TWEE-FACTOR-AUTHENTICATIE

AAN DE SLAG MET ZORGTECHNOLOGIE
FACTSHEET: TWEE-FACTOR-AUTHENTICATIE

DIGIVAARDIG IN DE ZORG

Inloggen in twee stappen

Als je tweestapsverificatie instelt, voeg je een extra beveiligingslaag toe aan apps, websites en accounts. Hierdoor hebben cybercriminelen aan een gebruikersnaam en een wachtwoord niet meer genoeg om je te hacken.

Een tweede beveiligingslaag

Als je tweestapsverificatie instelt, voeg je een extra beveiligingslaag toe aan je apps en accounts. Zo beveilig je verschillende programma's beter. Bijvoorbeeld het HIS, e-mailaccount en DigID. Hierdoor hebben cybercriminelen niet meer genoeg aan je gebruikersnaam en wachtwoord om jouw account te hacken.
Heel belangrijk. Want stel je voor:

- een cybercrimineel neemt jouw WhatsApp-account over en vraagt jouw vrienden en familie om geld (hulpvraagfraude);
- of een cybercrimineel neemt jouw app voor online bankieren over en haalt geld van een rekening.

Stap 1: Zorg voor een sterk en uniek wachtwoord!

Het is belangrijk dat je apps en accounts goed beveiligt met tweestapsverificatie.
Maar zorg je ervoor dat de eerste stap ook veilig is?

- ieder account een uniek wachtwoord
- een wachtwoord van minstens 8 tekens
- gebruik een wachtwoordmanager) om je wachtwoorden te onthouden

Check je wachtwoord met de wachtwoordkraaktest!

Stap 2: welke mogelijkheden zijn er?

Bij tweestapsverificatie voor een account wordt een toegangscode naar een vertrouwd apparaat of een app gestuurd om in te kunnen loggen:

- een sms met een inlogcode;
- via een authenticator-app haal je een inlogcode op (bijvoorbeeld google authenticator of Authy app).

Tweestapsverificatie voor een app is meestal:

- een pincode;
- biometrische herkenning; gezichtsherkenning of vingerafdruk.

Deze informatie is afkomstig van www.veiliginternetten.nl, www.androidworld.nl en www.applecoach.nl en bewerkt door ROER voor Digivaardig in de Zorg.
Heb je opmerkingen of vragen over dit lesmateriaal? Mail dan naar info@digivaardigindezorg.nl.