



SchoonePC Nieuwsbrief

De informatiebron voor uw computerproblemen

door Menno Schoone

Nieuwsbrief 113

20 juni 2022

Hallo SchoonePC-fan,

Het is weer eens tijd voor een nieuwsbrief met lezersvragen, interessant voor zowel Windows 11- als Windows 10-gebruikers! Bekijk de [video](#) en/of scroll naar beneden voor de betreffende onderwerpen. Vind je deze nieuwsbrief interessant? Ga dan aan de slag met de [computerbijbel voor Windows](#), mijn doel is immers om je computerwijzer en -vaardiger te maken!

Lezersvragen over actuele problemen



Menno Schoone
www.SchoonePC.nl

SchoonePC Nieuwsbrief 113



Ik wens je weer veel lees- en computerplezier, tot de volgende nieuwsbrief!

Menno Schoone

www.SchoonePC.nl



De Computerbijbel voor Windows

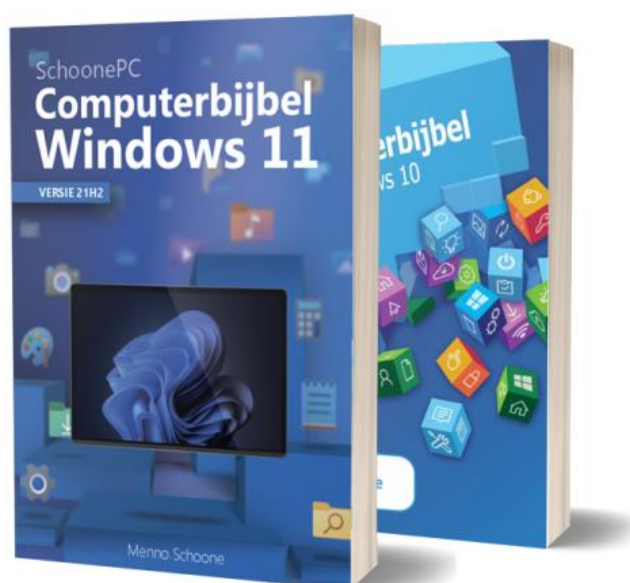
Werk je met Windows kan je wel wat hulp gebruiken omdat je regelmatig tegen problemen aanloopt? Of wil je gewoonweg het maximale uit je pc halen? Ga dan aan de slag met de [SchoonePC computerbijbel voor Windows!](#)

Er is een computerbijbel voor Windows 10 en een voor Windows 11. Beide boeken tellen ruim 400 pagina's en staan boordevol tips en trucs. Dit handboek blijkt dan ook een ideaal hulpmiddel te zijn om Windows onder de knie te krijgen, problemen zelf op te lossen en vooral computerwijzer en -vaardiger te worden. En kom je er met de computerbijbel niet uit, dan help ik je graag even verder. Deze hulp alleen al maakt de aanschaf van de computerbijbel een koopje!

Als ik de reacties van lezers mag geloven dan mag dit boek niet naast je computer ontbreken! Heb je ook interesse? De computerbijbels voor Windows 10 en Windows 11 zijn via de [website](#) te bestellen.

Aantrekkelijke combideal

Heb je de upgrade naar Windows 11 in de planning maar werk je voorlopig nog even door met Windows 10? Of wil je een kennis de computerbijbel cadeau doen? Maak dan gebruik van de aantrekkelijke combideal-korting zodat het extra boek slechts 13 euro kost!



"Ik vind het een haast ongelofelijke en een zeer ouderwetse topservice! Dat komt bijna niet meer voor. Ik zal tot in lengte der dagen jullie superduidelijke computerbijbel blijven raadplegen. Zonder klef te zijn promoot ik ook al jaren jullie boek en inzet bij computerproblemen."

Jan van Elst

"Ik ben zeer tevreden. Super goed afgeleverd. Heel mooi boek met veel interessante onderwerpen. Helemaal geen spijt van de aankoop. En de digitale versie is goed gelukt."

Johan Wenting

Meer informatie over de computerbijbel >

Zoekmachine DuckDuckGo, StartPage of toch Google?

