

To-faktor-godkendelse

Denne vejledning henvender sig til alle ansatte og beskriver, hvordan du opsætter to-faktor-godkendelse på dit login til Office 365. Det er kun nødvendigt med to-faktor-godkendelse, når du ikke er tilkoblet ITS'/skolens netværk eller VPN. To-faktor-godkendelse bidrager til at øge informationssikkerheden, når du ikke er tilkoblet VIAs netværk eller VPN.

Selvom du måske kun er på skolen netværk eller benytter dig af VPN, så opfordres du til at sætte tofaktor-godkendelse op!!

Vejledningen kommer ind på følgende:

- 1. Installation og opsætning af to-faktor-godkendelse (Microsoft Authenticator)
- 2. Brug af Microsoft Authenticator.

Installation og opsætning af to-faktor-godkendelse (Microsoft Authenticator)

Bemærk at opsætning af to-faktor-godkendelse kræver, at du bruger både din computer og mobiltelefon. Hver gang du skal skifte fra computer til mobil eller omvendt, vil det stå i vejledningen.

Start med at åbne websiden <u>https://aka.ms/mfasetup</u> fra din computer og log på med dit ITS Office 365 brugernavn.

Du kan blive bedt om at vælge dit ITS Office 365 brugernavn flere gange.

- 1. Vælg din konto.
- 2. Vælg Næste.

Du vil efterfølgende blive bedt om at fortsætte installationen fra din mobiltelefon.

Vderligere oplysninger krævet Din virksomhed har brug for at få flere oplysninger til et beskytte din konto Brug en anden konto Få mere at vide Næste



- 3. Hent "Microsoft Authenticator" på din mobiltelefon eller tablet, hvis du ikke har app'en i forvejen. Bemærk at der er flere apps der dukker op, når du søger på Microsoft Authenticator. Den korrekte app hedder <u>Microsoft</u> Authenticator <u>Direkte link til Microsoft Authenticator i Apple App Store finder du her</u> <u>Direkte link til Microsoft Authenticator i Google Play finder du her</u>
 - Tillad appen at sende dig notifikationer, hvis du ønsker at få en notifikation hver gang, du skal godkende login til en Office 365 løsning.
- 4. Vælg herefter Næste på computeren.

c	Beskyt din k Din organisation kræver, at du konfigurerer følger	KONTO nde metoder til at bevise, hvem du er.
	Metode 1 af 2: /	Арр
	Арр	2 Telefon
Micros	oft Authenticator	
9	Start med at hente appen Installér Microsoft Authenticator-appen på o Når du har installeret Microsoft Authenticat	din telefon. Hent nu or-appen på din enhed, skal du vælge "Næste".
	Jeg vil bruge en anden godkenderapp	Næste

Hvis du allerede har en ITS Office 365 konto i Microsoft Authenticator på din mobiltelefon eller tablet, så skal du slette den og oprette en ny. Punkt 5 nedenfor gennemgår, hvordan du opretter en ITS Office 365 konto på Android, mens punkt 6 gennemgår, hvordan du gør på iOS (Apple).

- 5. Tilføj din ITS Office 365 konto på Android:
 - Åbn Microsoft Authenticator appen på din mobiltelefon.
 - Vælg de tre lodrette prikker.
 - Vælg "Tilføj konto"
 - Vælg herefter "Arbejds- eller skolekonto".







7. Vælg Næste på computeren.



	Beskyt din	konto		
Dir	n organisation kræver, at du konfigurerer følge	nde metoder til at bevise, hvem du er.		
Metode 1 af 2: App				
	Ø App	2 Telefon		
Microso	oft Authenticator			
	Konfigurér din konto Tillad meddelelser, når du bliver spurgt om eller skole".	dette. Tilføj derefter en konto. og vælg "Arbejde		
L-J		Tilbage Naeste		

- 8. Vælg "Scan QR-kode"
 - Med din mobiltelefon, scan QR koden, der vises på din computer.
- 9. Vælg Næste på computeren.



Godkend beskeden i app'en på din mobiltelefon. Microsoft Authenticator er nu sat op.

Du skal nu tilknytte dit mobiltelefonnummer til Microsoft Authenticator på computeren.



- 10. Vælg den korrekte landekode (Danmark +45) og udfyld med det ønskede mobiltelefonnummer.
- 11. Sæt flueben i Send mig en kode på SMS.
- 12. Vælg Næste.

Metode 2 af 2: Telefon				
App		Telefon		
Telefon				
Du kan bevise din identiet ve Hvilket telefonnummer vil du	d at besvare et opkald på din bruge?	telefon eller skrive en kode til din telefon. 10		
 Send mig en kode på sm Ring til mig 	11	anger un bereronnammer		
SMS- og datatakster kan vær om beskyttelse af personlige	e gældende.Når du vælger N oplysninger og cookies.	æste, accepterer duServicebetingelserogErklæring Næste		

Microsoft Authenticator sender nu en SMS med en kode, der skal indtastes. Herefter er to-faktorgodkendelse færdigkonfigureret.

13. Vælg Udført.



Brug af Microsoft Authenticator

Hvis du <u>ikke</u> befinder dig på ITS'/skolens netværk eller er tilkoblet VPN, vil du blive bedt om at validere dig/godkende på mobiltelefonen for at kunne tilgå Office 365. Hvis du derimod befinder dig på ITS'/skolens netværk og er tilkoblet ITS'/skolens netværk eller VPN, vil du ikke skulle validere dig/godkende på mobiltelefonen.



Der kan dog være forskellige scenarier i forhold til, hvornår du skal validere dig/godkende på din mobiltelefon alt afhængig af, hvorvidt det Office 365 program/app du ønsker at tilgå giver dig mulighed for at udsætte næste validering med 14 dage på den enkelte enhed.

Nedenstående eksempel viser, hvordan Outlook på computeren beder om, at du skal godkende din logonanmodning. For at godkende skal du gøre følgende:

- 1. Åbn Microsoft Authenticator app'en på din mobiltelefon.
- 2. Godkend i appen.
 - Sæt evt. flueben i "Spørg mig ikke igen før om 14 dage" på computeren, før du godkender, hvis du vil udskyde næste validering med 14 dage.

