



SchoonePC Nieuwsbrief

De informatiebron voor uw computerproblemen

door *Menno Schoone*

Nieuwsbrief 148

2 juni 2026

Hallo SchoonePC-fan,

Na alle hectiek rondom de lancering van de nieuwe editie van de [computer-bijbel](#) hebben we uitgebreid de tijd genomen om weer een nieuwsbrief met interessante onderwerpen te schrijven!

De onderwerpen in deze nieuwsbrief:

- [Blauwe kaders Verteller uitschakelen](#)
- [Veilig online bankieren](#)
- [De Windows-partitie vergroten](#)
- [Betrouwbaarheid systeemtools](#)
- [Ernstig lek in BitLocker-encryptie](#)
- [Ontvangstproblemen bij het doorsturen van mail naar adressen van Microsoft](#)
- [E-mailberichten van Infomedics](#)

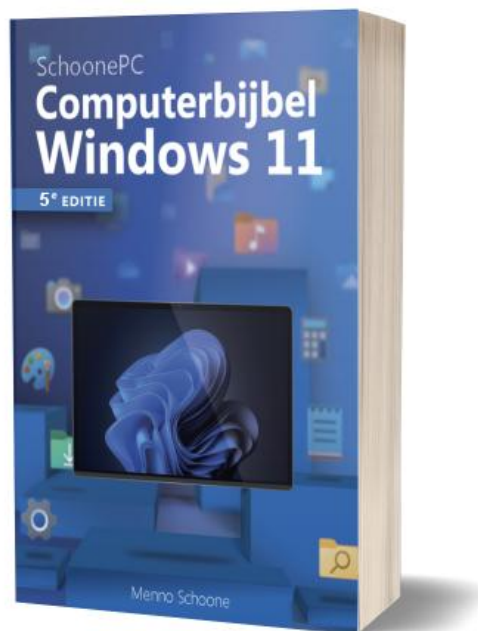
Ik wens je weer veel lees- en computerplezier. Tot de volgende nieuwsbrief!

Menno Schoone

www.SchoonePC.nl

Word computerwijzer en -vaardiger met de computerbijbel voor Windows 11

De nieuwe 5e editie van de computerbijbel voor Windows 11 is een **448 pagina's** tellend naslagwerk vol tips en trucs om Windows 11 de baas te worden en problemen voortaan zelf op te lossen. Bij elke nieuwe editie wordt de computerbijbel van A tot Z onder handen genomen, en aangevuld op basis van nieuw toegevoegde functies, interessante lezersvragen en voortschrijdend inzicht. Dat dit wordt gewaardeerd, blijkt wel uit de reacties van lezers. Ligt deze up-to-date computerbijbel dus nog niet naast je pc, bestel hem dan [via de website!](#)



"Dank voor de bijzonder nuttige computerbijbel. Voor veel van mijn vragen en problemen vond ik er de voorbije jaren dikwijls het juiste antwoord."

Frank

Het meest informatieve handboek voor Windows 11

Met deze 5e editie weet ik zeker dat de computerbijbel zijn reputatie als 'het meest informatieve handboek voor Windows' weet hoog te houden. Loop je dus regelmatig tegen computerproblemen aan en kan je wel wat hulp gebruiken? Of wil je gewoonweg Windows onder de knie krijgen en het maximale uit je pc halen? Ga dan aan de slag met mijn nieuwe computerbijbel!

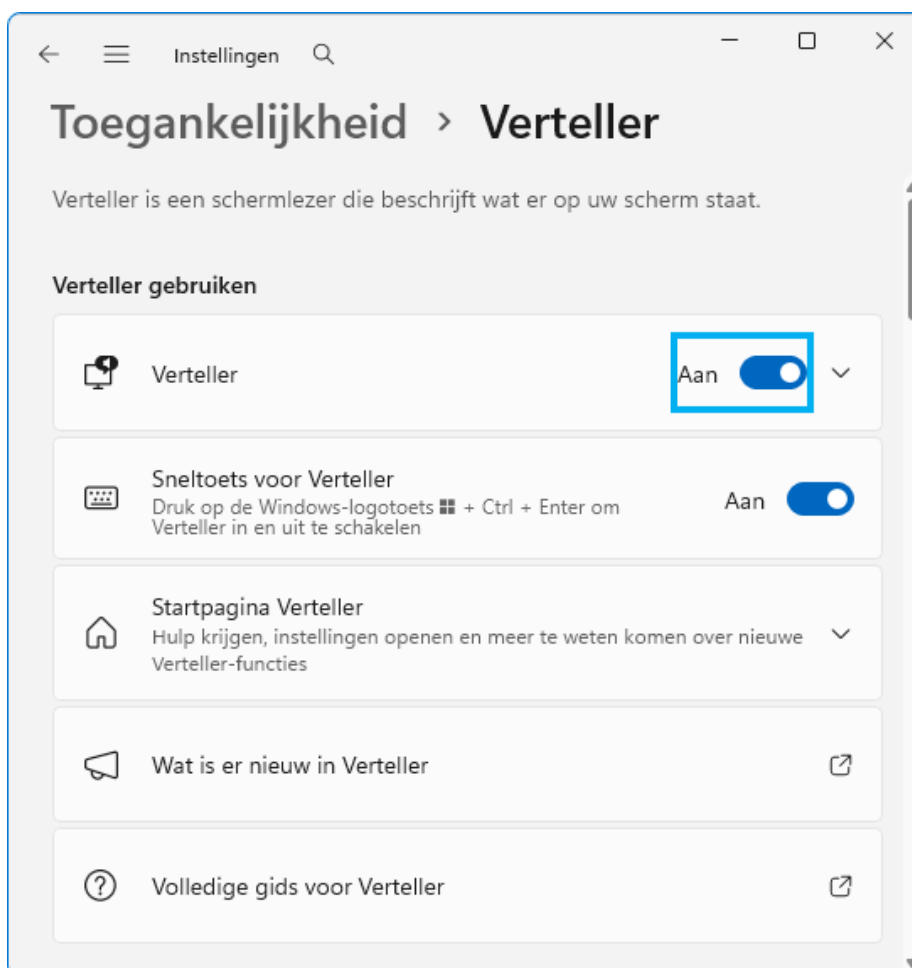
Kom je er niet uit? Dan help ik je graag even verder!

Ik heb maar één doel: je computerwijzer en -vaardiger maken. De computerbijbel is dan ook een ideaal hulpmiddel om problemen zelf op te lossen. Loop je desondanks tegen een probleem aan waar je niet uitkomt, dan help ik je graag even verder. Dat is onderdeel van mijn service! Volgens menig lezer maakt deze hulp alleen al de aanschaf van de computerbijbel een koopje, het raadplegen van een helpdesk is immers niet goedkoop.

