
Inhoudsopgave

Voorwoord	5
Introductie Visual Steps™	6
Wat heeft u nodig?	6
Uw voorkennis	7
Nieuwsbrief	7
Hoe werkt u met dit boek?	8
Website bij het boek	9
Toets uw kennis	9
Voor docenten	9
De schermafbeeldingen	10
1. Uw computer beveiligen	11
1.1 Wat is malware?	12
1.2 <i>Windows</i> updaten	13
1.3 Andere software en apps updaten	18
1.4 Antivirussoftware	22
1.5 Meldingen in het Actiecentrum	24
1.6 Het <i>Windows Defender-beveiligingscentrum</i>	25
1.7 <i>Windows Defender</i>	27
1.8 De real-timebeveiliging van <i>Windows Defender</i>	32
1.9 Uw computer scannen met <i>Windows Defender</i>	33
1.10 Omgaan met ransomware	37
1.11 <i>Windows Firewall</i> gebruiken	40
1.12 Phishing	42
1.13 Anti-phishingopties in internetbrowsers	43
1.14 Werken met extensies	47
1.15 Achtergrondinformatie	52
2. Uw privacy bewaren	59
2.1 Privacyinstellingen in <i>Windows 10</i>	60
2.2 Cookies	66
2.3 Privacyinstellingen in internetbrowsers	68
2.4 Browsegeschiedenis verwijderen	76
2.5 Veilig op <i>Facebook</i> en andere sociale media	80
2.6 Achtergrondinformatie	85
3. Veilig op internet	87
3.1 Spam	88
3.2 Sterke wachtwoorden maken	94
3.3 Wachtwoorden onthouden	96
3.4 Veilig internetbankieren	104
3.5 Veilig online winkelen	107

3.6 Veilig online betalen	110
3.7 Na het betalen	116
3.8 Achtergrondinformatie	117
3.9 Tips	120
4. Back-ups maken	125
4.1 Welk type back-up?	126
4.2 Een back-up maken van persoonlijke bestanden	127
4.3 Persoonlijke bestanden terugzetten	132
4.4 Een systeemkopie maken	133
4.5 Persoonlijke bestanden kopiëren naar een externe harde schijf of USB-stick	137
4.6 Herstelpunten maken	139
4.7 Herstelpunten terugzetten	142
4.8 <i>OneDrive</i> gebruiken	145
4.9 Achtergrondinformatie	151
4.10 Tips	155
5. Uw computer opruimen	157
5.1 Uw harde schijf opruimen	158
5.2 Programma's en apps deïnstalleren	161
5.3 Schijfcontrole	163
5.4 Optimaliseren	165
5.5 Systeeminformatie bekijken	169
5.6 <i>CCleaner</i> downloaden en installeren	172
5.7 Schijf analyseren en schoonmaken	178
5.8 Programma's deïnstalleren met <i>CCleaner</i>	184
5.9 Opstartprogramma's instellen	186
5.10 Browser plug-ins in- of uitschakelen	188
5.11 Gegevens wissen	189
5.12 Visual Steps-website en nieuwsbrief	191
5.13 Achtergrondinformatie	192
Bijlagen	
A. Hoe doe ik dat ook alweer?	195
B. Index	197

Hoe werkt u met dit boek?

Dit boek is geschreven volgens de Visual Steps™-methode. De werkwijze is eenvoudig: u legt het boek naast uw computer en voert alle opdrachten stap voor stap direct op uw computer uit. Door de duidelijke instructies en de vele schermafbeeldingen weet u precies wat u moet doen. Door de opdrachten direct uit te voeren, leert u het snelste werken met het programma.

In dit Visual Steps™-boek ziet u verschillende tekens. Die betekenen het volgende:

Handelingen

Dit zijn de tekens die een handeling aangeven:



Het toetsenbord betekent dat u iets moet typen op het toetsenbord.



De muis geeft aan dat u op de pc iets met de muis moet doen.