You  zie ook de instructievideo op 2:00

Ap vraagt: *"In nieuwsbrief 112 adviseer je om Google de standaard zoekmachine te maken. Ik wil voorstellen om dat te veranderen in DuckDuckGo, deze geeft dezelfde resultaten als Google maar dan zonder de vervelende advertenties. Over een schone pc gesproken..."*

En Robert M. vraagt: *"Google zoekt beter dan Bing, maar qua privacy ga je er niet op vooruit. Mijn advies is om startpage.com te gebruiken. Die maakt gebruik van de zoekkracht van Google maar zorgt voor een goede privacy, geen tracking, registreert niets en stuurt niets door."*

Antwoord: Naar aanleiding van mijn artikel in de vorige nieuwsbrief over het [wijzigen van de standaard zoekmachine Bing in Google](#) heb ik vele vergelijkbare reacties gekregen. Deze reacties gingen met name over zorgen

rondom de privacy bij het gebruik van Google (en terecht!). Ik heb in het verleden al vaker over deze alternatieve zoekmachines geschreven, maar gezien het aantal reacties op de vorige nieuwsbrief zal ik er nog eens nader op ingaan.

DuckDuckGo

Dat de zoekresultaten van DuckDuckGo door Google worden gegenereerd is een misvatting! Als je ze vergelijkt met die van Google en Bing dan valt direct op dat ze door Bing worden gegenereerd (en dat is niet best...). Je betaalt dan dus sowieso een prijs, de zoekresultaten van Google zijn nu eenmaal superieur, DuckDuckGo kan ik dan ook niet echt aanbevelen.

StartPage.com

StartPage laat wel de zoekresultaten van Google zien. Omdat StartPage wel respectvol met je privacy omgaat, heb ik deze zoekmachine al eens eerder aanbevolen in een [artikel over online privacy](#). Nadeel van deze zoekmachine is wel dat de extra features van Google (zoals geïndexeerde video's, een overzicht van veelgestelde vragen, integratie van Google Maps, bedrijfsinformatie e.d.) ontbreken! En dan ben je nog steeds niet af van de vele advertenties die boven de daadwerkelijke zoekresultaten worden weergegeven...

Google en je privacy

De zoekmachine van Google dankt zijn roem aan de betere zoekresultaten, maar op het gebied van privacy valt er nog wel wat te verbeteren. Gelukkig is daar wat aan te doen door eenvoudigweg de extensie [Ghostery](#) binnen de browser te installeren! Naast het blokkeren van advertenties (wat op zich al een verademing is...) voorkomt deze extensie ook dat je zoekgedrag door Google en andere trackers gelogd kan worden (mits het Google-account niet is aangemeld, anders worden de zoekgegevens alsnog aan je account gekoppeld!).

Als ook nog eens alle cookies bij afsluiten van de browser worden gewist, dan kunnen er niet veel privacygevoelige gegevens meer verzameld worden. Bij Edge gaat dat via de knop **Instellingen en meer**, optie **Instellingen**,

onderdeel **Privacy, zoeken en services**, onderdeel **Browsegegevens wissen**, optie **Selecteer wat u wilt wissen telkens wanneer u de browser sluit**. Ook het onderdeel **Traceringspreventie** is interessant in relatie tot je privacy, omdat daarmee op voorhand al wordt voorkomen dat cookies e.d. lokaal worden opgeslagen (zie de website voor meer informatie).

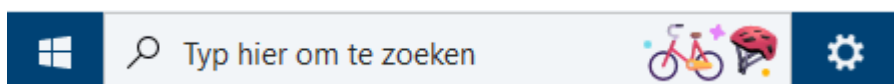
TIP: Cookies kunnen ook handig zijn, met name voor het bewaren van instellingen van bezochte websites. Als alternatief kan er ook met meerdere browsers worden gewerkt, waarbij elk zijn eigen cookie-instellingen heeft. Zo gebruik ik zelf Edge en Chrome (beide in combinatie met Ghostery) voor het bezoeken van mijn favoriete websites, dus met behoud van cookies. Daarnaast gebruik ik Firefox (eveneens met Ghostery) voor het onbezorgd googlen, waarbij ik alle cookies na afloop laat verwijderen.

