

Beveiligingstips en instellingen voor Windows 7



Windows[®] 7

PC beveiligen.nl

Inhoudsopgave:

Voorwoord	pagina 3
Basisinformatie	pagina 4
Tips & instellingen	
Virusscanner	pagina 5
Updaten	pagina 5
Extensies weergeven	pagina 7
Instellingen voor externe verbindingen	pagina 8
Remote registry	pagina 9
Tips voor je e-mail programma	pagina 11
Programma's	pagina 13
Copyright	pagina 25

Voorwoord

We gaan hier aan de hand van enkele basis tips, programma's en instellingen na een nieuwe installatie stapsgewijs laten zien hoe we een goede basis leggen voor een veiliger computergebruik. Deze tips, programma's en instellingen zijn hoofdzakelijk bedoeld voor computergebruikers die niet zo vertrouwd zijn met beveiligingsprogramma's en de instellingen van het hierboven genoemde besturingssysteem.

Bedenk wel dat deze handleiding geen garantie is dat je gespaard blijft van virussen en andere malware maar dat we het risico hierop wel willen verkleinen of zo minimaal mogelijk houden. Veel hangt af van je eigen surf en internet gedrag.

Basisinformatie:

Microsoft update

Belangrijk in de strijd tegen kwaadaardige software is updaten, met de nieuwste Microsoft updates bent u een stuk beter beschermd tegen virussen en malware. Zorg dus dat u de updates op automatisch heb staan of regelmatig Microsoft update bezoekt. Daar download u in ieder geval de essentiële updates, de overige updates kunt u stuk voor stuk bekijken of deze voor u van toepassing zijn. Op deze manier voorkomt u dat kwaadaardige software misbruik kan maken van fouten in het besturingssysteem.

Net zo belangrijk is het om je programma's up to date te houden, controleer dan ook regelmatig of er een update beschikbaar is. Belangrijke updates worden ook altijd gemeld op onze [website](#) en [forum](#).

Windows Defender

Windows Defender is een programma van Microsoft waarmee spyware tegengehouden en verwijderd kan worden. Bovendien is Defender geïntegreerd en standaard geactiveerd in Windows 7 en je wordt ook automatisch voorzien van de nieuwste updates. Hiermee probeert Microsoft om zoveel mogelijk Windows 7 gebruikers te beschermen tegen de steeds toenemende dreiging van malware. Windows Defender kan niet enkel gebruikt worden om computers te scannen, maar bevat ook een real-time beveiliging die constant een aantal Windows onderdelen controleert op wijzigingen die veroorzaakt kunnen worden door spyware.

De Windows firewall

De Windows Firewall is het onderdeel dat controleert of de data die via internet of netwerk binnenkomen veilig zijn. Niet-vertrouwde verbindingen worden geblokkeerd, terwijl vertrouwde gegevens worden doorgelaten, zodat u normaal kunt werken.

De firewall staat standaard ingeschakeld en wordt door diverse Windows onderdelen zodanig geconfigureerd dat hij u niet tot last is. Dat wil zeggen dat programma's zoals Internet Explorer, Microsoft Office en andere bekende programma's niet geblokkeerd worden. Zodra de Windows Firewall merkt, dat een onbekend programma contact probeert te maken met het netwerk of het internet, verschijnt er een melding. U kunt dan zelf aangeven of dit programma toegang moet krijgen tot het netwerk of het internet.

Virusscanner

Een Virusscanner controleert uw pc op kwaadaardige bestanden en verwijderd deze. Een pc heeft altijd kans om geïnfecteerd te raken. Dit kan bijv. gebeuren d.m.v. een e-mailbijlage, het downloaden van besmette bestanden of het bezoeken van kwaadaardige sites. Een virus zal altijd één of andere kwaadaardige uitwerking hebben, van extreem (wissen harde schijf of pc crashen) tot minimaal (andere startpagina of allerlei vervelende pop-ups).

Een virusscanner scant op verzoek de harde schijf af naar besmettingen en verwijderd deze, sommige anti virus programma's (meestal de betaalde) hebben ook een zgn. 'real-time-monitoring' functie, dit houdt in dat ieder bestand dat gelezen, geschreven of verplaatst wordt direct wordt gescand en nagekeken.

Links naar diverse antivirusproducten vindt u op onze website >> [link](#)

Malware

Malware is een verzamelnaam voor kwaadaardige en/of schadelijke software. Voorbeelden van malware zijn;

- Adware: Infecteert de computer met reclamesoftware, en zorgt doorgaans voor popups
- Boot sector virus: Infecteert de boot sector op een harde schijf of diskette
- Computervirus : Infecteert bestanden en richt vaak schade aan.
- Computerworm : Verspreidt zich direct over het netwerk en richt vaak schade aan.
- IRCBot : Verbindt de geïnfecteerde computer met een netwerk waaruit de computer bestuurd kan worden.
- Rootkit : Set programma's om een hacker toegang te geven tot een computer.
- Spyware : Geeft gegevens van de gebruiker door aan derden
- Trojan horse (Trojaans paard) : Doet zich voor als iets anders dan het daadwerkelijk is en richt dan schade aan of functioneert als spyware.

Tips & instellingen

We gaan er vanuit dat we een verse installatie van Windows 7 Ultimate uitgevoerd hebben.

Als eerste installeren we één virusscanner naar keuze.

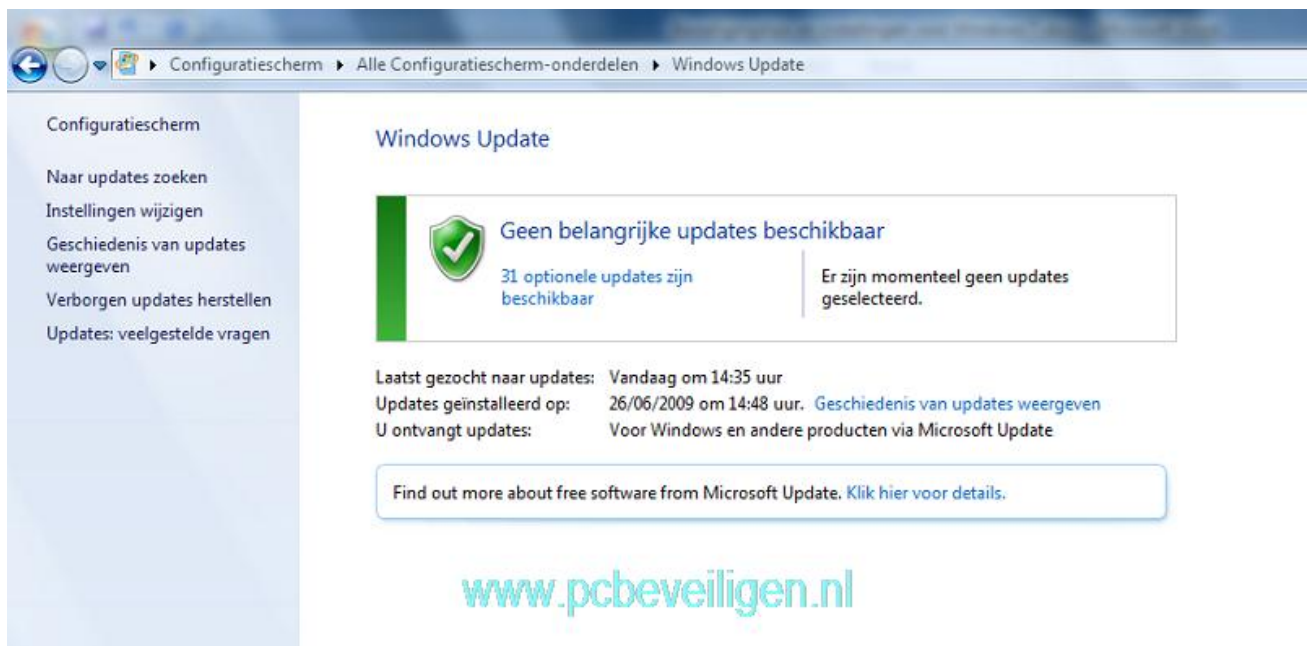
Eventueel als het programma erom vraagt doen we een herstart en updaten we onze virusdefinities.

Als tweede gaan we onze Windows 7 updaten.

Download in ieder geval de essentiële updates, de overige updates kunt u stuk voor stuk bekijken of deze voor u van toepassing zijn.

Hoe je bepaalt hoe Windows updates installeert doe je als volgt:

Ga naar Start > Configuratiescherm > Windows Update en je krijgt dan volgend scherm



In dit scherm kun je handmatig zoeken naar updates, Instellingen wijzigen, Geschiedenis van updates weergeven, Verborgene updates herstellen.

We klikken hier op **Instellingen wijzigen** en vervolgens krijgen we volgend scherm.

Bepaal hoe u Windows updates wilt laten installeren

Er kan automatisch naar belangrijke updates worden gezocht die op basis van de onderstaande instellingen automatisch worden geïnstalleerd. U kunt ook beschikbare updates installeren voordat u de computer afsluit.

[Wat zijn de voordelen van automatische updates?](#)

Belangrijke updates



Updates automatisch installeren (aanbevolen)

Install new updates:

Elke dag



om

3:00



Aanbevolen updates

Aanbevolen updates op dezelfde manier ontvangen als belangrijke updates

Wie kan updates installeren

Alle gebruikers toestaan updates op deze computer te installeren

Microsoft Update

Give me updates for Microsoft products and check for new optional Microsoft software when I update Windows

Softwaremeldingen

Show me detailed notifications when new Microsoft software is available

Opmerking: Windows Update wordt mogelijk eerst automatisch bijgewerkt voordat op andere updates wordt gecontroleerd. Lees de [onlineprivacyverklaring](#).

www.pcbeveiligen.nl

In dit scherm heb je de keuze uit diverse instellingen

Belangrijke updates

- Updates automatisch installeren (aanbevolen).
- Updates downloaden maar laat mij bepalen of ik ze wil installeren.
- Naar updates zoeken maar laat mij bepalen of ik ze wil downloaden en installeren.
- Nooit naar updates zoeken (niet aanbevolen).