De hand geeft aan dat u hier iets anders moet doen, bijvoorbeeld de computer aanzetten, of een reeds bekende handeling uitvoeren.

Naast deze handelingen wordt op sommige momenten extra hulp gegeven om met succes dit boek door te werken.

Hulp

Extra hulp vindt u bij deze tekens:



De pijl waarschuwt u voor iets.



Bij de pleister vindt u hulp mocht er iets fout zijn gegaan.



Weet u niet meer hoe u een handeling uitvoert? Dan kunt u dit met behulp van het cijfer achter deze voetstapjes opzoeken achter in het boek in de bijlage *Hoe doe ik dat ook alweer?*

In aparte kaders vindt u algemene informatie en tips.

Extra informatie

De kaders zijn aangeduid met de volgende tekens:



Bij het boek krijgt u extra achtergrondinformatie die u op uw gemak kunt doorlezen. Deze extra informatie is echter niet noodzakelijk om het boek door te kunnen werken.



Bij een lamp vindt u een extra tip voor het gebruik van het programma.

1. Uw computer beveiligen



Vandaag de dag kan een computer niet meer zonder goede beveiliging. Een goed beveiligingssysteem verkleint het risico op *malware* (virussen of andere schadelijke software) op uw computer zoveel mogelijk.

Als computergebruiker bent u verantwoordelijk voor de beveiliging van uw eigen pc. In de eerste plaats is het belangrijk dat u *Windows* en gewone programma's regelmatig *update*. Dit houdt in dat een nieuwe, verbeterde versie van een programma wordt geïnstalleerd. Hiermee worden onder andere recent ontdekte veiligheidsproblemen opgelost.

De beveiliging van uw pc in *Windows 10* wordt centraal geregeld vanuit het *Windows Defender-beveiligingscentrum*. Dit beveiligingscentrum heeft verschillende programma's en functies voor het beschermen van uw computer.

Het ingebouwde antivirusprogramma *Windows Defender* helpt u bij het vinden en tegenhouden van malware. Als u geen ander antivirusprogramma heeft, neemt *Windows Defender* die taak op zich.

Een ander programma, *Windows Firewall*, beschermt tegen ongewenste toegang door computercriminelen vanaf internet op uw pc.

Door de opkomst van *ransomware*, malware die computers gijzelt, is in *Windows 10* ook daarvoor een speciale beveiliging toegevoegd.

De standaard internetbrowser *Edge* in *Windows* heeft allerlei beveiligingsopties. Net als bij andere internetbrowsers is het belangrijk te controleren of die ingeschakeld zijn. Hiermee voorkomt u onder andere dat u het slachtoffer wordt van *phishingwebsites*. Dit zijn websites waarop met behulp van valse informatie wordt geprobeerd belangrijke gegevens, zoals uw toegangsgegevens voor internetbankieren, te stelen.

Extensies, ook wel bekend als *invoegtoepassingen*, *plug-ins* of *add-ons* voegen extra functies toe aan een internetbrowser. Soms geven die problemen bij het surfen. Dan is het handig als u ze zelf weet te beheren.

In dit hoofdstuk leert u:

- wat malware is;
- *Windows* updaten;
- andere software updaten;
- omgaan met antivirussoftware;
- werken met *Windows Defender*;
- werken met het *Windows Defender-beveiligingscentrum*;
- omgaan met ransomware;
- *Windows Firewall* gebruiken;
- omgaan met phishing;
- anti-phishing opties aanzetten in een internetbrowser;
- andere beveiligingsopties aanzetten in een internetbrowser;
- werken met extensies in internetbrowsers.

1.1 Wat is malware?

De term *malware* is een samentrekking van *malicious software*, oftewel kwaadaardige of schadelijke software. Het is een verzamelnaam voor software die schade kan aanrichten op uw computer.