[dit artikel is terug te vinden op de website](#)

Afbeelding in zoekvak verwijderen

You  zie ook de [instructievideo](#)

Frank Evertse vraagt: *"Na het openen van een website stond er opeens heel irritant een afbeelding in het zoekvak. Ik ben er niet in geslaagd om het kwijt te raken, weet jij nog iets sluits?"*



En Enno Borgsteede heeft een vergelijkbare vraag: *"Ik heb sinds een paar dagen last van een plaatje aan de rechterkant van de zoekbalk van Windows 10. Ik heb liever een kaal zoekvak, maar heb nog geen manier gevonden om het uit te zetten. Weet jij hoe?"*

Antwoord: Deze afbeelding is door een recente update aan het zoekvak van Windows 10 toegevoegd, het staat dus los van bezochte websites en is zeker geen malware. Wanneer je op de afbeelding klikt, opent het zoekvenster met een foto uit de fotocollectie van Microsoft Bing. Elke dag is er weer een ander thema, met een mooie foto en bijpassende afbeelding. Hoewel Microsoft dit vast goed bedoeld heeft, heb ik inmiddels van tientallen lezers de vraag ontvangen of deze afbeelding weer te verwijderen is... Blijkbaar is de optie lastig te vinden. En dat is niet zo vreemd, Microsoft noemt deze afbeelding namelijk een markering. Met deze kennis is de afbeelding snel verwijderd: klik met rechts op de afbeelding, optie **Zoeken** en deactiveer de optie **Markeringen zoeken weergeven!**

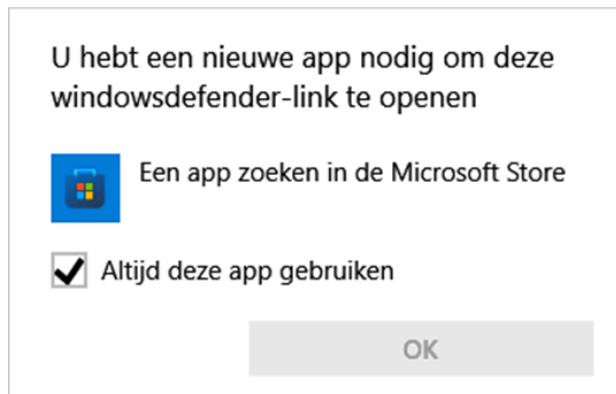
NB: Deze markeringen worden vooralsnog alleen in Windows 10 toegepast, maar zullen in de toekomst waarschijnlijk ook aan Windows 11 worden toegevoegd. In dat geval zijn de afbeelding en de bijbehorende foto uit te schakelen via **Instellingen > Privacy en beveiliging > Zoekmachtigingen**, optie **Zoekmarkeringen weergeven**.

[dit artikel is terug te vinden op de website](#)

Windows-beveiliging start niet meer op

You  zie ook de instructievideo

Jac Zwart vraagt: "Als ik Windows-beveiliging probeer te openen (via **Instellingen > Privacy en beveiliging > Windows-beveiliging**) dan komt er een venster met de tekst **U hebt een nieuwe app nodig om deze windowsdefender-link te openen**. Ik krijg daarbij de mogelijkheid om een app in de Microsoft Store te zoeken, daar kan ik echter niets vinden. Hoe los ik dit op?"



Willem Steenkist heeft een vergelijkbaar probleem: *"Ik heb de beveiligingssoftware van Ziggo en Malware Bytes verwijderd. Als het goed is zou Windows-beveiliging nu weer actief moeten zijn, maar elke keer als ik deze open wordt onderstaande melding getoond. Weet je daar misschien een oplossing voor?"*

Antwoord: Dit zijn zeker geen unieke gevallen! Bij veel lezers lukt het niet meer om Windows-beveiliging in te schakelen, in plaats daarvan krijgen ze dit venster te zien. De gemeenschappelijke factor is duidelijk: ze hebben allen alternatieve beveiligingssoftware verwijderd.... Vooralsnog heb ik dit probleem alleen bij Windows 11-gebruikers voorbij zien komen, het zou zich echter ook bij Windows 10 kunnen voordoen.

Dit probleem is (net als zoveel andere vage problemen...) op te lossen met onderstaande herstelcommando's. Open hiervoor een opdrachtvenster via een rechter muisklik op Start, optie **Terminal (beheerder)**, kopieer en plak (met de toetscombinaties **Ctrl-C** en **Ctrl-V**) onderstaande commandoregels één voor één naar dit opdrachtvenster en bevestig steeds met de **ENTER**-knop:

```
SFC /scannow
```

