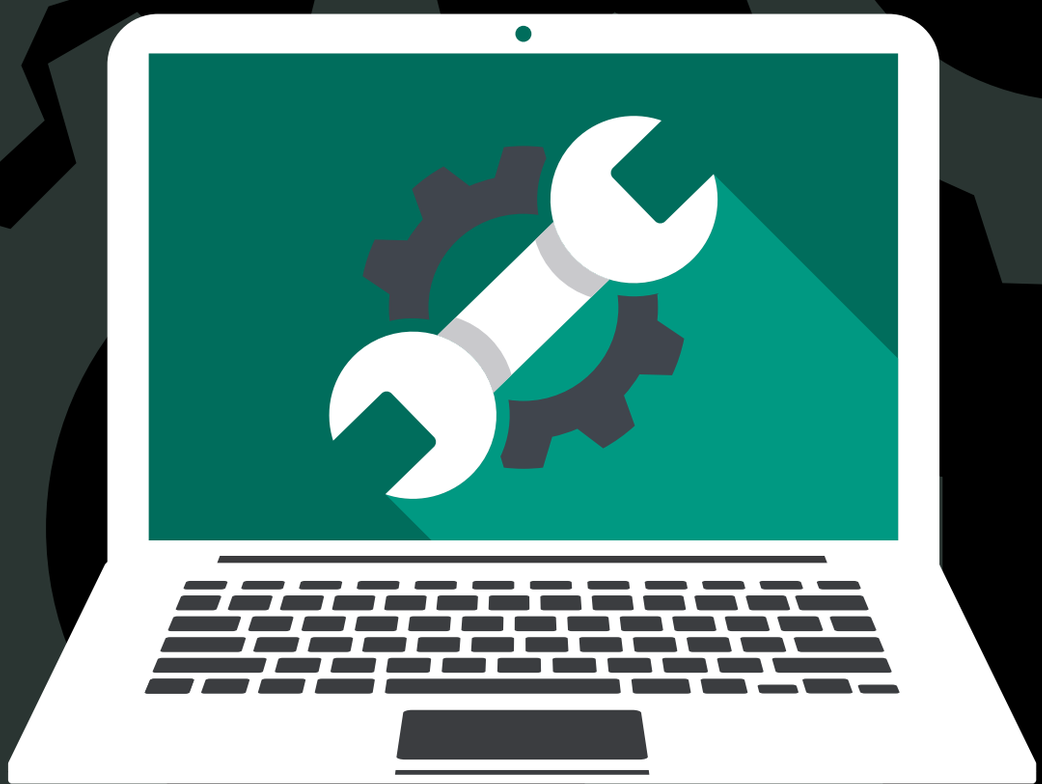
COMPUTER! TOTAAL
PCM
TIPS&TRUCS
Computer Idee

VEILIG ONLINE TOOLKIT



CHECKLIST: RANSOMWARE

Preventie en eerste hulp

BACK-UPPEN

Makkelijker dan je denkt!

+ KIES JE ANTIVIRUS OF INTERNETSECURITY?

BLIJF VEILIG ONLINE

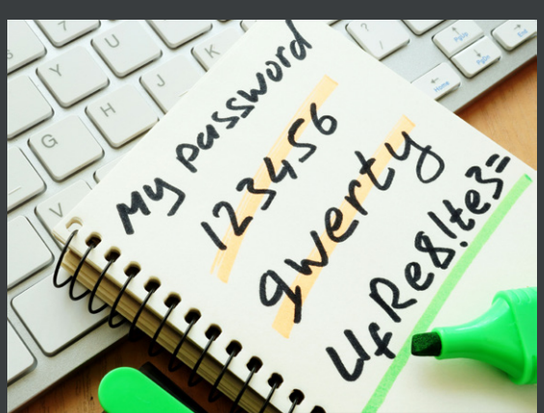
Simpele stappen voorkomen een hoop ellende

Je zou bijna geneigd zijn af te schrikken als je je verdiept in online bedreigingen, terwijl je je pc, laptop, tablet en smartphone een steeds grotere rol krijgt in leven. Van sociale contacten en (foto- en video)herinneringen tot bankzaken en belastingaangiftes. Met bewustwording, enkele simpele maatregelen én een actuele back-up nemen je zorgen al fors af. Met deze quickstart helpen we je daarmee op weg!



› Net als je huis op slot draaien: Maak het ze niet te makkelijk!

Dat online veiligheid een belangrijk thema is, wordt onderstreept door de Rijksoverheid, die zelf ook een campagne zijn gestart. Net als de campagne tegen inbraken, waarbij bijvoorbeeld werd geadviseerd de deur in het slot te draaien na het verlaten van je huis, geldt hier dezelfde slogan: “maak het ze niet te makkelijk”. Niet gek als je er over nadenkt, veel malwarebesmettingen en gegevensdiefstal vindt plaats door de gebruiker voor de gek te houden, met phishingsites bijvoorbeeld.



