Sommario

1. **Introduzione**
2. **Autenticazione a due fattori**
3. **Attivazione dell'autenticazione a due fattori**
4. **Disattivazione dell'autenticazione a due fattori**

1. Introduzione

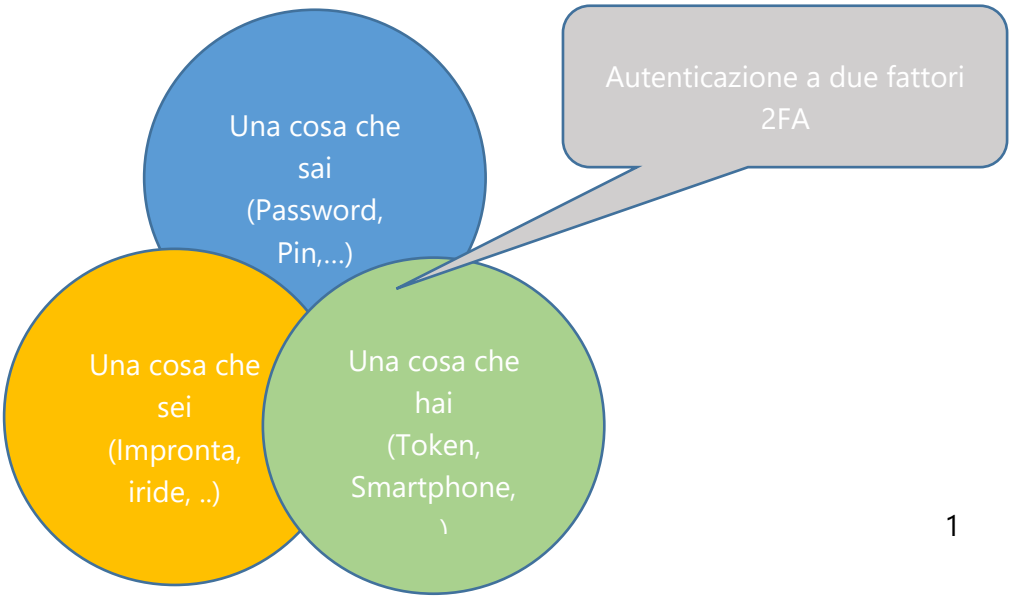
Un'autenticazione basata solo su password è intrinsecamente debole, anche se la password impostata è robusta, perché la sicurezza dell'account dipende da un solo fattore, appunto la password. Per innalzare i livelli di sicurezza sono state introdotte le tecniche di "strong authentication" o autenticazione a due fattori. L'autenticazione a due fattori è oggi un sistema di protezione sicuro a disposizione di ciascun utente dell' Ateneo per proteggere il proprio account dall'accesso Indesiderato.

2. Autenticazione a due fattori

L'autenticazione a due fattori non può più essere considerata un "lusso" da applicare solo negli account bancari, ma dovrebbe essere utilizzata per tutti quegli account nei quali si trovano dati importanti.

Per accedere a qualunque sistema digitale (computer, bancomat, siti web o altro) dobbiamo innanzitutto "presentarci" inserendo il nostro username. Poi "dimostrare" nella fase di Autenticazione che siamo proprio noi mediante uno o più fattori :

- Conoscenza: "Una cosa che sai", per esempio una password o il PIN.
- Possesso: "Una cosa che hai", come uno smartphone o un token di sicurezza .
- Inerenza: "Una cosa che sei", come l'impronta digitale, il timbro vocale, il viso, l'iride, o qualunque altro dato biometrico.

