

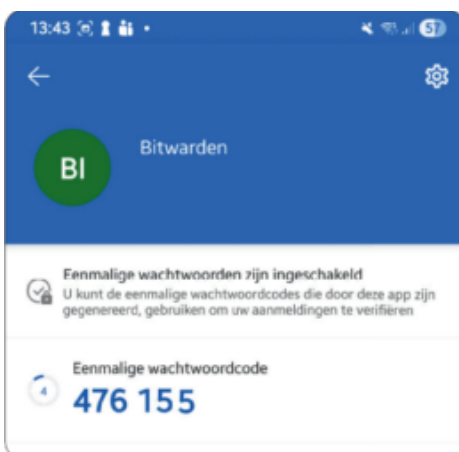
Tweefactorauthenticatie maakt je accounts veiliger, maar kan ook voor problemen zorgen. Wat als je geen code krijgt of je authenticator-app kwijt bent? Gelukkig is toegang vaak alsnog te herstellen.



Bij tweefactorauthenticatie (kortweg 2FA) voeg je een extra beveiligingslaag toe aan online diensten. Om toegang te krijgen is dan zowel een wachtwoord als een tweede manier van aanmelden vereist. In de praktijk is dat een code via je e-mail, een sms of een authenticator-app, of een bevestiging op een van je andere apparaten. Tweefactorauthenticatie verkleint het risico op misbruik van je accounts, maar heeft een keerzijde: bij problemen verlies je in het ergste geval de toegang tot accounts. Wij zetten veelvoorkomende problemen op een rij, met stappenplannen om ze op te lossen.

De ingevulde verificatiecode werkt niet, heb je een code ontvangen, maar wordt die niet door de website geaccepteerd?

1 Een verificatiecode bestaat vaak uit zes cijfers. Controleer eerst of je de code goed hebt overgenomen en geen typfout hebt gemaakt, bij voorbeeld door cijfers om te draaien.



► Is een code nog maar korte tijd geldig, wacht dan even op een nieuwe

2 Werkt de code nog niet? Mogelijk gebruik je een oude, verlopen code. Dat kan als je een code meerdere keren achter elkaar opvraagt. Alleen de meest recente verificatiecode werkt, alle voorgaande codes zijn ongeldig. Je code verloopt meestal snel. Wacht je te lang, dan moet je een nieuwe aanvragen.

Heb je een back-up gemaakt van de authenticator-app? Dan is herstel meestal eenvoudig

3 Gebruik je een authenticator-app? Controleer of je niet per ongeluk een code voor een ander account hebt gekozen. De codes worden na 30 seconden ververs. Maak het jezelf niet lastig: kopieer geen code die bijna verloopt, maar wacht op een nieuwe, zodat je genoeg tijd hebt om hem te gebruiken.

4 Heb je misschien meerdere authenticator-apps op de telefoon, bij voorbeeld van Microsoft en Google? Kijk of je de juiste gebruikt.

5 Is dit niet oplossing? Codes uit een authenticator-app werken alleen goed als de datum en tijd van de telefoon kloppen. Kijk of dat zo is. In Android: open de Instellingen en zoek naar Datum en tijd. Activeer de optie 'Automatisch datum en tijden 'Automatische tijdzone'. Staan ze al aan? Zet ze uit en weer aan. In iOS: open Instellingen > Algemeen > Datum en tijd. Activeer de optie 'Stel automatisch in' (of zet deze optie uit en weer aan).

Ik ontvang geen sms-code Wacht je op een sms-code die niet binnenkomt?

1 Mogelijk blokkeert je telefoon het bericht. In Android: open de Berichten-app, tik op je profielplaatje en kies Spam en geblokkeerd. In iOS: open de Berichten-app, tik rechts-boven op de drie streepjes > Spam.

2 Gebruik je de aanmelding per sms voor het eerst bij de dienst en lukt het aanmelden via e-mail wel? Controleer dan of je het juiste telefoonnummer hebt opgegeven bij de accountinstellingen op de web-site van de dienst. Uiteraard kan dat alleen als je via een andere weg nog wel toegang hebt tot de dienst om je gegevens te controleren

Geen meldingen?