Bij 'Install new updates' kies hier **elke dag** en **een uur** dat je pc hoogstwaarschijnlijk aanstaat zodat je Windows de mogelijkheid krijgt om te updaten. De andere instellingen mogen verder ongemoeid blijven. Bevestig met OK.

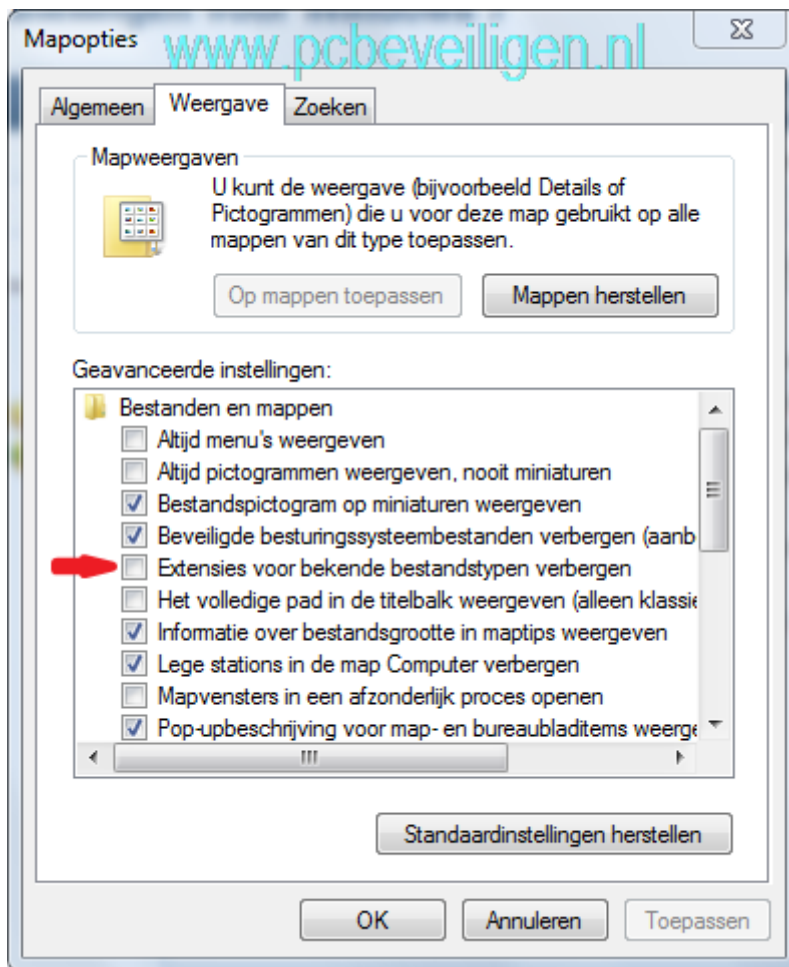
Extensies voor bekende bestandstypen weergeven.

In Windows 7 staat de optie "Verberg extensies voor bekende bestandstypen" standaard in Windows Verkenner Explorer aan, waardoor een virusschrijver een .exe bestand op een foto- of tekstbestand kan laten lijken.

Deze truc kan dan ook toegepast worden door virusschrijvers door bijvoorbeeld een virus genaamd valentijn.exe te hernoemen naar valentijn.jpg.exe, waardoor de echte extensie, dus de .exe, niet zichtbaar is in Explorer.

Daarnaast werd ook nog eens het icoontje veranderd, waardoor het bestand echt lijkt.

Via Start >> Configuratiescherm >> Mapopties krijgen we volgend scherm, In het tabblad Weergave haal je het linkje weg bij >> [Extensies voor bekende bestandstypen verbergen](#)



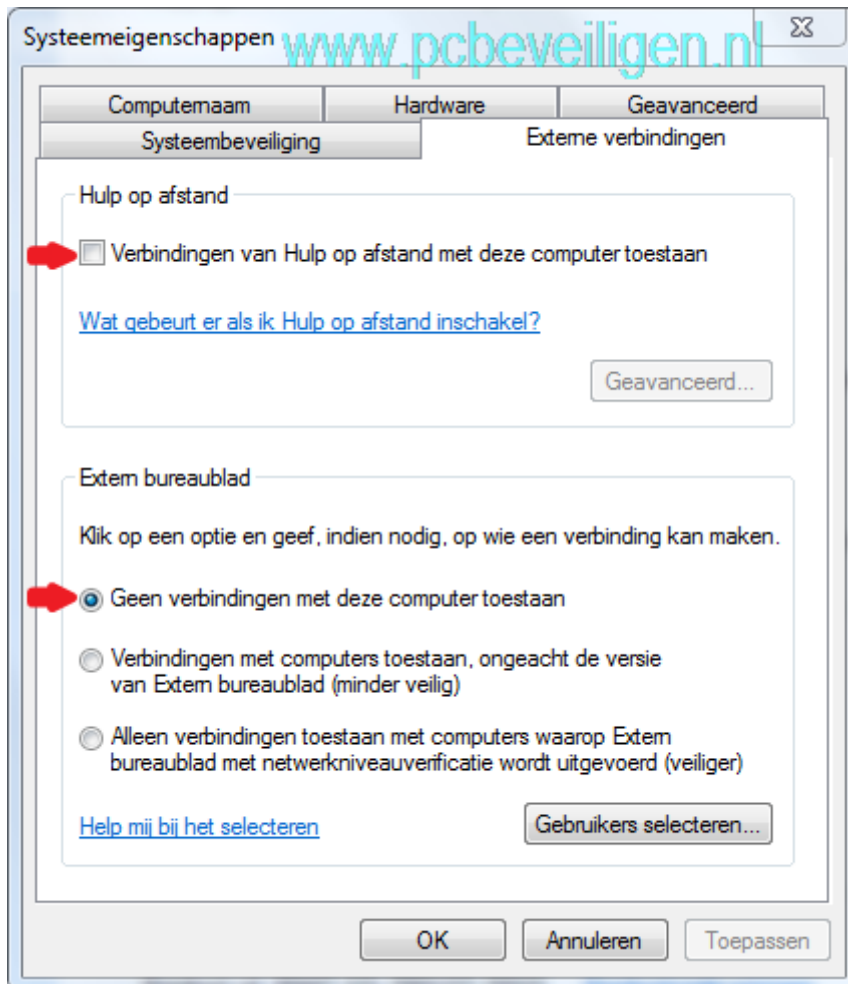
Klik op Toepassen & OK en de extensies zullen worden weergegeven.

Instellingen voor externe verbindingen.

Onder externe verbindingen hebben we;

- Hulp op afstand
- Extern bureaublad.

Ga naar Start > Configuratiescherm > Systeem en klik dan op **Instellingen voor externe verbindingen** waarna er volgend scherm verschijnt.



Bij **Hulp op afstand** haal je het vinkje weg bij >> Verbindingen van hulp op afstand met deze computer toestaan

Mocht je dit nadien toch willen gebruiken kun je het altijd terug aanvinken.

Maak je geen gebruik van **Extern bureaublad** selecteer dan >> Geen verbindingen met deze computer toestaan

Wil je nadien Extern bureaublad gebruiken kun je deze instelling eenvoudig wijzigen.

Klik op Toepassen & OK

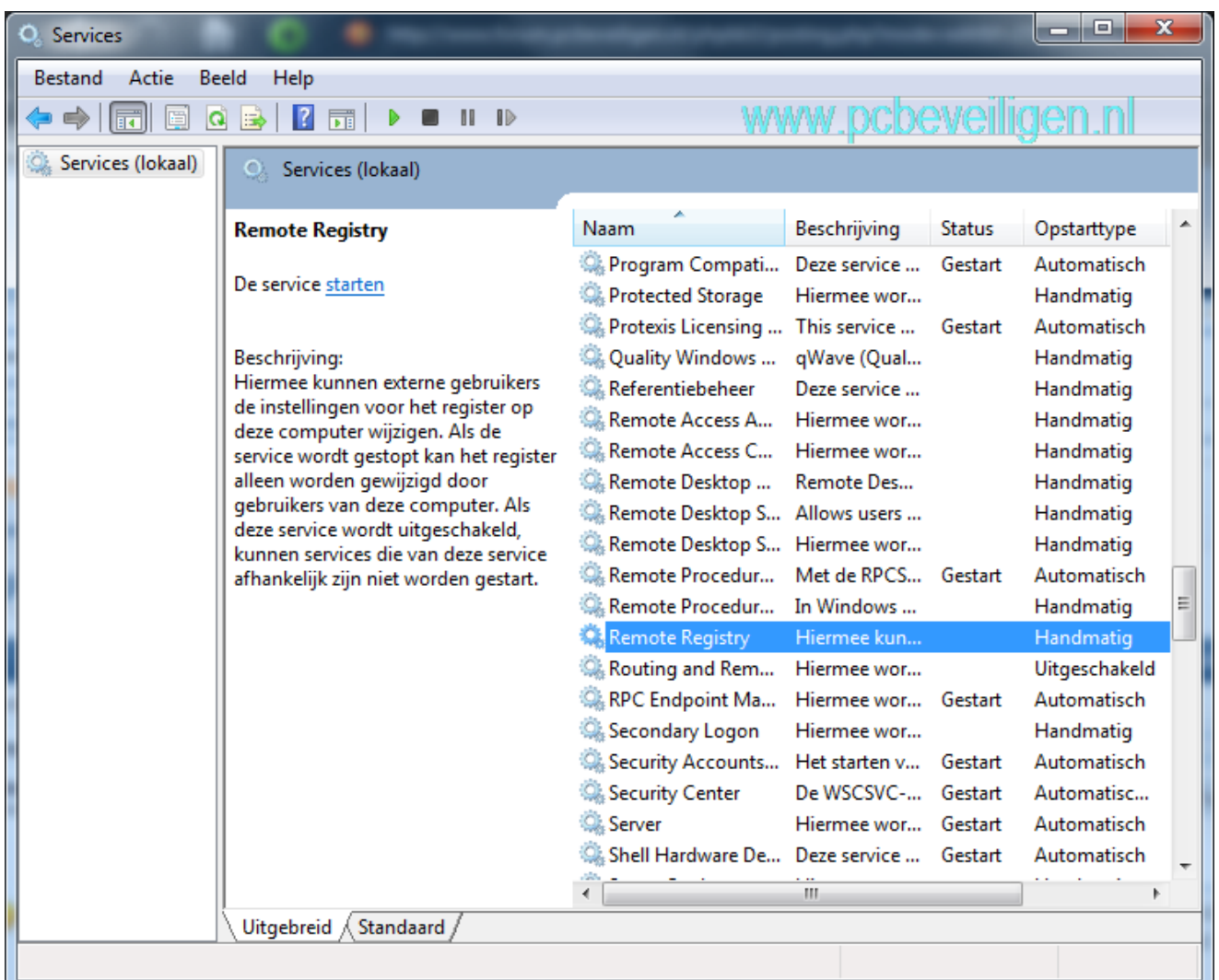
Remote Registry.