[Meer informatie over de computerbijbel >](#)

Blauwe kaders Verteller uitschakelen

Vraag van Bas: *"In al mijn programma's verschijnen opeens blauwe kaders. Wat kan dat zijn?"*



Deze blauwe kaders worden weergegeven door de Verteller, ook wel Narrator genoemd. De Verteller is te activeren via **Instellingen > Toegankelijkheid > Verteller**, of via de toetscombinatie **Win-Ctrl-Enter**. Deze functie leest hardop voor wat er op het scherm te zien is, en vertelt welk venster, menu, knop of optie geselecteerd is. Het blauwe kader markeert het element dat op dat moment wordt voorgelezen. Een reuze handige functie wanneer je slechtziend bent! Raak je de toetscombinatie echter per ongeluk aan (hetgeen deze vragensteller mogelijk gedaan heeft), ben je niet bekend met de Verteller en heb je ook nog eens het geluid uit staan dan kan ik mij voorstellen dat je geen idee hebt waar die irritante blauwe kadertjes opeens vandaan komen... En dus ook niet hoe je er weer vanaf kan komen! Weet je eenmaal dat het om de Verteller gaat dan is het 'probleem' gelukkig simpel op te lossen door de tool weer uit te schakelen (via het venster Instellingen of door de toetscombinatie nogmaals in te drukken). Wordt de Verteller vaker per ongeluk geactiveerd, schakel dan de toetscombinatie voor het openen van de Verteller uit (via **Instellingen > Toegankelijkheid > Verteller**, deactiveer optie **Sneltoets voor Verteller**).

TIP: Ben je geïnteresseerd in de mogelijkheden van de Verteller? Op de website van Microsoft is een [uitgebreide handleiding](#) te vinden.

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

Veilig online bankieren

Heb je angst voor online bankieren en gebruik je daarom nog steeds papieren overschrijvingsformulieren om je betalingen uit te voeren, weet dan dat je niet de enige bent! Sommigen zijn bang voor het onbekende, willen geen fouten maken of vrezen de controle over de bankrekening te verliezen. Maar de grootste angst is wellicht om slachtoffer te worden van internetcriminelen die je bankrekening leegplunderen. Die angst is echter ongegrond, zeker wanneer je de juiste voorzorgsmaatregelen neemt. Daarnaast levert online bankieren veel gemak op. Om de drempel naar het online bankieren te verlagen, leg ik in dit artikel uit wat er nodig is om dat veilig te doen.

Beheer je bankzaken uitsluitend via de app van de bank

Het is natuurlijk verstandig om voorzichtig te zijn wanneer het om je geld gaat. En het is ook een feit dat criminelen steeds nieuwe manieren verzinnen om via telefoon, e-mail, SMS, WhatsApp e.d. toegang tot je bankrekening te krijgen. Veruit de meeste risico's kunnen echter eenvoudig geëlimineerd worden door je bankzaken uitsluitend via de door de bank beschikbaar gestelde app te beheren! Wordt de website van de bank niet gebruikt dan kan je namelijk ook niet per ongeluk via een legitiem lijkende link op een kwaadwillende website terechtkomen (met alle gevolgen van dien...). Is het toch nodig om zaken via de website van de bank te regelen, open deze dan bij voorkeur vanuit de bank-app.

Een ander pluspunt van de bank-app is dat belangrijke zaken standaard via deze app gecommuniceerd worden. Ogenschijnlijk van de bank afkomstige telefoontjes, e-mail-, SMS- en WhatsApp-berichten kan je dus gewoon negeren, zeker wanneer deze een of andere actie van je vragen! De bank zal sowieso nooit telefonisch contact met je opnemen om zaken te regelen, tenzij je daar expliciet toestemming voor hebt gegeven. Word je toch gebeld, geef dan vooral geen persoonlijke gegevens door (die heeft je bank al...) en controleer vanuit de app of je daadwerkelijk door een medewerker van de bank wordt gebeld. Twijfel je, hang dan op en bel eventueel zelf naar de bank om navraag te doen.

NB: Er zijn alleen bank-apps voor Android of iOS ontwikkeld, niet voor Windows. Je ontkomt er dus niet aan om je bankzaken vanaf een mobiele telefoon (of tablet) te beheren.

De bank-app heeft meer voordelen

Het gebruik van de bank-app heeft nog meer voordelen. Zo kan je nooit per ongeluk geld naar een verkeerd IBAN-rekeningnummer overmaken. Wordt bijvoorbeeld een fout gemaakt bij het invoeren van het IBAN-rekeningnummer dan klopt het controlegetal niet en zal je dat direct te zien krijgen. Ook wordt meteen gecontroleerd of de opgegeven naam overeenkomt met de naam van de rekeninghouder. Daarnaast is er voor de app een limiet ingesteld aan het bedrag dat maximaal per dag overgemaakt kan worden (ver-

gelijkbaar met de daglimiet voor de bankpas). Voor het overmaken van een groter bedrag kan deze daglimiet tijdelijk worden verhoogd. Om te voorkomen dat je onder druk van een crimineel snel een groot bedrag overmaakt, wordt de verhoging van de daglimiet pas na enkele uren daadwerkelijk doorgevoerd.

Niemand krijgt zomaar toegang tot je bankrekening

Je kan via de bank-app niet zomaar toegang krijgen tot een bankrekening. Om te beginnen moet je je bij het instellen van de app identificeren met je bankpas en een geldig identiteitsbewijs om te bewijzen dat het bankrekeningnummer van jou is. Verder moeten zowel de telefoon als de app bij elk gebruik ontgrendeld worden met een pincode, vingerafdruk of gezichtsherkenning. Kies hiervoor unieke en onvoorspelbare pincodes, gebruik dus niet je geboortjaar of postcode, en bewaar deze niet in het hoesje van je telefoon...

Zolang je de aanmeldgegevens voor jezelf houdt en je bankpas en identiteitsbewijs veilig opbergt, is het voor derden vrijwel onmogelijk om toegang tot je bankrekening te krijgen. Kan je je bankpas even niet meer vinden dan kan je deze voor de zekerheid vanuit de app blokkeren (en weer deblokkeren zodra hij is teruggevonden). Vermoed je dat je aanmeldgegevens in verkeerde handen terechtgekomen zijn, is je mobiel of bankpas gestolen of bemerk je iets ongebruikelijks, aarzel dan niet om direct contact op te nemen met de bank. Zij kunnen met je meekijken en zo nodig je bankrekening tijdelijk blokkeren.

Wat je nog meer kan doen om veilig online te bankieren

Om de bank-app veilig te kunnen gebruiken, moeten zowel de app als het besturingssysteem van de telefoon up-to-date zijn. Zolang de app nog opstart, mag je ervan uitgaan dat dat het geval is. Hoewel het verleidelijk is om onderweg gebruik te maken van een openbaar wifi-netwerk, is het verstandiger om de bank-app alleen te openen wanneer is aangemeld op een veilige internetverbinding (zoals het mobiele netwerk van je telefoon of het thuisnetwerk van je internetprovider). Zodoende verlaag je het risico dat je internetverbinding (en daarmee de communicatie met je bank-app) wordt 'afge-

luisterd'. Wees daarnaast terughoudend met het installeren van vage apps, je wil immers niet dat je mobiel besmet raakt met malware (ook al is de kans klein dat malware misbruik kan maken van bank-apps).