Als je tevergeefs wacht op een melding, controleer dan ook of de telefoon verbonden is met het (mobiele) netwerk. Check daarnaast of de vliegtuigmodus niet actief is. Ook de 'Niet storen'-modus van de telefoon kan meldingen tegenhouden.

Ik ontvang de code niet via e-mail Verwacht je de verificatiecode via e-mail maar komt er niets binnen?

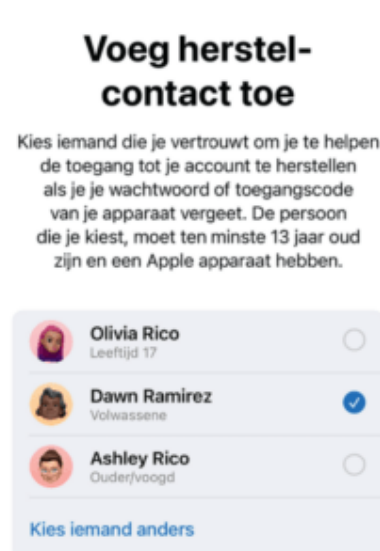
1 Controleer eerst of je het juiste e-mail-adres hebt opgegeven.

2 Kijk of de mail misschien in de spammap is beland.

Ik kan mijn authenticator-app niet gebruiken Kun je de authenticator-app niet meer gebruiken? Dat kan als je telefoon kwijt of gestolen is, de app is verwijderd of je hem niet hebt overgezet naar een nieuwe telefoon. Je kunt terugvallen op herstelmogelijkheden

1 Heb je eerder een back-up van de accountgegevens van de authenticator-app gemaakt? Dan is herstel meestal eenvoudig. Installeer de app opnieuw op je (nieuwe) telefoon. Zoek in de app naar een optie 'Herstellen van back-up' en meld je aan met het account dat je voor de back-up gebruikte.

2 Heb je geen back-up? Dan wordt het lastiger. De authenticator-app valt tijdelijk af als optie. Gebruik een ander kanaal voor het ontvangen van verificatiecodes, als je dat tenminste hebt ingesteld. Bij voorbeeld een code via je e-mail. Ben je de toegang tot de authenticator-app kwijt, maar heb je nog wel toegang tot de telefoon?



Laat de code per sms toesturen of laat je bellen om de code door een computer te laten voorlezen. Voeg hierna de 'nieuwe' authenticator-app toe aan het account en verwijder de verwijzing naar de eerdere authenticatorapp in je profiel

3 Heb je geen toegang tot de alternatieve kanalen voor het ontvangen van de verificatiecode? Gebruik een herstelcode om de toegang te herstellen. Bij het instellen van tweefactorauthenticatie heb je een lijst met herstelcodes (of 'backupcodes') gekregen, maar die moet je toen wel hebben bewaard. Elke code kun je één keer gebruiken om je alsnog bij het account aan te melden. Noteer welke je hebt gebruikt, zodat je deze later niet nogmaals probeert.

4 Heb je een **herstelcontact** (zoals een gezinslid of vriend) opgegeven? Dan kun je dat contact gebruiken om alsnog toegang te krijgen tot je account. Diensten van bij voorbeeld Google en Apple bieden deze mogelijkheid. Je deelt een code die binnen een kwartier door je contactpersoon moet worden geverifieerd en bevestigd

5 Soms kun je een ander apparaat gebruiken om je alsnog aan te melden. Heb je een app op meerdere apparaten staan (zoals telefoon, tablet en laptop)? Zoek dan naar de optie om een melding te tonen op

Ongevraagde code

1 Ontvang je een verificatiecode of via de authenticator-app een verzoek om een aanmelding goed te keuren, terwijl je hier niet om hebt gevraagd? Dan probeert iemand anders op je account in te loggen. Uiteraard ga je hier niet op in.

2 Verander het wachtwoord voor het betreffende account en controleer de inloggeschiedenis, waarin je tijdstip en locatie van de aanmeldpogingen naloopt. Twijfel je hierna nog aan de veiligheid van het account, neem dan contact op met de helpdesk.

Een van je andere apparaten en je identiteit te bevestigen. Dit kan bij voorbeeld bij de YouTube-app. De optie heet vaak 'Stuur een notificatie naar een ander vertrouwd apparaat'.