Remote Registry is een service die we willen uitschakelen. Via deze service kunnen externe gebruikers de instellingen van het register wijzigen op onze computer. Als we deze service uitschakelen kan het register enkel gewijzigd door gebruikers van deze computer. We doen dit als volgt;

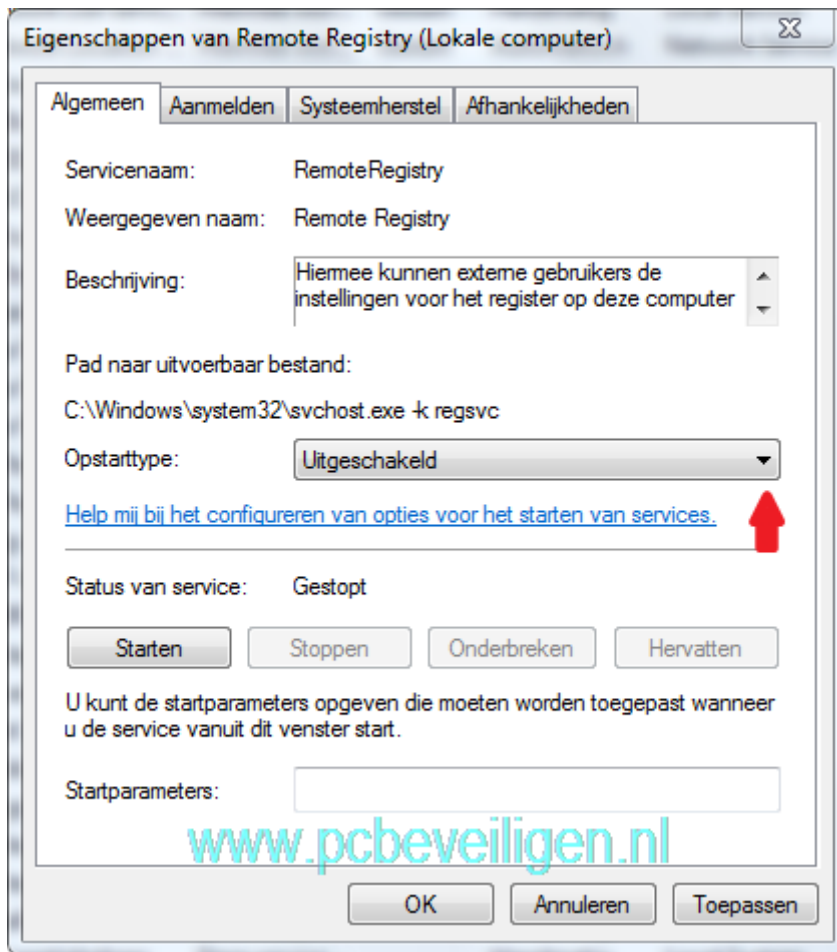
Druk op de Windows + r toets
Het uitvoeren venster verschijnt.



Typ hier services.msc en klik op OK en het volgende scherm verschijnt.



Nu zoeken we de service Remote Registry en dubbelklikken hierop en de Eigenschappen voor Remote Registry worden in een nieuw venster geopend.



Onder **Opstarttype** kies je voor **Uitgeschakeld** klik op Toepassen en bevestig met OK Bij de volgende keer dat de computer wordt opgestart is deze services uitgeschakeld.

Tips voor je e-mail programma .

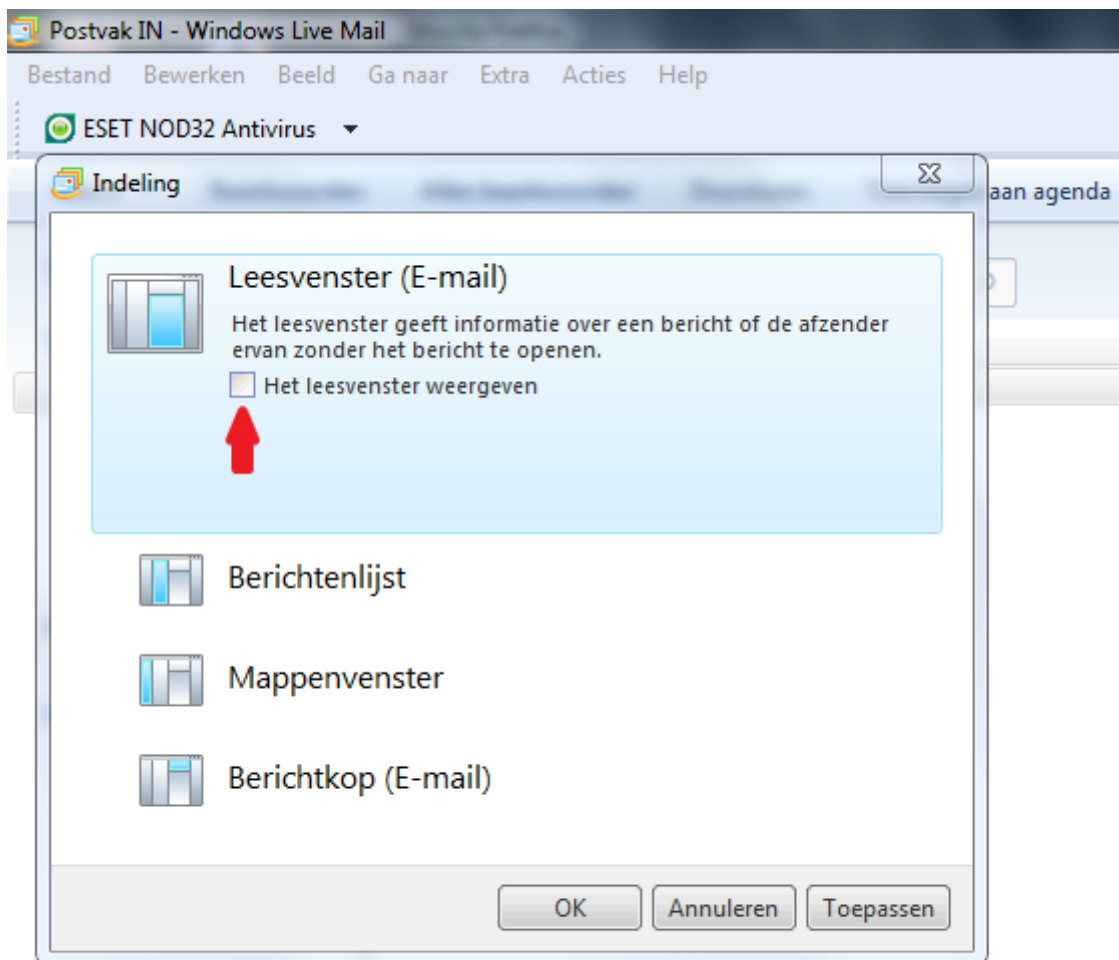
Daar er in Windows 7 standaard geen e-mail cliënt zit gebruiken we Windows Mail als voorbeeld. De instelling die we hier gaan veranderen is in de meeste e-mail programma's terug te vinden. Met vragen over andere e-mail programma's kan je terecht op ons [forum](#)

- Uitschakelen van het voorbeeldvenster:

Omdat virussen misbruik kunnen maken door code op te starten in het voorbeeldvenster wordt het aanbevolen om dit voorbeeldvenster uit te schakelen.

Hoewel het een voordeel is dat je de e-mails gelijk kunt lezen, ben je dus ook kwetsbaarder voor bepaalde virussen.

Open Windows live mail, boven in de werkbalk klik je op **Beeld** >> **Indeling** en het volgende scherm verschijnt.



www.pcbeveiligen.nl

Haal het vinkje weg bij >> [Het leesvenster weergeven](#)

Klik op Toepassen & OK en het voorbeeldvenster wordt niet meer weergegeven.

- Leesbevestigingen.

In een mailprogramma zit een functie om een leesbevestiging te versturen naar de afzender van het verstuurd bericht.

Het automatisch verzenden van een leesbevestiging wordt niet aanbevolen daar spammers of andere onbekende figuren daarmee een bevestiging krijgen dat je e-mailadres bestaat.

Open Windows live mail, boven in de werkbalk klik je op **Extra** >> **Opties** het venster Opties

verschijnt en selecteer hier het tabblad **Bevestigingen**.



Onder **Leesbevestigingen verzenden** hebben we 3 opties.