MEER LEZEN?

Wil je meer lezen over de do's en don'ts bij online bankieren, neem dan eens een kijkje op een van de volgende websites:

- www.voorkomfraude.nl
- www.veiligbankieren.nl
- www.fraudehelpdesk.nl
- En uiteraard de website van je eigen bank...

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

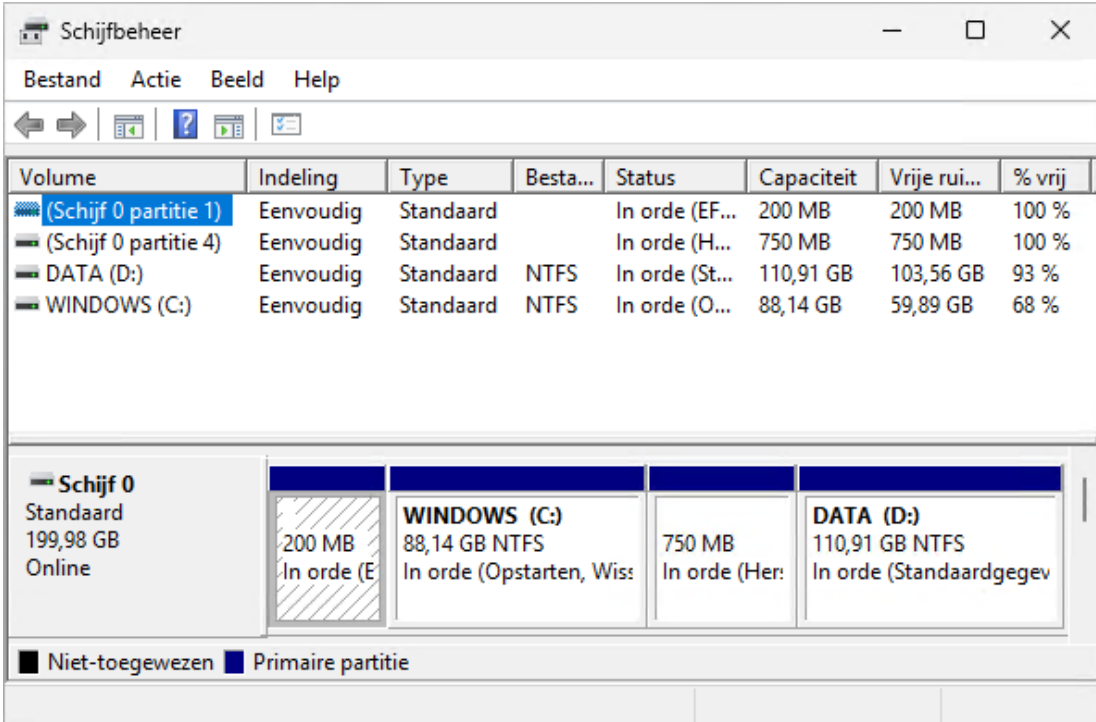
De Windows-partitie vergroten

Is Windows op een te kleine partitie geïnstalleerd dan loop je vroeg of laat tegen problemen aan. Denk bijvoorbeeld aan een traag systeem, vastlopende programma's en het niet meer kunnen updaten van Windows. In het ergste geval kan Windows zelfs compleet vastlopen! Vaak is er nog wel opslagruimte te winnen door persoonlijke bestanden, programma's en/of [overbodige bestanden](#) te verwijderen. Is het ruimtegebrek daar echter niet (meer) mee op te lossen dan moet je rigoureuzer te werk gaan.

Is de Windows-partitie (doorgaans C:) zo groot dat deze vrijwel de gehele schijf in beslag neemt dan zit er niets anders op dan een grotere schijf aan te schaffen (hierna zal je Windows nog wel opnieuw moeten installeren of overzetten met een clonetool zoals [Macrium Reflect](#)). Staat er echter nog een andere partitie met voldoende vrije ruimte op de schijf (bijvoorbeeld een datapartitie) dan kan deze met behulp van partitioneringssoftware worden verkleind, om vervolgens met de vrijgekomen schijfruimte de Windows-partitie te vergroten. Omdat deze procedure niet eenvoudig is, leg ik in dit artikel stap voor stap uit hoe dit in zijn werk gaat.

De partitionering aanpassen met Schijfbeheer

Het is belangrijk om eerst de huidige partitionering in kaart te brengen, hiervoor kan bijvoorbeeld **Schijfbeheer** van Windows worden gebruikt (te openen via een rechter muisklik op Start). Onderstaand voorbeeld toont een Windows-partitie (C:) van 88 GB, een datapartitie (D:) van 111 GB en twee systeempartities, waarvan er eentje tussen C: en D: ligt (zie de visuele weergave onderin Schijfbeheer). Deze tussenliggende herstelpartitie is door de setup van Windows aangemaakt en kan beter niet worden verwijderd, dit vraagt dus om een specifieke aanpak (let op: in dit geval is sprake van één herstelpartitie, het kunnen er echter ook meerdere zijn).



The screenshot shows the Windows Disk Management tool. The main table lists the following partitions:

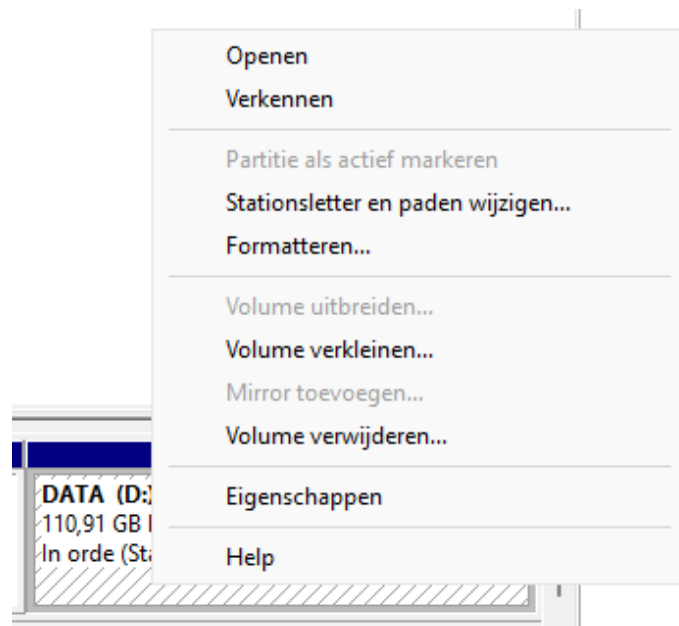
Volume	Indeling	Type	Besta...	Status	Capaciteit	Vrije rui...	% vrij
(Schijf 0 partitie 1)	Eenvoudig	Standaard		In orde (EF...	200 MB	200 MB	100 %
(Schijf 0 partitie 4)	Eenvoudig	Standaard		In orde (H...	750 MB	750 MB	100 %
DATA (D:)	Eenvoudig	Standaard	NTFS	In orde (St...	110,91 GB	103,56 GB	93 %
WINDOWS (C:)	Eenvoudig	Standaard	NTFS	In orde (O...	88,14 GB	59,89 GB	68 %

Below the table, a visual representation of 'Schijf 0' (199,98 GB, Online) is shown. It consists of four partitions:

- A 200 MB partition (shaded with diagonal lines) labeled 'In orde (E...'.
- A partition labeled 'WINDOWS (C:)' with a capacity of 88,14 GB NTFS, status 'In orde (Opstarten, Wis:'.
- A 750 MB partition labeled 'In orde (Her:'.
- A partition labeled 'DATA (D:)' with a capacity of 110,91 GB NTFS, status 'In orde (Standaardgege...'.

