2024-03-19

Multifaktorautentisering (MFA)

Multifaktorautentisering (MFA), även känd som tvåstegsverifiering, innebär att du som en extra säkerhetsåtgärd använder dig av två olika verifieringssteg för att få tillgång till vissa tjänster, såsom e-post, Microsoft SharePoint och Microsoft Teams, osv. Efter steg ett där du anger ditt användarnamn och lösenord måste du ge ytterligare godkännande i nästa steg. Det andra steget utförs via din mobiltelefon och applikationen Microsoft Authenticator.

Varför krävs MFA?

Multifaktorautentisering är ett krav från Myndigheten för samhällsskydd och beredskap (MSB) enligt föreskrift (2020:07).

MFA gör det möjligt för studenter att bevisa att de är den de utgör sig vara. Eftersom du själv måste aktivt godkänna din inloggning i ett andra steg utesluter du effektivt obehöriga inloggningar. Skulle en obehörig lyckas komma över dina kontouppgifter kommer de inte åt ditt MDU-konto/tjänst/applikation eftersom du själv måste utföra steg två i inloggningsförfarandet.

Som student, med en MDU e-postadress, innefattas du av dessa krav och kommer per automatik bli aktiverad för MFA, man har sedan 14 dagar på sig att registrera MFA.

För att kunna registrera MFA behöver du som student en iPhone med stöd för iOS 15.0 eller senare/Android med operativsystem 8.0 eller senare. Applikationen Microsoft Authenticator finns tillgänglig till Android och iOS. Se till att du håller dig uppdaterad med den senaste Android- eller iOS-versionen för den bästa autentiseringsupplevelsen.

Observera att det finns andra applikationer med liknande namn och ikon, så försäkra dig om att det är Microsoft Authenticator av Microsoft Corporation som du installerar.

Aktivera MFA för första gången

Börja med att installera applikationen Microsoft Authenticator på din mobiltelefon. Du kan hitta applikationen i Play Store/App Store.

Observera att endast applikationen Microsoft Authenticator är godkänd av MDU att användas som autentiseringsapplikation. Se till att det är den korrekta applikationen när du installerar den.

- Starta Microsoft Authenticator på din mobila enhet och godkänn villkoren.
- Börja med att välja **Lägg till ett konto**.
- Välj **Arbete eller skolkonto**.
- Klicka på **Skanna QR-koden** och ge åtkomst till kameran samt tillåt aviseringar och meddelanden från applikationen.

Gå sedan till Microsoft-sidan för hantering av MFA-applikationen, helst från en dator:
https://mysignins.microsoft.com/security-info

- Klicka på **Nästa** i de följande rutorna tills en sida med en QR-kod visas.
- Använd nu din mobila enhet för att skanna QR-koden genom Microsoft Authenticator.
- Klicka sedan på **Nästa**.
- Du kommer nu att bli ombedd att verifiera detta, matcha siffrorna från skärmen och ange siffrorna i applikationen.
- Klicka på **Nästa** och nu har du framgångsrikt lagt till tvåstegsverifieringen. Du kan nu stänga fönstret.

Godkänn inloggningen

Viktigt Godkänn aldrig en inloggning som du inte förväntar dig. Om du är osäker är det bättre att neka inloggningen.

När du loggar in med ditt MDU-konto måste du som nästa steg godkänna inloggningen i Microsoft Authenticator på din mobila enhet.

- Logga in på ditt MDU-konto på en dator eller mobil enhet.
- En ruta för godkännande kommer visa sig.
- I den rutan kommer en siffra finnas, den siffran måste du skriva in i Microsoft Authenticator på din mobila enhet som du registrerat MFA på.
- Du kan även passa på att bocka i rutan **Don't ask again for 14 days**. Inloggningen på den specifika enheten du använder kommer då att vara giltig i 14 dagar.
- När du har skrivit in siffran i Microsoft Authenticator, tryck **Ja**.

Lägg till en ny enhet till befintlig MFA

Till exempel, starta Google Chrome-webbläsaren på din dator.

- I adressfältet måste du ange https://mysignins.microsoft.com/security-info
- Logga in med din MDU-e-postadress och lösenord, godkänn inloggningen i Microsoft Authenticator på den mobila enhet där du redan har konfigurerat MFA.
- Klicka på **Security info** i vänstra fältet och sedan på **Add sign-in method**.
- Välj **Authenticator app** och klicka sedan på **Add**.
- En ruta kommer nu komma upp med en guide som ska följas.
- Hitta enheten du vill lägga till i MFA och installera Microsoft Authenticator från enhetens appbutik. Starta Microsoft Authenticator och godkänn villkoren.

Observera att endast applikationen Microsoft Authenticator är godkänd av MDU att användas som autentiseringsapplikation. Se till att det är den korrekta applikationen när du installerar den.

- Starta Microsoft Authenticator på din mobila enhet.
- På din mobila enhet väljer du **Skanna en QR-kod**.
- På din mobila enhet godkänner du åtkomstbegäran till kameran.
- På datorn klickar du på **Nästa** när du ombeds ladda ner Microsoft Authenticator.
- På datorn klickar du på **Nästa** när du ombeds konfigurera ditt konto.
- Rikta din mobila enhets kamera mot din datorskärm och skanna QR-koden.
- På datorn klickar du på **Nästa** när du har skannat QR-koden.
- På din mobila enhet, skriv in siffran som visas på datorn.
- Klicka på **Ja**.

Ta bort en enhet i MFA

Till exempel, starta Google Chrome-webbläsaren på din dator.

- I adressfältet måste du ange https://mysignins.microsoft.com/security-info
- Logga in med din MDU-e-postadress och lösenord, godkänn inloggningen i Microsoft Authenticator på den enhet där du redan har konfigurerat MFA.
- Tryck på **Delete** bredvid enheten som du vill ta bort.

Förlorad/trasig enhet

Har du inte tillgång till din registrerade telefon? På campus så kan du återställa din multifaktorautentisering i en datorsal, du följer rutinen som finns under rubriken “Ta bort en enhet i MFA”.

Har du inte möjlighet att ta dig till campus måste du kontakta studenttorget för att få hjälp med att återställa din autentisering. För att studenttorget ska kunna hjälpa dig att återställa din enhet behöver du ansluta via Zoom och legitimera dig.