VEILIGHEID & PRIVACY

1

Veiligheid voor alles! In dit hoofdstuk zorgen we voor een goede bescherming tegen virussen en ander digitaal leed. Ook gaan we in op de bescherming van je privacy en het maken van een back-up, mocht het noodlot toeslaan.

Voordat we aan de slag gaan met Windows, is het belangrijk om het systeem te beveiligen. Vooral tijdens het surfen op internet zijn er allerlei bedreigingen. Het gaat niet alleen om virussen die de computer onbruikbaar maken. Er is ook ander digitaal leed. We sommen de belangrijkste risico's op:

• **Phishing**

Via nepmails, valse sms- of chatberichten proberen criminelen bankgegevens en andere persoonlijke data te ontfutselen. Ze gebruiken die gegevens voor criminele activiteiten, zoals het leeghalen van je bankrekening.

• **Malware**

Door kwaadaardige software op de computer te plaatsen, achterhalen criminelen kredietkaartnummers of andere privégegevens voor geldelijk gewin. Malware is een verzamelnaam voor computerinfecties als virussen en Trojaanse paarden.

• **Ransomware**

Ook gijzelsoftware genoemd. Bij dit type malware worden bestanden op de harde schijf door criminelen gekaapt (versleuteld) en pas weer vrijgegeven na het betalen van losgeld (zie kader "Betaal geen losgeld!").

• **Rootkit**

Dit is malware die zich diep in het besturingssysteem nestelt. Hij is daardoor moeilijk op te sporen en ook lastig te verwijderen. Een rootkit kan ervoor zorgen dat het systeem instabiel wordt.

• **Adware**

Minder riskant, maar wel hinderlijk: software die extra advertenties toevoegt aan websites, bijvoorbeeld in de vorm van vervelende pop-ups. De makers hopen zo een extra zakcentje te verdienen.

• **Spyware**

Programma's die informatie vergaren over de computergebruiker. Dat kan een keylogger zijn die je toetsenbordinvoer registreert om bv. kredietkaartgegevens buit te maken, maar de digitale spion kan ook uit zijn op informatie om gerichte advertenties te tonen.

• **Riskante websites**

Met name kleinere sites worden nogal eens slachtoffer van hackers waardoor ze – vaak onbewust – kwaadaardige software verspreiden. Ook kan er gevaarlijke code worden verspreid via advertenties.

• **Ongewenste programma's**

Bij het installeren van software komt het nogal eens voor dat er ongevraagd extra programma's op de computer worden gezet. Er is ook software die ongevraagd een toolbar (knoppenbalk) voor de browser installeert.

• **Spiedende adverteerders**

Om advertenties af te stemmen op de interesses van websitebezoekers, bouwen adverteerders profielen op van gebruikers. Dit is een inbreuk op de privacy, omdat gebruikers hiervan niet op de hoogte worden gesteld.

Betaal geen losgeld!

Slachtoffer van ransomware? Betaal geen losgeld. De kans bestaat dat je geen (werkende) sleutel krijgt van de criminelen om de computer te ontgrendelen. Bovendien houd je, door te betalen, het criminele systeem in stand. Kijk op de site **www.nomoreransom.org** welke opties er zijn. Dit is een site van de politie, Europol, Kaspersky en Intel. De beste beveiliging tegen ransomware blijft weliswaar een goede back-up.

Gelukkig heeft Windows mogelijkheden ingebouwd om je te beschermen tegen dit soort digitale rampspoed. Een virusscanner (par. 1.1 en 1.2) kan ervoor zorgen dat er geen malware op de computer komt. Met een back-up (par 1.4) kun je de computer herstellen als het toch misgaat. Ook als het gaat om privacy zijn er maatregelen mogelijk. Zo kun je de instellingen van Windows wijzigingen, waardoor er minder persoonlijke informatie richting Microsoft gaat (par. 1.3).