Voor een deel worden deze programma's gemaakt door personen die het leuk vinden om in te breken in computers (ook wel *hacken* genoemd) of vervelende programma's te verspreiden. Maar vooral professionele criminelen houden zich tegenwoordig bezig met deze lucratieve vorm van misdaad. Met computercriminaliteit of *cybercrime* zijn namelijk miljoenen te verdienen.

Malware is onder te verdelen in verschillende soorten:

- *Virus* is een verzamelnaam voor kleine programma's die zelfstandig kunnen functioneren, maar meeliften in een ander programma. Als het besmette programma wordt geopend, wordt automatisch het virus geactiveerd. Sommige virussen richten weinig schade aan. Ze laten bijvoorbeeld een bepaalde boodschap op uw beeldscherm zien op een bepaalde datum, maar doen niet meer dan dat. Andere, meer agressieve, virussen nemen steeds meer ruimte in op uw harde schijf en besmetten steeds meer programma's, zodat u op een gegeven moment niet meer kunt werken op uw computer. Een belangrijke eigenschap van virussen is dat ze zich makkelijk vermenigvuldigen en verspreiden, bijvoorbeeld door zichzelf te versturen via e-mails aan mensen in uw adresboek.
- *Wormen* en *Trojaanse paarden* zijn varianten op virussen. Ook deze programma's zijn net zo schadelijk als virussen, maar ze functioneren los van andere programma's. Ze worden vaak gebruikt door hackers (computerinbrekers) om uw computer over te nemen voor criminele activiteiten, zoals het inbreken op grote bedrijfsnetwerken.
- *Spyware* is geen virus, maar schadelijke software die stiekem op uw computer wordt geplaatst wanneer u een besmet programma installeert of een schadelijke website bezoekt. Spyware wordt gebruikt om uw computer te bespioneren en uw gegevens via internet door te geven aan criminelen. Die gebruiken uw gegevens bijvoorbeeld om u ongewenste reclamemails (spam) te sturen of ze tegen winst door te verkopen.
- *Adware* plaatst tijdens het surfen advertenties in uw internetbrowser of een apart venster. Adware verschijnt vaak nadat u een gratis programma heeft geïnstalleerd.
- *Ransomware* is software die uw computer gijzelt. Hierbij wordt uw computer lamgelegd of bestanden onbereikbaar gemaakt. U krijgt de mededeling dat u door geld te storten uw computer weer 'terugkrijgt'. Een variant hierop is een valse mededeling van ransomware dat u zogenaamd illegale activiteiten met uw computer heeft uitgevoerd en dat u door geld te storten, arrestatie door de politie kunt voorkomen. U moet nooit op dit soort afpersing ingaan en aangifte doen bij de politie.

1.2 Windows updaten

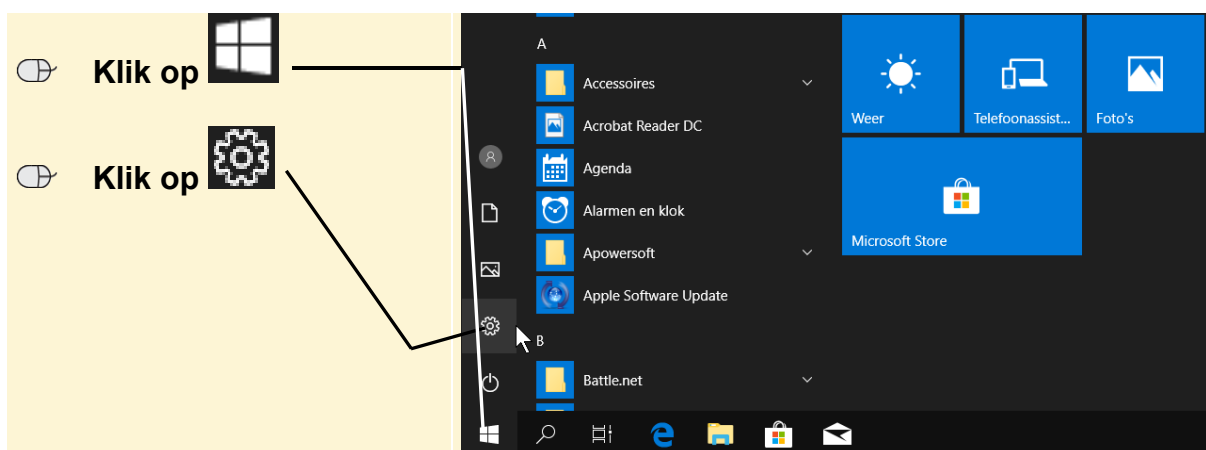
Een belangrijk onderdeel van *Windows* is *Windows Update*. Dit is een systeem dat controleert of u de meest recente versie van *Windows 10* gebruikt. *Windows 10* wordt continu aangepast, uitgebreid en verder beveiligd en verbeterd. Deze toevoegingen en verbeteringen worden door Microsoft in de vorm van software updates verspreid.