› Gebruik altijd een sterk wachtwoord en voorkom ‘hergebruik’.

Wachtwoord123

Maar ook als je niet voor de gek te houden bent, kun je het kwaadwillenden onbedoeld veel te makkelijk maken. Door je programma’s niet up-to-date te houden bijvoorbeeld, achteloos omgaat met malwarebescherming op je pc, of nog altijd wachtwoord123 als gebruiken voor al je accounts. En vergeet niet hoe makkelijk je het ransomware-beheerders maakt als je geen back-up hebt? Bovendien, hoe goed je je beveiliging ook in orde hebt: ransomware kan altijd toeslaan. De oorzaak achterhalen heeft dan niet je prioriteit, het veiligstellen van je data wel.

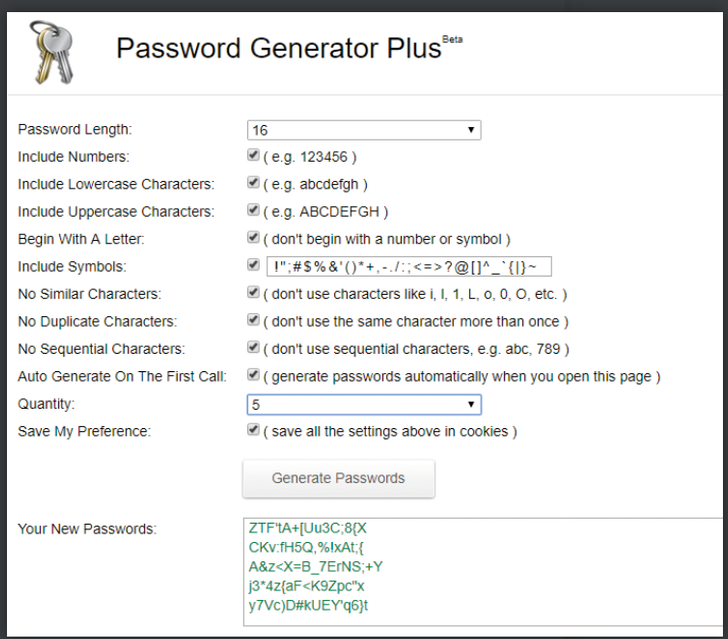
Met een paar simpele stappen ben jij geen makkelijk doelwit. Deze Quickstart helpt je hiermee, maar neem ook gerust een kijkje op de campagnesites van de Rijksoverheid zoals maakhetzeniettemakkelijk.nl en veiliginternetten.nl.

SLIM WACHT-WOORDBEHEER

(Ont)houd het veilig!)

Voor al die verschillende websites en diensten waar u een account hebt een verschillend wachtwoord bedenken, dat is niet meer te onthouden. Maar telkens hetzelfde wachtwoord gebruiken is ook geen optie, dat is onveilig. We stellen u daarom een paar systemen en (gratis) tools voor waarmee u toch veilig aan de slag kunt zonder uw geheugen te pijnigen.

