1. Uw computer beveiligen

Voor computers die verbinding maken met internet is goede beveiliging essentieel. Een goed beveiligingssysteem verkleint het risico op *malware* (virussen of andere schadelijke software) op uw computer.
Een met virussen besmette computer kan erg frustrerend zijn. Niet alleen voor u, maar ook voor anderen. Als uw computer besmet is, kan deze ook andere computers infecteren. Dit gebeurt ongemerkt, bijvoorbeeld wanneer u een e-mail verzendt of als u bestanden deelt.
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.
Windows 10 helpt bij beschermen tegen malware met *Windows Defender*. Een ander beveiligingshulpmiddel van *Windows* is het venster *Beveiliging en onderhoud*. Hier kunt u de beveiligingsinstellingen voor *Windows* controleren op uw computer en, indien nodig, aanpassen. U ziet dan ook of *Windows Firewall*, de bescherming tegen ongewenste toegang, is ingeschakeld.
Ook is het belangrijk dat de beveiligingsopties van internetbrowsers als *Edge* 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 toegangscodes voor internetbankieren, te stelen.
Invoegtoepassingen, ofwel *plugins* of *add-ons*, voegen extra functies toe aan een internetbrowser. Meestal functioneren ze goed, maar soms kunnen ze problemen geven. Daarom is het handig als u ze zelf weet te beheren. In *Edge* kunt u op moment van schrijven van dit boek geen invoegtoepassingen gebruiken. Als u deze wel wilt gebruiken, moet u een andere internetbrowser gebruiken, zoals *Internet Explorer*.

In dit hoofdstuk leert u:

- wat malware is;
- *Windows* updaten;
- andere software updaten;
- over antivirussoftware;
- werken met het venster *Beveiliging en onderhoud*;
- werken met *Windows Defender*;
- *Windows Firewall* gebruiken;
- kennismaken met phishing;
- anti-phishing opties aanzetten in een internetbrowser;
- andere beveiligingsopties aanzetten in een internetbrowser;
- werken met invoegtoepassingen of plugins in internetbrowsers.

1.1 Wat is malware?

De term *malware* is een samentrekking van *malicious software*, ofwel 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 kunnen vermenigvuldigen en zichzelf zelfstandig kunnen verspreiden, bijvoorbeeld door zichzelf te versturen via e-mails aan mensen in uw adresboek.

- *Wormen* en *Trojaanse paarden* zijn varianten op virussen. Ook dit zijn programma's die net zo schadelijk kunnen zijn als virussen, maar los van andere programma's functioneren. Ze worden vaak gebruikt door hackers (computerinbrekers) om uw computer over te nemen voor criminele activiteiten, zoals voor het inbreken op grote bedrijfswebsites.

- *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 malafide organisaties en criminelen. Die gebruiken uw gegevens bijvoorbeeld om u ongewenste reclamemails (spam) te sturen.

- *Adware* plaatst tijdens het surfen advertenties in uw venster of een apart venster. Adware verschijnt vaak nadat u een gratis programma heeft geïnstalleerd.

- Daarnaast is er het zogenaamde *ransomware* (gijzelvirus) in opkomst. Hierbij wordt met malware uw computer lamgelegd. 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.

U gaat deze instellingen even bekijken.

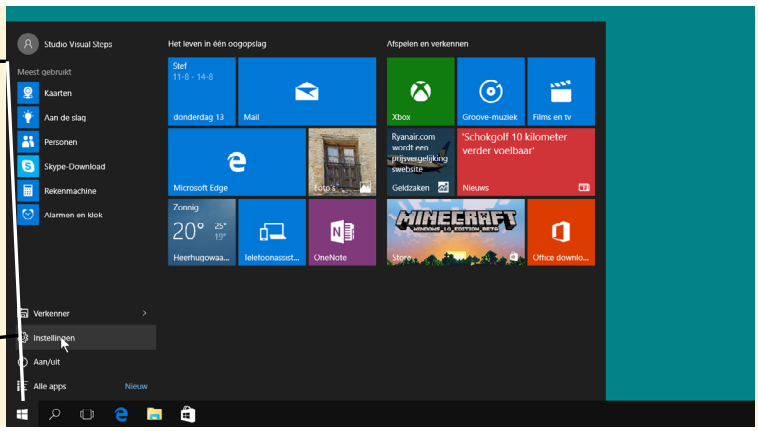
Let op!