Let op!

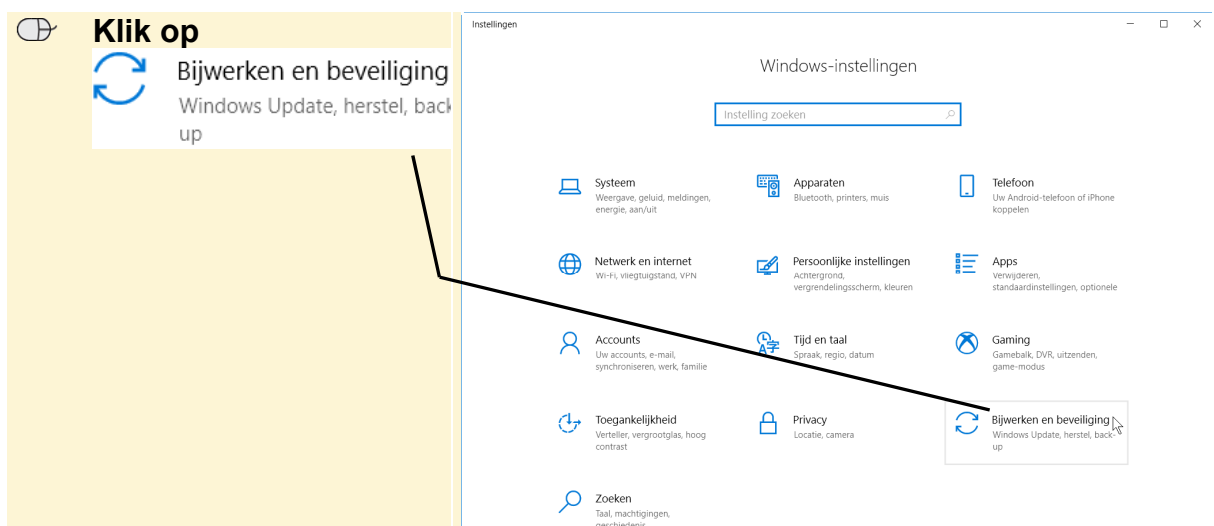
Microsoft verstuurt nooit software updates per e-mail. Als u een e-mail ontvangt waarin staat dat de bijlage Microsoft-software of een *Windows*-update bevat, open dan nooit de bijlage. Verwijder de e-mail onmiddellijk en vergeet niet deze ook uit de map *Verwijderde items* te verwijderen. Dergelijke e-mails worden door criminelen verstuurd die proberen schadelijke software op uw computer te installeren.

In *Windows 10* wordt het updaten altijd automatisch geregeld. U hoeft daarvoor dus niets meer te doen. Wel kunt u eventueel zelf naar nieuwe updates zoeken. Dat is bijvoorbeeld handig als u merkt dat uw computer niet helemaal goed werkt. Een update helpt dan soms het probleem op te lossen.