TOON VAN DAELE

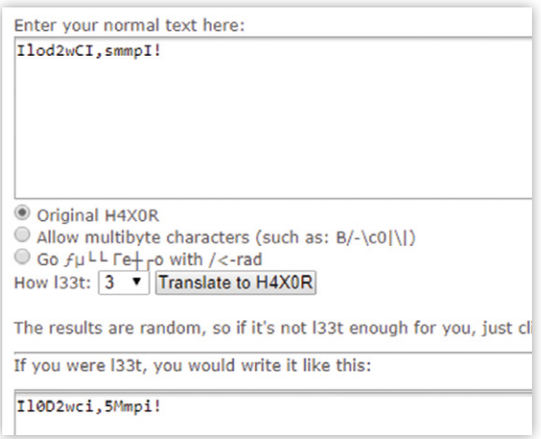


01 U hebt ijzersterke wachtwoorden nodig? Password Generator Plus levert ze!

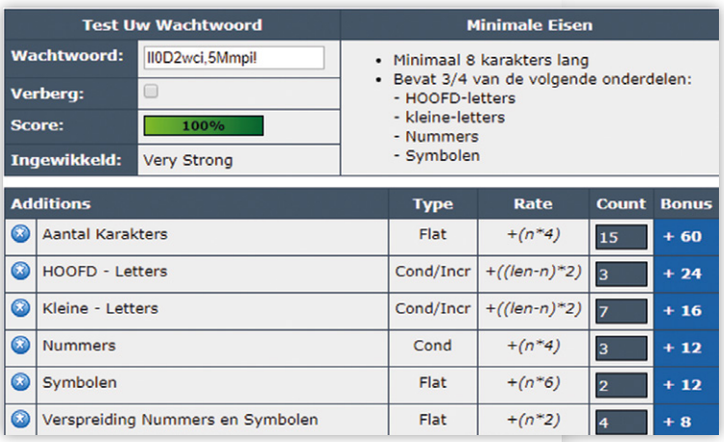
Veel gebruikers hanteren weliswaar een complex wachtwoord, maar zetten dat ene wachtwoord in voor verschillende diensten. Dat is uiteraard niet verstandig: krijgt een hacker dit wachtwoord in handen, dan kan hij zich toegang verschaffen tot al die services. Anderen gebruiken weliswaar een verschillend wachtwoord voor elke dienst, maar die blijken dan weer te gemakkelijk. Zo waren volgens beveiligingsexpert SplashData de vijf meest populaire wachtwoorden van 2017: 123456, password, 12345678, qwerty en 12345.

1 'Sterk' wachtwoord

Heel wat gebruikers hebben trouwens een verkeerd idee van wat een 'goed' wachtwoord is. Ze denken bijvoorbeeld dat de naam van hun huisdier veilig genoeg is, maar verliezen uit het oog dat dergelijke informatie vaak moeiteloos uit sociale media op te vissen valt. En hackers zijn heus wel bekend met trucjes als namen in omgekeerde volgorde of in combinatie met een cijfercode (zoals 123geheim). Vermijd ook woorden die letterlijk in een woordenboek staan. Immers, wanneer hackers de (versleutelde) database met wachtwoorden in handen krijgen, kunnen ze kraaktools inzetten die tegen een indrukwekkende snelheid alle woorden uit een woordenboek uitproberen.
Over het algemeen zijn beveiligingsspecialisten het er wel over eens dat een sterk wachtwoord minimaal 14 à 16 tekens dient te bevatten, in een combinatie van cijfers, symbolen, spaties, kleine letters en hoofdletters. Zo'n wachtwoord moet bovendien vrij zijn van herhaling, bestaande woorden, gebruikersnamen en id's. Er zijn hiervoor genoeg wachtwoordgenerators beschikbaar, zoals op **www.passwordsgenerator.net** (klik op **Advanced** als u meerdere wachtwoorden tegelijk wilt genereren) **(afbeelding 1)**.



› 02 Eventueel kunt u sommige letters door cijfers vervangen.



‹ 03 U kunt online controleren hoe sterk uw wachtwoord is.

2 Ezelsbruggetje

Zo'n willekeurig gegenereerd wachtwoord is natuurlijk wat lastig te memoriseren. Veel gebruikers hanteren daarom liever een 'ezelsbruggetje'. Hierbij gaat u uit van een zin en vormt u een wachtwoord met de eerste letter van elk woord uit die zin, eventueel aangevuld met een paar symbolen of leestekens. Een zin als **Ik lees om de 2 weken Computer Idee, samen met mijn partner Ina!** kan dan resulteren in een wachtwoord als **Ilod2wCI,smmpI!**.

Sommige tekens kunt u bovendien vervangen door een cijfer. Een S wordt een 5, een E wordt een 3 enzovoort. Dit wordt ook wel eens HaXoR of leet-speak genoemd. U vindt een online convertor op **www.ypass.net/misc/haxor**. Ons wachtwoord wordt dan iets als Il0D2wci,5Mmpi! **(afbeelding 2)**. Op een site als **www.wachtwoordtesten.nl**, waar u de sterkte van wachtwoorden kunt testen, leverde dit alvast een fraaie score van 100% op **(afbeelding 3)**.

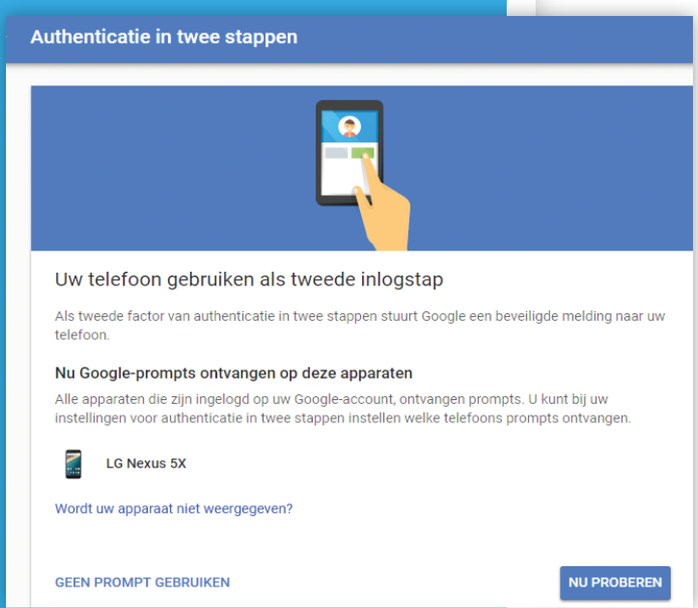
Natuurlijk, één sterk wachtwoord is nog haalbaar, maar het wordt wel heel lastig als u pak-hem-beet een dozijn van zulke exemplaren moet zien te onthouden. Toch zou dat nodig zijn, om te vermijden dat u in de kwalijke gewoonte vervalt uw wachtwoorden op een papiertje te noteren en op de rand van uw scherm te plakken. Gelukkig zijn er enkele methodes en tools die u bij dit wachtwoordbeheer kunnen helpen.

