



SchoonePC Nieuwsbrief

De informatiebron voor uw computerproblemen

door Menno Schoone

Nieuwsbrief 112

23 mei 2022

Hallo SchoonePC-fan,

Na enkele nieuwsbrieven over Windows 11 is het de hoogste tijd voor informatie die ook voor Windows 10-gebruikers interessant is! Zo besteed ik deze keer aandacht aan het wijzigen van de standaard zoekmachine Bing in het veel betere Google, het voorkomen van aanmeldproblemen en wetenswaardige tips met betrekking tot spamfilters.

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!

**De standaard
zoekmachine Bing
wijzigen in Google**

Menno Schoone
www.SchoonePC.nl

SchoonePC Nieuwsbrief 112

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

Menno Schoone

www.SchoonePC.nl



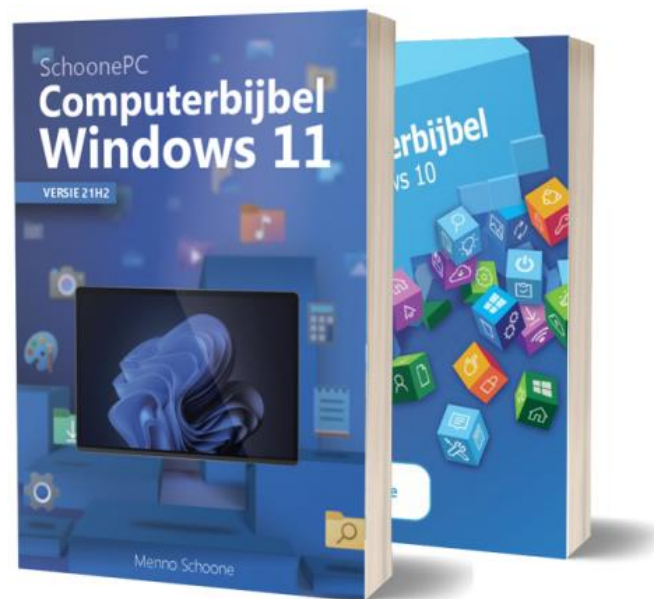
De Computerbijbels voor Windows 10 en Windows 11

Werk je met Windows 10 of Windows 11 en 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 wel in de planning maar werk je voorlopig nog even 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!



"Door de duidelijke taal kan je bij een probleem rustig op zoek gaan naar de oorzaak en de oplossing stapsgewijs toepassen. Dat zorgt voor minder frustraties, hartelijk dank daarvoor."

Bruno Vermeulen

"Jullie boeken zijn als parels die het computeren tot een uiterst aangename en leuke hobby maken!"

Johan Castermans

[Meer informatie over de computerbijbel >](#)

Zoekmachine Bing wijzigen in Google

You  [zie ook de instructievideo op 0:50](#)

Tot ongenoegen van velen heeft Microsoft de zoekmachine Bing geïntegreerd in Windows. Geef je bijvoorbeeld een zoekopdracht vanuit het startmenu dan wordt voor de weergave van de online zoekopdracht de zoekmachine Bing in de [browser Edge](#) opgestart.

Helaas bevat Windows geen instelling om de als standaard ingestelde zoekmachine Bing aan te passen. Ook de [workaround met Edge-Deflector](#), die in het verleden nog gebruikt kon worden om de zoekmachine te wijzigen in het (veel betere) Google, is door een wijziging in Windows niet meer mogelijk. Wat nog wèl kan, is het wijzigen van de standaard in de browser Edge toegepaste zoekmachine Bing. In dit artikel leg ik uit hoe je deze zoekmachine kunt vervangen door Google. Het gaat daarbij om de startpagina van Edge, de startpagina van een nieuw geopend tabblad én de zoekfunctie van de adresbalk.

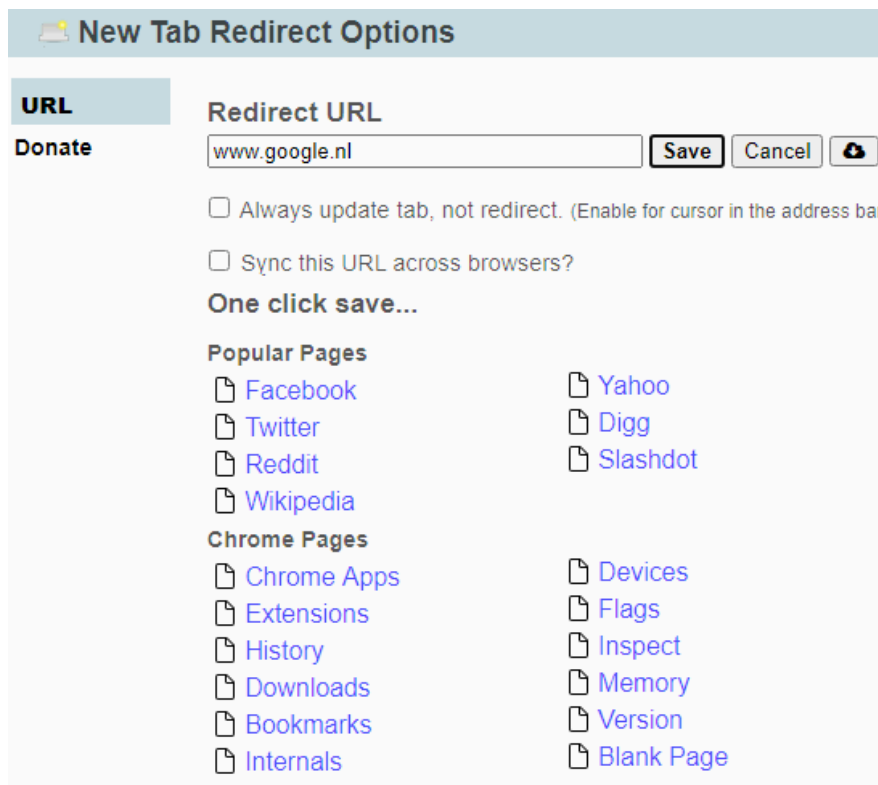
De browser laten openen met de startpagina van Google

De startpagina van Edge is eenvoudig te wijzigen via de knop **Instellingen en meer** (de drie puntjes rechts bovenin het venster), optie **Instellingen**, onderdeel **Tabbladen, Start, Home en Nieuw**, activeer de optie **Deze pagina's openen**, knop **Een nieuwe pagina toevoegen**. Geef hier het adres van de gewenste zoekpagina op (in dit voorbeeld de zoekmachine **www.google.nl**) en bevestig met de knop **Toevoegen**.

TIP: Voeg je meerdere pagina's toe, dan worden deze bij het opstarten van de browser elk in een apart tabblad geopend.