U opent *Windows Update* via *Instellingen*:




U opent het venster *Bijwerken en beveiliging*:

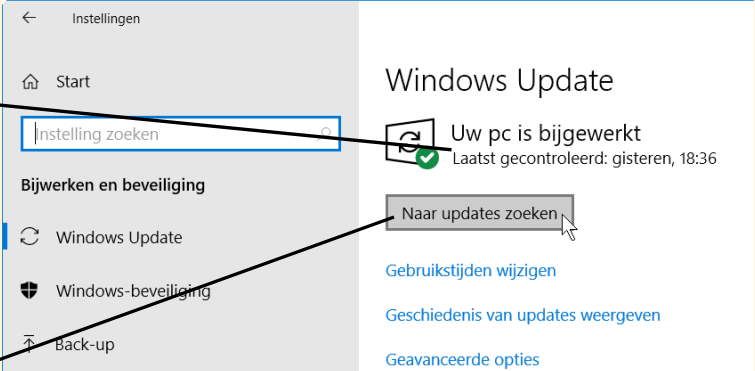


Het venster met het tabblad *Windows Update* wordt geopend:

U ziet wanneer het laatst gecontroleerd is op updates:

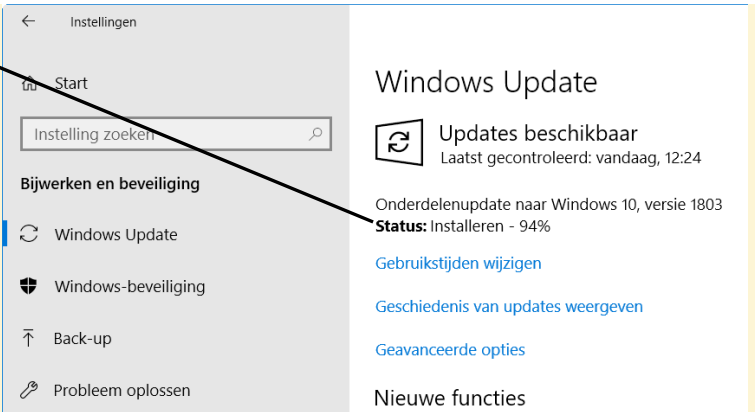
Om zelf naar updates te laten zoeken:

 **Klik op**
Naar updates zoeken



In dit voorbeeld is er een nieuwe update:

Deze wordt meteen gedownload. Dat kan wel even duren. In de tussentijd kunt u gewoon verder werken op de computer. Het kan zijn dat internet wel iets trager werkt.




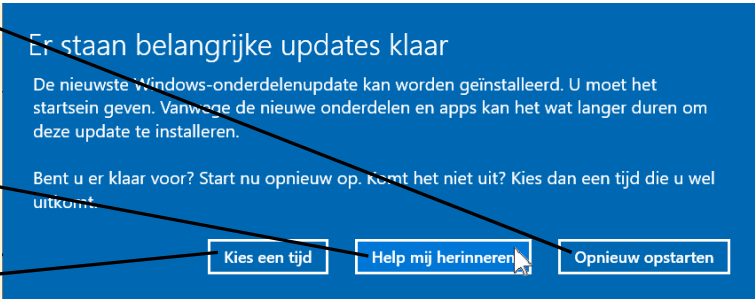
Na het installeren van een nieuwe update moet de computer altijd opnieuw worden opgestart. U ziet daarom dit venster na het downloaden van de update:

Nu opnieuw opstarten:

Nu nog niet opstarten, maar later een herinnering geven:

Nu nog niet opstarten maar een precieze tijd kiezen:

 **Klik op de gewenste optie**



Let op!


Zorg ervoor dat u voor het opnieuw opstarten van de computer eerst geopende bestanden opslaat en geopende programma's sluit.

Het installeren van een *Windows* update neemt enige tijd in beslag. U mag tijdens die periode niets met de computer doen.

