



Per contrastare i casi di violazione delle caselle di posta elettronica, sempre più frequenti, la Direzione ICT ha deciso di attivare l'**autenticazione a più fattori (MFA)**.

Cos'è l'autenticazione a più fattori?

L'autenticazione a più fattori (o MFA) è un sistema che garantisce una maggiore sicurezza durante la fase di accesso alla propria casella di posta o al proprio account Microsoft 365. Per farlo prevede un ulteriore step di autenticazione, oltre al normale utilizzo di nome utente e password. Questo nuovo passaggio può essere personalizzato dall'utente.

Come funziona l'autenticazione a due fattori di Microsoft?

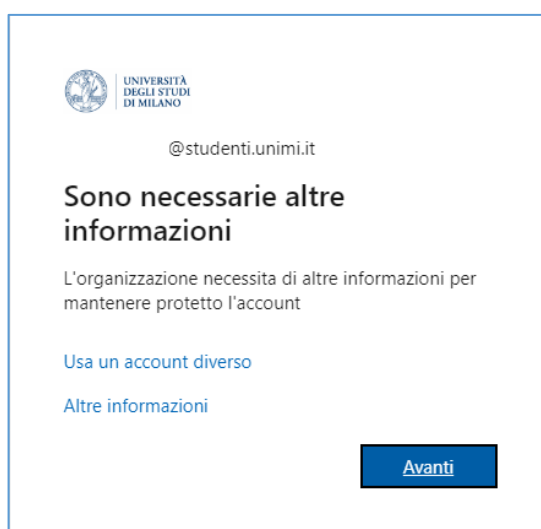
L'accesso ai servizi Microsoft con MFA prevede la ricezione sul proprio smartphone di un **codice temporaneo**, che viene richiesto dopo l'inserimento di nome utente e password.

Per ricevere il codice temporaneo si può utilizzare:

- **app Microsoft Authenticator**, scaricabile gratuitamente su tutti gli smartphone Android e iOS
- **app di autenticazione di terze parti**, come ad esempio Google Authenticator
- **SMS**, se non si desidera o non è possibile installare applicazioni sul proprio telefono.

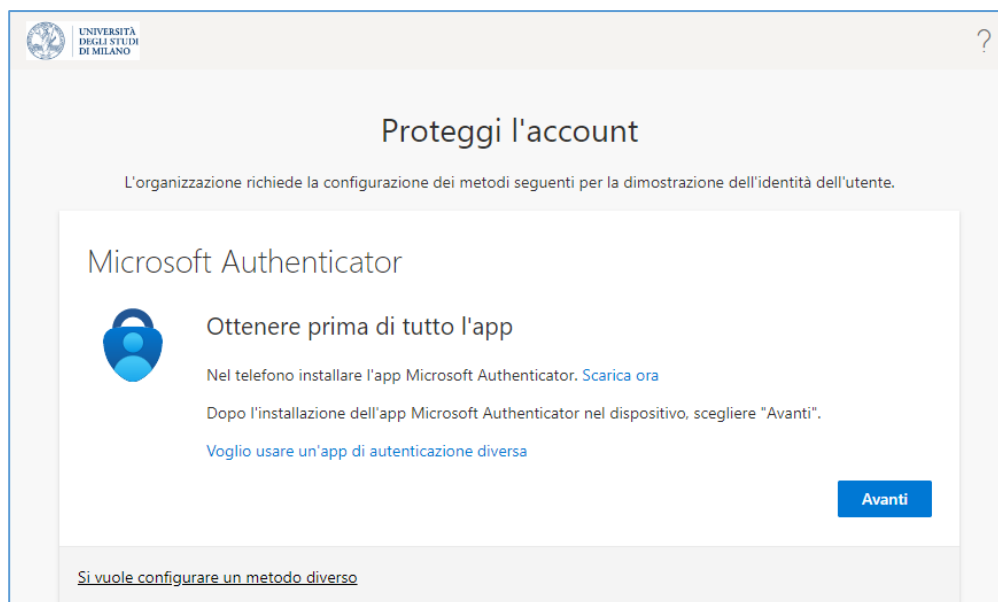
Cosa devo fare per configurare la MFA?

1. Vai al link <https://aka.ms/MFASetup>
2. fai il login con il tuo user id e password di Ateneo
3. il sistema informa che sono necessarie altre informazioni: clicca sul tasto **Avanti**