3 Basis+formule

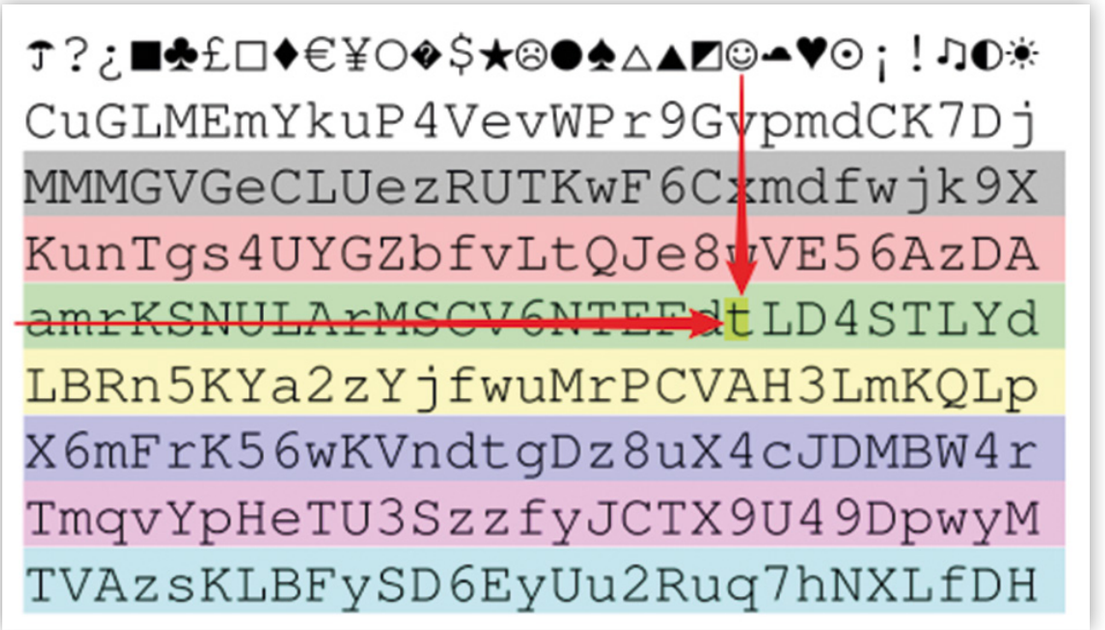
Een veelgebruikte methode is dat u een enkel basiswachtwoord gebruikt van bijvoorbeeld 10 tekens, waarna u een 'formule' bedenkt om daar een aantal tekens aan toe te voegen, bijvoorbeeld 2 vooraan en 2 achteraan. Deze formule baseert u op de naam van de service of app. Een voorbeeld: u neemt de laatste en de eerste letter van de naam, gevolgd door de derde letter en een cijfer dat het aantal letters in die naam aangeeft. Stel, uw basiswachtwoord is BgpZC3qZEz en

2FA

Hoe sterk uw wachtwoord ook is, 100% veilig wordt het nooit: als iemand uw wachtwoord in handen krijgt, kan diegene toegang krijgen tot de dienst waarvoor u het gebruikt. Daarom ondersteunen steeds meer services zogenoemde multifactorauthenticatie. Dat betekent dat u zich op meerdere manieren moet authenticeren voordat u toegang krijgt. In de meeste gevallen gaat het om tweefactorauthenticatie (2FA), wat inhoudt dat er twee methodes vereist zijn. Gewoonlijk is dat iets wat u weet (zoals een wachtwoord) in combinatie met iets wat u hebt (zoals een code die op dat moment naar uw mobiel wordt gestuurd). In een volgend nummer van Computer Idee gaan we verder in op tweefactorauthenticatie.



› Door tweefactorauthenticatie is uw account beter beveiligd dan met alleen een wachtwoord.