- 1) - Nooit een leesbevestiging verzenden.
- 2) - Een melding weergeven als er om een leesbevestiging wordt gevraagd.

De volgende melding wordt weergegeven als de afzender om een leesbevestiging vraagt.



Hier kan men dan een gepaste actie selecteren door op **Ja** of **Nee** te klikken naargelang men de afzender kent of niet.

- 3) - Altijd een leesbevestiging versturen. (Deze optie wordt niet aanbevolen)

Programma's

Tot slot willen we nog een aantal programma's aan bod laten komen die een bijdrage leveren aan een veiliger internetgebruik.

- Spyware Blaster

Spyware Blaster kan geen ongewenste software of andere malware van je computer verwijderen maar probeert te verhinderen dat deze in de eerste plaats geïnstalleerd kan worden

Wat doet Spyware Blaster;

- Blokkeert gevaarlijke ActiveX bestanden, adware, dialers, browser hijackers en andere ongewenste software.
- Blokkeert spyware en tracking cookies in uw browser.
- Blokkeert websites die spyware bevatten.

Spyware Blaster hoeft niet op de achtergrond actief te zijn om je te beschermen tegen eerder vermelde gevaren.

Eens geïnstalleerd, geconfigureerd en geüpdate volstaat het om regelmatig te updaten.

Spyware Blaster kan je [hier downloaden](#)

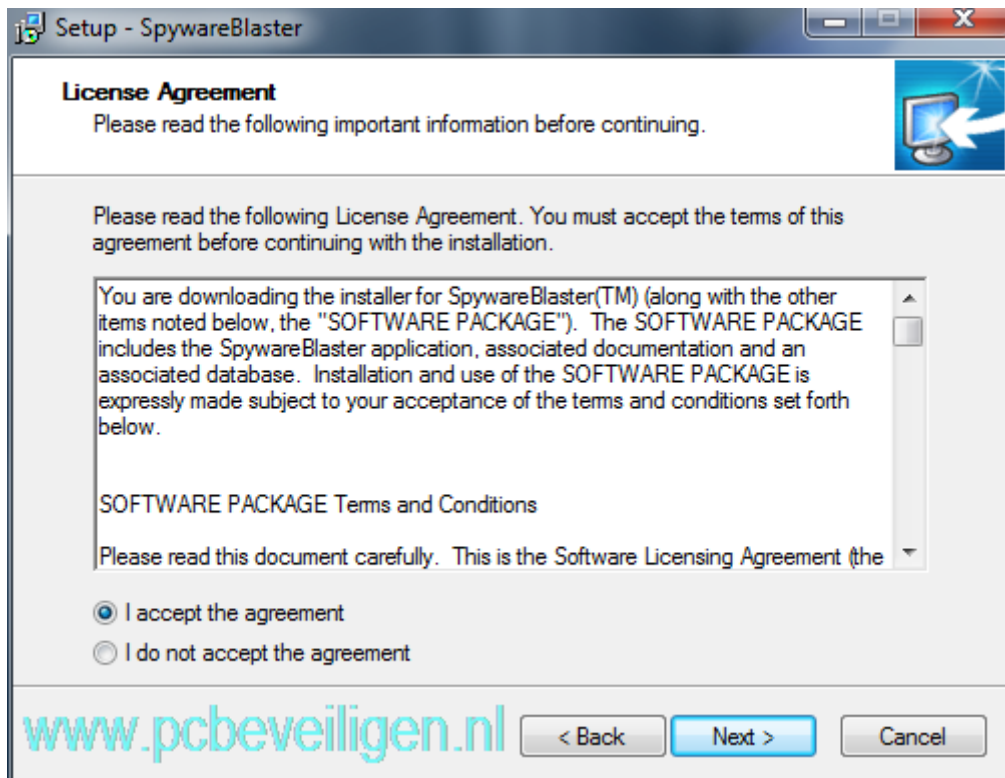
De installatie

Dubbelklik op het bestand dat je via bovenstaande link gedownload hebt en de installatie kan beginnen.

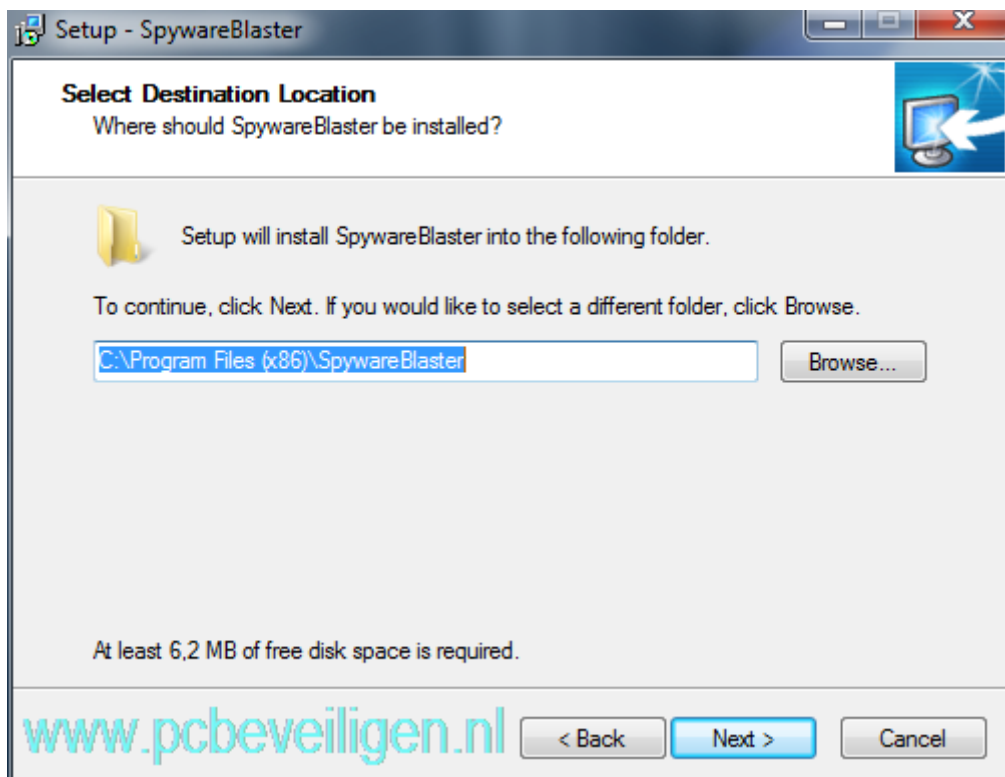
We krijgen vervolgens het welkomst scherm van de setup wizard die ons door de installatie begeleid.



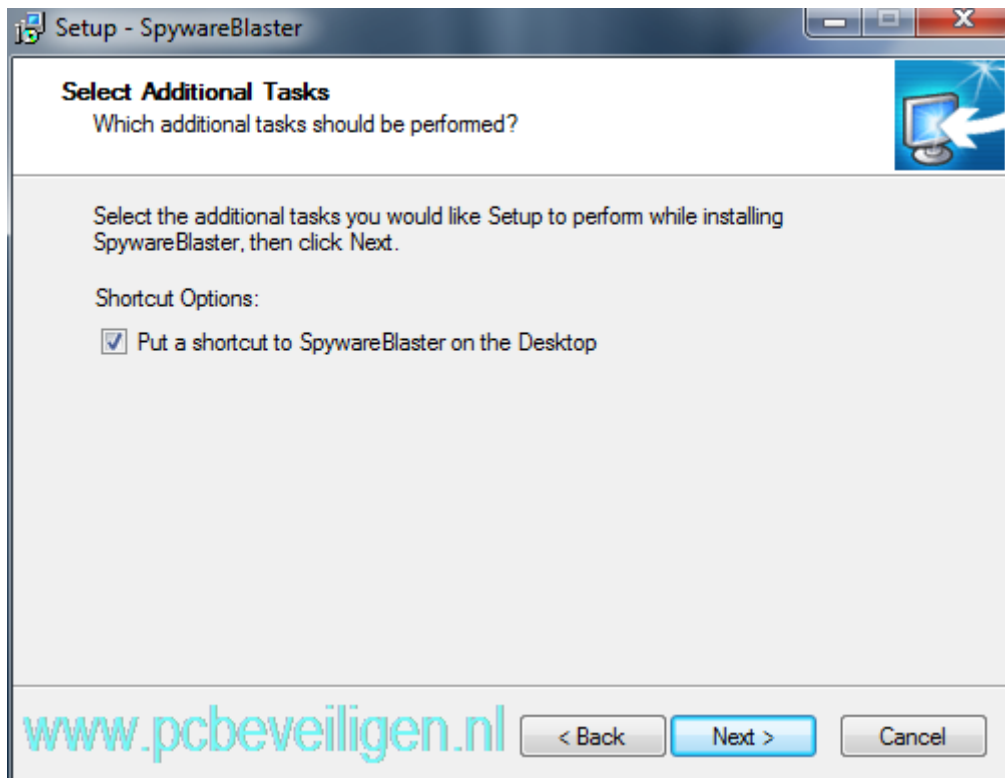
We klikken op **Next** en het scherm voor het accepteren van de licentievoorwaarden verschijnt.