Legend: ■ Niet-toegewezen ■ Primaire partitie

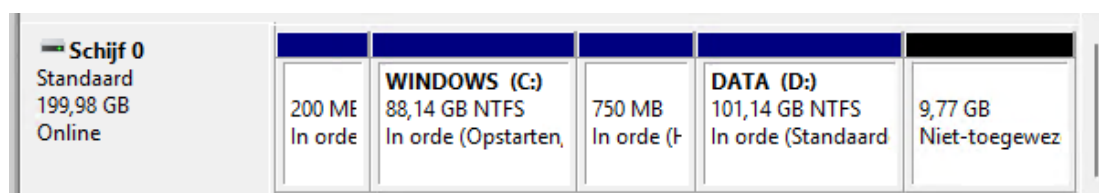
Het verkleinen van de D:-partitie gaat via een rechter muisklik op de partitie, optie **Volume verkleinen**.



Geef vervolgens aan met hoeveel MB de D:-partitie verkleind moet worden, in onderstaand voorbeeld is dat met 10.000 MB (oftewel 10 GB). Meestal is dat wel genoeg, tenzij je grootse plannen hebt...



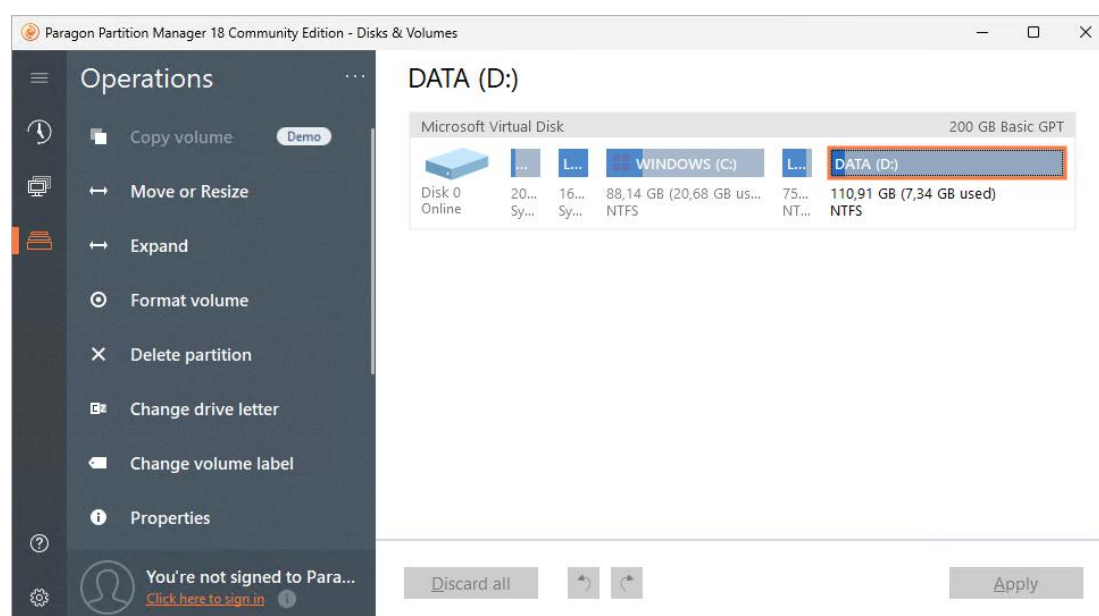
De 10 GB aan vrijgekomen schijfruimte wordt in de visuele weergave rechts van de D:-partitie weergegeven, als niet-toegewezen ruimte.



Om de vrijgekomen schijfruimte aan de C:-partitie toe te kunnen voegen, moeten de D:-partitie en de tussenliggende herstelpartitie eerst geheel naar rechts worden verplaatst zodat de niet-toegewezen schijfruimte direct naast de Windows-partitie komt te staan. Dit is echter niet mogelijk met Schijfbeheer, velen lopen hier dan ook vast!

De partitionering aanpassen met Paragon

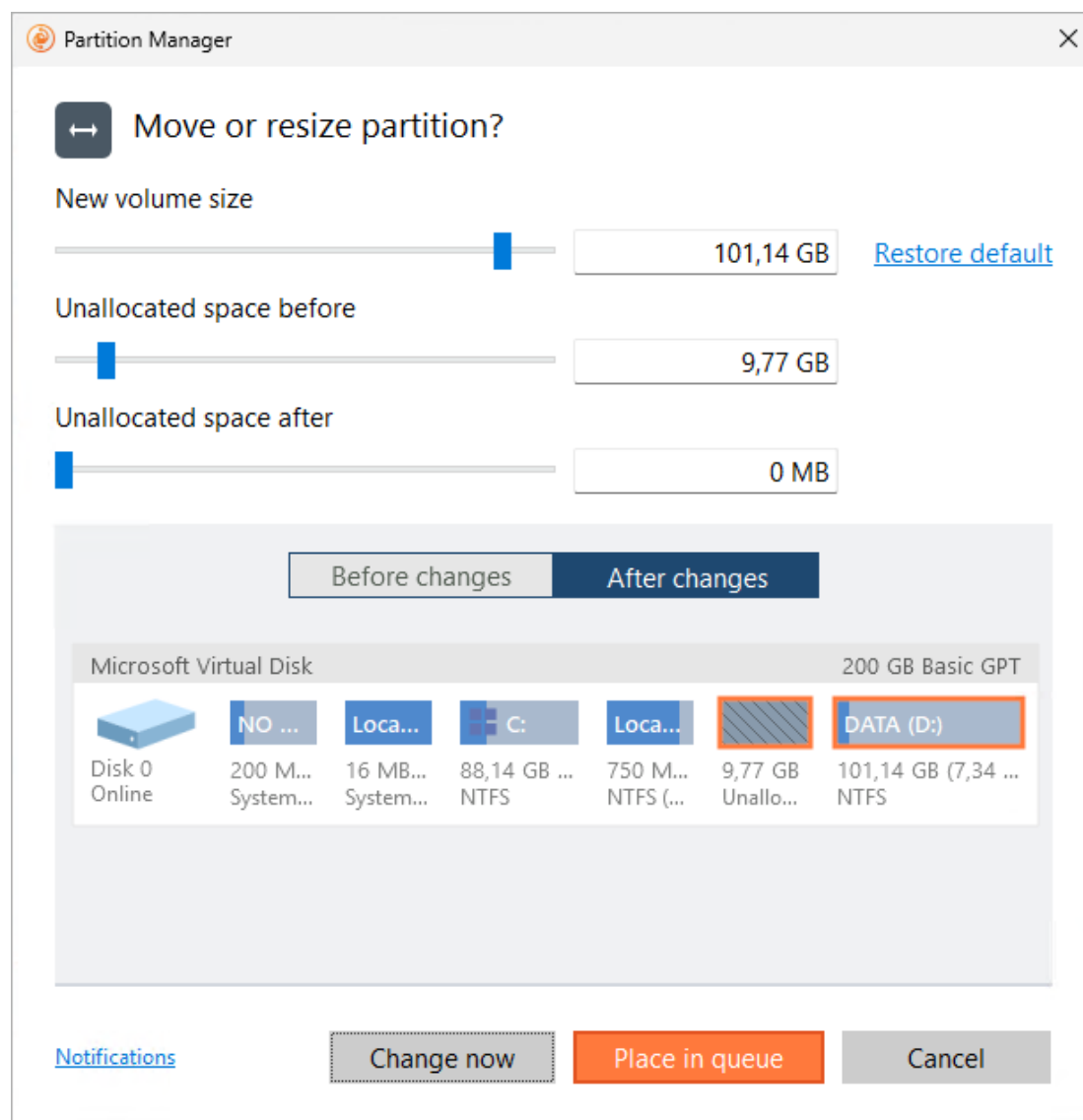
Weet je vooraf al dat er partities verplaatst moeten worden dan kan je beter direct gebruikmaken van een alternatieve partitioneringstool zoals de gratis Community-editie van **Paragon Partition Manager** (download: www.paragon-software.com). Ook Paragon toont een visuele weergave van de huidige partitie-indeling:



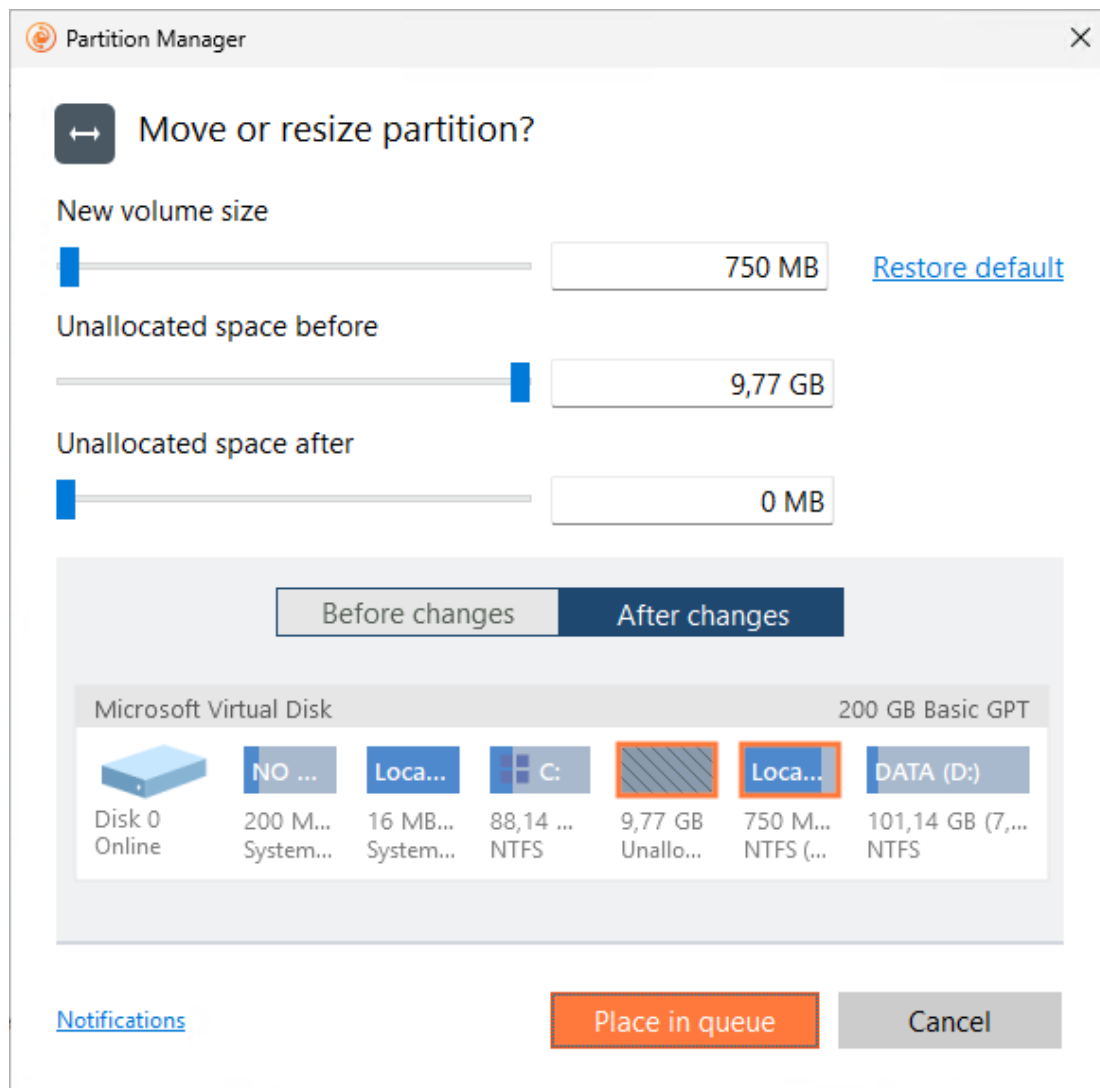
LET OP: Toont Paragon een hangslot-icoontje bij een van de partities dan is de betreffende partitie versleuteld (met [Apparaatversleuteling of BitLocker](#)). Dergelijke partities kunnen pas bewerkt worden nadat de versleuteling is uitgeschakeld.

Bij Paragon gaat het verkleinen van de D:-partitie als volgt: selecteer de D:-partitie, optie **Move or Resize** en zet **Unallocated space before** op 10 GB. Met deze wijziging wordt aan de voorkant van de D:-partitie (visueel gezien links van de partitie) ruimte vrijgemaakt, deze ruimte krijgt dan het label **Unallocated**. Let op dat je **Unallocated space after** op 0 MB laat staan,

deze maakt de partitie namelijk aan de verkeerde kant kleiner! Je zou de aangebrachte wijziging direct kunnen doorvoeren (knop **Change now**), het is echter makkelijker om deze eerst in de wachtrij te zetten (knop **Place in queue**) omdat er nog meer aanpassingen volgen.