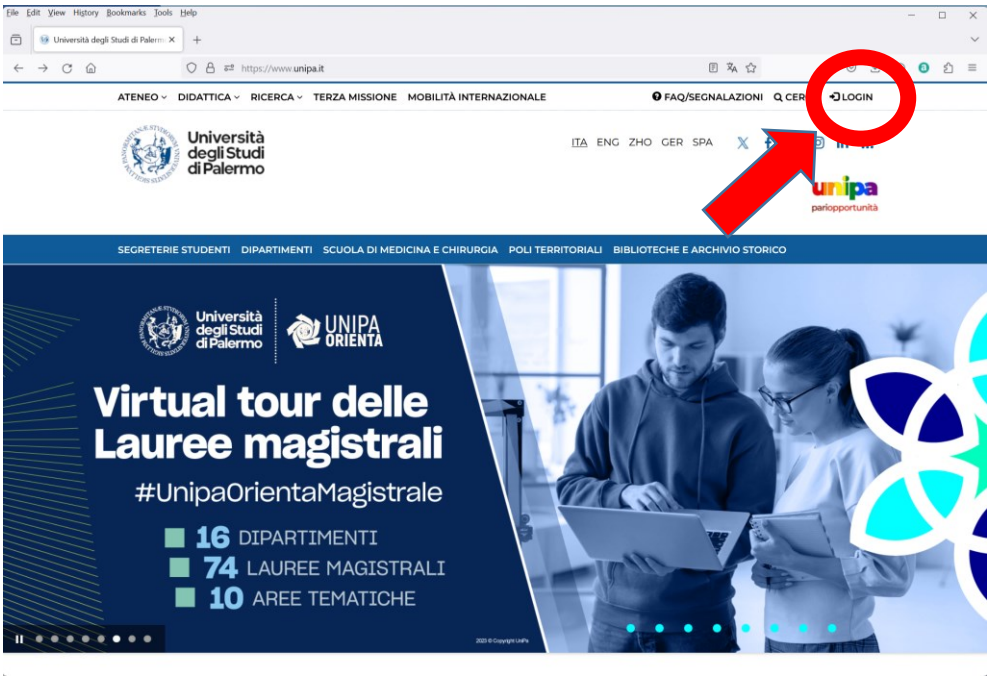


Per utilizzare l'autenticazione a due fattori 2FA, dopo aver inserito la password (primo fattore) del proprio account, sarà richiesto di digitare un secondo fattore, che nella maggior parte dei casi è un codice numerico. Questo secondo fattore viene ottenuto attraverso lo smartphone tramite un'apposita applicazione.

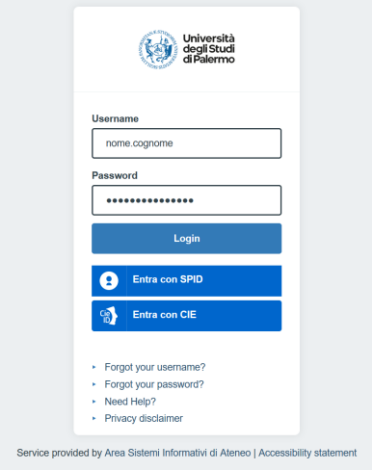
A differenza della password, il secondo codice è di fatto inattaccabile, perché generato in maniera pseudocasuale secondo uno specifico algoritmo ed ha una durata molto limitata nel tempo (alcuni secondi). Per questo motivo, lo si definisce anche OTP: "one time password".

3. Attivazione dell' "autenticazione a due fattori"

Per attivare sul portale Unipa l'autenticazione a due fattori, per prima cosa va effettuato il login dopo aver digitato l'URL https://www.unipa.it/:

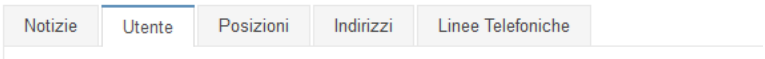


Verrete reindirizzati sulla pagina di login dell'Università degli studi di Palermo :



Verrano quindi richiesti la vostra User id e la vostra password per effettuare il login sui sistemi Unipa.

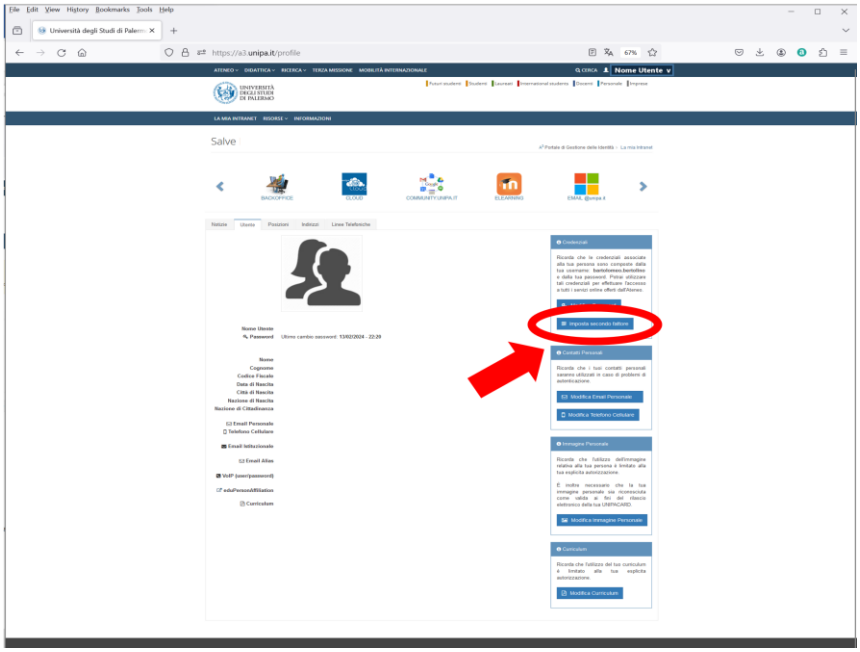
Successivamente verrete reindirizzati sulla pagina "intranet " di Ateneo (o la selezionerete manualmente dall'elenco a discesa presente in alto a sinistra), dove sono presenti diverse schede :