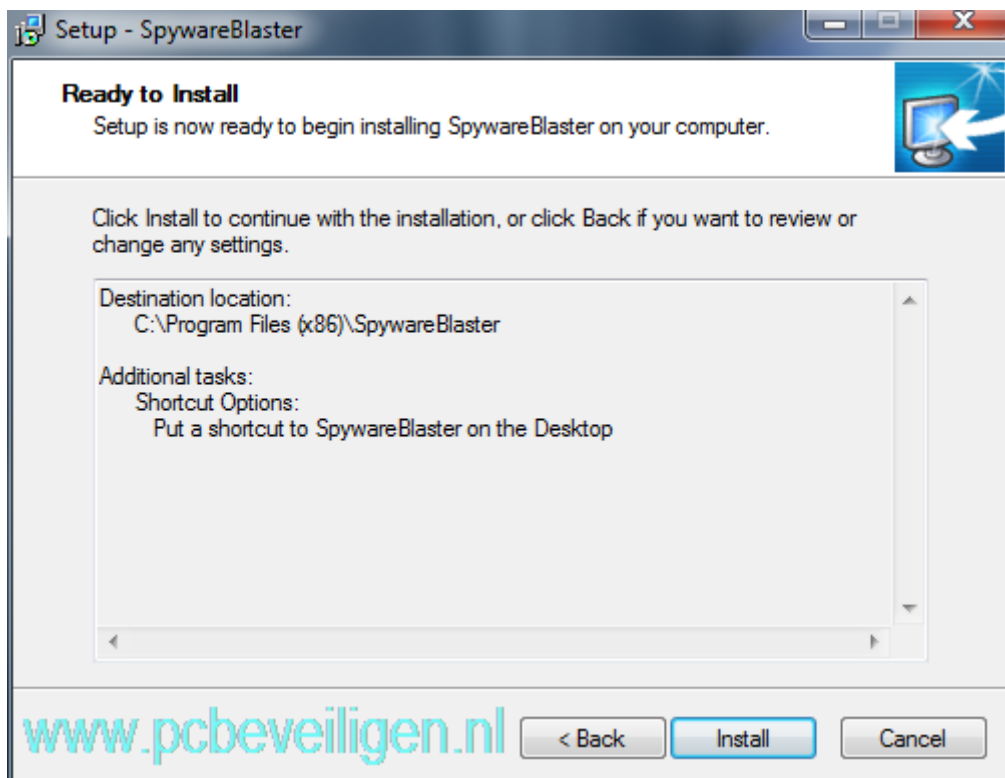
Vink hier **I accept the agreement** aan klik op **Next** en volgend scherm verschijnt.



Hier wordt het installatie pad getoond klik op **Next** en het volgende scherm van de wizard verschijnt.

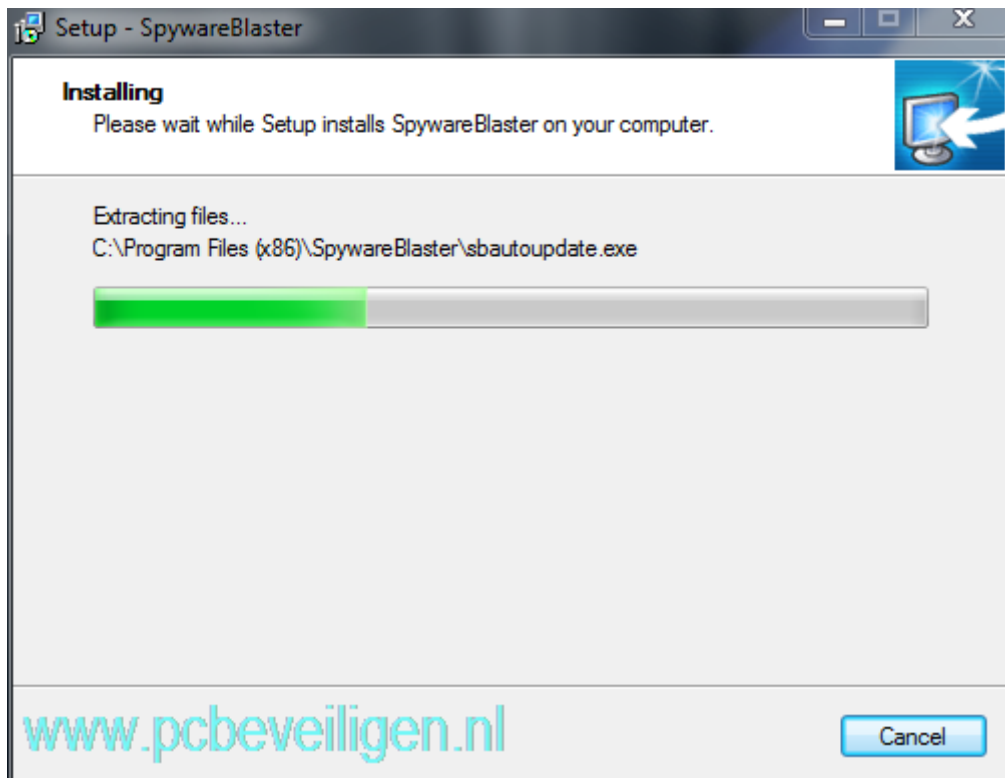


Hier kun je het maken van een snelkoppeling in of uitschakelen klik op **Next** en we zetten de installatie verder het volgende scherm verschijnt.



Hier krijgen we een overzicht van de gekozen instellingen. Klik op **Install** en de installatie kan beginnen.

In het volgende scherm wordt de vooruitgang van de installatie getoond.



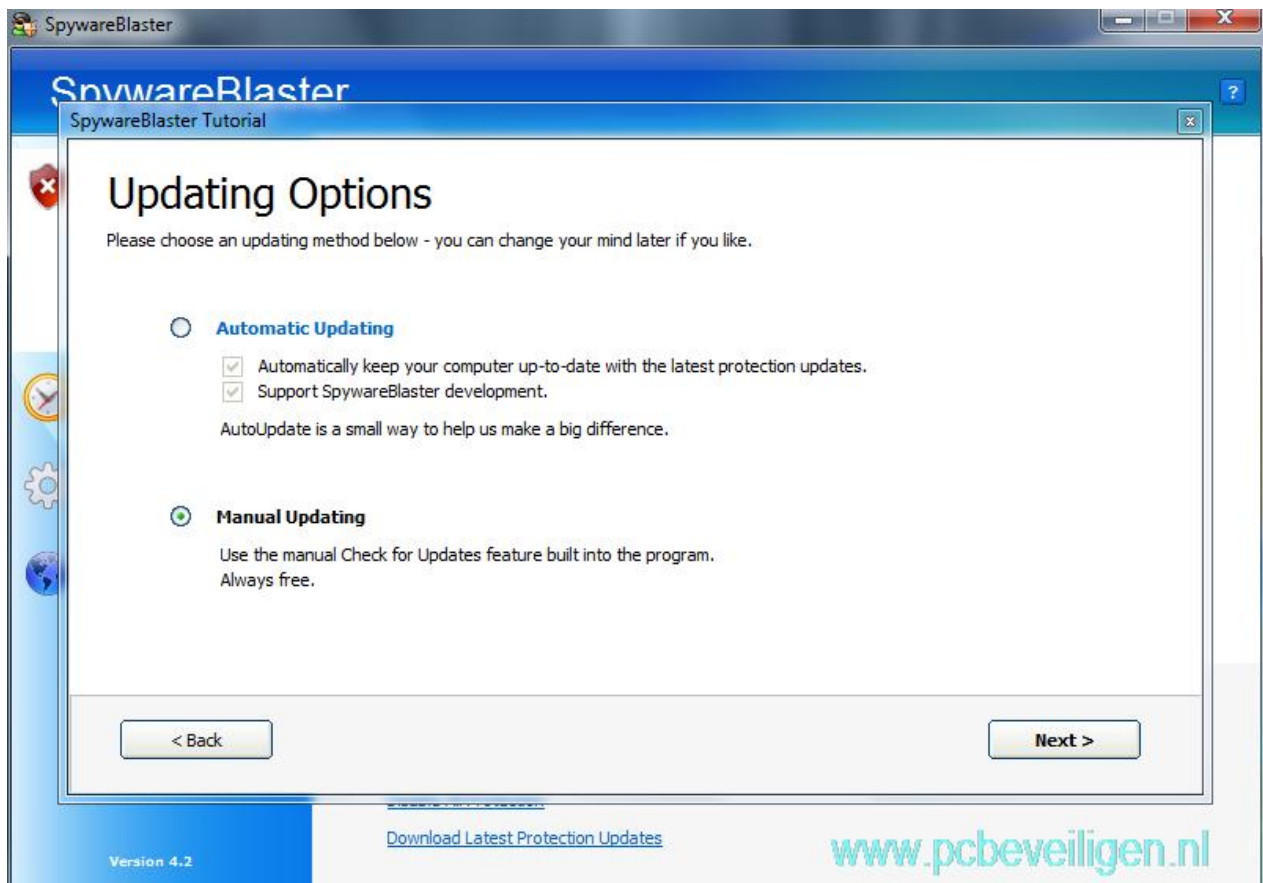
Als de installatie is afgerond krijgen we volgend scherm.