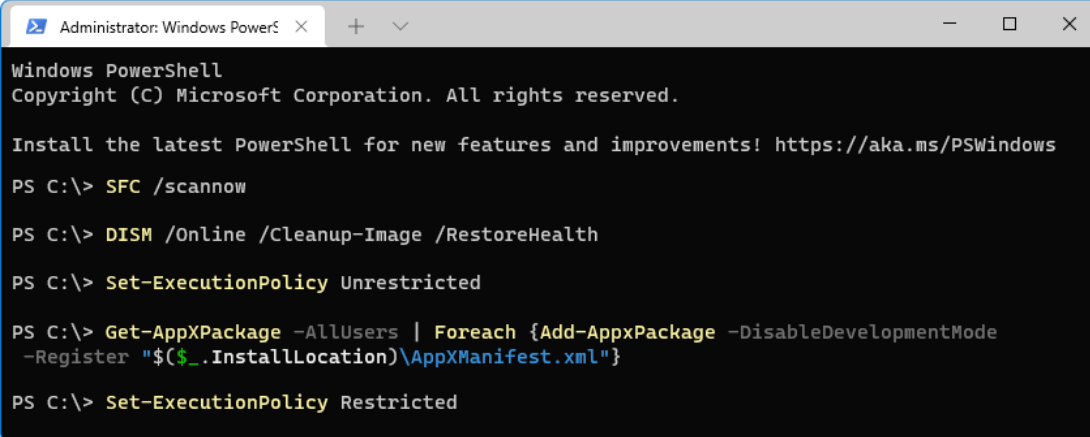
```
DISM /Online /Cleanup-Image /RestoreHealth
```

```
Set-ExecutionPolicy Unrestricted
```

```
Get-AppXPackage -AllUsers | Foreach {Add-AppxPackage -
```

```
DisableDevelopmentMode -Register  
"$($_.InstallLocation)\AppXManifest.xml"}
```

```
Set-ExecutionPolicy Restricted
```



```
Administrator: Windows PowerShell  
Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.  
  
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows  
PS C:\> SFC /scannow  
  
PS C:\> DISM /Online /Cleanup-Image /RestoreHealth  
  
PS C:\> Set-ExecutionPolicy Unrestricted  
  
PS C:\> Get-AppXPackage -AllUsers | Foreach {Add-AppxPackage -DisableDevelopmentMode  
-Register "$($_.InstallLocation)\AppXManifest.xml"}  
  
PS C:\> Set-ExecutionPolicy Restricted
```

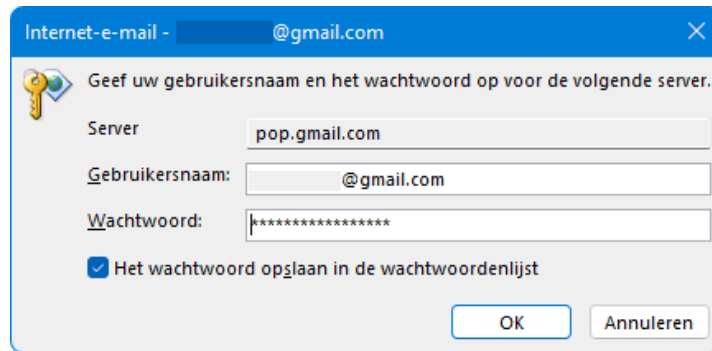
Vaak is er echter meer aan de hand, zo komt het regelmatig voor dat ook de Terminal - die nodig is voor het uitvoeren van de commando's - niet meer wil openen! Dit is gelukkig eenvoudig op te lossen door de Terminal te resetten via **Instellingen > Apps > Apps en onderdelen > Terminal > Geavanceerde opties** (via de drie puntjes), knop **Opnieuw instellen**. Heeft dit geen effect, verwijder de app dan met de knop **Verwijderen** en installeer deze opnieuw via de [Microsoft Store](#) (zoek naar **Windows Terminal**). Nadat de Terminal is hersteld, kunnen bovenstaande commando's alsnog worden uitgevoerd.

[dit artikel is terug te vinden op de website](#)

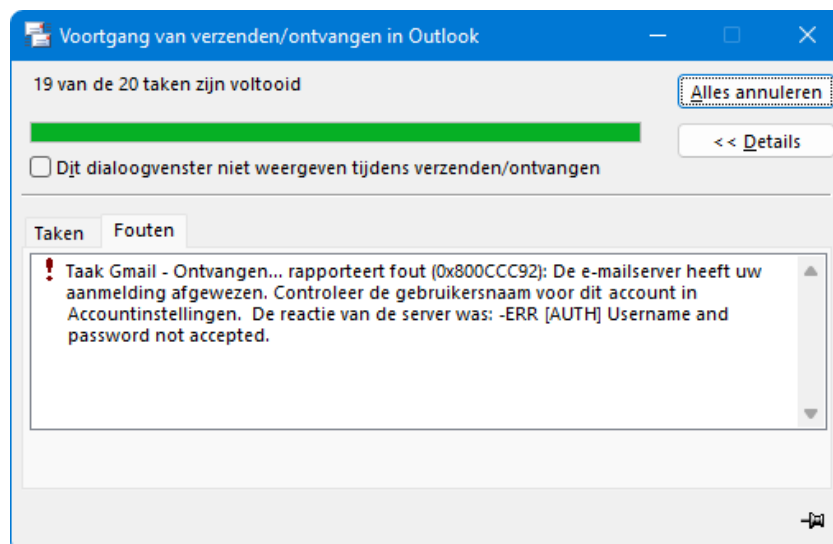
Aanmeldproblemen bij Gmail in een e-mailprogramma