Veilig online

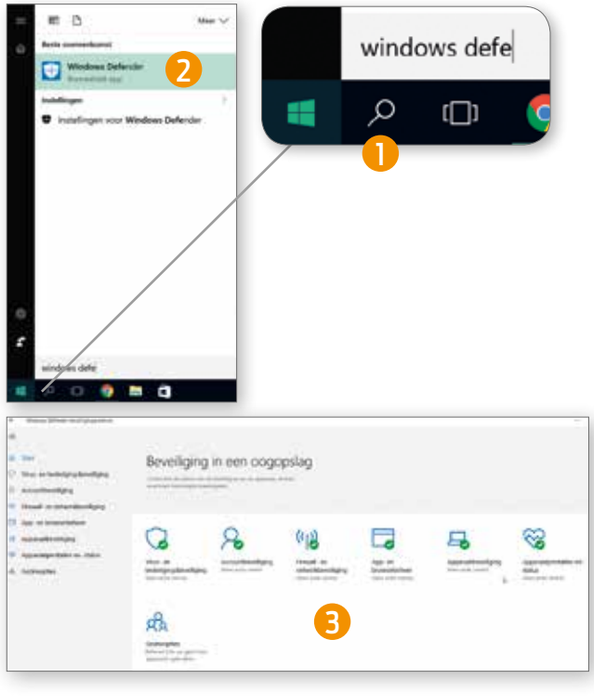
Meer tips om veilig te surfen vind je in de gids **Veilig online – 80 tips om jezelf te beschermen** (ref. 149). Als abonnee van het magazine Test Aankoop betaal je enkel € 1,95 administratiekosten. Bestellen kan via 02 290 34 86 of **testaankoop.be/praktischegidsen**.

1.1 WINDOWS DEFENDER

Om Windows 10 veilig te kunnen gebruiken, is bescherming tegen malware essentieel. Het systeem beschikt over een ingebouwde virusscanner in de vorm van Windows Defender. Windows Defender is het absolute minimum om beschermd te zijn tegen malware. Uit onze tests blijkt dat antiviruspakketten van andere softwaremakers beter op hun taak toegerust zijn (de resultaten vind je op **www.testaankoop.be/vergelijkantivirus**). Wie geen ander pakket wil, moet in ieder geval Windows Defender gebruiken.

1.1a Windows Defender aanzetten

Windows Defender staat automatisch aan als er geen andere virusscanner is geïnstalleerd. Toch is het voor de zekerheid nuttig om dit te controleren.



Windows Defender

1. Klik op Zoeken (zie het kader “Programma’s starten via Zoeken”) en typ “Windows Defender”.
2. Klik op het eerste resultaat om het Windows Defender-beveiligingscentrum te openen.
3. We overlopen enkele interessante onderdelen:

- **Virus- en bedreigingsbeveiliging:** de ingebouwde virusscanner wordt automatisch geactiveerd wanneer je geen eigen antivirus installeert, of wanneer die verlopen is.
- **Firewall- en netwerkbeveiliging:** de ingebouwde firewall is automatisch actief als je geen firewall hebt geïnstalleerd.
- **App- en browserbeheer:** hier beheer je de instellingen voor Windows Defender Smartscreen, de in Windows en Edge ingebouwde bescherming tegen schadelijke programma’s en websites. Kies bij elk onderdeel voor de optie “Waarschuwen”. Je krijgt dan een melding wanneer je een schadelijk programma of website dreigt te openen.
- **Apparaatprestaties- en status:** hier krijg je informatie over de toestand van je pc (of je systeem up-to-date is, of er problemen zijn met de batterij …). Bij een probleem worden de nodige acties voorgesteld.

Programma’s starten via “Zoeken”

We gebruiken in dit boek de functie “Zoeken” om programma’s te starten of instellingen te vinden. Klik daarvoor linksonder in de taakbalk op het zoekicoontje (het vergrootglas naast het Windows-icoon). Typ daarna de naam van het gewenste programma of de instelling.
De zoekfunctie van Windows gaat dan aan het werk om het programma te vinden. Het is ook mogelijk om programma’s of instellingen op andere manieren te vinden, bijvoorbeeld via de lijst met programma’s in het startmenu. Instellingen zijn terug te vinden via de Windows-onderdelen “Instellingen” en “Configuratiescherm”. Als je bepaalde programma’s of instellingen vaak gebruikt, kun je ze aan het Startmenu (zie par. 5.1a) of de Taakbalk (zie par. 5.3) toevoegen.

1.1b Minder notificaties

Notificaties van Windows Defender verschijnen in het Actiecentrum. Dit is de centrale plek binnen Windows waar alle berichten terechtkomen. We gaan overigens op diverse plaatsen in dit boek nader in op het Actiecentrum (zie ook par. 5.10). Als je vindt dat er te veel meldingen van Windows Defender in beeld komen, is dat eenvoudig uit te zetten.