Selezionando la scheda "Utente" verrà mostrata una pagina personalizzata contenente la vostra foto (se inserita), il nome utente, l'ultimo cambio password, i giorni residui di validità

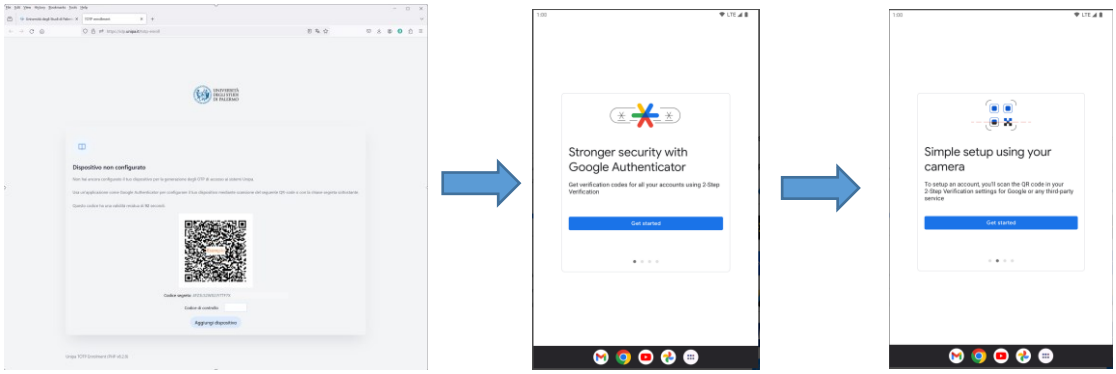
della password, i vostri dati personali, l'user e la password del voip ed i ruoli coperti in Ateneo.

Sulla vostra sinistra avrete la possibilità di modificare la password, modificare la mail personale, modificare il numero di cellulare, modificare l'immagine personale, modificare il curriculum e **impostare l'autenticazione a due fattori** :



Selezionando il pulsante "Imposta secondo fattore" come indicato nell'immagine a fianco, l'utente viene rediretto nella pagina di login Unipa per motivi di sicurezza. Inseriti nuovamente nome utente e passoword si arriva ad una schermata contenente un Qr-Code oltre ad una chiave segreta alternativa da digitare manualmente.

Visualizzata la schermata contenente il codice QR occorre configurare un dispositivo utilizzando un applicazione come Google Authenticator:

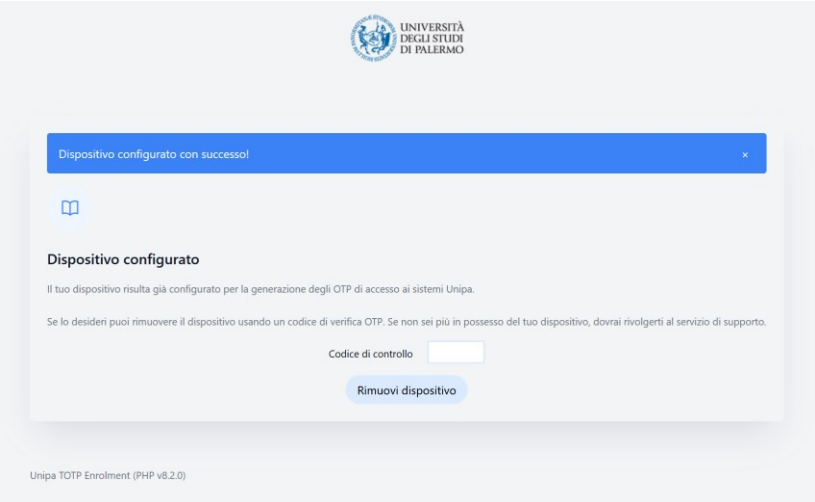


Mediante la scansione del codice QR con l'applicazione Google Authenticator, sarete reindirizzati sul proprio smartphone ad una pagina contenente le scritte (esempio) :