YouTube [zie ook de instructievideo](#)

Gerrit Meils vraagt: *"Outlook 2007 blijft vragen om een wachtwoord voor mijn Gmail-account. Ik heb Office al een keer opnieuw geïnstalleerd, maar dat heeft niet geholpen. Wat zou ik hieraan kunnen doen?"*



Antwoord: Beheer je je Gmail in een e-mailprogramma dan heb je onlangs wellicht een e-mail van Google ontvangen met de mededeling '**Vanaf 30 mei raak je mogelijk de toegang kwijt tot apps die gebruikmaken van een minder beveiligde inlogtechnologie**'. Een wat cryptisch bericht, waarvan ik me kan voorstellen dat je deze destijds slechts voor kennisgeving hebt aangenomen. Nu het zover is, ondervinden vele Gmail-gebruikers echter problemen bij het ophalen van berichten van de mailserver van Gmail: het e-mailprogramma vraagt herhaaldelijk om het wachtwoord (en toont soms ook nog een vage foutmelding, met bijvoorbeeld foutcode 0x800CCC92). Zonder de benodigde kennis lijkt het erop dat Gmail niet meer vanuit het e-mailprogramma beheerd kan worden.



Wat is er aan de hand?

Het gebruik van e-mailprogramma's met het [POP- of IMAP-protocol](#) is uiteraard veilig, mits de communicatie versleuteld plaatsvindt. Google vindt het echter onveilig wanneer het wachtwoord van een Google-account in een e-

mailprogramma (zoals [Outlook](#)) wordt gebruikt en staat het daarom niet meer toe (zie support.google.com). Daar hebben ze een goede reden voor: dat wachtwoord geeft namelijk toegang tot alle aan het Google-account gekoppelde diensten (zoals Google Maps, Google Ads e.d.), het is dus belangrijk dat kwaadwillenden dit wachtwoord niet zomaar kunnen achterhalen.

Minder goed beveiligde apps en je Google-account

Google biedt vanaf **30 mei 2022** geen support meer voor het gebruik van apps of apparaten van derden die je vragen om in te loggen op je Google-account met alleen je gebruikersnaam en wachtwoord. We doen dit om je account te beschermen.

Belangrijk: Deze deadline is niet van toepassing op Google Workspace- of Google Cloud Identity-kanten. De datum waarop dit voor deze klanten ingaat wordt op een later tijdstip aangekondigd in de Workspace-blog.

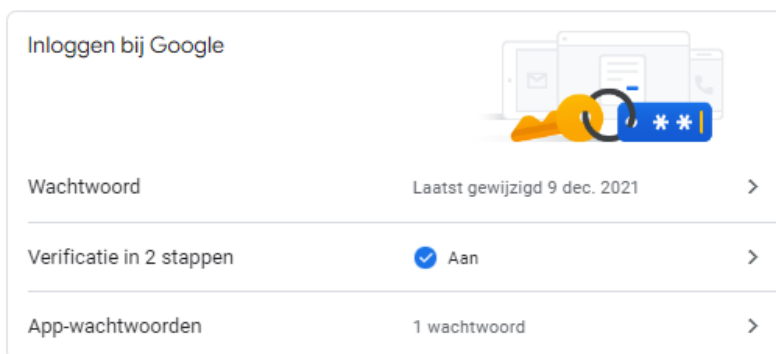
[Lees verder voor meer informatie.](#)

Nu doet de berichtgeving van Google voorkomen alsof het helemaal niet meer mogelijk is om Gmail met een e-mailprogramma te beheren, dat is echter niet het geval! Met een kleine aanpassing is het namelijk geen enkel probleem om Gmail op de gebruikelijke wijze vanuit een e-mailprogramma te beheren, zonder het wachtwoord van het Google-account te gebruiken! Jammer dat Google hier nauwelijks ruchtbaarheid aan geeft, waardoor veel onwetende Gmail-gebruikers nu met de handen in het haar zitten...