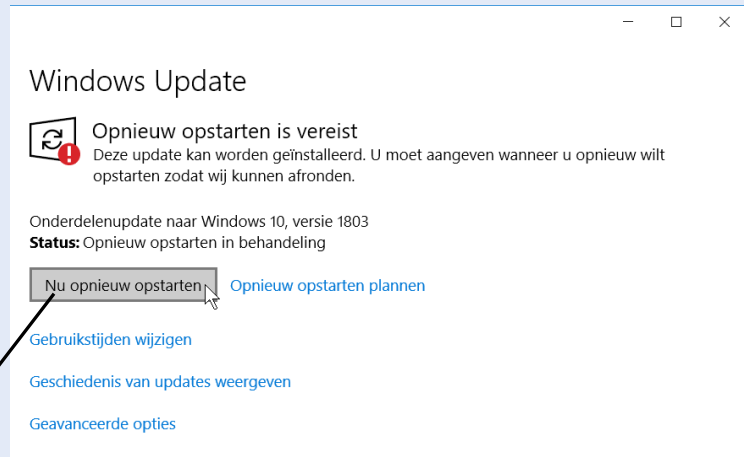
**Tip****Toch zelf direct opnieuw opstarten**

Als u na een *Windows* update gekozen heeft om later pas de computer opnieuw op te starten, kunt u toch nog zelf eerder de computer opnieuw laten starten. Bijvoorbeeld als u op dat moment toch de computer niet gebruikt:


Op het *Windows Update* tabblad:

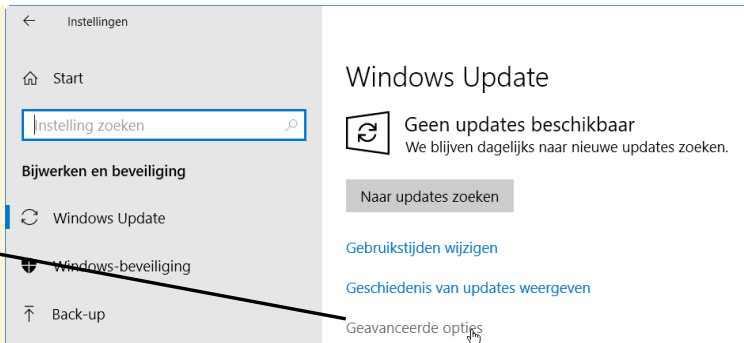
 **Sla geopende bestanden op en sluit programma's**

 **Klik op**
Nu opnieuw opstarten



Hoewel het downloaden van *Windows* updates automatisch gaat, is er wel een aantal opties die u kunt instellen:

 **Klik op**
Geavanceerde opties



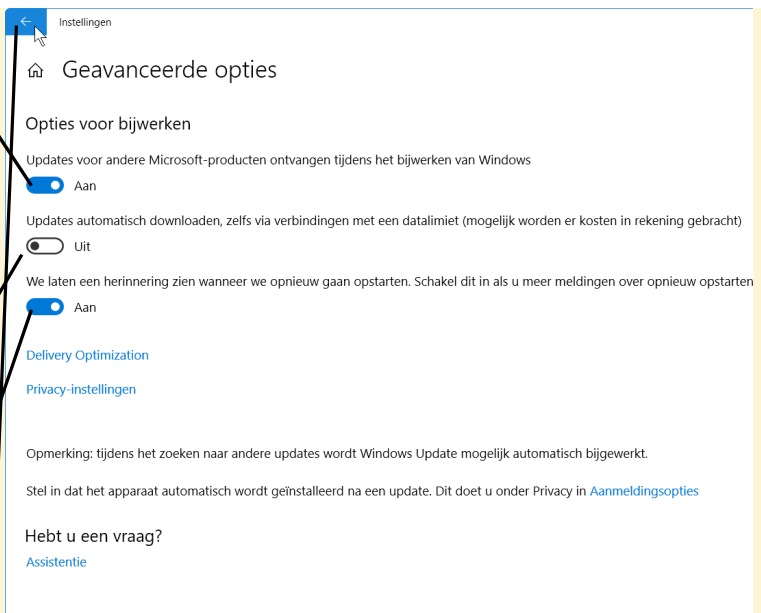
Updates downloaden voor andere Microsoft-programma's:

Updates ook downloaden bij een 3G/4G-verbinding (alleen van toepassing voor mobiele apparaten):

Herinnering weergeven bij opnieuw opstarten computer:

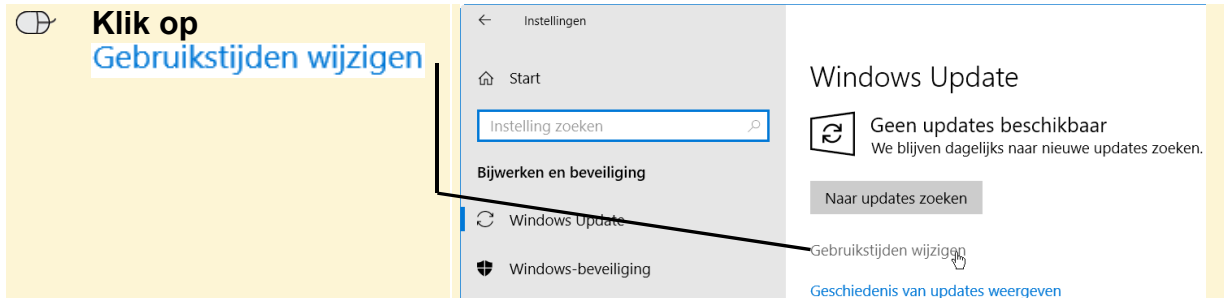
De opties instellen zoals in deze schermafbeelding, is de beste keuze.

 **Klik op** 

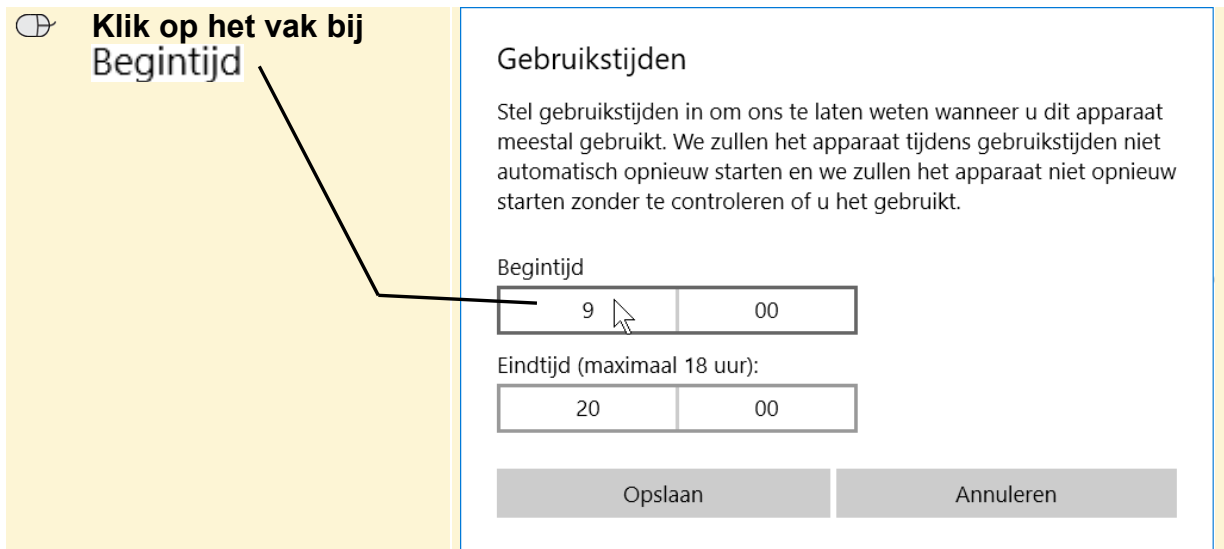


Vervelend is soms dat na de update uw computer opnieuw moet worden opgestart. Dit gebeurt automatisch als u niets anders aangeeft. Als u op dat moment niet achter uw computer zit, kan het gebeuren dat openstaande programma's en bestanden ongevraagd worden afgesloten.

