



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?

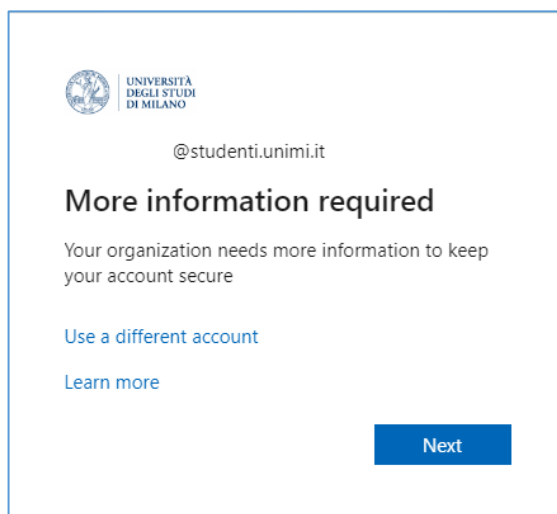
To access Microsoft services with MFA, users receive a **temporary code** on their smartphone, to be entered after their username and password.

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.

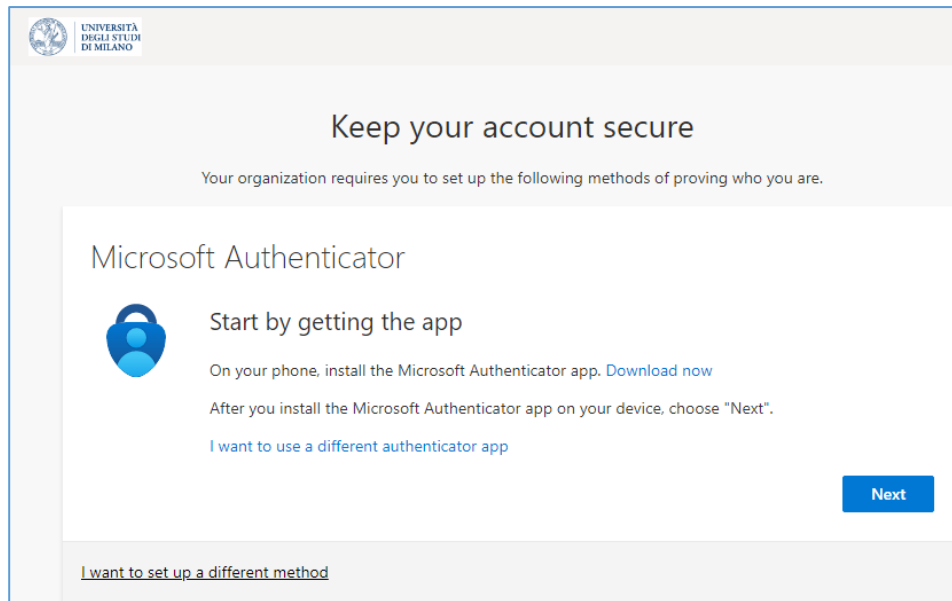
What should I do to set up the MFA system?

