hcc noord-nederland

Wat is tweestapsverificatie?

Tweestapsverificatie: extra beveiliging

Door het instellen van tweestapsverificatie voeg je een extra beveiligingslaag toe aan je WhatsApp, e-mailaccount of de apps waar je gebruik van maakt.

Er zijn verschillende vormen van tweestapsverificatie, ook wel 2FA of dubbele beveiliging genoemd.

Eén daarvan is een toegangscode die naar een vertrouwd apparaat van jou wordt gestuurd om in te kunnen loggen. Hackers hebben dan aan je gebruikersnaam en wachtwoord alleen niet meer genoeg om toegang tot je account te krijgen. Daarnaast heb je een authenticatie-app of gezichtsherkenning (biometrische authenticatie). Naast de toegangscode bestaat er bijvoorbeeld ook een fysieke beveiligingssleutel als security key.

De eerste stap van inloggen in twee stappen is natuurlijk je wachtwoord. Zorg voor een sterk en uniek wachtwoord.

Hoe stel ik mijn 2 factor authenticatie in (2fa) op HCC

Om bepaalde taken uit te voeren is het noodzakelijk twee factor authenticatie in te stellen.

Dat doe je als volgt:
Allereerst inloggen op een van de hcc-sites. Bijvoorbeeld de site van hcc.nl. Je gaat dan naar het menu 'HCC" en kiest voor 'mijn gegevens'. Onder de tab 'account' vindt je de tap 'Mijn authenticatie'.

Lees meer

hcc noord-nederland

Op welke manieren kan je inloggen in twee stappen gebruiken

SMS

Als je inloggen in twee stappen hebt ingesteld via sms dan krijg je bij het inloggen een sms gestuurd. Hierin staat een verificatiecode die je moet invullen.

Pincode

Om een app (applicatie) te beveiligen gebruik je vaak een pincode. Zo zijn apps voor thuisbankieren naast een wachtwoord vaak beveiligd met een pincode. Ook voor WhatsApp is de tweede beveiligingslaag een pincode.

Authenticatieapp

Je gebruikt één app die je koppelt aan verschillende accounts. Zodra je inlogt genereert de app een unieke code die je moet invullen bij het inloggen op je account.

Wat is tweestapsverificatie en hoe stel ik het in?

Als je tweestapsverificatie instelt, voeg je een extra beveiligingslaag toe aan je apps en je accounts. Als je inlogt, moet je niet alleen je wachtwoord invullen, maar ook nog op een andere manier aangeven dat je bent wie je beweert te zijn. Hiermee ben je beter beveiligd tegen hacken.

- Er wordt een toegangscode naar een vertrouwd apparaat van jou gestuurd. Deze code moet je vervolgens doorgeven om in te kunnen loggen. Online criminelen kunnen dan niet meer alleen met je gebruikersnaam en wachtwoord toegang tot je account krijgen.
- Daarnaast bestaat er de authenticatie-app. Als je bij bepaalde accounts inlogt met je gebruikersnaam en wachtwoord, wordt er om een code gevraagd in je authenticatie-app. Als je de app opent, zie je een unieke code. Deze code moet je vervolgens doorgeven aan het account waar je wil inloggen.

Hoe stel je tweestapsverificatie in?
Hieronder vind je de links naar informatie over het instellen van inloggen in twee stappen voor deze accounts of apps:

- WhatsApp
- Facebook
- Instagram
- LinkedIn
- Gmail
- Apple
- Dropbox
- Microsoft
- Snapchat
- TikTok (tekst in het Engels)
- X

Wat is een authenticatie-app?
Een authenticatie-app (verificatie-app) gebruik je als middel om in twee stappen in te loggen op een account.
Zo'n app genereert een unieke code die je moet gebruiken als je inloggen in twee stappen hebt gekoppeld aan een account.
Je logt in op je account met een wachtwoord. Vervolgens krijg je de melding om naar je authenticatie-app te gaan en de code over te nemen.
Hiermee maak je inloggen op een account een stuk veiliger.

Dit zijn een aantal bekende authenticatie-apps:

- Microsoft Authenticator
- Google Authenticator
- Authy
- Duo Mobile
- 1Password
- 2FAS
- Dashlane authenticator
- Bitwarden authenticator
- LastPass authenticator