticator app, you can choose to set up a different method (Phone).



10. You will receive an SMS with a code to be entered in the authentication page.



11. The authentication process has been completed.