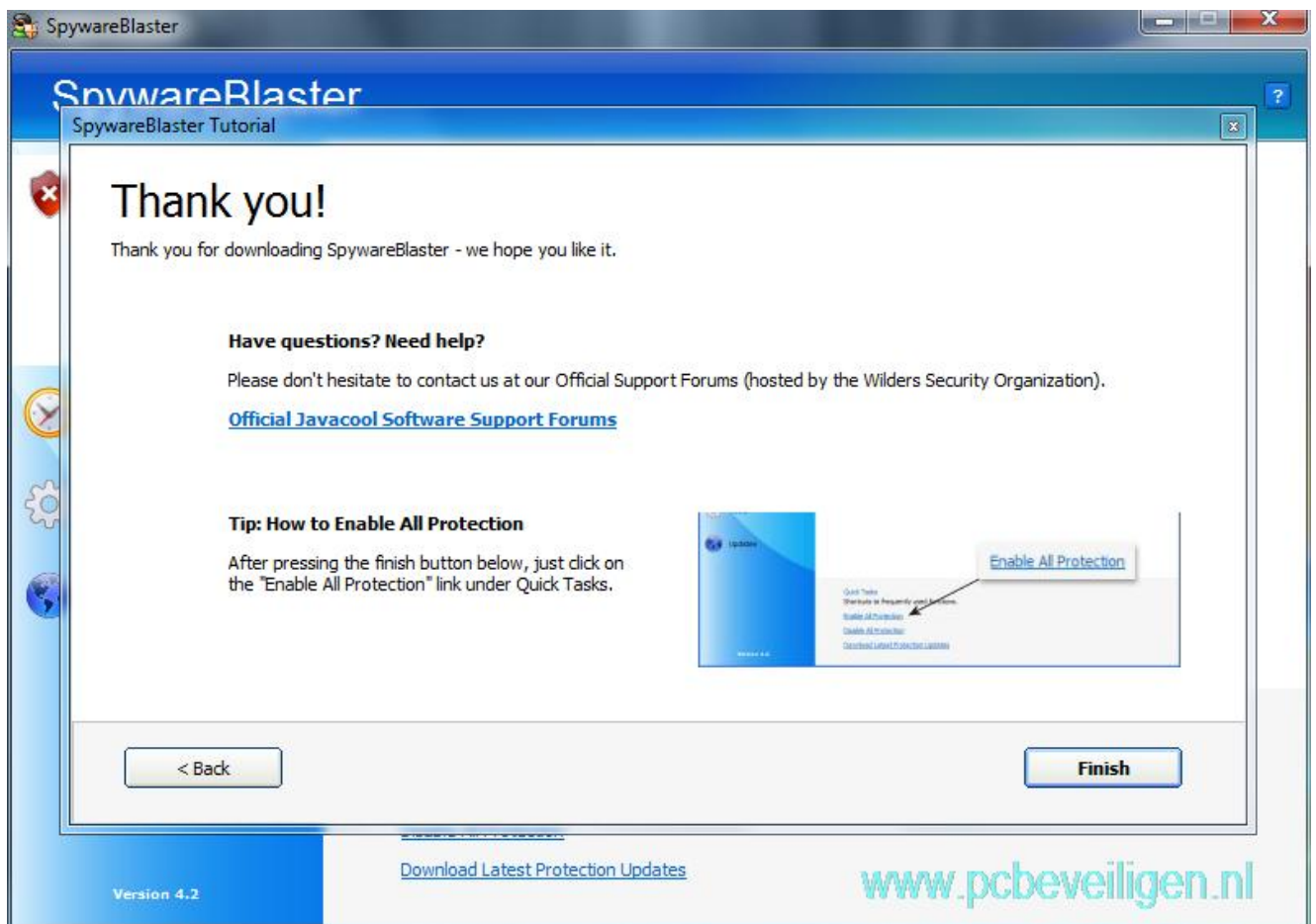
Zorg dat **Run Spyware Blaster** is aangevinkt en klik op **Finish**. De installatie is klaar en Spyware Blaster word voor de eerste keer opgestart. Een welkomst venster verschijnt.



We klikken op **Next** en het keuze scherm voor hoe we willen updaten verschijnt.

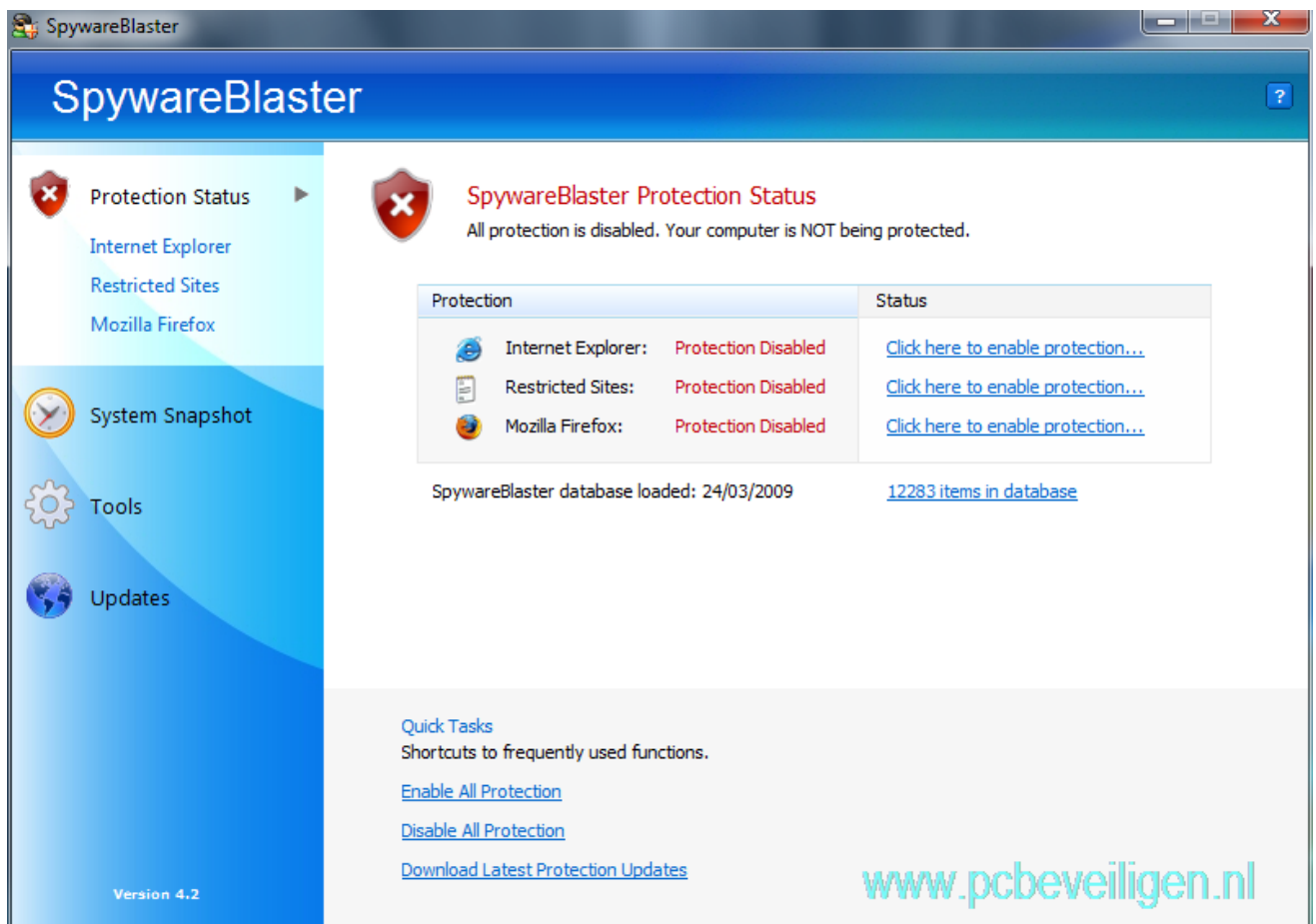


Vink hier **Manual Updating** aan. Voor Automatic Updating moet je beschikken over een licentie. Klik op **Next** en het volgende scherm komt te voorschijn.



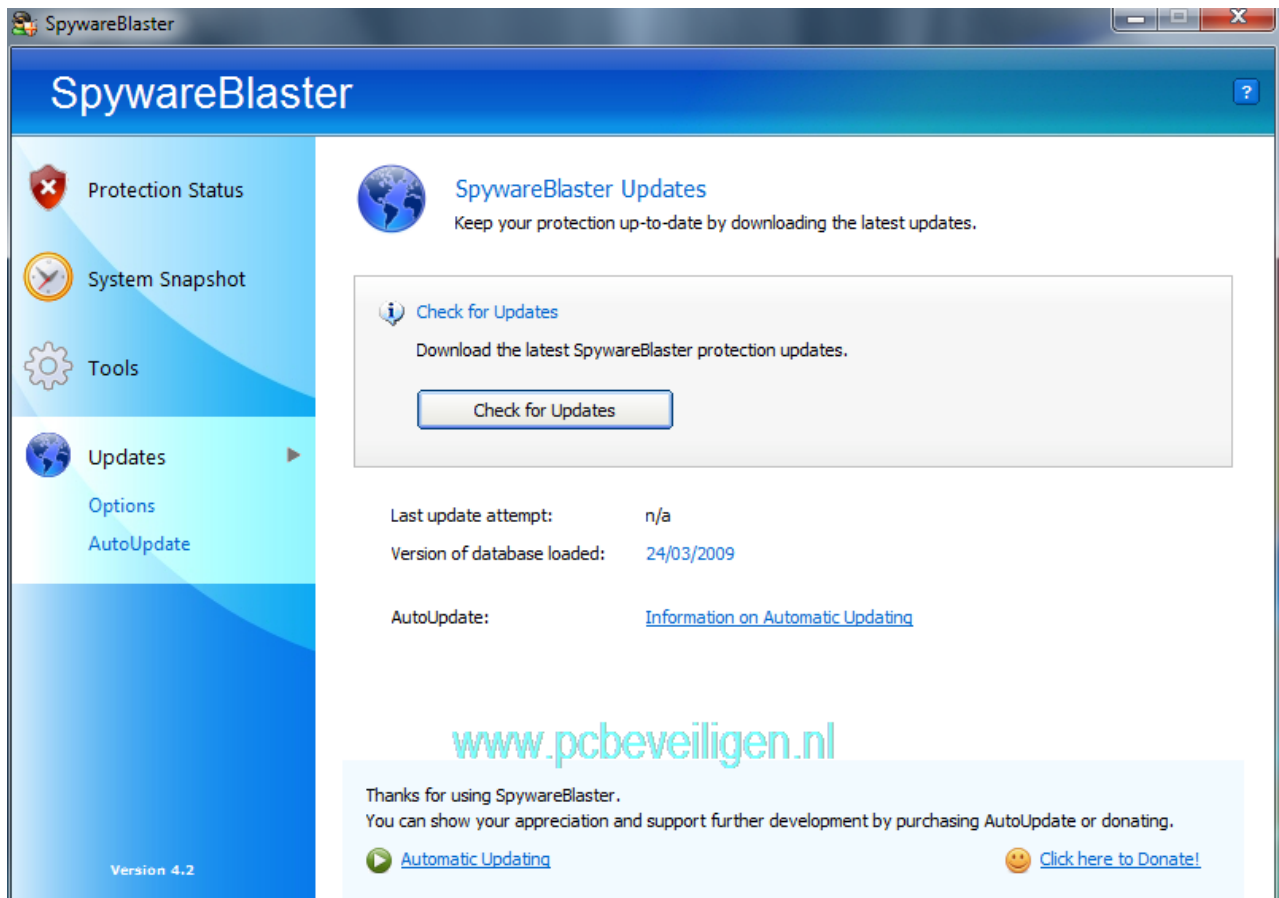
Hier vinden we een dankwoord van de makers van Spyware Blaster en de tip hoe we alle bescherming kunnen aanzetten.

