Abilitazione autenticazione a più fattori per tutti gli utenti di Ateneo

Gentili utenti,

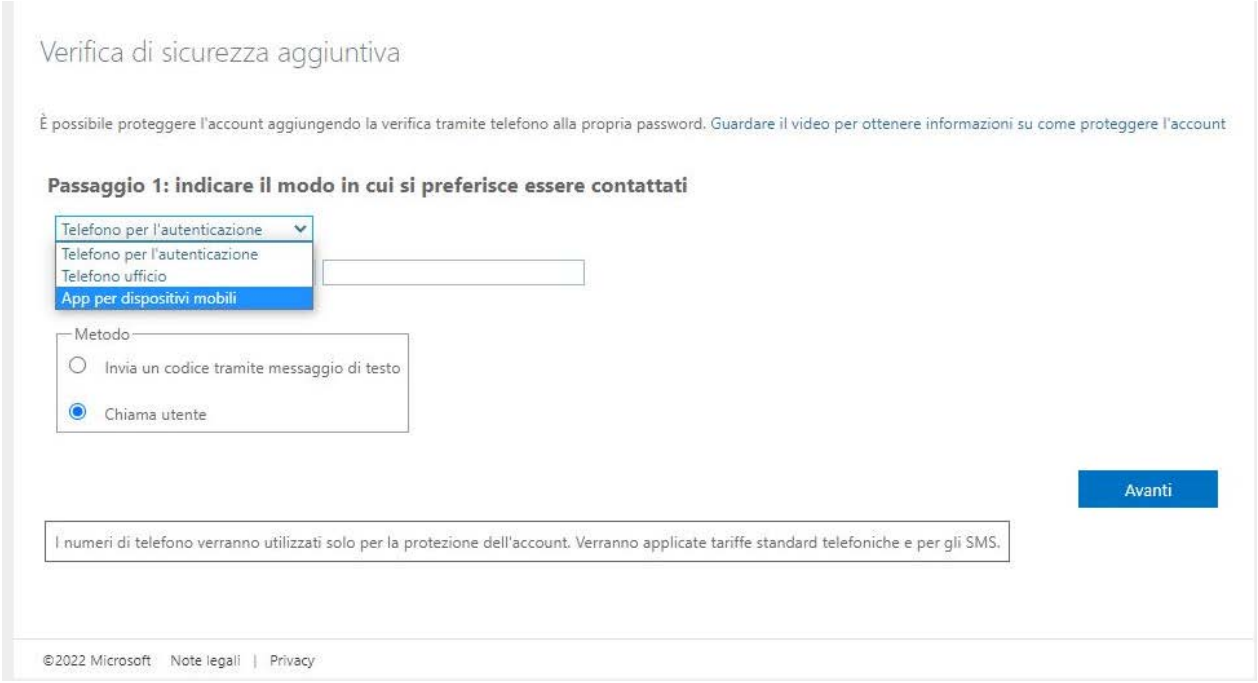
nell'ambito del processo di miglioramento dei servizi informatici, tenuto conto della crescente necessità di migliorare la sicurezza di tutti i servizi offerti dall'Ateneo, visto inoltre le recenti normative per il lavoro agile, visto i recenti furti di credenziali avvenuti ai danni di singoli utenti, la presente è per informarvi che verrà forzata l'autenticazione a più fattori - due - (MultiFactor Autentication - MFA) per tutti gli utenti Microsoft (Studenti, Docenti e Personale di Ateneo).

L'autenticazione a più fattori che verrà attivata, in base anche alla recente direttiva NIST SP 800-63B, è quella che richiede di utilizzare durante la fase di login due fattori di riconoscimento ed in particolare:

1) Qualcosa che si conosce (password)
2) Qualcosa che si possiede (telefono/smartphone)

Questo cambiamento aumenterà di molto la sicurezza di tutti gli utenti dal furto delle credenziali al pari di quello che attualmente avviene per i servizi bancari.

Questo significa che all'atto del primo login - successivo all'introduzione di MFA - su qualsiasi dispositivo, verrà richiesto di scegliere un secondo fattore di identificazione a scelta tra i seguenti:



1. App Microsoft Authenticator – Si tratta di un'applicazione mobile molto semplice da installare sullo smartphone che permette di memorizzare il proprio "account" e quindi di abilitare in modo molto semplice il login (simile al token su applicativo delle APP bancarie) – Questo meccanismo permette l'autenticazione ovunque si sia in possesso dello smartphone.
2. Telefono Ufficio/stanza – Si tratta di specificare un numero di telefono fisso cui ricevere il secondo fattore di autenticazione – Questo meccanismo vincola l'autenticazione all'essere presenti nel proprio ufficio/stanza dove è presente il telefono fisso.
    a. Chiamata

3. Telefono personale – Si tratta di specificare un numero di telefono mobile cui ricevere il secondo fattore di autenticazione – Questo meccanismo permette l'autenticazione ovunque si sia in possesso del numero di telefono personale.
    a. Chiamata
    b. SMS

NB. l'utilizzo del metodo 2. e del metodo 3. obbliga l'utente a settare una nuova password da impostare negli applicativi client, in quanto questi non supportano il telefono come secondo fattore (Outlook, Apple mail, etc).