1.1c Grondige scan

Windows Defender beschikt over meerdere soorten scans. Kies voor een eenvoudige controle op besmettingen voor de snelle scan. In dat geval onderzoekt de software plekken en bestanden die het meeste risico lopen op besmetting. Klik bij het onderdeel “Virus- en bedreigingsbeveiliging” op “Nu scannen”.

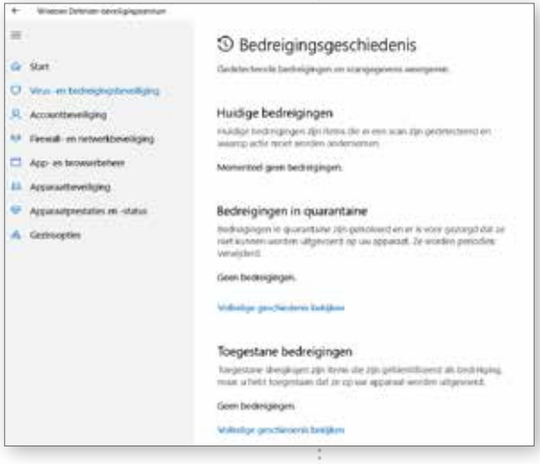
Windows Defender

1. Start Windows Defender en klik linksonder op “Instellingen”.
2. Selecteer welke meldingen je wilt ontvangen (zet het schuifje desgewenst op “Uit” door het naar links te schuiven).

Om alle hoeken en gaten van de computer te laten doorzoeken, kies je voor de volledige scan (klik op “Een nieuwe geavanceerde scan uitvoeren”, selecteer “Volledige scan” en kies dan “Nu scannen”). Het is aan te raden om de eerste keer een volledige scan uit te voeren. Daarna kun je meestal af met de snelle scan, al kan het geen kwaad eens in de zoveel tijd volledig te scannen.

1.1d Bij lastige malware: offline scan

De volledige scan is niet de uitgebreidste variant. Er is ook de Windows Defender Offline-scan. Die komt van pas als de computer is besmet met malware of een rootkit die lastig is te verwijderen. De kans dat het weghalen van een virus lukt, is groter als de computer wordt opgestart in een speciale modus via de offline scan. Selecteer “Windows Defender Offline-scan” en klik op “Nu scannen”.



1.1e Gevonden virussen weergeven

Nadat de offline scan is uitgevoerd, ben je waarschijnlijk nieuwsgierig naar de resultaten. Die vind je terug in Windows Defender bij Virus- en bedreigingsbeveiliging. Klik op “Bedreigingsgeschiedenis” om een overzicht van de gevonden bedreigingen te vinden.

1.1f Meldingen over malware

Als er een virus is gevonden, is daarvan ook een melding te vinden in het “Actiecentrum”.

1.2 KIES EEN BETERE VIRUSSCANNER

Windows Defender is zeker niet de beste virusscanner. Omdat het gratis wordt meegeleverd met Windows gebruiken veel mensen het, maar uit onze test bleek dat de bescherming tegen malware op het nippertje een goede score krijgt. Andere gratis virusscanners doen het soms wat beter, maar toch halen ze het niveau van de beste betaalde antivirussoftware niet. Daar komt bij dat de gratis virusscanners vaak hinderlijke advertenties bevatten voor de betaalde variant en je soms genoegen moet nemen met een pakket in het Engels (bijvoorbeeld Bitdefender Free).

Voor meer comfort is het dus aan te raden om te kiezen voor een betaald pakket. Om uit te vinden welke het beste bevalt, is het bij de meeste pakketten mogelijk om ze een periode gratis te gebruiken. Het is overigens geen goed idee om telkens een tijdje een proefversie van verschillende leveranciers na elkaar te installeren. Bij het de-installeren blijven er altijd onderdelen achter, waardoor de computer op termijn vertraagt.

1.2a Bitdefender (betaald) en Eset

Uit onze meest recente test blijkt dat de gratis scanners van Bitdefender (Beste Koop) en Avast extra bescherming bieden, maar de minste kans op besmetting door malware en andere kwaadaardige zaken heb je bij de betaalde versie van Bitdefender (Beste van de Test) en Eset. Beide virusscanners zijn ook een optie als je een oudere pc met weinig geheugen wil upgraden naar Windows 10. Ze koppelen prima bescherming aan een lage belasting (geheugengebruik) van je computer.