Klik op **Finish** en we komen in het volgende scherm.



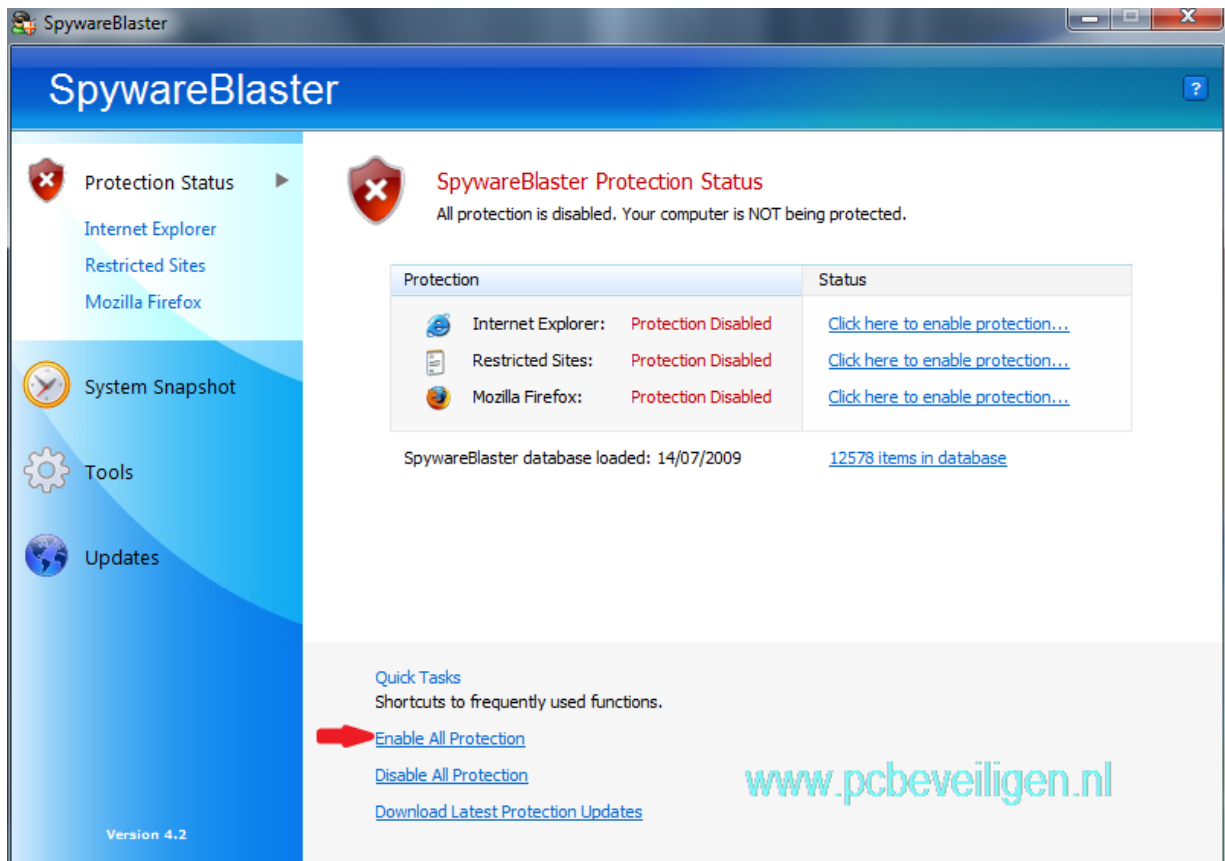
Hier wordt de beschermingsstatus weergegeven en daar we nog niet geüpdate hebben wordt het schild rood weergegeven. Na een geslaagde update en alle bescherming ingeschakeld te hebben krijgt het schild een groene kleur.

We gaan nu eerst de definities updaten. Klik op **Updates** en we krijgen onderstaand scherm.

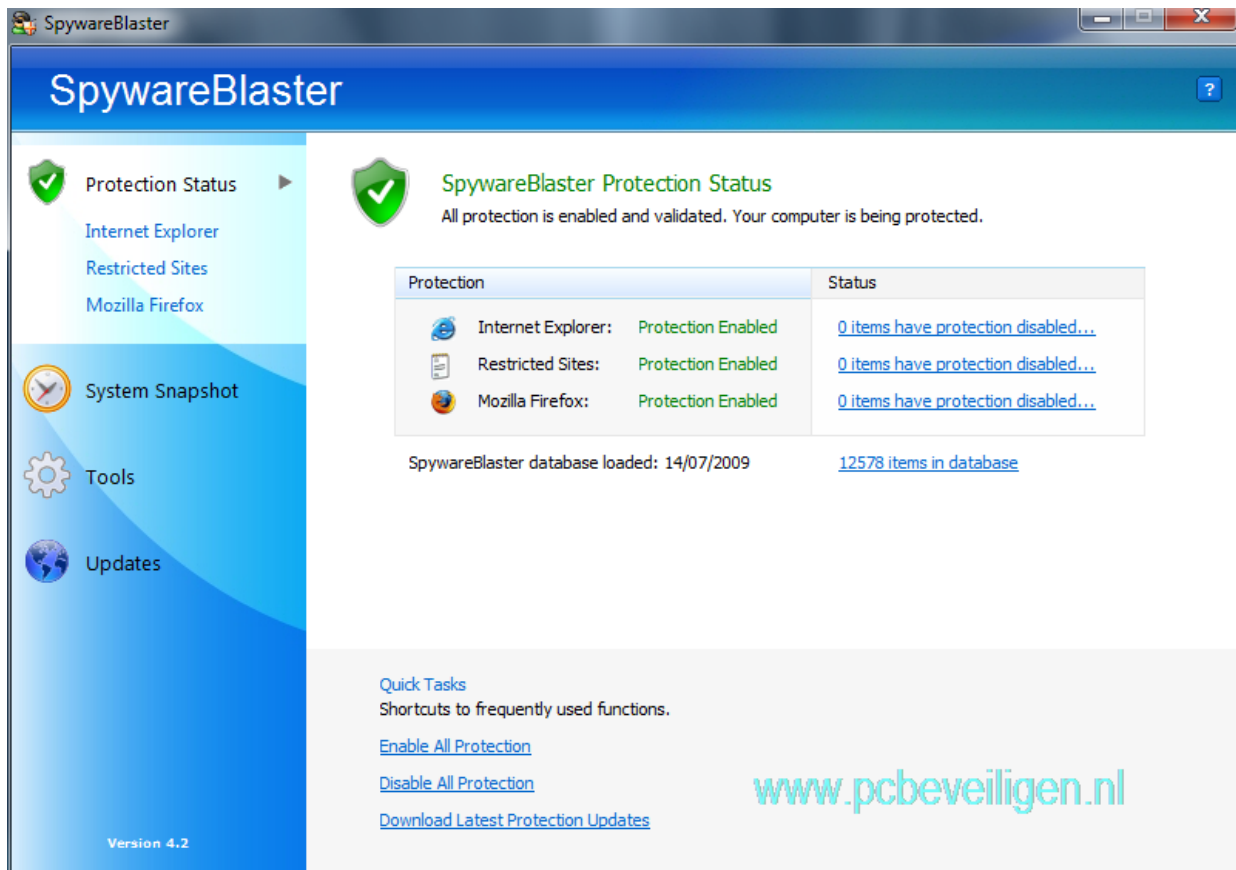


Klik op **Check for Updates** vervolgens wordt er een balk getoond waarin je de vooruitgang van het updaten kunt volgen.
Na een geslaagde update krijgt men de melding **Update Successful / SpywareBlaster has successfully downloaded the latest database**

Bevestig met **OK** en we keren terug naar **Protection Status**



Om de laatste definities te laden klikken we op **Enable All Protection** en nu kom onze **Protection Status** er zo uit te zien als in de volgende afbeelding.



Hier kan men ook zien afhankelijk van welke browser je geïnstalleerd hebt of de bescherming is ingeschakeld.

Verder ziet men nog het tijdstip van de laatste update en hoeveel items er in de database zitten. De database wordt regelmatig bijgewerkt en door wekelijks even de tijd te nemen om handmatig te controleren op updates is men dan ook verzekerd van de laatste database.

- McAfee SiteAdvisor

SiteAdvisor is een gratis invoegtoepassing voor browsers. SiteAdvisor werkt met Internet Explorer (alleen Windows) en Firefox (Mac en Windows). Hiermee kun je zien welk veiligheidsrisico het bezoeken van een bepaalde website inhoud.

Eenmaal SiteAdvisor geïnstalleerd worden er kleine pictogrammen voor de sitewaardering toegevoegd, evenals een browserknop en een optioneel zoekvenster. Hiermee wordt u gewaarschuwd voor mogelijke risicovolle sites en wordt u geholpen om veilige alternatieven te vinden.