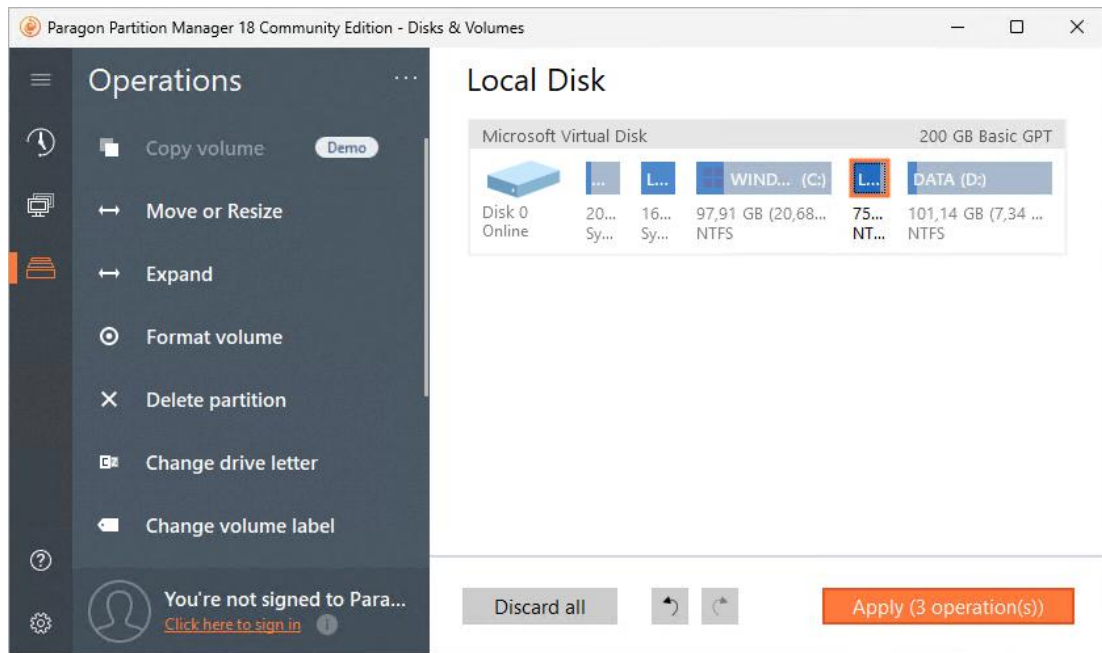


De aangemaakte vrije schijfruimte **Unallocated** staat nu virtueel tussen de herstelpartitie en de D:-partitie. Om de vrije schijfruimte direct achter de C:-partitie te krijgen, moet de herstelpartitie zo ver mogelijk naar rechts verplaatst worden. Selecteer hiervoor de herstelpartitie, optie **Move or Resize**, wijzig de optie **Unallocated space after** in 0 MB (zodat de 10 GB vrije schijfruimte tussen de C:-partitie en de herstelpartitie wordt weergegeven) en zet deze wijziging in de wachtrij (knop **Place in queue**).



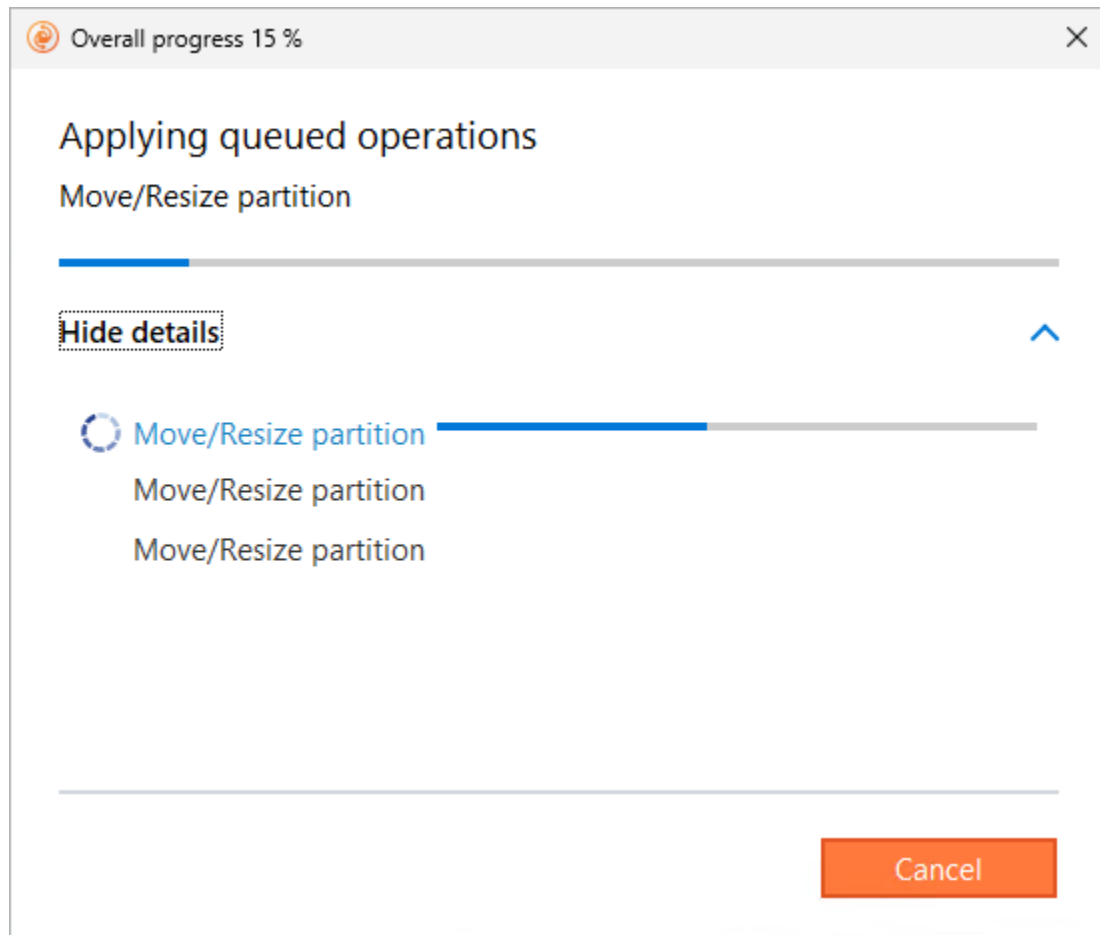
TIP: Een partitie kan ook worden verplaatst door de muis aan de onderkant van de partitiebalk te plaatsen (zodat de tekst **Click and drag here to move partition** wordt weergegeven) en de partitie vervolgens te verslepen. De partitiegrootte kan op vergelijkbare wijze worden aangepast door de haak aan de linker- of rechterkant van de partitie te verslepen.

Tot slot kan de C:-partitie op vergelijkbare wijze worden vergroot: selecteer de C:-partitie, optie **Move or Resize**, wijzig de optie **Unallocated space after** in 10 MB. Zet ook deze wijziging in de wachtrij. Het hoofdscherm ziet er dan als volgt uit:



De visuele weergave laat zien hoe de nieuwe partitie-indeling er na het doorvoeren van de in de wachtrij geplaatste wijzigingen uit komt te zien. Ben je niet tevreden dan kunnen de geplande wijzigingen met de linker pijlknop stuk voor stuk weer uit de wachtrij worden verwijderd (te beginnen bij de laatst toegevoegde aanpassing). En met de rechter pijlknop kunnen verwijderde wijzigingen eventueel weer worden toegevoegd. Met de knop **Discard all** kunnen de aan te brengen wijzigingen ook allemaal in één moeite worden verwijderd.