Nieuw tabblad laten openen met de startpagina van Google

De ingestelde startpagina wordt getoond bij het opstarten van de browser. Open je echter een nieuw tabblad (via de **+**-knop rechts van de geopende tabbladen) dan wordt nog steeds de startpagina van Bing voorgeschoteld... Wil je de startpagina van nieuwe tabbladen ook wijzigen in de startpagina van Google, maak dan gebruik van de extensie **New Tab Redirect**: open de pagina <https://microsoftedge.microsoft.com> in Edge (gebruik eventueel de zoekfunctie) en installeer de extensie via de knop **Downloaden**, knop **Extensie toevoegen**. Nieuw geïnstalleerde extensies worden uit veiligheidsoogpunt standaard uitgeschakeld (zie de melding in Edge), de extensie zal dus eerst nog geactiveerd moeten worden via de knop **Instellingen en meer**, optie **Extensies**, optie **Extensies beheren** (hier is de extensie ook weer uit te schakelen of te verwijderen). Klik vervolgens op de link **Set Options** (in het nieuw geopende tabblad) om de startpagina voor nieuwe tabbladen in te stellen: geef bij **Redirect URL** het websiteadres op (in dit voorbeeld **www.google.nl**) en bewaar deze met de knop **Save**.



Open vervolgens een nieuw tabblad en bevestig de in Edge getoonde pop-up **Is dit het nieuwe tabblad dat u verwachtte?** met de knop **Wijzigingen behouden**. Wil je de ingestelde startpagina achteraf aanpassen, dan kan dat via **Instellingen en meer**, optie **Extensies**, optie **Extensies beheren**, link **Details**, link **Extensie-opties**.

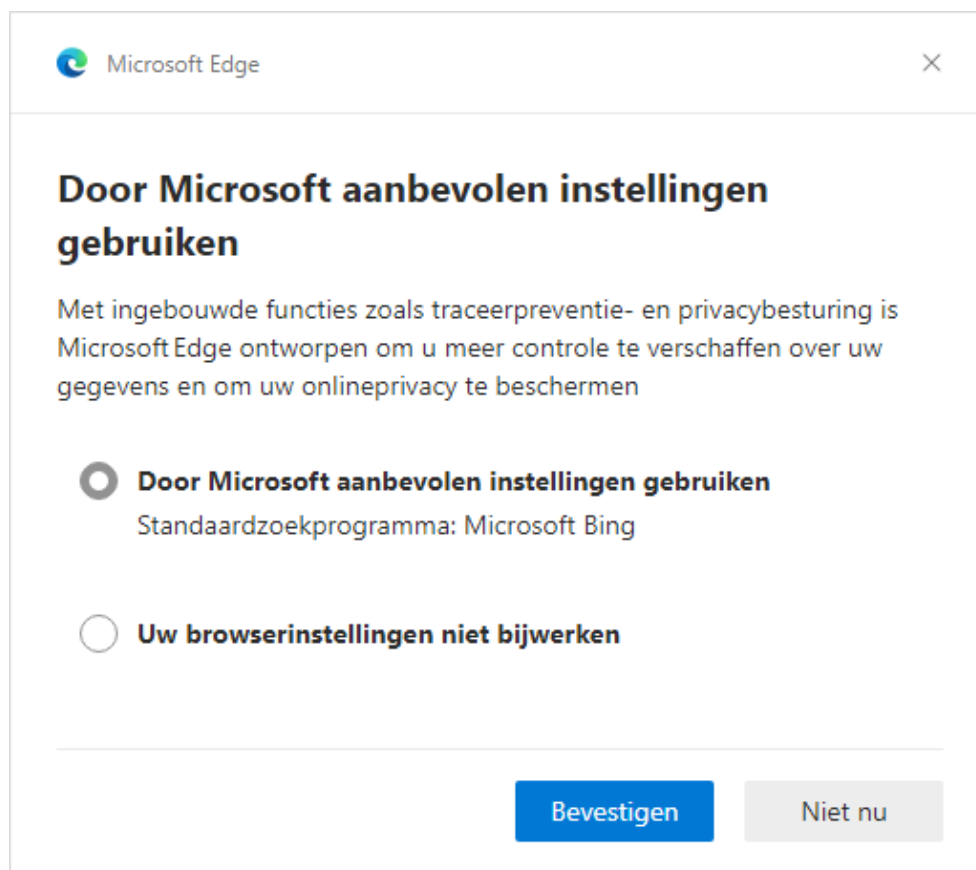
TIP: Volgens de standaard instellingen mag New Tab Direct elke geopende pagina doorzoeken. Heb je daar om privacyredenen moeite mee, wijzig de machtigingen dan door via de link **Details** optie **Toegang tot site** te wijzigen van **Op alle sites** in **Op specifieke sites** en vervolgens een niet bestaand websiteadres op te geven.

De zoekmachine van de adresbalk wijzigen in Google

Ook bij een zoekopdracht vanuit de adresbalk van de browser wordt standaard de zoekmachine Bing gebruikt. Deze kan eenvoudig wor-

den gewijzigd via **Instellingen en meer**, optie **Instellingen**, sub **Privacy, zoeken en services**, optie **Adresbalk en zoeken** (onderaan de pagina), optie **Zoekprogramma dat in de adresbalk wordt gebruikt**, selecteer hier de gewenste zoekmachine (in dit voorbeeld **google.nl**).

TIP: Wordt bij het opstarten van de browser (of bij aanmelden van het gebruikersaccount) een venster getoond, met als onderwerp **Door Microsoft aanbevolen browserinstellingen gebruiken?** Selecteer dan de optie **Uw browserinstellingen niet bijwerken**. Wordt klakkeloos de standaard geactiveerde optie **Door Microsoft aanbevolen browserinstellingen gebruiken** gekozen, dan wordt de zoekmachine Microsoft Bing weer ingeschakeld!