Toch Gmail beheren met je favoriete e-mailprogramma?

Google wil dus niet meer dat het wachtwoord van het Google-account in een e-mailprogramma wordt gebruikt. Dit is echter makkelijk te verhelpen door in plaats daarvan gebruik te maken van een uniek app-wachtwoord, speciaal voor het betreffende e-mailprogramma. Dit app-wachtwoord moet apart voor het e-mailprogramma worden aangemaakt, en kan alleen worden gebruikt voor het beheren van je e-mail. Voor het aanmaken van een app-wacht-

woord is het wel noodzakelijk om tweestapsverificatie te activeren. Er zijn dus twee stappen nodig:



LET OP: Ondersteunt het e-mailprogramma de tweestapsbeveiliging **Oauth2** (zoals de nieuwste versies van Outlook en Thunderbird) dan is het voor het IMAP-protocol niet nodig om een app-wachtwoord aan te maken.


Stap 1: Activeer tweestapsverificatie

Tweestapsverificatie is te activeren via de beveiligingspagina van het Google-account (<https://myaccount.google.com/security>), onderdeel **Inloggen bij Google**, activeer optie **Verificatie in 2 stappen**. Met tweestapsverificatie wordt bij de eerste keer aanmelden niet alleen om het wachtwoord gevraagd, maar ook om een naar de mobiele telefoon verzonden code (of om een goedkeuring vanuit de app op de mobiele telefoon). Deze extra controle-slag maakt het voor derden haast onmogelijk om toegang tot het Google-account te krijgen! Is tweestapsverificatie nog niet geactiveerd dan is het dus belangrijk om dat zo snel mogelijk alsnog te doen.

Stap 2: Stel een app-wachtwoord in

Maak vervolgens voor het betreffende e-mailprogramma een uniek app-wachtwoord aan via de pagina <https://myaccount.google.com/security>, onderdeel **Inloggen bij Google**, optie **App-wachtwoorden**. Selecteer in het geopende venster achtereenvolgens **E-mail** en **Anders (aangepaste naam)**, en wijzig het veld in iets herkenbaars (bijvoorbeeld de naam van het e-mailprogramma).

Je app-wachtwoorden

Naam	Gemaakt	Laatst gebruikt	
Gmail in Outlook	20 nov. 2018	00:07	

Selecteer de app en het apparaat waarvoor je het app-wachtwoord wilt genereren.

E-mail ▼

- Apparaat selecteren
- iPhone
- iPad
- BlackBerry
- Mac
- Windows-telefoon
- Windows-computer
- Anders (aangepaste naam)

GENEREREN

Hiermee wordt voor het betreffende e-mailprogramma (app) eenmalig een uniek 16-letterig app-wachtwoord gegenereerd. Selecteer dit wachtwoord met de muis en kopieer deze met de toetscombinaties **Ctrl-C** en **Ctrl-V** naar het veld voor het wachtwoord in het betreffende e-mailprogramma (negeer de spaties). Hierna moet de e-mail van Gmail weer probleemloos beheerd kunnen worden. Dit app-wachtwoord hoeft je verder niet te onthouden, er kan immers altijd weer een nieuwe worden aangemaakt.

Gegenereerd app-wachtwoord

Je app-wachtwoord voor Windows-computer

fnea smcg dfhx jsdn

Instructies voor gebruik

Ga naar de instellingen voor je Google-account in de app die of op het apparaat dat je wilt instellen. Vervang je wachtwoord door het wachtwoord van 16 tekens dat hierboven wordt getoond.

Met dit app-wachtwoord krijg je, net zoals met je normale wachtwoord, volledige toegang tot je Google-account. Je hoeft het app-wachtwoord niet te onthouden, dus noteer het wachtwoord niet en deel het niet met anderen.