Als u dat niet wilt, geeft u de gebruikstijden voor uw computer op. *Windows* wordt dan niet automatisch opnieuw opgestart tijdens die gebruikstijden:



U geeft de gewenste gebruikstijden voor de computer op:



Klik op het uur dat u meestal begint met werken op de computer

Klik op ✓

...n weten wanneer u dit apparaat
...raat tijdens gebruikstijden niet
...zullen het apparaat niet opnieuw
...t gebruikt.

Annuleren

Klik op het vak bij Eindtijd

Stel gebruikstijden in om ons te laten weten wanneer u dit apparaat meestal gebruikt. We zullen het apparaat tijdens gebruikstijden niet automatisch opnieuw starten en we zullen het apparaat niet opnieuw starten zonder te controleren of u het gebruikt.

Begintijd

10	00
----	----

Eindtijd (maximaal 18 uur):

20	00
----	----

Opslaan Annuleren

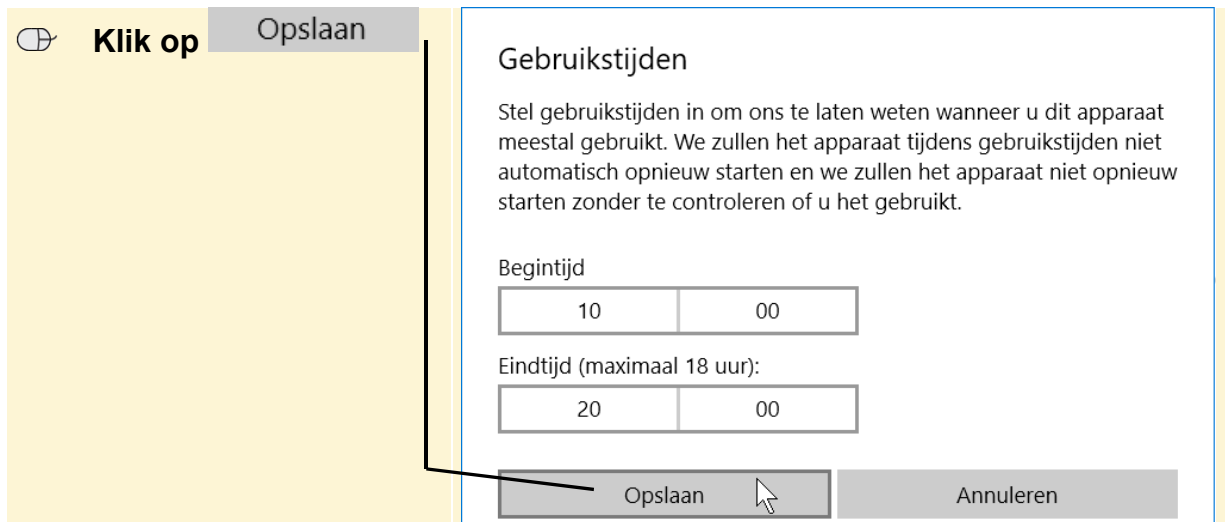
Klik op het uur dat u meestal stopt met werken op de computer

Klik op ✓

...raat tijdens gebruikstijden niet
...zullen het apparaat niet opnieuw
...t gebruikt.

Annuleren

Om de gebruikstijden op te slaan:



De gebruikstijden zijn opgeslagen. Pas buiten deze tijden wordt uw computer na een update opnieuw opgestart.

 **Sluit Instellingen**  ¹