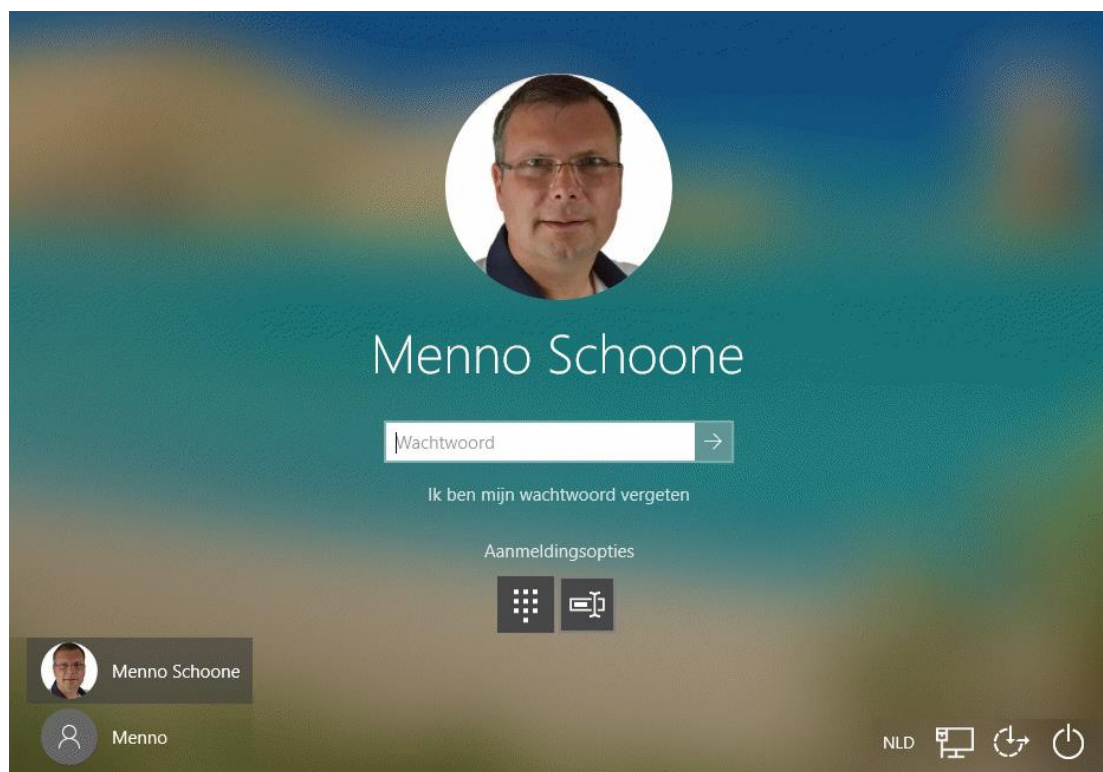


[dit artikel is terug te vinden op de website](#)

Voorkomen dat de toegang tot je (gebruikers)account wordt geblokkeerd

YouTube zie ook de instructievideo op 5:27

Ik ontvang nog wel eens een hulpvraag van lezers die geen toegang meer kunnen krijgen tot hun gebruikersaccount, bijvoorbeeld vanwege een fout verlopen Windows-update, corrupte gebruikersaccountbestanden, blokkerende beveiligingssoftware, etc. Maar de meest voorkomende reden is waarschijnlijk wel buitensluiting vanwege authenticatieproblemen, bijvoorbeeld door een vergeten wachtwoord of een ontoegankelijke tweestapsverificatie. Dat zorgt vaak voor enorme frustraties, zonder toegang tot Windows is er immers ook geen toegang tot de persoonlijke bestanden, e-mail e.d.! Jezelf buitensluiten wil je echt niet meemaken, hoog tijd dus om hier eens aandacht te besteden.



Aanmeldproblemen en het type gebruikersaccount

Bij aanmeldproblemen is het van belang te weten of het om een [lokaal gebruikersaccount](#) gaat, of om een gebruikersaccount dat is gekoppeld aan een [Microsoft-account](#). Het wachtwoord van een lokaal gebruikersaccount kan relatief eenvoudig vanuit een administratoraccount worden gewijzigd (hoe dat moet, staat beschreven op de pagina over het [verborgen administratoraccount](#)). Is het gebruikersaccount echter gekoppeld aan een Microsoft-account, dan zitten er meer haken en ogen aan! Hierna volgen drie mogelijke oorzaken met bijbehorende oplossingen.

Oorzaak 1: Het wachtwoord werkt niet meer

Voor het aanmelden met een Microsoft-account kan een e-mailadres van Microsoft (zoals @outlook.com of @hotmail.com), een willekeurig ander e-mailadres of een telefoonnummer worden gebruikt. De voorkeur gaat uit naar een e-mailadres van Microsoft, er wordt dan namelijk voor alle diensten van Microsoft (zoals de webmail [www.outlook.com](#) en [OneDrive](#)) één en hetzelfde wachtwoord gebruikt. Bij gebruik van een willekeurig ander e-mailadres als Microsoft-account is dat anders: het Microsoft-account en het e-mailadres staan dan los van elkaar en hebben dus elk een eigen wachtwoord. Vaak wordt echter voor beide accounts hetzelfde wachtwoord ingesteld omdat men zich er niet bewust van is dat het om twee verschillende accounts gaat. Dat zorgt geheid voor problemen wanneer één van beide wachtwoorden wordt aangepast, en er met dit nieuwe wachtwoord geprobeerd wordt bij het andere account aan te melden! Gelukkig is dit 'aanmeldprobleem' eenvoudig op te lossen door het oorspronkelijke wachtwoord te gebruiken, mits je deze nog weet natuurlijk...

Ook na de installatie van een update kunnen er aanmeldproblemen ontstaan, waarbij het niet meer lukt om met het wachtwoord of de Windows Hello-pincode aan te melden op het gebruikersaccount. Deze problemen kunnen bijvoorbeeld ontstaan door een beschadigd gebruikersaccountprofiel (mogelijk als gevolg van geïnstalleerde beveiligingssoftware). Het eerste deel van de oplossing is het terugzetten van een systeemherstelpunt, zodat de installatie van de update ongedaan wordt gemaakt. Vanwege de aanmeldproblemen zal de herstelmodus buiten Windows om opgestart moeten worden (door de **Shift**-toets ingedrukt te houden tijdens het opstarten van de pc, tegel **Problemen oplossen**, tegel **Geavanceerde opties**, tegel **Updates verwijderen** of tegel **Systeemherstel**). De herstelprocedure kan ook automatisch worden uitgevoerd door het opstarten van Windows meermaals achter elkaar te onderbreken met de herstartknop van de computer. Zodra het account weer toegankelijk is, kan het onderliggende probleem worden opgelost.

Oorzaak 2: Het wachtwoord is vergeten

Anders is het wanneer je het wachtwoord van het Microsoft-account werkelijk bent vergeten. In dat geval moet een nieuw wachtwoord worden ingesteld via de pagina

<https://account.live.com/password/reset> (deze pagina is eenvoudig te openen via de link **Ik ben mijn wachtwoord vergeten** in het aanmeldvenster). Voordat je een nieuw wachtwoord kunt instellen, wordt geverifieerd of je de rechtmatige eigenaar van het Microsoft-account bent. Deze controle verloopt via het bij Microsoft opgegeven alternatieve e-mailadres of telefoonnummer, zolang je toegang tot de bijbehorende mailbox of telefoon hebt dan lukt het dus nog wel. Zo niet, dan wordt het spannend of je genoeg gegevens over

het account en de recente geschiedenis kan oplepelen om je eigenaarschap te bewijzen en weer toegang te verkrijgen...