Is alles in orde dan kunnen alle in de wachtrij geplaatste aanpassingen in één moeite definitief worden doorgevoerd met de knop **Apply (3 operation(s))**. Omdat hierbij bestanden verplaatst moeten worden, kan dit wel vrij lang duren. Let op: sluit Windows niet af tijdens deze bewerkingen want dan ontstaan er geheid grote problemen!



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

Betrouwbaarheid systeemtools

Er is een groot aanbod aan geavanceerde systeemtools, zowel gratis als betaald. Denk bijvoorbeeld aan partitioneringstools (om de partitie-indeling van schijven aan te passen), imagingtools (om systeembak-ups te maken en weer terug te zetten), clonetools (om schijven te dupliceren) en recovery-tools (om per ongeluk verwijderde bestanden te herstellen). Het aanbod verandert met enige regelmaat, de afgelopen jaren is er echter een opmerkelijke trend waarneembaar: terwijl menig klassieke systeemtool niet meer wordt onderhouden of alleen nog als betaalde software beschikbaar wordt gesteld, winnen de systeemtools met een Chinese achtergrond (zoals EaseUS, Hasleo, NIUBI, DiskGenius, AOMEI e.d.) steeds meer aan populariteit. Het is vast het gevolg van het hoogstaande bèta-onderwijs in China, daar kunnen we nog veel van leren!

Chinese software is doorgaans van een hoog niveau, vandaar dat hun systeemtools door vele gespecialiseerde websites en computermagazines worden aanbevolen. Ook marketingtechnisch hebben Chinese softwareproducenten een enorme inhaalslag gemaakt. Zo stellen ze vrijwel altijd een gratis versie met veel functionaliteit beschikbaar. Vaak ziet hun website er overtuigend uit en is deze (net als de tool) in vrijwel alle talen beschikbaar. Het is dan ook logisch dat ze een groot bereik hebben, en dat je er gewoonweg niet omheen kan wanneer je op zoek bent naar zo'n tool.

Nu er steeds meer zorgen zijn over de invloed van de Amerikaanse overheid op big tech (en daarmee op onze maatschappij), lijkt de aandacht voor de risico's bij Chinese hard- en software naar de achtergrond te verdwijnen. Het Nationaal Cyber Security Centrum (NCSC) en de Nederlandse inlichtingen- en veiligheidsdiensten AIVD en MIVD waarschuwen echter niet voor niets al jaren voor de inmenging van de Chinese overheid. Hoewel die waarschuwingen niet specifiek over deze systeemtools gaan, is het niet ondenkbaar dat ze voor een veiligheidsprobleem kunnen zorgen (blijven systeemtools bijvoorbeeld permanent op de achtergrond actief dan geeft dat op zichzelf al een verhoogd risico). Daarnaast kunnen als veilig bestempelde programma's door de installatie van een update alsnog onveilig worden. Je mag er dan ook vanuit gaan dat de waarschuwingen van de NCSC, AIVD en MIVD ook op deze tools van toepassing zijn.

Let wel, ik heb zelf geen enkele indicatie dat er op dit moment daadwerkelijk een veiligheidsprobleem is, wat dat betreft ontbreekt het mij aan kennis. Het lijkt mij echter verstandig om niet naïef te zijn en ook bij deze systeemtools voorzichtigheid in acht te nemen. Kan je niet zonder dan zou je de risico's kunnen verkleinen door de tools uitsluitend offline te gebruiken, de software na gebruik weer te verwijderen, na afloop een eerder gemaakt [systeemherstelpunt](#) terug te zetten en in de tussentijd de vingers gekruist te houden :-).

GRATIS SOFTWARE

Bij gratis software is het uiteraard altijd oppassen, je wilt immers niet opgezadeld worden met kwaadwillende malware. Het is daarom verstandig om een gedownload installatiebestand eerst via www.virustotal.com te laten controleren (deze website scant het bestand met tientallen virusscanners). Zelf test ik nieuwe software ook nog in [Sandbox of een virtuele pc](#) voordat ik deze daadwerkelijk op mijn pc installeer.

Dergelijke vluchtige controles geven natuurlijk geen 100% zekerheid, en daarnaast kan geïnstalleerde software door een update alsnog voor problemen gaan zorgen. Ik wil daarom ook altijd weten welk bedrijf er achter een tool zit, de bedrijfsinformatie op hun website geeft vaak een aardige indicatie hoe groot de risico's zijn. Denk bijvoorbeeld aan het achtergrondverhaal van de eigenaar, de missie, het smoelenboek, de locatie van het hoofdkantoor e.d. En geeft de website geen duidelijkheid over de eigenaar dan kom je via [Copilot](#) en www.whois.com gelukkig ook een heel eind.

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

Ernstig lek in BitLocker-encryptie

Recent is bij de BitLocker-versleuteling van Windows 11 een achterdeurtje in de herstelomgeving ontdekt waarmee de versleuteling van de schijf ongedaan gemaakt kan worden. Dit lek (bekend onder de naam [YellowKey](#)) is ernstig omdat daarmee in een handomdraai toegang kan worden verkregen tot met BitLocker versleutelde partities! Op zich hoef je je hier geen zorgen over te maken, tenzij er ooit een versleutelde pc van je is gestolen. Verkeert deze namelijk nog in dezelfde staat als destijds dan kunnen de versleutelde bestanden dankzij dit lek alsnog toegankelijk worden gemaakt. Nu heeft een dief doorgaans meer interesse in de hardware, maar als het hem om de gevoelige informatie te doen was (en de pc daarom bewaard heeft) dan is er wel een serieus probleem!

TIP: Loop je een verhoogd risico op diefstal van je laptop (bijvoorbeeld omdat je vaak op reis bent) en staat er gevoelige informatie op? Dan is het een optie om, zolang het achterdeurtje niet is gedicht, tijdelijk het wachtwoord van het BIOS in te schakelen. Houd er dan wel rekening mee dat je er het risico op jezelf buitensluiten voor terugkrijgt!

TWEEDE VEILIGHEIDSLEK: GREENPLASMA

Tegelijk met het YellowKey-lek is een tweede veiligheidslek ontdekt, bekend onder de naam [GreenPlasma](#). Hiermee kan een standaard gebruikersaccount van geavanceerde administratorrechten worden voorzien, zodat de pc eenvoudig overgenomen kan worden. Ook ernstig.

Zet de updatefunctie niet langdurig uit!