Ik ontvang geen melding van mijn authenticator-app Online diensten sturen soms geen verificatiecode, maar een melding via de authenticator-app. Dan hoeft de aanmelding alleen te bevestigen door de code in de app te typen of aan te wijzen. Krijg je geen melding?

1 Check of je de nieuwste versie van de authenticator-app gebruikt: werk de app op je telefoon bij via Google Play of Apple App Store

De basis op orde

Zorg dat de basis van 2FA op orde is en vergroot zo de kans op succes bij problemen. Een checklist:

Actuele gegevens

Houd voor elk account de lijst met kanalen actueel: werk in het profiel elke wijziging van bij voorbeeld telefoonnummer en e-mailadres bij. Vul zoveel mogelijk herstelopties in.

Accountherstel

Indien mogelijk: wijs een of meerdere vertrouwde personen aan als herstelcontact. Zij kunnen helpen om weer toegang te krijgen tot je account. Goed om te weten: deze mensen hebben geen toegang tot je account. Om kaping van je account te voorkomen, kan het tot een week duren voordat een persoon als herstelcontact wordt geaccepteerd.

Herstelcodes

Genereer de lijst met herstelcodes van elk account (zoek naar 'Herstelcodes' of 'Back-upcodes') en bewaar de lijst op een veilige plaats, bij voorbeeld in een kluis of in een wachtwoordmanager. Gebruik je bij nood een eenmalige code, streep deze dan af.

Reservekopie

Maak regelmatig een reservekopie van de accountinstellingen. Gebruik de back-upfunctie van de authenticator-app. In Microsoft Authenticator: tik op de drie streepjes of puntjes bovenin het scherm. Tik op Instellingen > Cloudback-up. In Google Authenticator: open de app en tik op het pictogram met de wolk naast de afbeelding van je gebruikersaccount. De back-up wordt gemaakt.

Updates

Houd de authenticator-app up-to-date. Kies voor één authenticator-app, bij voorbeeld Microsoft Authenticator, Google Authenticator of Authy. Controleer handmatig op meldingen

2 Nog steeds geen melding? Open de authenticator-app, eventueel na geforceerd herstarten, en controleer op nieuwe meldingen. Je kunt in de app vaak ook handmatig controleren op meldingen: als die meldingen er zijn, worden ze dan alsnog getoond. In Microsoft Authenticator: tik op de drie puntjes en kies Controleren op meldingen. De Google Authenticator heeft deze functie niet.

3 Check of de app meldingen mag tonen op je telefoon. Android of iOS kan meldingen blokkeren. In Microsoft Authenticator: tik op de drie puntjes en kies Instellingen> Meldingsinstellingen. Zorg dat 'Meldingen toestaan' aan staat.

4 Heb je meerdere authenticator-apps op de telefoon? Voorkom verwarring en controleer of je de juiste app opent.

Er wordt niet gevraagd om een 2FA-code

Vraagt de dienst niet om een verificatie-code, terwijl je dat wel hebt ingesteld? Controleer de accountinstellingen en bevestig dat 2FA is geactiveerd. Mogelijk wordt de vraag om een code overgeslagen omdat je apparaat in een lijst met vertrouwde apparaten staat. Zo'n mechanisme maakt aanmelden eenvoudiger en sneller, maar dat betekent niet dat 2FA uit staat. Wil je weer de vraag krijgen om een code in te voeren? Zoek in de instellingen naar 'Vertrouwde apparaten' en verwijder het apparaat, of kies **Afmelden bij alle apparaten**.

Ik heb alles geprobeerd, niets heeft geholpen Heb je alle alternatieven geprobeerd om toegang te krijgen tot je account? Vaak kun je een proces starten om toegang te herstellen. De vereiste stappen verschillen per aanbieder, maar meestal is dit een handmatig proces dat enkele dagen duurt. De aanbieder controleert je identiteit op een andere manier, bij voorbeeld door een code te sturen naar je e-mailadres en je hiernaar te vragen. Zoek naar een optie zoals 'Accountherstel'.

Bron: Consumentenbond, DIGITAALGIDS – JANUARI/FEBRUARI 2026 In geval van nood kan een vertrouwd persoon je helpen om toegang tot je account te herstellen Met een bevestiging kun je via een ander vertrouwd apparaat inloggen