Oorzaak 3: Buitengesloten door tweestapsverificatie

Tweestapsverificatie is een belangrijke extra beveiligingsschil voor het verkrijgen van toegang tot het gebruikersaccount. Is tweestapsverificatie geactiveerd (via de pagina <https://account.live.com/proofs/Manage/additional>), dan moet bij het aanmelden naast het wachtwoord óók een (per e-mail, SMS of app toegezonden) wachtwoordcode worden opgegeven. Als aanvulling hierop adviseert Microsoft gebruik te maken van de app **Microsoft Authenticator** (download: www.microsoft.com/nl-nl/account/authenticator; scan de QR-code om de app op je mobiel te installeren). Met deze app kan je niet alleen eenvoudig wachtwoordcodes genereren, maar ook direct via een pop-up op je mobiel de tweestapsverificatie goedkeuren.



Tweestapsverificatie: buitensluiten voorkomen

Voor het doorlopen van de tweestapsverificatie heb je dus óf toegang tot je e-mailaccount, óf toegang tot je mobiele telefoon nodig. Dit maakt de extra beveiligingsmaatregel gevoelig voor buitensluiten, want hoe moet je de tweestapsverificatie doorlopen wanneer je geen toegang meer tot je e-mailadres of mobiel hebt? Ben je je mobiel kwijtgeraakt dan kan uiteraard een nieuwe simkaart worden aangevraagd. Bij een prepaid simkaart is het echter maar de vraag of je je mobiele nummer weer terug kan krijgen. En wat als het destijds opgegeven telefoonnummer of e-mailadres inmiddels is opgezegd, bijvoorbeeld uit kostenbesparing of na een overlijden? Zeg een internet- of telefoonabonnement dus pas op wanneer je er absoluut zeker van bent dat deze niet meer nodig is om toegang tot een account te krijgen.












Zorg voor extra verificatiemogelijkheden

Tweestapsverificatie kan voor serieuze aanmeldproblemen zorgen. Toch is het pure noodzaak om deze extra beveiligingsschil te gebruiken, het zorgt er namelijk voor dat onbevoegden geen toegang tot je account kunnen krijgen. Bouw echter wel preventief extra verificatiemogelijkheden in, voor het geval er geen toegang meer is tot het voor de tweestapsverificatie ingestelde e-mailadres of de telefoon! Dit is eenvoudig te realiseren door extra e-mailadressen en/of telefoonnummers toe te voegen. Zodoende is er altijd nog een alternatieve verificatiemogelijkheid voorhanden om weer toegang te verkrijgen. Voor een Microsoft-account kan dit via de pagina <https://account.live.com/proofs/Manage/additional>, link **Een methode voor aanmelden of verifiëren kiezen**. Zo zou je bijvoorbeeld het mobiele nummer van je partner als extra verificatiemogelijkheid aan je eigen Microsoft-account kunnen toevoegen, of je

eigen nummer aan de Microsoft-accounts van je ouders en/of kinderen.


Manieren om te bewijzen wie u bent

Beheer de aanmeldings- en verificatieopties voor uw Microsoft-account. [Meer informatie over aanmelden en verifiëren.](#)

>	 Wachtwoord invoeren	 Bijgewerkt
>	 Een code per e-mail verzenden	info@mennoschoone.nl  Bijgewerkt
>	 Een code per e-mail verzenden	info@schoonepc.nl  Bijgewerkt
>	 Een code verzenden via sms	+31630314090  Bijgewerkt
>	 Aanmeldingsmelding verzenden	 Bijgewerkt
 Een methode voor aanmelden of verifiëren kiezen		

Extra beveiliging

Verhoog uw beveiliging door twee stappen te vereisen om uw account te verifiëren wanneer u zich aanmeldt. [Meer informatie over de vraag of dit geschikt is voor u.](#)



Verificatie in twee stappen
AAN
Uitschakelen

Extra verificatiemogelijkheden bij andere accounts

Tweestapsverificatie is inmiddels gemeengoed geworden. Het wordt dus niet alleen bij Microsoft-accounts toegepast, maar ook bij websites zoals Dropbox, Gmail, Facebook, Twitter, LinkedIn etc. Het risico op buitensluiting moet ook hier niet worden onderschat! Beschikt de aanbieder van de betreffende dienst over een helpdesk die de toegang kan herstellen, dan is het risico uiteraard beperkt. De problemen ontstaan vooral bij gratis diensten waarbij niet kan worden teruggevallen op een helpdesk (zoals social media-accounts, webmail en online opslag). Het is dus verstandig om ook bij deze

accounts een alternatieve verificatieoptie toe te voegen. Om een idee te krijgen hoe dat in zijn werk gaat, volgen hier twee voorbeelden:

- **Dropbox**

Bij [Dropbox](#) kan via de pagina www.dropbox.com/account/security een extra telefoonnummer worden opgegeven (zie afbeelding).

Tweestapsverificatie Aan
Vereis naast het wachtwoord ook een beveiligingssleutel of -code.

Voorkeursmethode Kies hoe je de beveiligingscodes wilt ontvangen.	Sms (+31 6 30314090)	Bewerken
Alternatieve methode Voeg een reservetelefoonnummer toe voor beveiligingscodes.	+31 104545454	Bewerken
Herstelcodes Ontvang beveiligingscodes die je kunt gebruiken wanneer je geen toegang hebt tot je telefoon.		Weergeven
Beveiligingssleutels Vereis voor het aanmelden een fysieke beveiligingssleutel die wordt aangesloten op de USB-poort.		Toevoegen
Vertrouwde apparaten Trek de vertrouwde status in voor je apparaten die tweestapsverificatie overslaan.		Alles intrekken

- **Google-account**

Google-accounts worden vaak gekoppeld aan een Android-telefoon of -tablet, het is dus belangrijk dat ook dit account toegankelijk blijft! Via de pagina <https://myaccount.google.com/signinoptions/two-step-verification> (zie afbeelding) zijn extra verificatiemogelijkheden in de vorm van telefoonnummers aan het account toe te voegen. Installeer tevens de **Google Authenticator**-app (via de Google Play Store op je Android-telefoon) en schakel **Google-prompts** in, zodat op je telefoon een verificatiepop-up wordt getoond om snel akkoord te kunnen gaan. De Google Authenticator wordt




overigens ook door vele andere websites gebruikt om de toegang tot hun platform met tweestapsverificatie te beveiligen!




Verificatie in 2 stappen staat AAN sinds 14 mei 2012 [UITSCHAKELEN](#)



Beschikbare tweede stappen

Met een tweede stap nadat je je wachtwoord hebt opgegeven, kun je bevestigen dat jij het bent die inlogt. [Meer informatie](#)

Opmerking: Google-prompts worden toegevoegd als alternatieve methode voor verificatie in 2 stappen als je inlogt op je Google-account op een geschikte telefoon.

