

Wat is Tweefactorauthenticatie (2FA)?

In de zorg werk je dagelijks met privacygevoelige en medische gegevens. Een simpel wachtwoord biedt onvoldoende bescherming, want wachtwoorden kunnen makkelijk worden gelekt of gekraakt. Tweefactorauthenticatie (2FA) voegt een extra beveiligingslaag toe, waardoor jouw data beter beschermd blijft tegen hackers en ongeautoriseerde toegang.

De gegevens achter slot en grendel

Zie een wachtwoord als een sleutel: als iemand een kopie maakt, kan diegene zo naar binnen. Tweefactorauthenticatie voegt een extra slot toe. Naast je wachtwoord heb je een tweede verificatiemethode nodig, zoals een code via een app of een SMS. Hierdoor wordt het voor hackers veel moeilijker om toegang te krijgen tot je gegevens. Andere namen voor tweefactorauthenticatie zijn tweestapsverificatie of multifactorauthenticatie (MFA).

De voordelen van tweefactorauthenticatie

- **Sterkere beveiliging** – Zelfs als een wachtwoord wordt onderschept, blijft toegang zonder de tweede factor geblokkeerd.
- **Bescherming tegen datalekken** – Voorkomt ongeautoriseerde toegang tot gevoelige informatie, zoals medische en privacygevoelige gegevens.
- **Flexibel in gebruik** – Kies zelf een verificatiemethode die bij jou past, zoals een sms-code, een app of biometrische herkenning.
- **Minimale impact op gebruiksgemak** – Na de eenmalige instelling kost 2FA je slechts een paar extra seconden bij het inloggen.

Hoe werkt tweefactorauthenticatie?

Bij het inloggen op een zorgsysteem of applicatie doorloop je als gebruiker twee verificatiestappen. Eerst wordt een gebruikersnaam en wachtwoord ingevoerd. Vervolgens is een extra controle nodig om de identiteit te bevestigen.

De tweede verificatiestap kan op verschillende manieren:

- **Authenticator-app** – Zoals Microsoft Authenticator, die een tijdelijke code genereert. Deze code lees je af van je telefoon en voert deze handmatig in bij het inloggen.
- **SMS-code** – Een eenmalige code wordt verzonden naar een geregistreerd telefoonnummer die gekoppeld is aan je account.
- **Biometrische herkenning** – Identificatie via een vingerafdrukscan of gezichtsherkenning, waarbij de app je biometrische gegevens verifieert voor toegang.

Eenvoudig in gebruik

Het instellen van Tweefactorauthenticatie duurt **eenmalig 5 minuten**, afhankelijk van de gekozen methode. Dit lijkt misschien een extra stap, maar de verbeterde beveiliging weegt ruimschoots op tegen de tijdsinvestering. Zodra 2FA is geactiveerd, kost het dagelijks inloggen **slechts enkele seconden** extra, terwijl je gegevens aanzienlijk beter beschermd blijven.

Zo zet je je tweefactorauthenticator aan in slechts 3 stappen

1. **Download een authenticatorapp**, zoals *Microsoft Authenticator*, *1Password* of *Google Authenticator*. Deze apps zijn via je telefoon veilig te downloaden via de Appstore of via Google Play.
2. **Ga naar de beveiligingsinstellingen van je account of applicatie**. Deze vind je in je persoonlijke profiel of bij je algemene instellingen.
3. **Volg de stappen van de software**. Hierbij moet je een QR-code scannen via je telefoon of krijg je een eenmalige code binnen via de applicatie.

Bronnen:

<https://www.digitaltrustcenter.nl/tweefactorauthenticatie>

<https://www.consumentenbond.nl/veilig-internetten/activeer-tweestaps-authenticatie>

<https://www.microsoft.com/nl-nl/security/business/security-101/what-is-two-factor-authentication-2fa>