Email

securesally@gmail.com

Password

●●●●●●●●●●●●●●

KLAAR

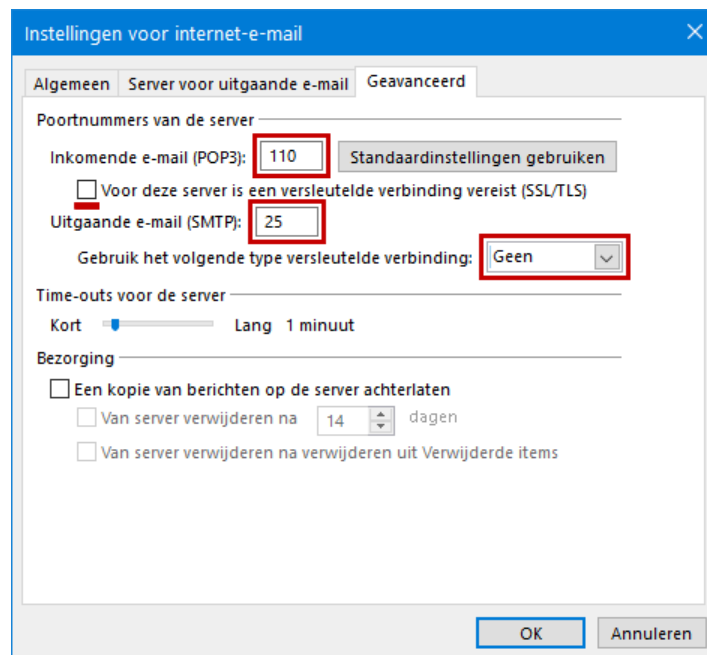
Krijg je Gmail nog steeds niet aan de praat?

Lukt het nog steeds niet om Gmail met het POP- of IMAP-protocol aan de praat te krijgen? Controleer dan via de pagina <https://mail.google.com/mail/u/0/#settings/fwdandpop> of POP dan wel IMAP is ingeschakeld. En twijfel je of de juiste instellingen zijn toegepast, klik dan via diezelfde pagina door naar de configuratie-instructies om te controleren welke poortnummers e.d. toegepast moeten worden (zie de website voor meer informatie over [instellingen voor Gmail](#)).

[dit artikel is terug te vinden op de website](#)

Maak voor het ontvangen en verzenden van e-mail geen gebruik meer van POP-poort 110 en SMTP-poort 25

Als aanvulling op de vorige vraag heb ik nog een tip voor het beheren van e-mail met het POP-protocol! Het valt namelijk op dat sommige lezers nog steeds POP-poort 110 en SMTP-poort 25 kunnen gebruiken voor het ophalen en verzenden van e-mail vanuit een e-mailprogramma zoals [Outlook](#). Bij gebruik van poort 110 vindt de communicatie met de mailserver echter onversleuteld plaats, de aanmeldgegevens worden dus open en bloot meegezonden! Kwaadwillenden hoeven dan simpelweg het netwerkverkeer te onderscheppen om het wachtwoord te achterhalen, waarna ze ongemerkt je e-mail kunnen meelezen. Het is dan ook onbegrijpelijk dat dit bij sommige e-mailadressen nog steeds mogelijk is!



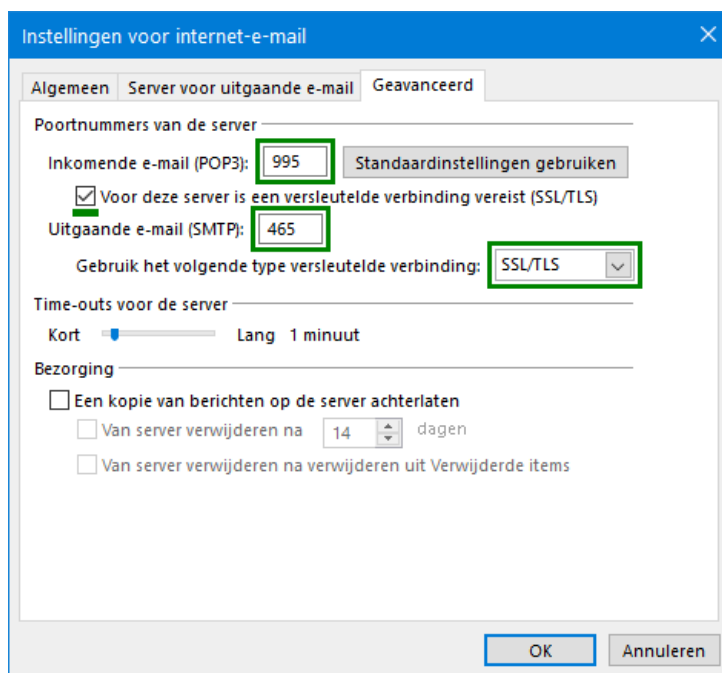
Poortnummers aanpassen

Gebruik je nog poort 110 en besluit je e-mailprovider het gebruik van onbeveiligde poorten niet meer toe te staan, dan toont het e-mailprogramma bij het controleren op nieuwe berichten een (wat cryptische) foutmelding dat de verbinding niet is beveiligd. Hiermee wordt dus bedoeld dat het poortnummer aangepast moet worden en de verbinding met SSL moet worden beveiligd.