 **Authenticator-app (Standaard)** 
Authenticator op Android 
Toegevoegd: Zojuist
[TELEFOON WIJZIGEN](#)

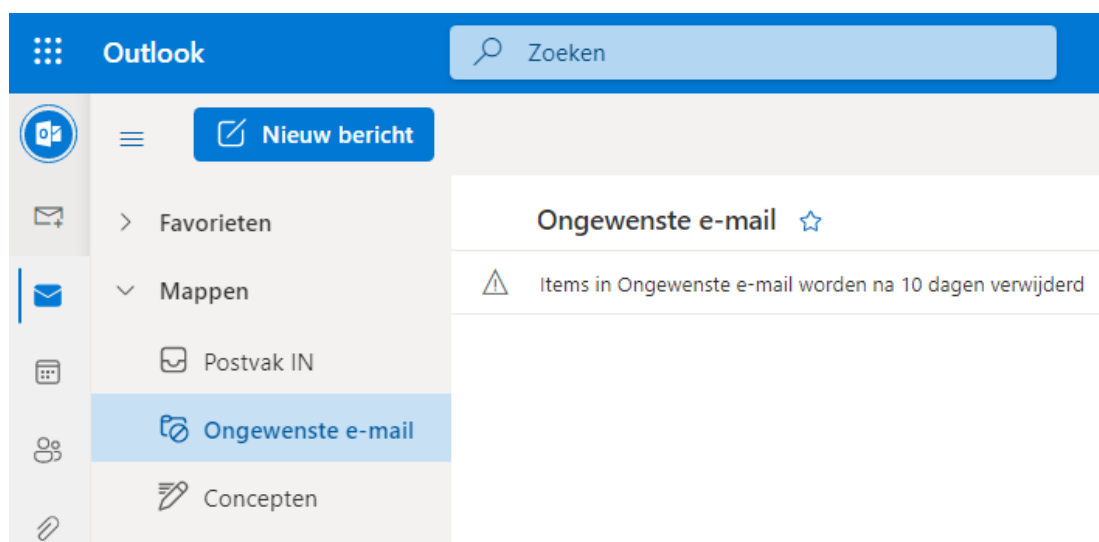
 **Spraakbericht of sms**
06 30314090 **Geverifieerd** 
Verificatiecodes worden via sms verzonden.
010 454 5454 **Geverifieerd** 
Verificatiecodes worden via spraakberichten verzonden.
[TELEFOONNUMMER TOEVOEGEN](#)

 **Back-upcodes**
Er zijn momenteel 10 eenmalige codes actief, maar je kunt er zo nodig  meer genereren.
[CODES WEERGEVEN](#)

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

Een vertrouwde afzender op de whitelist van het spamfilter zetten

Het gebeurt regelmatig dat gewenste e-mail (berichten van bekenden, bedrijven, instanties e.d.) tóch door het spamfilter van de e-mailprovider wordt aangemerkt als spam, en als zodanig naar de map met ongewenste e-mail worden verplaatst. De berichten in deze map worden na enige tijd automatisch verwijderd (bij Outlook bijvoorbeeld al na 10 dagen!). Heb je daar geen erg in, dan loop je al snel belangrijke e-mail mis.



Het is dus aan te raden om de spammap van het e-mailaccount regelmatig te controleren. Deze map is te benaderen vanuit de [online omgeving van het e-mailadres](#) (of vanuit het e-mailprogramma, wanneer het e-mailadres met behulp van het [IMAP-protocol](#) wordt beheerd). Heb je te maken met ongewenst als spam gemarkeerde berichten (ook wel false positives genoemd), ga dan als volgt te werk:

- **Markeer het bericht als gewenst**

Markeer het bericht als gewenst zodat deze direct naar de map

Postvak IN wordt verplaatst. Deze optie is doorgaans bereikbaar met een knop (te herkennen aan een term als **Geen ongewenste e-mail** of **Geen spam**), of via een optie uit het contextmenu (te openen met rechter muisklik op het bericht).

- **Zet de afzender op de whitelist (of pas een filter toe)**

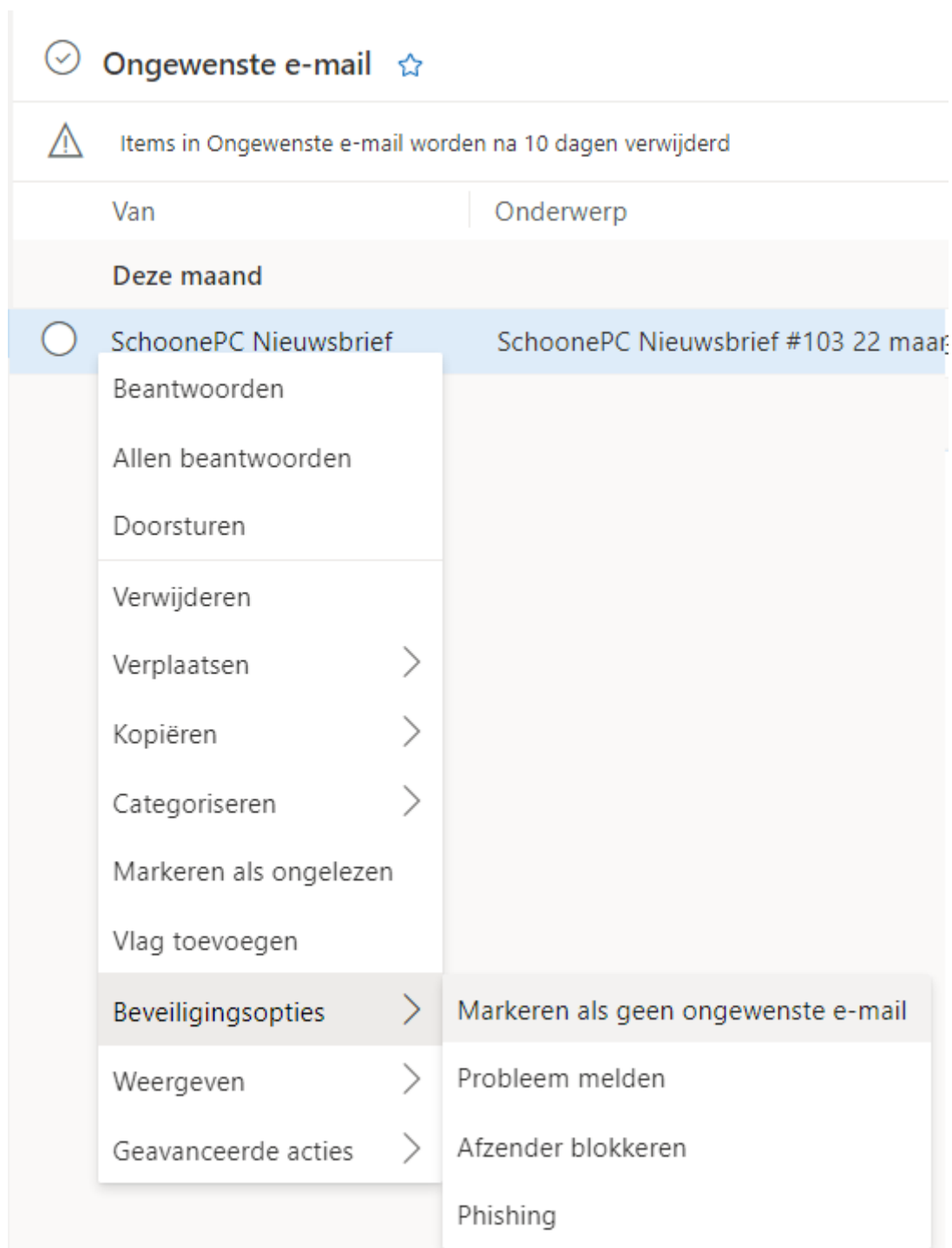
Om te voorkomen dat toekomstige berichten van een afzender opnieuw als spam gemarkeerd worden, toont de melding voor het als gewenst markeren vaak gelijk al de optie om de betreffende afzender ook aan de whitelist toe te voegen. Het aan de whitelist toevoegen kan ook handmatig: zoek binnen de webmail naar de instellingen van het spamfilter (vaak toegankelijk via het tandwiel) en voeg het e-mailadres van de afzender (bijvoorbeeld **nieuws@schoonepc.nl** voor de SchoonePC-nieuwsbrief) toe aan de lijst met veilige afzenders. In plaats van een e-mailadres kan ook het domein (in dit voorbeeld **schoonepc.nl**) worden toegevoegd zodat álle e-mailadressen van de betreffende website als veilig worden gemarkeerd. Maakt de e-mailprovider geen gebruik van een whitelist (zoals Gmail), controleer dan of er een filter aangemaakt kan worden waarmee toekomstige e-mailberichten van betreffende afzenders altijd in de inbox geplaatst zullen worden (en dus nooit in de spammap).