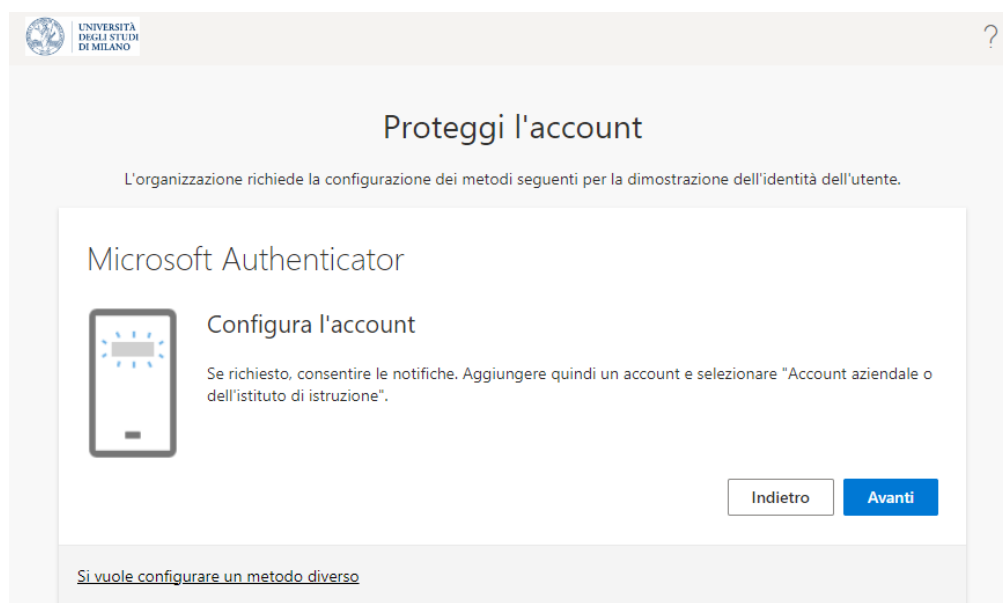




4. installa l'app Microsoft Authenticator sul cellulare e clicca su Avanti (se non vuoi installare l'app sul tuo dispositivo puoi usare gli SMS. Salta al punto 9).

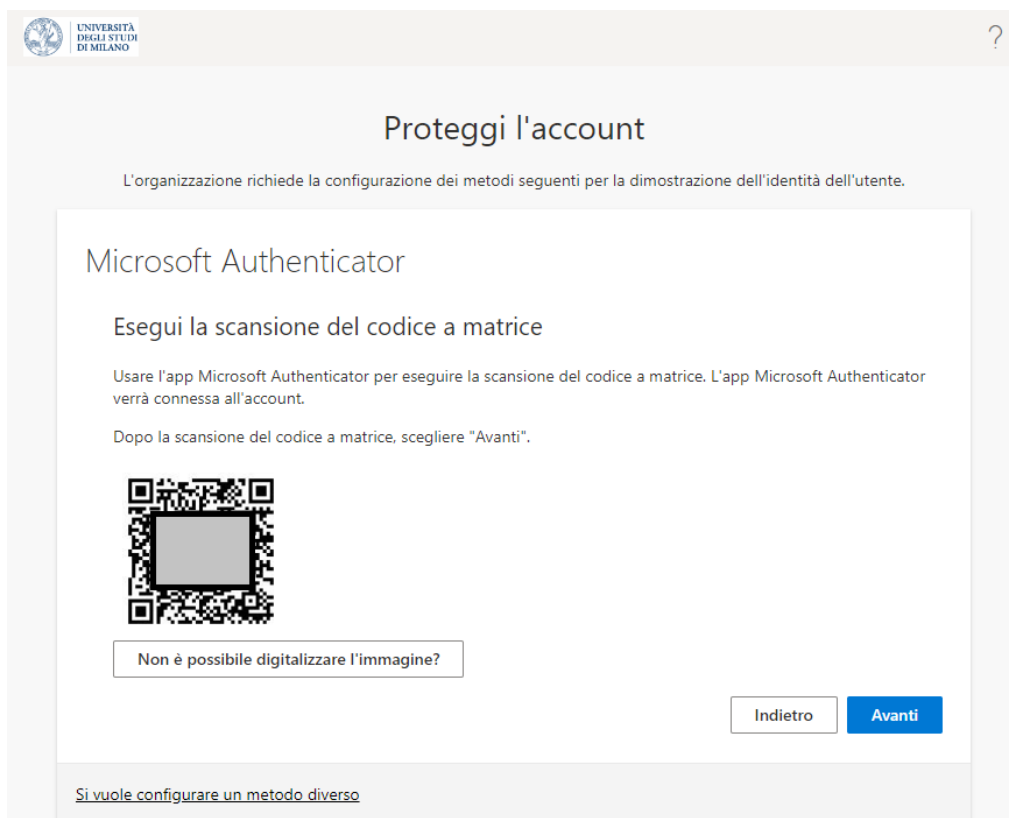


5. segui le istruzioni della schermata successiva e clicca su Avanti.