Maar ook als je provider het nog wel toestaat is het verstandig om de toegepaste instellingen van de e-mailaccount(s) te controleren. Voor het versleuteld ophalen en verzenden van e-mail kan meestal gebruik worden gemaakt van de poortnummers **995** (voor POP) en **465** (voor SMTP). Sommige e-mailproviders hanteren echter andere instellingen, deze zijn te achterhalen via hun website en vaak eenvoudig te vinden door te googlen naar "instellingen POP3 SMTP *provider*naam".

Hoe de poortnummers aangepast kunnen worden, verschilt per e-mailprogramma. Bij het populaire [Outlook](#) (onderdeel van Microsoft Office) gaat dat bijvoorbeeld via tabblad **Bestand**, knop **Accountinstellingen**, optie **Profielen beheren**, knop **Ja**, knop **E-mailaccounts**, tabblad **E-mail**, selecteer het e-mailadres, knop **Wijzigen**, knop **Meer instellingen**, tabblad **Geavan-**

ceerd. Wordt in dit venster bij inkomende e-mail POP3-poort **110** vermeld, activeer dan de optie **Voor deze server is een versleutelde verbinding vereist (SSL/TLS)** zodat het verzenden van e-mail voortaan wordt versleuteld (het poortnummer wijzigt automatisch in **995**). Versleutel tevens de uitgaande e-mail (SMTP) door het poortnummer te wijzigen van **25** in **465** en het type versleuteling te wijzigen in **STARTTLS** (of anders **SSL/TLS**).



Controleer na het aanpassen van de poortnummers of het ophalen en verzenden van e-mail nog naar behoren functioneert. Wijzig voor de zekerheid ook nog even het wachtwoord (via de website van de e-mailprovider), je weet immers nooit zeker of het wachtwoord al was onderscheept...

Met dank aan Hans van Duivenboden

[dit artikel is terug te vinden op de website](#)

Nieuw op mijn YouTube-kanaal!

Op [mijn YouTube-kanaal](#) zijn naast nieuwsbriefvideo's ook handige instructievideo's met interessante lezersvragen terug te vinden! Hieronder staan de recent toegevoegde video's. Vind je ze leerzaam, vergeet dan niet om op mijn kanaal te abonneren!

Lezersvragen over actuele problemen
Menno Schoone
www.SchoonePC.nl
SchoonePC Nieuwsbrief 113

Afbeelding in zoekvak verwijderen
Menno Schoone
www.SchoonePC.nl
Lezersvraag

Windows-beveiliging wil niet meer openen
Menno Schoone
www.SchoonePC.nl
Lezersvraag

Aanmeldproblemen Gmail in een e-mailprogramma
Menno Schoone
www.SchoonePC.nl
Lezersvraag

Nieuwsbrief 112 gemist?

Heb je nieuwsbrief 112 gemist? Vraag deze dan op [via de website](#) en/of download het [PDF-bestand](#). Uiteraard is de bijbehorende [video](#) ook nog beschikbaar!

De standaard zoekmachine Bing wijzigen in Google
Menno Schoone
www.SchoonePC.nl
SchoonePC Nieuwsbrief 112

Een greep uit de vele reacties van gebruikers van de computerbijbel

"Zoals gewoonlijk weer zeer duidelijk en goede hulp om te finetunen."

"Zeer mooi boek om te lezen (ook het papier/materiaal) en een nette verzending. Leuk-helder bedrijf!"

"Het boek voor Windows 11 is geweldig!"

"Ik vind je computerbijbel zeer leesbaar, duidelijk en er staat een schat aan informatie in."

"Bedankt voor het meedenken, het boek is zijn geld nu al waard."

"Klasse voor het monnikenwerk."

"Een razendsnelle levering (gisteren besteld en vandaag al binnen) en het boek was werkelijk subliem verpakt!"

"De computerbijbel is wat mij betreft een must have. Top Menno, ga zo door. Ik raadpleeg je computerbijbels voor W10 en W11 regelmatig met succes voor de aangedragen oplossingen."

Meer informatie over de computerbijbel >

www.SchoonePC.nl | [Aanmelden nieuwsbrief](#)

© 2001-2022 - SchoonePC - Rotterdam - The Netherlands