Zonder voorbeeld blijft het wellicht vaag, vandaar dat ik in een tweetal voorbeelden laat zien hoe dat bij Microsoft- en Gmail-accounts in zijn werk gaat.

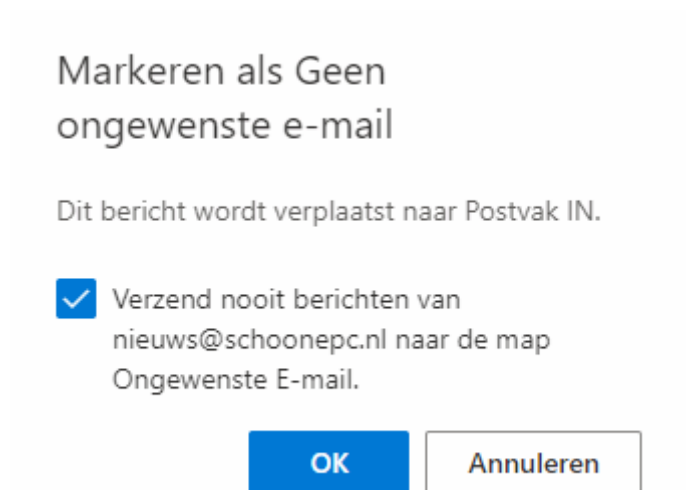
Voorbeeld 1: E-mailadres van Microsoft (@outlook.com, @hotmail.com, @live.com, @msn.com)

Log via www.outlook.com in op de webmail van Microsoft en verplaats het ten onrechte in de map **Ongewenste e-mail** geplaatste

e-mailbericht naar de map **Postvak IN** via een rechter muisklik op het bericht, optie **Beveiligingsopties**, optie **Markeren als geen ongewenste e-mail** (of selecteer het bericht en klik op de knop **Geen ongewenste e-mail**), knop **OK**.



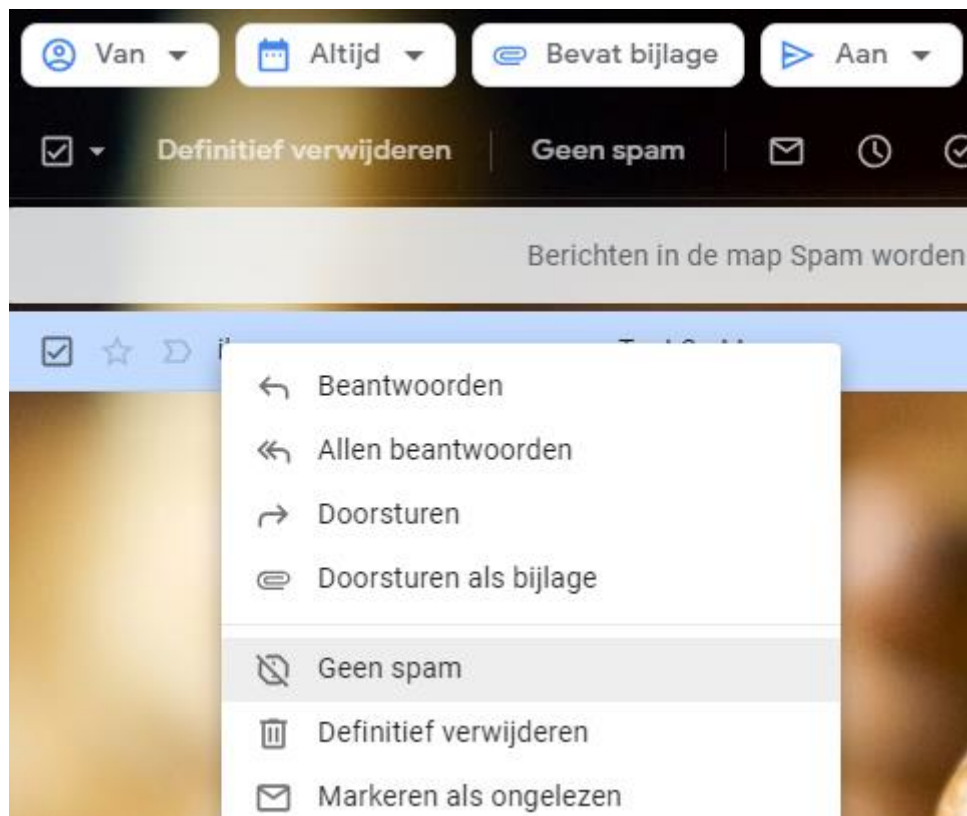
Is de optie **Verzend nooit berichten van ... naar de map Ongewenste E-mail** geactiveerd (in de pop-up), dan wordt het betreffende e-mailadres automatisch aan de whitelist toegevoegd zodat toekomstige berichten van deze afzender niet meer in de map **Ongewenste e-mail** worden geplaatst.



Wil je liever het bijbehorende domein aan de whitelist toevoegen? Ga dan naar het tandwiel, link **Alle Outlook-instellingen weer-geven**, menu **E-mail**, submenu **Ongewenste e-mail**, kopje **Veilige afzenders en domeinen**, link **+ Toevoegen**, vul het domein (bijvoorbeeld **schoonepc.nl**) in en bevestig met **ENTER**.