Second opinion

Er zijn meer programma's die werken als tweede verdedigingslinie naast de reguliere scanner. Veel computergebruikers installeren Malwarebytes Anti-Malware (**nl.malwarebytes.com**) of Hitman Pro (**www.hitmanpro.com**) voor een extra check op malware.
Deze programma's zijn ook in staat om bedreigingen te verwijderen. Let er bij het installeren van Malwarebytes Anti-Malware op dat je de gratis versie installeert.

1.2b Gebruikersaccounts

Voordat je Windows 10 in gebruik neemt, moet er een account worden aangemaakt. Microsoft stuurt erop aan gebruik te maken van een Microsoft-account, bijvoorbeeld een mailadres dat eindigt op hotmail.com. Dat heeft bepaalde voordelen. Zo werken Mail, Agenda en OneDrive direct, zonder extra instellingen. Ook kan de gebruiker apps downloaden uit de Windows Store.

Shoppen loont

Bij de aanschaf van een virusscanner loont het de moeite om prijzen te vergelijken bij verschillende (web)winkels. Bizar genoeg zijn soms de fysieke pakketten in een winkel minder duur dan de downloadversie, al bevatten ze enkel een code die ... een gewone download toelaat!
De genoemde pakketten zijn soms met een aantrekkelijke korting te verkrijgen, zeker wanneer de licentie haar einde nadert. Om een kat in de zak te voorkomen, is het wel belangrijk om te kopen bij een betrouwbare leverancier.

Wie geen behoefte heeft aan een Microsoft-account, kan ook kiezen voor een lokaal account. Wil je later toch gebruikmaken van een Microsoftdienst, zoals OneDrive of Skype, dan moet je je daarvoor apart aanmelden.

Administrator

Het eerste account is altijd een account met administratorrechten. Daarmee heb je alle beheerrechten, waaronder het installeren van software, het wijzigen van systeeminstellingen en het wijzigen van andere belangrijke instellingen.
Het wordt aangeraden om daaropvolgende accounts geen administratorrechten te geven. Kies in plaats daarvan voor een standaardaccount.

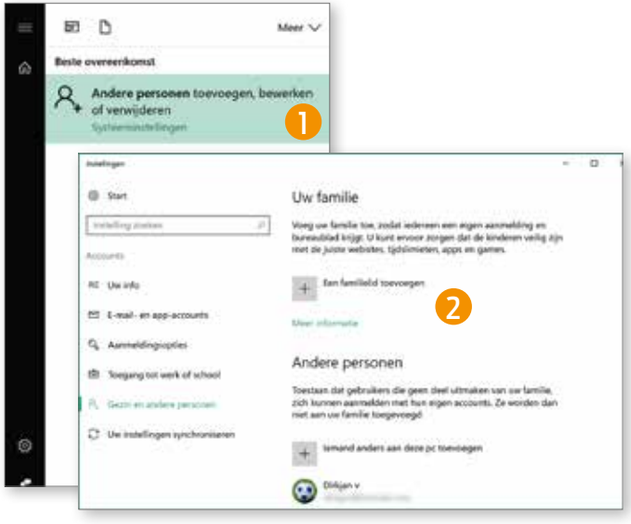
Meerdere gebruikers

Het aanmaken van extra gebruikersaccounts is handig als de computer wordt gedeeld. Door er een standaardaccount van te maken voorkom je dat de andere gebruiker per ongeluk instellingen wijzigt of software installeert waardoor de computer op tilt slaat.
Ook als je de enige persoon bent die de computer gebruikt, is een tweede account handig. Kies voor een standaardaccount om te voorkomen dat een onhandige actie het systeem in de war schopt. Pas als je software wilt installeren of wijzigingen wilt aanbrengen, schakel je even over naar het administratoraccount.

Windows 10

1 Klik op Zoeken en typ “Andere personen”. Selecteer “Andere personen toevoegen […]”.
2 Kies hier voor het type account dat je wilt toevoegen: een familielid of iemand anders.