› 04 Onthoud de beginlocatie van uw 'formule' en de kaart doet de rest.

u wilt een wachtwoord voor **Fa**ce**b**oo**k**. De extra tekens zijn dan, in volgorde: k, F, c en 8. Het gecombineerde wachtwoord voor uw Facebook-account wordt dan: **kF**BgpZC3qZEz**c8**.

4 Persoonlijke wachtwoordkaart

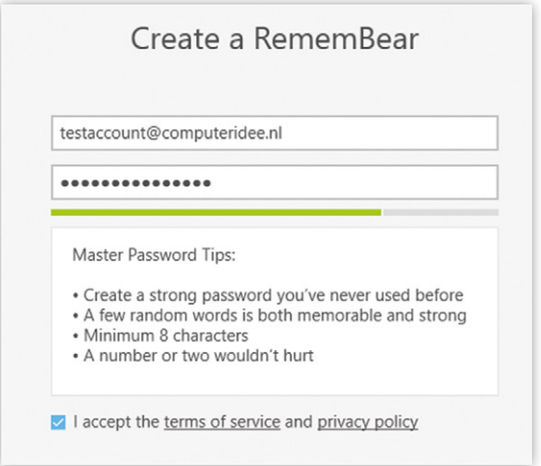
Een ander mogelijk systeem is een 'wachtwoordkaart' op (gelamineerd) papier, ter grootte van een creditcard, waarbij u een patroon van willekeurige letters, cijfers en symbolen noteert. Zo'n kaart kan bijvoorbeeld 30 kolommen en 10 rijen bevatten, waarbij u eventueel voor de bovenste rij opvallende symbolen gebruikt en u elke rij anders inkleurt. De bedoeling is nu dat u elke service associeert met een bepaald symbool uit de bovenste rij (zoals een lachende smiley) en een specifieke rijkleur (groen, bijvoorbeeld). Het eerste teken van het wachtwoord bevindt zich dan op het snijpunt van beide. Vervolgens past u voor elke service dezelfde 'leesformule' toe om de rest van uw wachtwoord te vinden, bijvoorbeeld '4 naar onderen en 9 naar rechts'. In ons voorbeeld zou dat dan worden: tA49q7hNXLfDHT) **(afbeelding 4)**.
Zorg er wel voor dat u een (al dan niet digitale) kopie van uw kaart op een veilige plaats bewaart voor het geval u uw kaart verliest.

5 Master Password

U kunt natuurlijk ook een programma inzetten om uw wachtwoorden te beheren, dan hoeft u nog minder te onthouden. Hier zijn heel veel tools voor; we bekijken de (wat minder bekende) gratis tool Master Password (**www.masterpasswordapp.com**), beschikbaar als webapp maar ook voor mobiele omgevingen, MacOS en Windows. We gaan aan de slag met de Windows-versie, die in de vorm van een Java-app komt.
Met een dubbelklik op het gedownloade bestand, start u de applicatie. Via het plusje voegt u eerst uw (volledige) naam toe, samen met een sterk hoofdwachtwoord. Vervolgens vult u de naam of url van de beoogde service in (bijvoorbeeld Facebook of www.facebook.com). Aan de hand van uw naam, wachtwoord en url berekent de tool vervolgens (op basis van cryptografische hashfuncties) een complex wachtwoord dat specifiek hoort bij de opgegeven naam of url van die service. Wanneer u zich met hetzelfde id bij Master Password aanmeldt, wordt voor dezelfde service (zoals Facebook) telkens hetzelfde wachtwoord gegenereerd **(afbeelding 5)**. Deze wachtwoorden worden dus niet opgeslagen en u hoeft ze ook niet te onthouden. Het proces is niet omkeerbaar: op basis van een gegenereerd wachtwoord kan noch de naam van de service noch uw hoofdwachtwoord worden berekend.



› 05 Wachtwoorden worden nergens opgeslagen maar telkens opnieuw berekend.



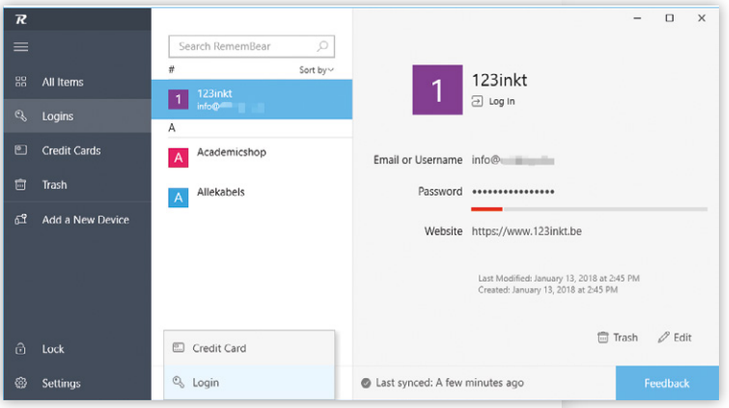
› 06 Wachtwoorden worden nergens opgeslagen maar telkens opnieuw berekend.