Voorbeeld 2: E-mailadres van Gmail (@gmail.com)

Log via www.gmail.com in op de webmail van Gmail en verplaats het ten onrechte in de map **Spam** geplaatste e-mailbericht naar de map **Inbox** via een rechter muisklik op het bericht, optie **Geen spam** (of selecteer het bericht en klik op de knop **Melden dat dit geen spam is**). Zie je de map **Spam** niet staan, klap het menu dan uit via de link **Meer**.



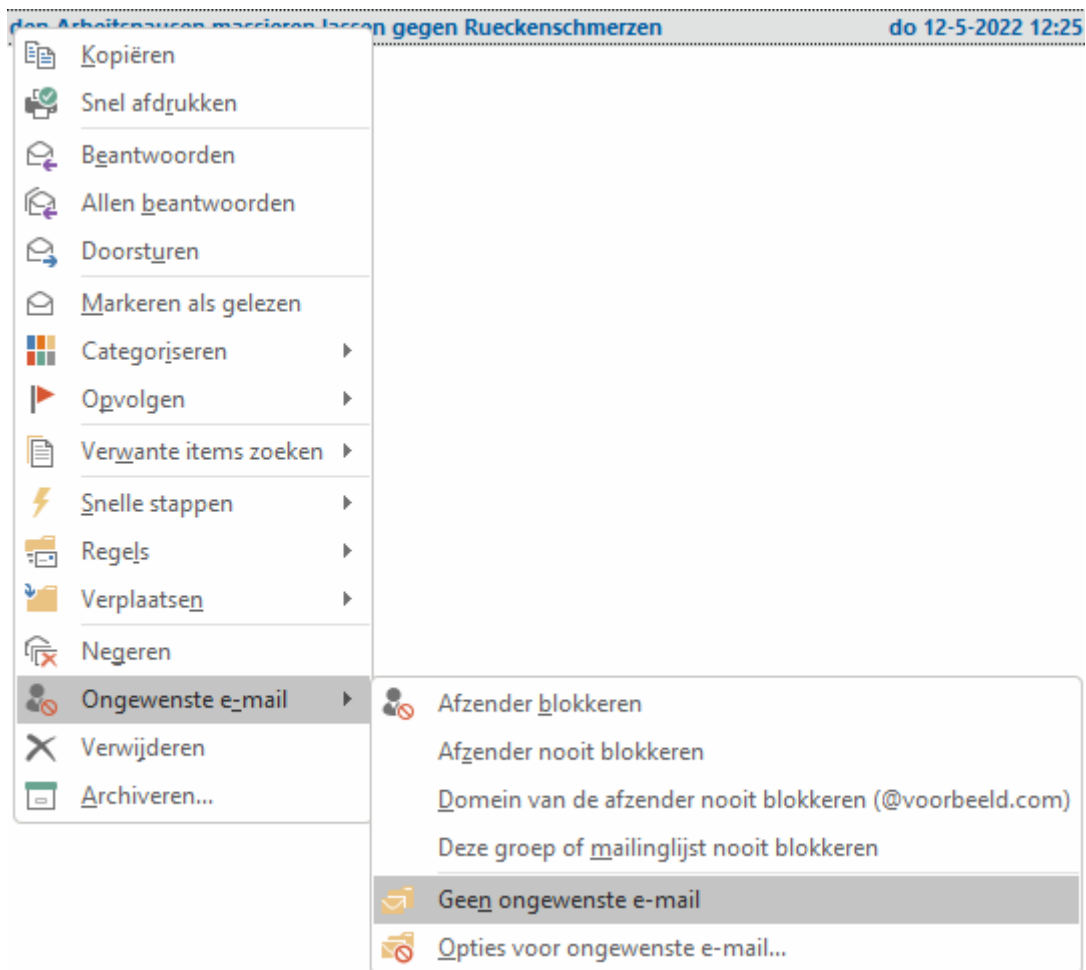
Om te voorkomen dat e-mailberichten van deze afzender in de toekomst weer als spam worden gemarkeerd, kan de afzender aan de contacten worden toegevoegd. Voeg je liever een domein toe, maak dan een filter aan via het tandwiel, knop **Alle instellingen bekijken**, tabblad **Filters en geblokkeerde adressen**, link **Nieuw filter maken**, vul bij **Van** het domein in (bijvoorbeeld **schoonepc.nl**), knop **Filter maken**, activeer de optie **Nooit naar Spam sturen**, knop **Filter maken**.

Beheer vanuit een e-mailprogramma

Wordt het e-mailaccount vanuit een lokaal geïnstalleerd e-mailprogramma (zoals [Mail](#) of [Outlook](#)) beheerd dan kan dat op twee manieren: [met het IMAP-](#) of [met het POP-protocol](#). Bij het IMAP-protocol werk je in het e-mailprogramma, maar blijft alle e-mail online op de mailserver van de e-mailprovider staan. Kijk je vanuit het e-mailprogramma in de spammap, dan zie je dus dezelfde

berichten als wanneer je via de webmail op het e-mailaccount zou inloggen. Wordt de e-mail met het POP-protocol beheerd, dan worden uitsluitend de berichten van de inbox gedownload en lokaal opgeslagen. De berichten uit de spammap worden bij POP dus níet gedownload en zie je dan ook niet terug in het e-mailprogramma!

Worden de berichten met het POP-protocol beheerd, dan is het dus nog steeds belangrijk om de spammap van het e-mailaccount regelmatig via de webmail op false positives te blijven controleren. Aangezien dit nogal bewerkelijk is, kan het spamfilter van de e-mailprovider wellicht beter worden uitgeschakeld zodat alle berichten standaard in de inbox terechtkomen. Eventuele spamberichten kunnen dan altijd nog door het spamfilter van het e-mailprogramma worden afgehandeld. Houd er rekening mee dat ook dit spamfilter gewenste e-mail als spam kan markeren! Deze berichten zijn, net als bij de webmail, via het contextmenu naar de map Postvak IN te verplaatsen. Bij de app [Mail](#) gaat dit via de map **Meer**, map **Ongewenst** (deze naam kan afwijken), klik met rechts op het betreffende bericht, optie **Markeren als geen ongewenste e-mail**. Bij het e-mailprogramma [Outlook](#) gaat dit met een rechter muisklik op het bericht (in de map **Ongewenste e-mail**), optie **Ongewenste e-mail**, optie **Geen ongewenste e-mail** (of de optie **Domein van afzender nooit blokkeren**); bevestig vervolgens met de knop **OK** om aan te geven dat toekomstige berichten van de betreffende afzender ook vertrouwd mogen worden.