Deze sitewaarderingen zijn gebaseerd op tests die worden uitgevoerd door McAfee met een groot aantal computers waarmee naar alle soorten bedreigingen wordt gezocht. Het resultaat is dan ook dat u heel wat veiliger kunt internetten.

McAfee SiteAdvisor is gratis, en er worden geen persoonlijke gegevens verzameld.

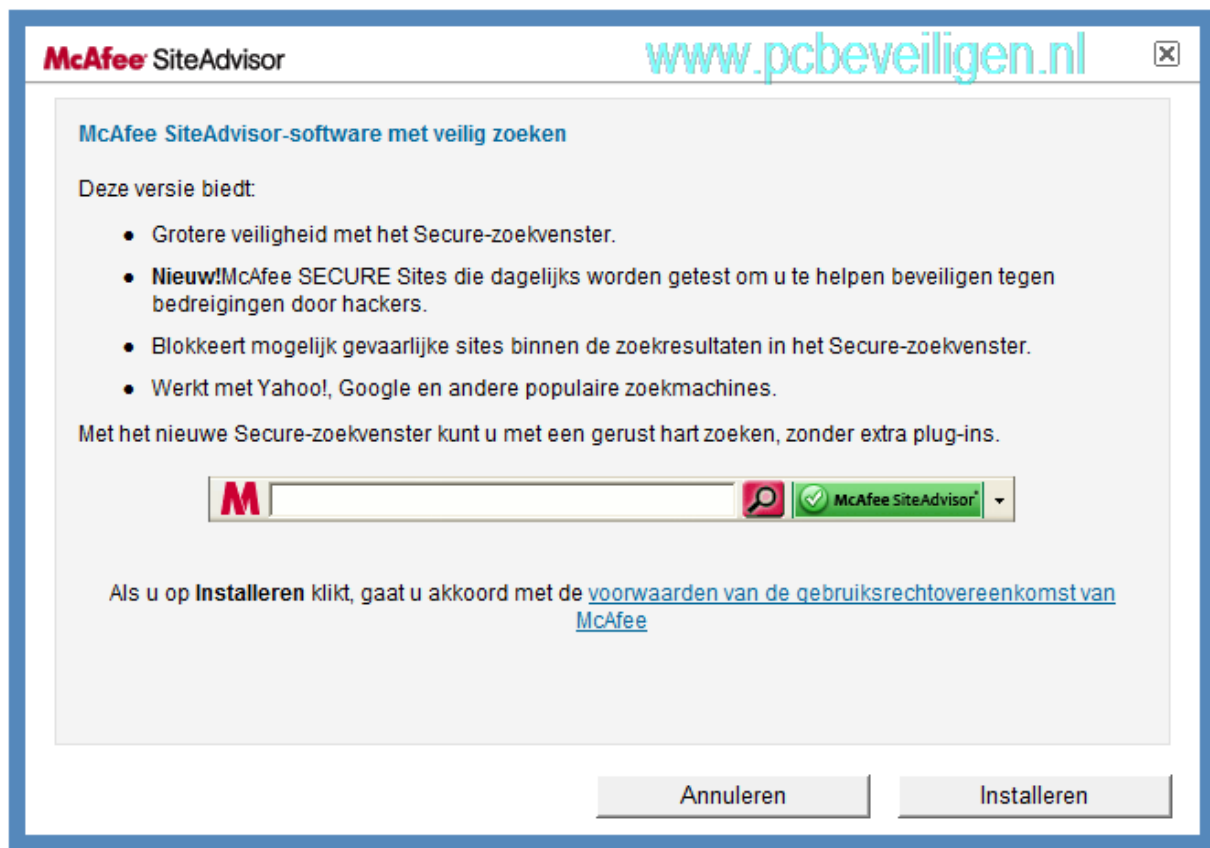
McAfee SiteAdvisor kan je [hier downloaden](#)

De installatie gaat makkelijk en snel.

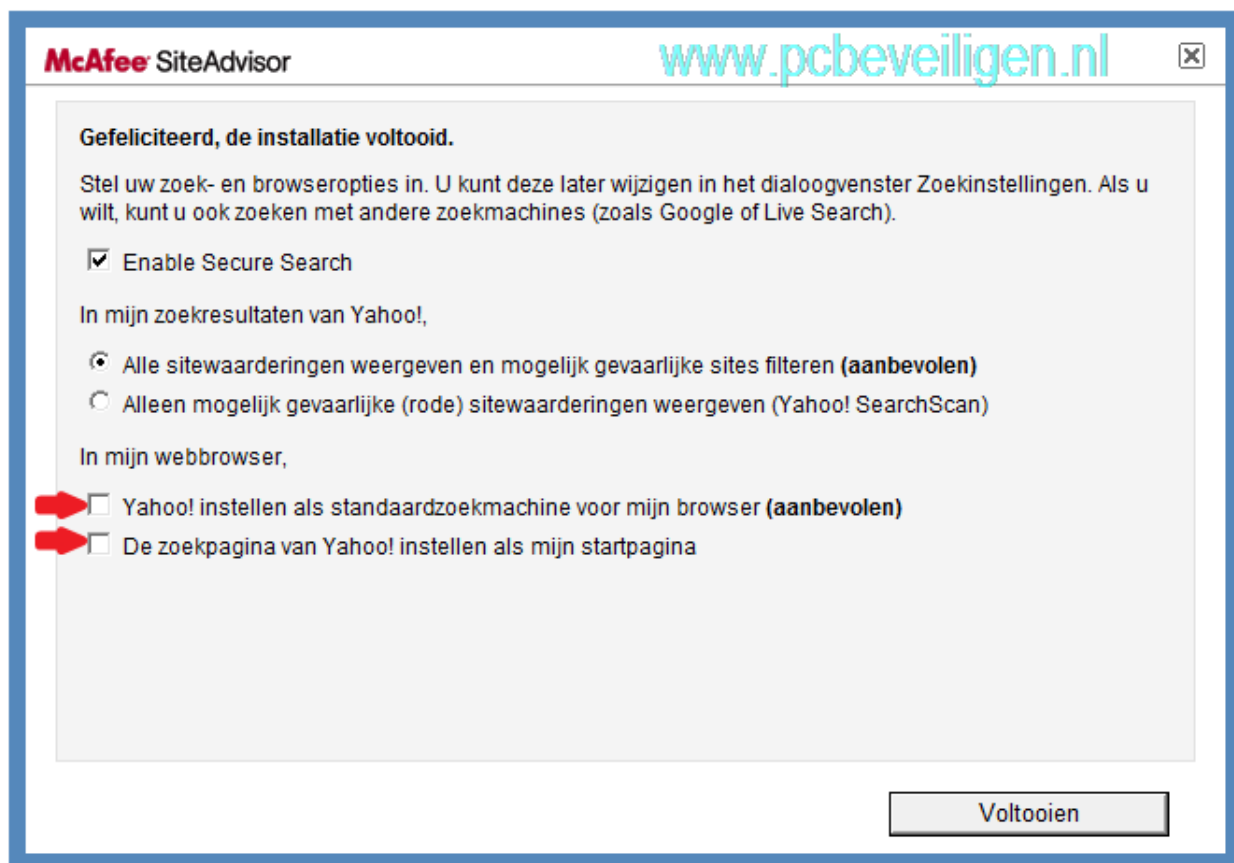
Dubbeltklik op het bestand dat je via bovenstaande link gedownload hebt en de installatie kan beginnen.

We krijgen volgend scherm met info en mogelijkheden van McAfee SiteAdvisor, ook de gebruikersovereenkomst kunnen we hier lezen.

Tevens wordt het secure zoekvenster wordt hier vermeld.



Klik op **Installeren** en we zetten de installatie voort in volgend scherm.



Secure Search functie

Wil je geen gebruik maken van de Secure Search functie van SiteAdvisor vink dit dan eventueel uit. Maak je wel gebruik van de Secure Search functie vink dan [Alle site waarderingen en mogelijk gevaarlijke sites filteren \(aanbevolen\)](#) aan. In de zoekresultaten van Yahoo via de Secure Search functie worden gevaarlijke sites wel weergegeven maar zijn niet bereikbaar.

In mijn webbrowser.






Hier kun je aangeven of je Yahoo wilt instellen als standaard zoekmachine in je browser. Ook kun je hier aangeven of je de zoekpagina van Yahoo wilt instellen als startpagina.

Klik op **Voltooien** en de installatie is beëindigd. Vervolgens wordt je naar een site gebracht waar je nog wat info vindt. Na een herstart van je browser is SiteAdvisor actief en kan je heel wat veiliger surfen.



Waarderingspictogrammen

Aan de hand van de getoonde waarderingspictogrammen kun je afleiden of een bezoek aan een website gevaar vormt.

Waarderingspictogrammen

-  **McAfee SECURE:** dagelijks getest op kwetsbaarheid voor hackers.
-  **VEILIG:** zeer laag of geen risico.
-  **LET OP:** laag risico.
-  **WAARSCHUWING:** ernstig risico.
-  **ONBEKEND:** nog geen beoordeling. Wees voorzichtig.

Pictogrammen voor Secure-zoeken

-  **SECURE-ZOEKVENSTER:** zoeken zonder zorgen.
-  **BROWSERKNOP:** valideert sitewaardering.

www.pcbeveiligen.nl

Aan de hand van bovengenoemde tips & instellingen hebben we een goede basis gecreëerd voor de beginnende gebruiker en vanwaar men verder kan werken aan het nog beter beveiligen van je pc.

Copyright 2009 www.pcbeveiligen.nl

Niets uit deze uitgave mag worden verspreid of gekopieerd zonder behoud van de oorspronkelijke bronvermelding (www.pcbeveiligen.nl)



Met vragen over beveiliging en instellingen kan men steeds terecht op het [forum](#).

Discussie en besprekingen vinden plaats op het [weblog](#).

<http://www.pcbeveiligen.nl/>