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

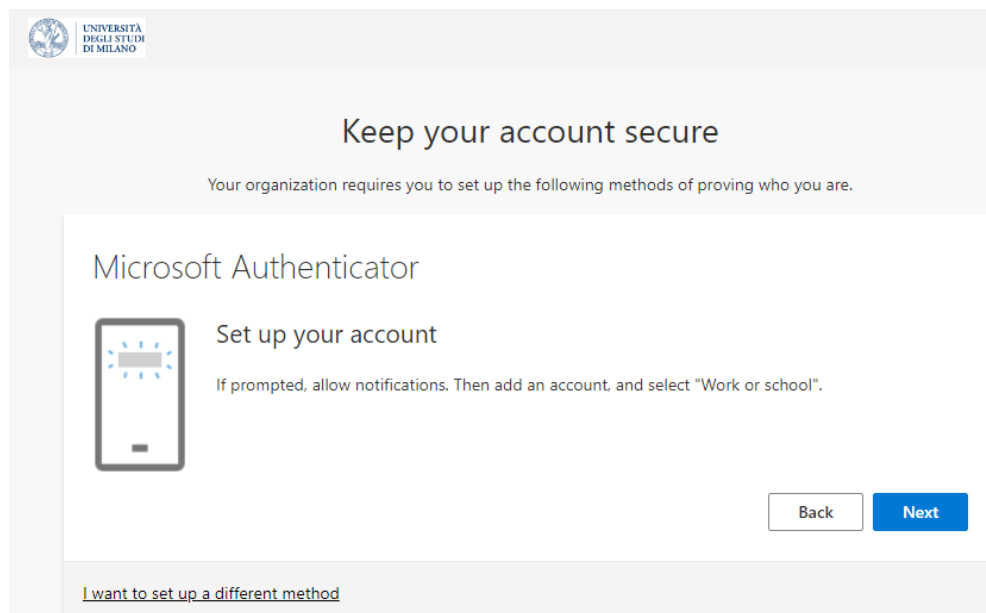




4. Download the Microsoft Authenticator app on your mobile and click on Next (if you don't want to download the app, you can use the SMS service. Skip to step 9).