Dergelijke gaten zijn helaas geen uitzondering. Sterker nog: vrijwel alle software bevat gaten, zeker wanneer deze door de mens is geprogrammeerd. Die gaten zorgen echter pas voor een veiligheidsprobleem wanneer ze worden ontdekt, gedocumenteerd en gepubliceerd. Vaak wordt de softwarefabrikant voorafgaand aan de publicatie al op de hoogte gebracht zodat deze de tijd krijgt om het gat met een update te repareren. Schakel de updatefuncties van Windows en programma's dus nooit langdurig uit. Steker nog: het up-to-date houden van je software kan de komende jaren wel eens belangrijker worden dan ooit! We zijn namelijk in een wereld terechtgekomen waarbij AI veel beter en sneller kan programmeren dan de mens. AI is ook veel beter in staat om programmacode te onderzoeken, fouten op te sporen én er met hetzelfde gemak misbruik van te maken... Deze ontwikkelingen gaan veel sneller dan menigeen beseft. Wacht dus niet te lang met het [installeren van updates](#) als je je computer in deze continu veranderende wereld veilig wilt houden!

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

Ontvangstproblemen bij het doorsturen van e-mail naar adressen van Microsoft

In de vorige nieuwsbrief liet ik al weten dat het steeds moeilijker werd om de SchoonePC nieuwsbrief bij e-mailadressen van Microsoft af te leveren. De verzending van de eerste 5.000 nieuwsbrieven verliep altijd vlekkeloos, maar daarna ontstonden er al snel afleverproblemen. Ik was bij elke nieuwsbrief genoodzaakt om het verzendtempo laag te houden om het risico op een totale blokkade te voorkomen. Uiteindelijk is dit probleem opgelost door het SPF-record aan te passen zoals Microsoft het graag ziet. Het gaat alleen wel gepaard met een vreemd neveneffect: e-mailberichten afkomstig van het betreffende domein (zoals SchoonePC.nl) die door de ontvangende mailserver naar een e-mailadres van Microsoft worden doorgestuurd (geforward), worden niet meer geaccepteerd door de mailserver van Microsoft. Dit komt omdat er volgens het aangepaste SPF-record strikt gecontroleerd moet worden of de mailserver (in dit geval de server die het bericht doorstuurt) gerechtigd is om berichten namens het betreffende domein te verzenden. Aangezien doorgestuurde berichten niet aan die voorwaarde voldoen, zullen ze door de mailserver van Microsoft geblokkeerd worden...

Als je dus e-mail laat doorsturen naar een e-mailadres van Microsoft, houd dan rekening met de mogelijkheid dat niet alle berichten aankomen. Je merkt hier zelf niets van, alleen de afzender wordt ervan op de hoogte gebracht. Om dergelijke meldingen in de toekomst te voorkomen zal menig beheerder het betreffende e-mailadres direct uit de mailinglijst verwijderen, waarna je helemaal geen berichten meer van de betreffende afzender ontvangt... Het is maar dat je het weet!

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

E-mailberichten van Infomedics

Ik ontving ook nog een melding over de e-mailberichten van Infomedics (het bedrijf dat de facturatie en incasso regelt voor vele zorgverleners zoals tandartsen, fysiotherapeuten en huisartsen). Een nieuwsbrieflezer had hun berichten ten onrechte als spam aangezien, en kwam in de problemen omdat daardoor de factuur niet werd betaald. Hij zal vast niet de enige zijn!

Rekening van Infomedics namens XXX



Infomedics B.V. <rekening@infomedics.nl>



2-3-2026



Uw rekening van XXX

Beste heer/mevrouw Schoone,

Namens XXX sturen we u deze rekening. U heeft 30 dagen de tijd om deze rekening te betalen. Download uw rekening om te zien voor welke zorgkosten u betaalt.

Gegevens van uw rekening

Betalingskenmerk:	42287608768760
Datum rekening:	2 maart 2026
Bedrag:	€ 74,20

Betaal met iDEAL

U betaalt het makkelijkst en snelst met iDEAL via de knop hieronder. Het bedrag staat dan direct op onze rekening. Zo weet u zeker dat uw betaling op tijd is.

Op zich logisch dat er argwaan ontstaat wanneer een voor jou onbekende afzender je vraagt om geld over te maken voor een openstaande rekening. Zeker wanneer er veel tijd zit tussen de behandeling en het toezenden van de factuur, waardoor het lastig is om die relatie te leggen. En dan worden er ook nog eens op grote schaal nepfacturen 'namens' Infomedics verstuurd, ik kan mij dus goed voorstellen dat hun berichten als spam worden gezien.

Wordt de rekening echter niet betaald dan volgt een aanmaning, welke gek genoeg eveneens per e-mail wordt verzonden. Behandel je ook dit bericht als spam dan worden ook nog eens incassokosten in rekening gebracht. Die ervaring heb ik zelf ooit eens gehad en zie ik ook in mijn omgeving gebeuren, met name bij ouderen die hun mailbox nauwelijks tot niet lezen.

Om dergelijke problemen te voorkomen, heb ik mijn tandarts enige tijd geleden verzocht om de facturen (en eventuele aanmaningen :-)) van Infomedics voortaan per post te laten verzenden. Dat heeft meerdere voordelen: omdat ik de factuur per post ontvang, hoef ik mij geen zorgen meer te maken dat ik deze mis en opgezadeld wordt met incassokosten. Ik hoef mijzelf ook niet meer bij elk bericht van Infomedics af te vragen of deze echt is, spam wordt door de komst van AI namelijk steeds geavanceerder. Het is natuurlijk beter voor het milieu en het bespaart kosten wanneer de factuur (en aanmaning) per e-mail toegezonden wordt, het is alleen niet de bedoeling dat je daar zelf de prijs voor moet betalen. Wil je dat voorkomen, laat je behandelaar dan weten dat je de factuur in het vervolg ook liever per post ontvangt!

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

Nieuwsbrief 147 gemist?

Heb je nieuwsbrief 147 gemist? Vraag deze dan op via de [website](#) en/of download het [PDF-bestand](#).

Een greep uit de vele reacties van gebruikers van de computerbijbel

"Je boek ziet er bijzonder verzorgd uit en geeft veel essentiële informatie."

"Heel fijn boek om te lezen. Makkelijk, begrijpbaar en voorzien van duidelijke illustraties. Complimenten!"

"Wat een prachtige uitgave!!!"

"Elke keer is het weer genieten om door de computerbijbel te bladeren!"

"Ik ben blij met je nieuwe boek."

"Een toegankelijk, compleet en waardevol naslagwerk."

"Een dikke proficiat en een dikke pluim voor al jullie werk!"

"Bedankt voor het mooie en duidelijke werk - het boek is echt zeer nuttig."

"Zonder uw boeken was ik nooit zover gekomen in het computeren."

[Meer informatie over de computerbijbel >](#)

AFSLUITENDE CHECKLIST

Heb je (weer) veel geleerd?

Breng je kennis dan op de hoogte van deze nieuwsbrief zodat ook zij computerwijzer en -vaardiger kunnen worden! Inschrijven kan vanaf elke pagina van mijn website www.SchoonePC.nl.

Heb je een nieuwsbrief gemist?

De [laatste 5 nieuwsbrieven](#) zijn nog via de website op te vragen en/of als PDF-bestand te downloaden.

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

© 2001-2026 - SchoonePC - Rotterdam - The Netherlands