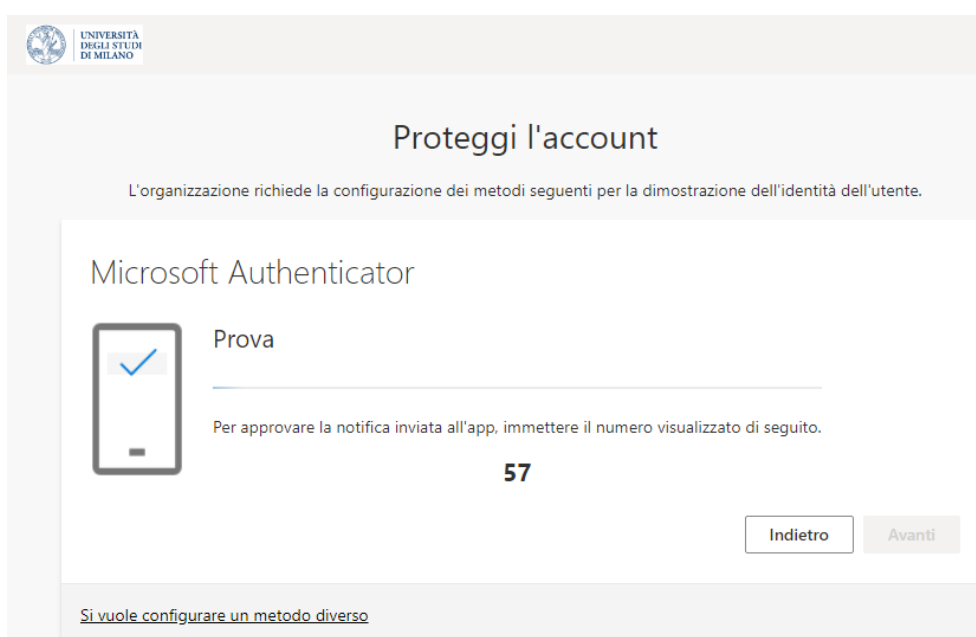




- sull'app Microsoft Authenticator aggiungi un account cliccando sul segno + e seleziona "Account aziendale o dell'istituto di istruzione". Scansiona il codice QR e dopo clicca su Avanti.



- Nella schermata verrà proposto un numero di due cifre che andrà inserito nell'app Microsoft Authenticator per verifica.





8. La procedura si è conclusa.

The screenshot shows the 'Proteggi l'account' (Protect your account) screen. At the top left is the University of Milan logo. The main heading is 'Proteggi l'account'. Below it, a message states: 'L'organizzazione richiede la configurazione dei metodi seguenti per la dimostrazione dell'identità dell'utente.' The central content area is titled 'Microsoft Authenticator' and features a green checkmark icon with the text 'La notifica è stata approvata'. To the left of this text is a small icon of a smartphone displaying a checkmark. At the bottom right of the content area are two buttons: 'Indietro' (Back) and 'Avanti' (Next). At the bottom left of the screen, there is a link: 'Si vuole configurare un metodo diverso'.

9. Se preferisci non utilizzare l'app Microsoft Authenticator puoi scegliere di configurare un metodo diverso (Telefono).

The screenshot shows the 'Proteggi l'account' (Protect your account) screen for the 'Telefono' (Phone) method. At the top left is the University of Milan logo. The main heading is 'Proteggi l'account'. Below it, a message states: 'L'organizzazione richiede la configurazione dei metodi seguenti per la dimostrazione dell'identità dell'utente.' The central content area is titled 'Telefono'. Below the title, it says: 'È possibile dimostrare la propria identità rispondendo a una telefonata o con l'invio di un codice al telefono tramite SMS.' The next line is 'Specificare il numero di telefono da usare.' Below this, there is a dropdown menu showing 'Italy (+39)' and a text input field containing '3331111111'. There are two radio buttons: 'Invia un SMS' (selected) and 'Chiama'. Below these, it says: 'È possibile che vengano applicate le tariffe per messaggi e dati. Scegliendo Avanti si accettano le Condizioni del servizio e l'Informativa sulla privacy e sui cookie.' At the bottom right of the content area is a blue 'Avanti' button. At the bottom left of the screen, there is a link: 'Si vuole configurare un metodo diverso'.



10. Viene inviato un SMS con un codice da inserire nella pagina.

The screenshot shows a web interface for account protection. At the top left is the University of Milan logo. The main heading is 'Proteggi l'account'. Below it, a message states: 'L'organizzazione richiede la configurazione dei metodi seguenti per la dimostrazione dell'identità dell'utente.' The section is titled 'Telefono'. It contains the text: 'Un codice di 6 cifre è stato appena inviato a +39' and 'Immettere il codice più avanti.' Below this is a text input field with the placeholder 'Immettere il codice'. A link 'Invia di nuovo il codice' is positioned below the input field. At the bottom right of the form area are two buttons: 'Indietro' and 'Avanti'. At the bottom left of the page, there is a link: 'Si vuole configurare un metodo diverso'.

11. La procedura è terminata.

The screenshot shows the same 'Proteggi l'account' page. The heading and introductory message are the same. The 'Telefono' section now displays a green checkmark icon followed by the text: 'Verificato tramite SMS. Il telefono è stato registrato.' A blue 'Avanti' button is located at the bottom right of the form area.