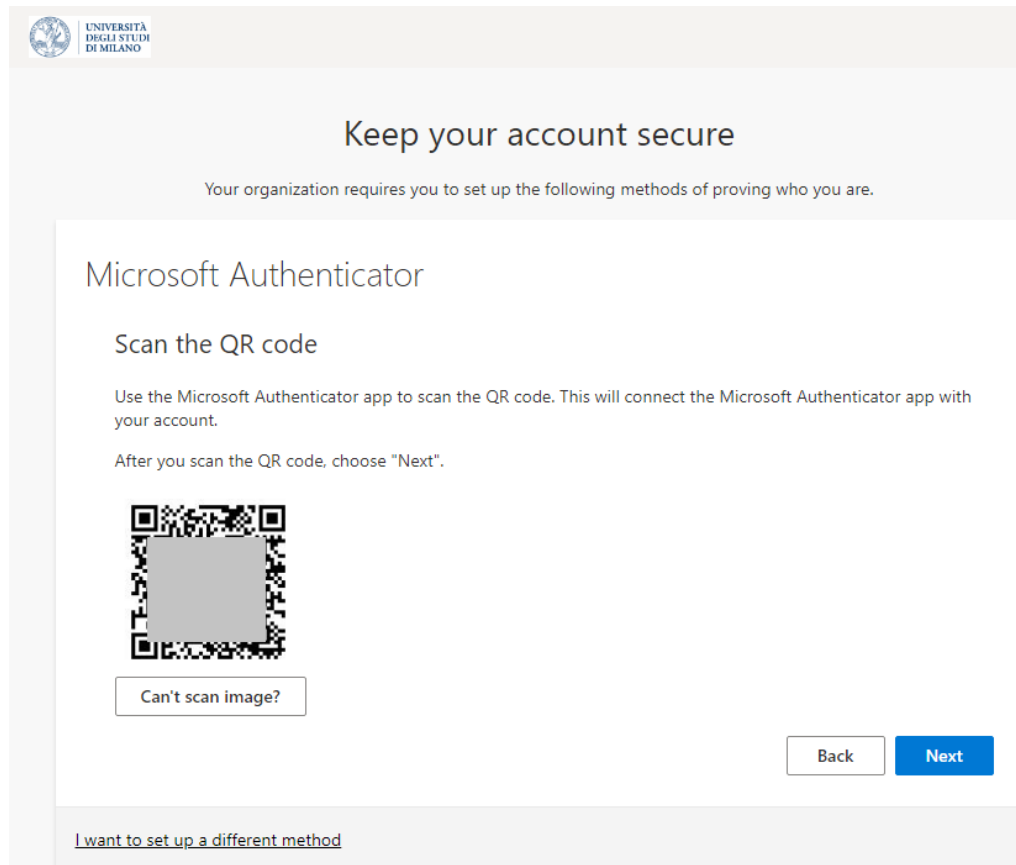


5. Follow the instructions on the following page and click on Next.

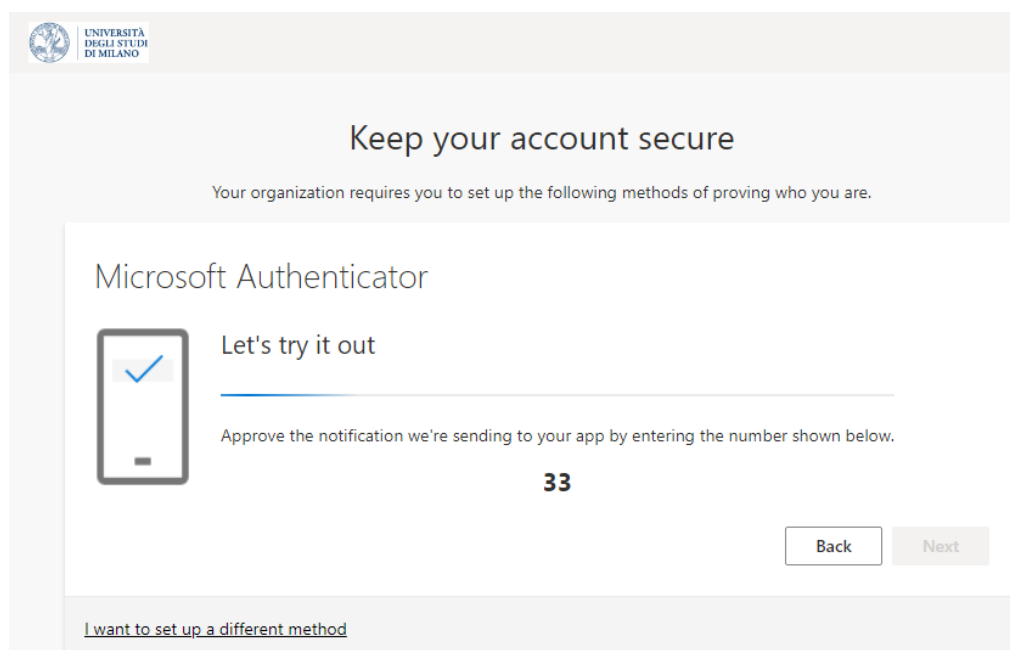




6. On the Microsoft Authenticator app, click on + to add an account, then select “Work or school”. Scan the QR code and click on Next.



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.

The screenshot shows the 'Keep your account secure' screen for the Microsoft Authenticator app. It features the University of Milan logo in the top left. The main heading is 'Keep your account secure', followed by the text 'Your organization requires you to set up the following methods of proving who you are.' Below this, the 'Microsoft Authenticator' section displays a green checkmark icon and the text 'Notification approved'. At the bottom right, there are 'Back' and 'Next' buttons. A link at the bottom left reads 'I want to set up a different method'.

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

The screenshot shows the 'Keep your account secure' screen for the Phone method. It features the University of Milan logo in the top left. The main heading is 'Keep your account secure', followed by the text 'Your organization requires you to set up the following methods of proving who you are.' Below this, the 'Phone' section explains that the user can prove their identity by answering a call or texting a code. It asks 'What phone number would you like to use?' and provides a dropdown menu currently set to 'United States (+1)' and a text input field labeled 'Enter phone number'. There are two radio buttons: 'Text me a code' (selected) and 'Call me'. A disclaimer states: 'Message and data rates may apply. Choosing Next means that you agree to the Terms of service and Privacy and cookies statement.' A 'Next' button is located at the bottom right. A link at the bottom left reads 'I want to set up a different method'.



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

The screenshot shows a web interface for account security. At the top left is the University of Milan logo. The main heading is "Keep your account secure". Below it, a subheading states: "Your organization requires you to set up the following methods of proving who you are." The section is titled "Phone". It contains the text "We just sent a 6 digit code to" followed by a blank space and "Enter the code below." Below this is a text input field with the placeholder "Enter code". A blue link "Resend code" is positioned below the input field. At the bottom right of the form area are two buttons: "Back" and "Next". At the very bottom of the page, there is a link: "I want to set up a different method".

11. The authentication process has been completed.

This screenshot shows the same "Keep your account secure" page, but the authentication is complete. The "Phone" section now displays a green checkmark icon followed by the text "SMS verified. Your phone was registered successfully." A blue "Next" button is located at the bottom right of the form area. The University of Milan logo and the main heading remain the same.