6 RememBear: installatie

Als laatste stellen we u een echte wachtwoordmanager voor: RememBear (**www.remembear.com**). Dit is een relatieve nieuwkomer, afkomstig van de makers van TunnelBear, een populaire vpn-service. Zoals de meeste andere wachtwoordbeheerders, bewaart de tool al uw id's in een database die wordt vergrendeld met uw eigen hoofdwachtwoord. De tool is beschikbaar voor Windows, macOS, iOS en Android. We geven eerst aan hoe u aan de slag gaat met de desktopvariant voor Windows. Meteen na de (eenvoudige) installatie start u RememBear op en klikt u **Create an Account** aan. Zo'n account is nodig omdat RememBear de id's die u gaat creëren – versleuteld – verstuurt naar een online database. Vul uw e-mailadres en hoofdwachtwoord in, bij voorkeur tot het balkje groen kleurt **(afbeelding 6)**. Bevestig dit wachtwoord en druk op **Confirm**. Het programma biedt via de knop **Open and Print PDF** een functie aan om dit wachtwoord te printen. Doe dit alleen als u denkt het niet te kunnen onthouden en bewaar het dan op een zéér veilige plek.

7 RememBear: logins

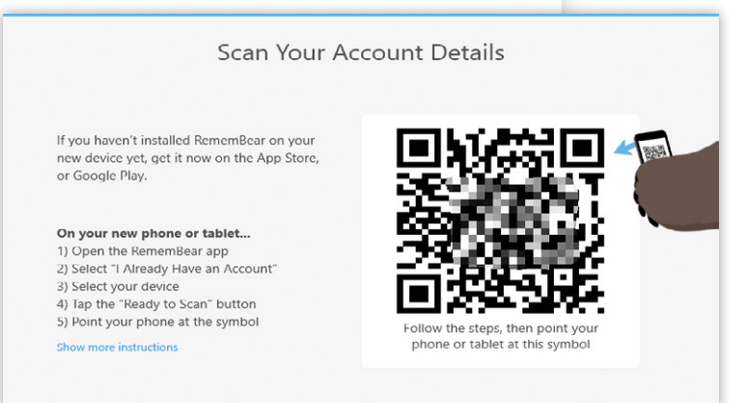
Meteen erna geeft de knop **Search For Logins** u al de gelegenheid allerlei inloggegevens te importeren die RememBear bijvoorbeeld uit uw browser(s) weet op te vissen. Vervolgens wordt u aangeraden de bijhorende plug-in voor uw browser(s) te installeren, die kan er namelijk voor zorgen dat logins automatisch in RememBear worden opgeslagen en voor u worden ingevuld. Zodra u met **Finish** bevestigt, belandt u in het hoofdvenster van de tool.
De geïmporteerde inloggegevens vindt u hier standaard in alfabetische volgorde **(afbeelding 7)**. Via het potloodicoon kunt u de gegevens altijd nog aanpassen. U hoeft hier trouwens maar een login aan te klikken om u meteen op de bijhorende webpagina in de browser aan te kunnen melden. Een nieuwe login (of creditcard-gegevens, want dat kan ook) voegt u toe via **Add New** of via de geïnstalleerde browserplug-in.



› 07 De inloggegevens die zich in de versleutelde database van RememBear bevinden.

8 RememBear: synchronisatie

Het feit dat RememBear uw wachtwoorden online bewaart, heeft natuurlijk als voordeel dat u ook onderweg uw bestaande logins kunt gebruiken. Overigens hoeft u zich niet al te veel zorgen over de veiligheid te maken: de database wordt met 256bit-encryptie versleuteld en dat geldt eveneens voor de synchronisatie tussen uw apparaten en de cloud.
We geven nog even aan hoe u de tool op een Android-toestel gebruikt. U vindt Remembear Password Manager in de Play Store. Na installatie van de app, meldt u zich met hetzelfde RememBear-account aan als op uw andere toestellen, zodat synchronisatie via de cloud mogelijk wordt. U kiest hiervoor **I Already Have an Account** en vervolgens **PC or Mac** bij **What is Your Other Device**. Open dan RememBear op uw pc en kies **Settings, Add a New Device**, **Phone or Tablet**. U krijgt een qr-code te zien die u via **Ready to Scan** op uw mobiele apparaat scant **(afbeelding 8)**. Niet schrikken: de beer hapt toe en u hoeft alleen nog maar uw hoofdwachtwoord in te vullen. Zodra u zich bij de app aanmeldt, duiken – na automatische synchronisatie – uw logins op. U kunt ermee aan de slag.