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.

U opent *Windows Update* via *Instellingen*:

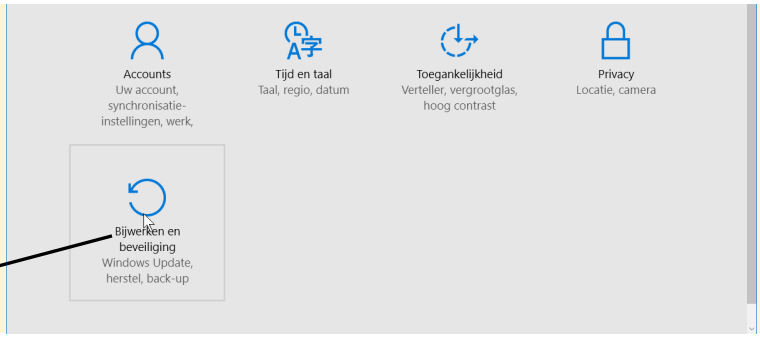
Klik op

Klik op Instellingen



U opent het venster *Bijwerken en beveiliging*:

Klik op Bijwerken en beveiliging, Windows Update, herstel, back-up



Het venster *Bijwerken en beveiliging* wordt geopend:

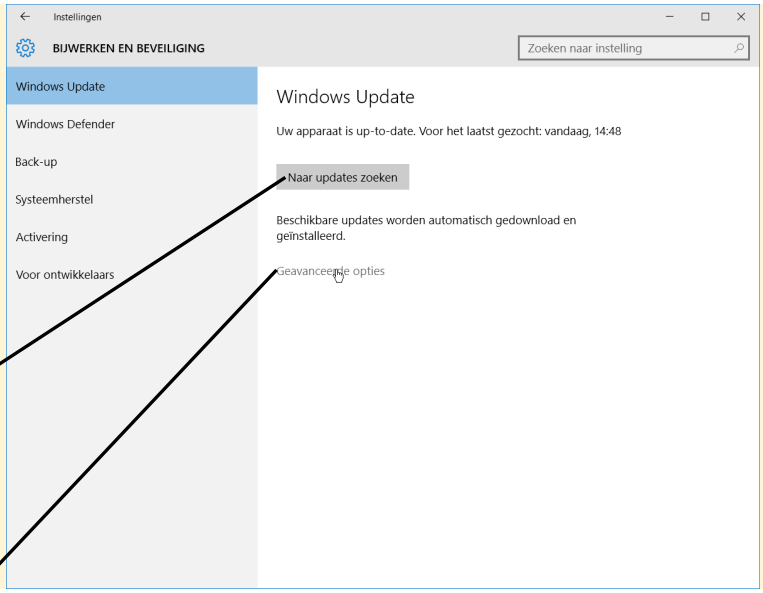
Er wordt automatisch naar updates voor *Windows* gezocht:

U kunt zelf tussentijds kijken of er nieuwe updates zijn door te klikken op

Naar updates zoeken:

U bekijkt de instellingen van *Windows Update*:

Klik op Geavanceerde opties

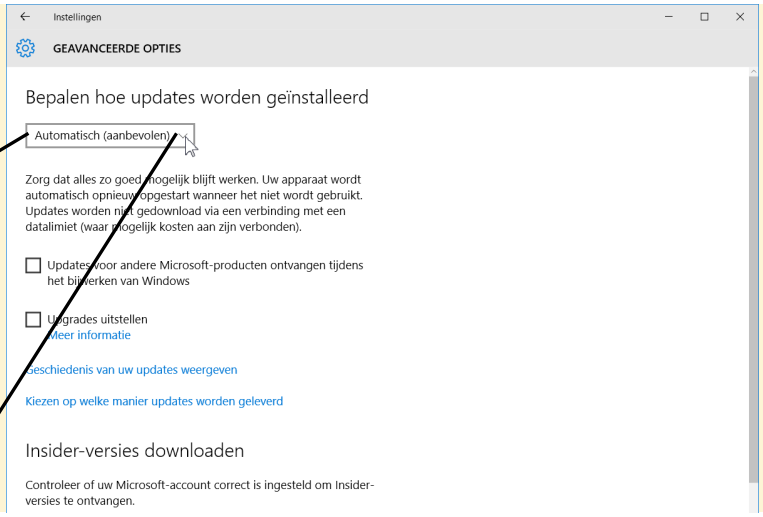


Als u Automatisch (aanbevolen) ziet in het venster, staat automatisch updaten aan:

Ziet u dit niet:

Klik bij Bepalen hoe updates worden **op**

Klik op Automatisch (aanbevolen)



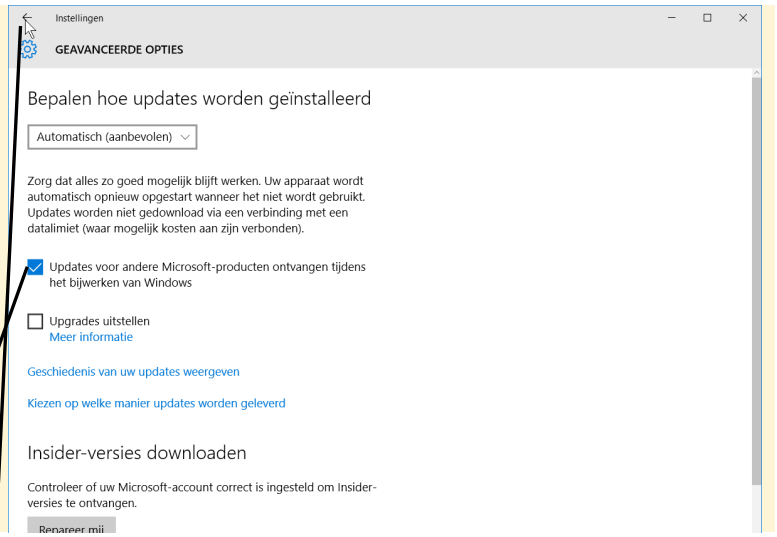
U kunt het ontvangen van updates voor andere Microsoft-producten ook, indien nodig, aanzetten:

Als u geen vinkje bij
Updates voor andere Microsoft-p
het bijwerken van Windows
ziet:

Klik een vinkje bij
Updates voor andere Micro
het bijwerken van Windows

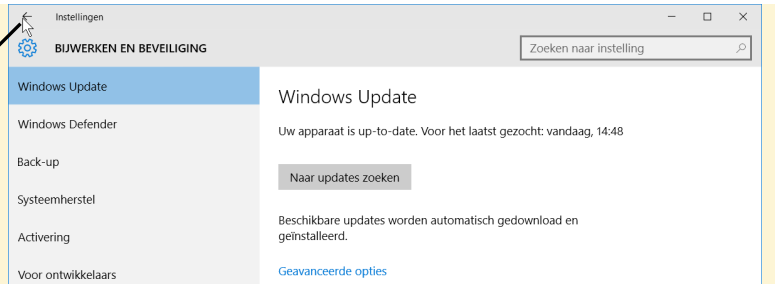
U slaat de instellingen op:

Klik op ←



In het venster *Bijwerken en beveiliging*:

Klik op ←



De instellingen voor *Windows Update* zijn opgeslagen.

Sluit *Instellingen* [1]

Tip

De nadelen van automatisch updaten

Een nadeel van automatisch laten controleren en updaten, is dat *Windows* soms op onverwachte momenten uw computer wil laten herstarten. Dat kan vervelend zijn als u op dat moment bijvoorbeeld midden in een activiteit zit die u niet wilt afbreken.
U kunt dan wel in een pop-up venster opgeven dat u wilt dat de herstart pas later plaatsvindt.
Het kan nog vervelender zijn als u een programma met een bestand open heeft staan waarmee u aan het werk bent. Als u op het moment van aankondigen van een herstart, weg bent van uw computer (meestal na tien minuten), merkt u bij terugkomst dat uw computer opnieuw is opgestart en uw niet opgeslagen werk kwijt bent.
Als u dit wilt voorkomen, kunt u er bij de instellingen voor kiezen zelf te bepalen wanneer de updates worden geïnstalleerd.