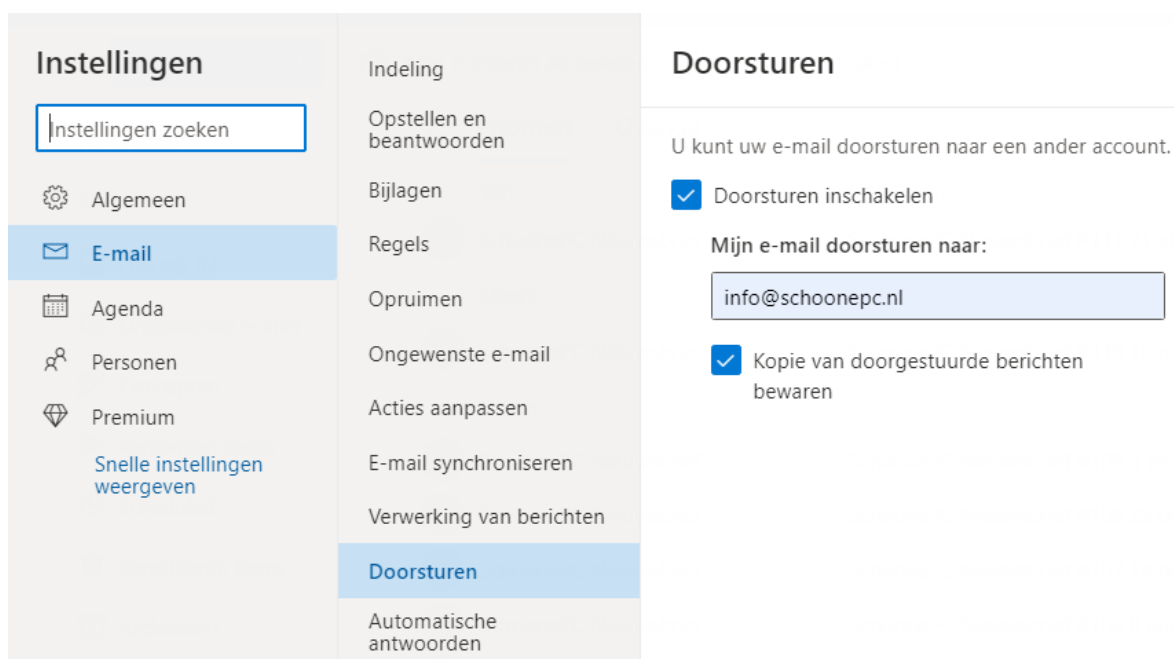
TIP: De instellingen van het spamfilter van Outlook zijn toegankelijk via de optie **Ongewenste e-mail**, optie **Opties voor ongewenste e-mail** in het contextmenu.

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

Laat e-mail niet (meer) automatisch doorsturen naar een andere mailbox

Recent merkte ik bij toeval op dat ik e-mails van bedrijven, en zelfs van de Belastingdienst misliep. Er was geen spoor van te bekennen,

ze waren zelfs niet in de spammap geplaatst. Dit bleek te komen omdat ik e-mail van verschillende e-mailaccounts automatisch liet doorsturen (forwarden) naar de mailbox van een ander e-mailadres. Dit automatisch forwarden is handig om meerdere e-mailadressen vanuit één mailbox te kunnen beheren (zeker wanneer je een overbodig geworden e-mailadres wilt uitfaseren!). In onderstaand voorbeeld zie je hoe deze instelling er bij www.outlook.com uit ziet.



Het probleem speelt sinds DMARC op steeds meer mailservers wordt geactiveerd. Met deze technologie wordt namelijk gecontroleerd of het ontvangen bericht daadwerkelijk is verzonden door de mailserver die bij het e-mailadres van de vermelde afzender hoort. Aangezien een spammer zelden toegang heeft tot deze server wordt spam vrijwel altijd met een andere mailserver verzonden. Zodoende kunnen spamberichten eenvoudig met behulp van DMARC worden uitgefilterd. Het nadeel is echter dat DMARC geen onderscheid maakt tussen doorgestuurde berichten en daadwerkelijke spam. Worden de uitgefilterde berichten in de spammap geplaatst, dan is het probleem nog te overzien. Mijn ervaring is echter dat door DMARC als

spam gemarkeerde e-mail (waaronder dus ook doorgestuurde e-mail) vaak ongemerkt worden verwijderd, zowel voor de verzender als voor de ontvanger! Je weet dus nooit zeker of je iets hebt gemist hebt...

Belangrijke berichten wil je uiteraard niet missen, het is daarom verstandig e-mail (zoals ook de SchoonePC nieuwsbrief... ;-) niet langer automatisch door te laten sturen naar een een van je andere e-mailadressen. Het betreffende e-mailadres kan dan beter apart worden beheerd (bijvoorbeeld met het [POP-protocol](#) vanuit een e-mailprogramma zoals [Outlook](#)) zodat ze alsnog in een gezamenlijke **Postvak IN** van het e-mailprogramma terechtkomen.

LET OP: Bij het doorsturen kan je er meestal voor kiezen om een kopie van de doorgestuurde berichten op de mailserver achter te laten (in bovenstaande afbeelding van Outlook heet deze optie **Kopie van doorgestuurde berichten bewaren**). Mocht je denken dat je het probleem hiermee oplost dan moet ik je helaas teleurstellen. De mailserver van de verzender ontvangt dan namelijk nog steeds een melding dat het bericht is geblokkeerd. Betreft het een nieuwsbrief dan wordt dit wellicht ook meteen de laatste, aangezien door DMARC-gefilterde berichten meestal automatisch van een mailinglijst worden verwijderd...

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

Nieuwsbrief 111 gemist?

Heb je nieuwsbrief 111 gemist? Vraag deze dan op [via de website](#) en/of download het [PDF-bestand](#). Uiteraard is de bijbehorende [video](#) ook nog beschikbaar!

Windows 11:
venster Instellingen
deel 2 



Menno Schoone
www.SchoonePC.nl

SchoonePC Nieuwsbrief 111



Een greep uit de vele reacties van gebruikers van de computerbijbel

"De computerbijbel voor Windows 11 ziet er goed uit!"

"Ik ben zeer tevreden en heb al veel problemen opgelost dankzij je boek."

"Diverse malen heb ik profijt gehad van uw computerbijbels bij het oplossen van problemen."

"Dank voor de snelle levering. Ik ben zeer tevreden met het Windows 11-boek."

"Ik ben geweldig blij met die bijbel, zonder twijfel."

"Het is een goed te lezen boek met veel wetenswaardigheden."

"Fijn naslagwerk."

"U heeft een bijzonder goed en mooi boek gemaakt. Het zal erg veel tijd gekost hebben om dit voor elkaar te krijgen!"

"Hartelijk dank voor de info. Ik heb al veel gehad aan de computerbijbel voor Windows 11."

Meer informatie over de computerbijbel >

www.SchoonePC.nl | Aanmelden nieuwsbrief

© 2001-2022 - SchoonePC - Rotterdam - The Netherlands