› 08 Via de qr-code kunt u beide apparaten op elkaar afstemmen.

CHECKLIST: RANSOMWARE

Preventie en eerste hulp

Je computer valt altijd te herstellen en in geval van absolute pech kun je onderdelen of het hele systeem vervangen. Het zijn je persoonlijke gegevens die onvervangbaar zijn. Laat daarom ransomware niet met je gegevens aan de haal gaan. Er zijn een paar zaken die je in acht moet nemen als je jouw gegevens tegen ransomware wilt beschermen.

Back-up

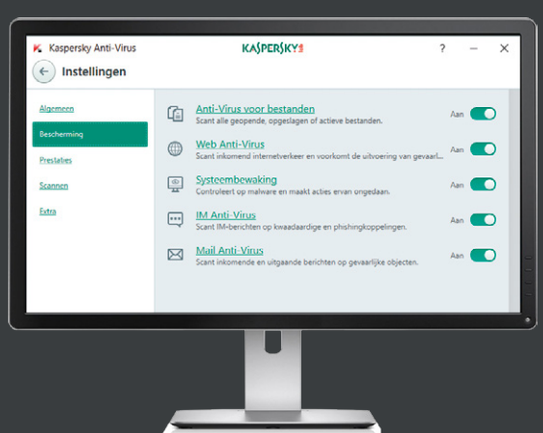
Te beginnen met de open deur die niet vaak genoeg herhaald kan worden: zorg altijd voor een recente back-up! Zorg ervoor dat je deze back-up niet bewaart op je systeem zelf (dus ook niet op bijvoorbeeld de D-schijf). Je kunt ervoor kiezen je back-up op een externe schijf te zetten, op een netwerkschijf of in de cloud. Iets wat je hierbij wel goed moet onthouden: als jij er via de verkenner zonder wachtwoord bij kunt, dan is ransomware daar ook toe in staat. En wanneer ransomware zowel je systeem als je back-up gijzelt, zit je toch met een fors probleem. Koppel daarom de externe schijf na gebruik altijd los van je pc en sluit deze alleen aan wanneer je er zeker van bent dat er geen malware op je computer staat. Zorg er ook voor dat de toegang tot netwerklocaties en cloudopslag via de verkenner, pas verkregen kan worden na apart inloggen.
Voor het maken van een back-up zijn verschillende goede (gratis) tools verkrijgbaar, zoals EaseUS Todo **Backup (www.tiny.cc/easeust).**



› Koppel na het maken van een back-up altijd je externe schijf los van de computer.

Beveiligingssoftware

Voorkomen is natuurlijk beter dan genezen, en dat geldt zeer zeker voor ransomware. Wanneer je met Windows werkt, zorg je dat er altijd een virusscanner actief is. Ook wanneer je denkt dat jij nooit getroffen zult worden. De meeste malware is zo ontwikkeld dat je niet door hebt besmet te zijn, met als doel bijvoorbeeld jouw systeem op te nemen in een botnet of gegevens af te kijken, zoals wachtwoorden en creditcardinformatie (meer info over botnets via: **www.tiny.cc/botn**). Een besmetting van ransomware heb je overigens meestal wel meteen door: er verschijnt een venster met de vraag om te betalen en je kunt niet meer bij je bestanden.
Wanneer je Windows gebruikt, is het dus enorm belangrijk om beveiligingssoftware te installeren. Daarvoor zijn diverse betaalde en gratis programma's. Windows 7



‹ Gebruik altijd een goede virusscanner om ransomware voor te zijn. ›

heeft standaard geen malwarebescherming aan boord. Windows 8 en Windows 10 zijn uitgerust met Windows Defender. Deze beveiliger heeft een wisselende reputatie opgebouwd, en was in het verleden lang niet altijd goed in het snel ontdekken van malware zoals ransomware. Defender kun je zien als basisbeveiligingsoplossing, maar ook op deze versies van Windows is het veiliger om andere antivirussoftware te installeren. Om met een veiliger gevoel online bankzaken te regelen of voor bescherming tegen ransomware kun je het best beveiligingssoftware kiezen die specifiek tegen deze vorm van cybercriminaliteit beschermt. Dit doet bijvoorbeeld de software van **Kaspersky Lab**, dat recentelijk uit onze virusscanner-test als beste uit de bus kwam en bescherming biedt tegen ransomware voordat het kan toeslaan. Ook het onafhankelijke testlab AV-test beoordeelt Kaspersky al jaren goed, met zelfs de hoogst mogelijke score, terwijl het oordeel over Windows Defender schommelt **(www.tiny.cc/avtest).**