Login Unipa: nome.cognome 123 456

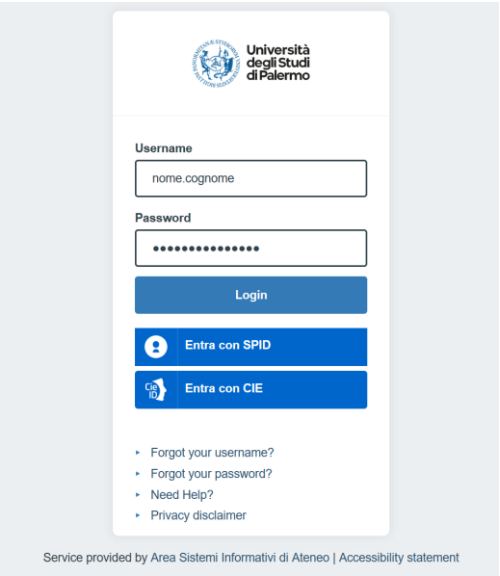
le due coppie di numeri vanno inseriti appena sotto il codice QR della pagina di attivazione del secondo fattore, per poi cliccare su aggiungi dispositivo.

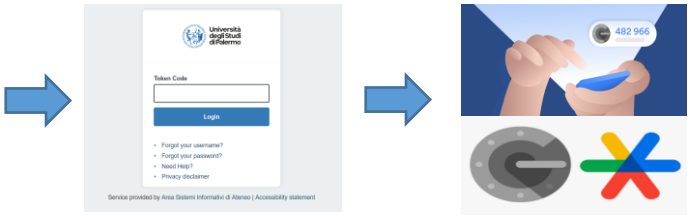
Si viene quindi reindirizzati ad una seconda pagina sul browser che attesta l'avvenuta configurazione di un dispositivo per l'autenticazione a due fattori:



Da questo momento in poi per accedere al portale Unipa sarà richiesta l'autenticazione a due fattori, ovvero dopo aver inserito il nome utente e la password, comparirà la richiesta di inserimento di un token temporaneo (OTP) utilizzando l'applicazione Google Authenticator.

Senza tale token non è possibile effettuare l'accesso:





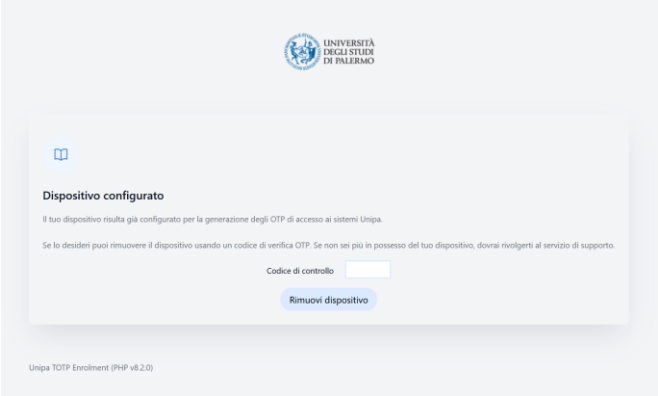
Come si vede dalla sequenza di immagini, l'utente per accedere al portale unipa dovrà inserire il Token code proveniente dall'applicazione Google Authenticator.

E' possibile in ogni momento disattivare l'autenticazione a due fattori.

4. Disattivazione dell' "autenticazione a due fattori"

Per disattivare l'autenticazione a due fattori, occorre nuovamente effettuare il login sul portale unipa ed accedere all'area intranet sulla scheda "utente" come descritto al punto 3.

Cliccando sul bottone "imposta Secondo Fattore" comparirà la seguente schermata , dove è possibile inserire il token temporaneo presente sul applicazione Google authenticator per rimuovere il dispositivo.



Rimosso il dispositivo si ritorna alla normale configurazione nome utente e password.