Gebruikersaccount aanmaken



Familielid

Als je hier kiest voor familielid, zijn er uitgebreide mogelijkheden om als beheerder te controleren welke activiteiten de gebruiker onderneemt. Dit is handig voor wie kinderen binnen het gezin toegang wil geven. Zo kun je in de gaten houden welke apps er worden gebruikt en beperken welke sites bezocht mogen worden. Ook kun je de schermtijd beperken zodat de kinderen niet eindeloos achter de computer hangen. Deze mogelijkheden zijn er alleen in combinatie met een Microsoft-account.

Andere personen

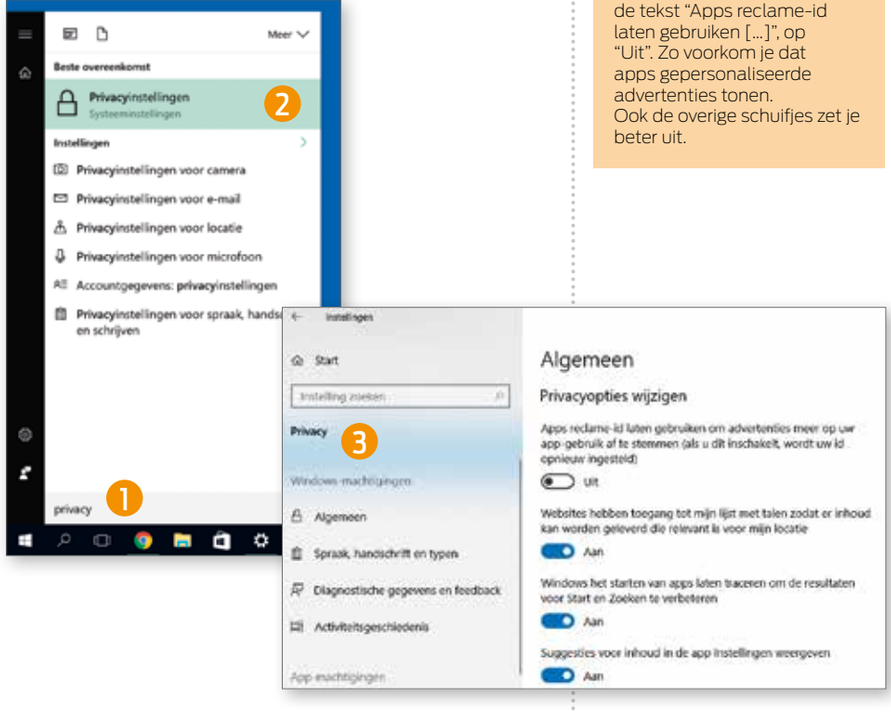
Je kan ook een gastaccount aanmaken voor het geval een bezoeker even je computer wil gebruiken. Kies dan voor “Iemand anders aan deze pc toevoegen”. Ook hier wil Windows graag dat er een Microsoft-account gekoppeld wordt aan het account, maar dit is niet noodzakelijk. Kies in dat laatste geval voor “Ik beschik niet over aanmeldgegevens van deze persoon”, en klik in het volgende scherm op “Gebruiker zonder Microsoft-account toevoegen”. Kies tot slot een naam voor het gastaccount (bijvoorbeeld “Gastgebruiker”) en eventueel een wachtwoord.

1.3 WAAK OVER JE PRIVACY

Windows 10 staat niet goed bekend als het gaat om privacy. Microsoft verzamelt veel informatie over zijn gebruikers, veel meer dan in vorige Windowsversies. Gelukkig is het wel mogelijk om dat tegen te gaan.
In Windows 10 is namelijk een privacymenu te vinden. Klik op Zoeken en typ “Privacyinstellingen” om erheen te gaan. Het is verstandig hier alle submenu’s af te gaan en alle privacyopties uit te zetten of op een minder nieuwsgierige stand. We bespreken de belangrijkste instellingen.

1.3a Algemene privacyinstellingen

Als je aan de slag gaat met de privacyinstellingen, kom je eerst terecht in een scherm om enkele algemene zaken aan te passen:



Privacy

1 Klik op Zoeken en typ “privacy”.
2 Windows vindt “Privacyinstellingen”. Klik erop.
3 Zet in het scherm “Privacyopties wijzigen” het eerste schuifje, met de tekst “Apps reclame-id laten gebruiken […]”, op “Uit”. Zo voorkom je dat apps gepersonaliseerde advertenties tonen.
Ook de overige schuifjes zet je beter uit.