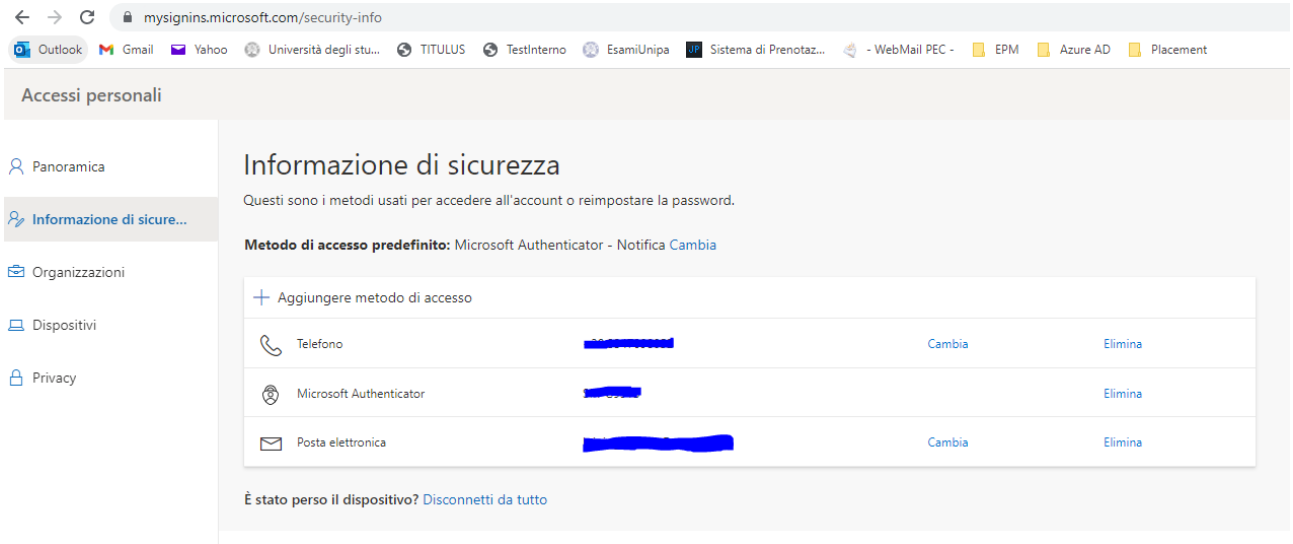
Considerando le peculiarità di tali meccanismi di autenticazione è altamente consigliato l'utilizzo **dell'APP Mobile Microsoft Authenticator**, oppure in seconda battuta del Telefono personale.

NB. È altamente consigliato effettuare il primo login successivo all'attivazione del MFA utilizzando un browser web in modo da settare in maniera appropriata tutte le peculiarità dello stesso.

NB. Il secondo codice di autenticazione verrà richiesto solo in fase di login.

NB. Cogliamo inoltre l'occasione per ricordare a tutti gli utenti di effettuare una verifica (Molto importante) sulla disponibilità ed aggiornamento delle informazioni che permettono il recupero della password dell'account Microsoft.

Per poter effettuare tale verifica è necessario loggarsi al seguente link: https://mysignins.microsoft.com/security-info e quindi verificare la sussistenza di almeno uno tra telefono e posta elettronica (l'indirizzo di posta elettronica alternativa deve essere su un dominio diverso da quello Parthenope). In caso contrario sarà necessario inserire/aggiornare le dovute informazioni.



NB. A partire dalla data di abilitazione del MFA molti client di posta che utilizzano protocolli antiquati e poco sicuri (pop3, imap, etc.) potrebbero non funzionare e pertanto l'Ateneo consiglia di installare client di posta che supportino la "Moder Authentication" come, ad esempio, il client Microsoft Outlook fornito gratuitamente all'interno del pacchetto Office 365 di Ateneo.

Esempio di client che utilizza (di default) un protocollo obsoleto è Thunderbird, in tal caso va configurato il protocollo OAuth 2.0.

Per qualsiasi informazione e/o problema con MFA, è stato predisposto un apposito ticket di assistenza all'interno della piattaforma di ticketing di Ateneo: https://supporto.uniparthenope.it/

Ulteriori informazioni su MFA, sull'APP Microsoft Authenticator e sulla Moder Authentication sono disponibili qui:

1. https://docs.microsoft.com/it-IT/azure/active-directory/authentication/concept-mfa-howitworks
2. https://docs.microsoft.com/it-it/azure/active-directory/authentication/concept-authentication-authenticator-app
3. https://docs.microsoft.com/it-it/microsoft-365/enterprise/hybrid-modern-auth-overview?view=o365-worldwide