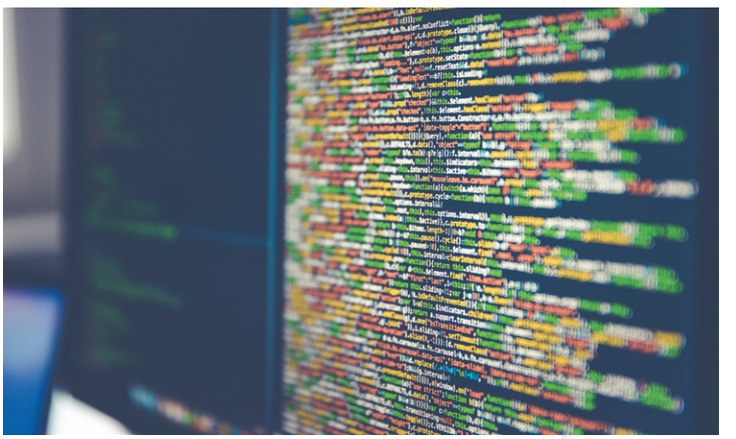
› NoMoreRansom is een initiatief om de schade van ransomware te beperken.

Eerste hulp bij besmetting

Welke maatregelen je ook treft tegen ransomware, het kan altijd gebeuren dat je systeem of dierbare bestanden gekaapt worden door criminelen die er geld voor terug willen zien. Dit kan bijvoorbeeld gebeuren als malware een nog onontdekte kwetsbaarheid uitbuit in Windows, of als er een advertentieserver gehackt wordt waarna een advertentie op een onschuldige website malware op je systeem zet. Maar het kan natuurlijk ook een menselijk foutje zijn, wanneer je bijvoorbeeld in een moment van onoplettendheid de bijlage van een niet-onschuldig mailtje opent.

De oorzaak van ransomwarebesmetting doet er op zo'n moment ook niet meer toe. Je dierbare bestanden zijn gegijzeld. En die wil je terug. De criminelen het geëiste losgeld (meestal in bitcoins) betalen wordt niet aanbevolen, je hebt immers geen garantie dat je na betaling wel de toegang terugkrijgt via een ontsleutelcode.

Mocht je systeem getroffen zijn door ransomware, pak dan eerst de bron aan. Stuur je virusscanner op de besmetting af. Schakel eventueel eenmalig de hulptroepen van Emsisoft Emergency Kit in (een portable malwarescanner, **www.tiny.cc/eek**). Start je systeem



helemaal niet meer, dan kun je met Kaspersky Rescue Disk 10 **(www.tiny.cc/rescuedisk)** een opstartbare cd of usb-stick maken, die vervolgens je pc opschoont. Zo'n disk kun je nu alvast maken en achter hand houden, of na besmetting op een ander systeem maken.

NoMoreRansom

Het lastige deel is het terugkrijgen van je versleutelde bestanden. Als je geluk hebt zijn de ontsleutelscodes gekraakt door beveiligers en gepubliceerd op **www.nomoreransom.org**. Deze site is door samenwerking met onder andere Kaspersky Lab en politiediensten in het leven geroepen, met als doel zowel te informeren over de gevaren van ransomware als slachtoffers sleutels te bieden om gegevens te herstellen. Zonder te hoeven betalen natuurlijk. Op dit moment staan er 52 gratis decryptietools online die kunnen worden gebruikt om 84 ransomware-varianten te decoderen. Hier zijn afgelopen februari de vrijgegeven decryptiesleutels voor de Cryakl-ransomware aan zijn toegevoegd. Ruim 35.000 mensen zijn er intussen in geslaagd hun bestanden gratis terug te halen via deze site, waardoor betrokken criminelen meer dan 10 miljoen euro zijn misgelopen.

Herstelpunten niet voldoende

Systeemherstel is een praktisch onderdeel van Windows 7, 8 en 10. Gaat er iets mis, bijvoorbeeld met een update of installatie van een programma? Geen zorgen: Systeemherstel brengt je min of meer terug in de tijd naar een opgeslagen systeemherstelpunt. Het is een handige functie die je in verschillende situaties uit de brand kan helpen. Maar zie het als een laatste noodgreep om je systeem weer werkend te krijgen. Je persoonlijke bestanden bescherm je er niet mee: ransomware houdt ze dus in zijn greep. Bovendien ben je afhankelijk van de gemaakte herstelpunten: worden deze ook door de malware gegrepen of heb je geen actuele herstelpunten?

Dan kun je niet meer terug.

SURFEN ZONDER POTTENKIJKERS

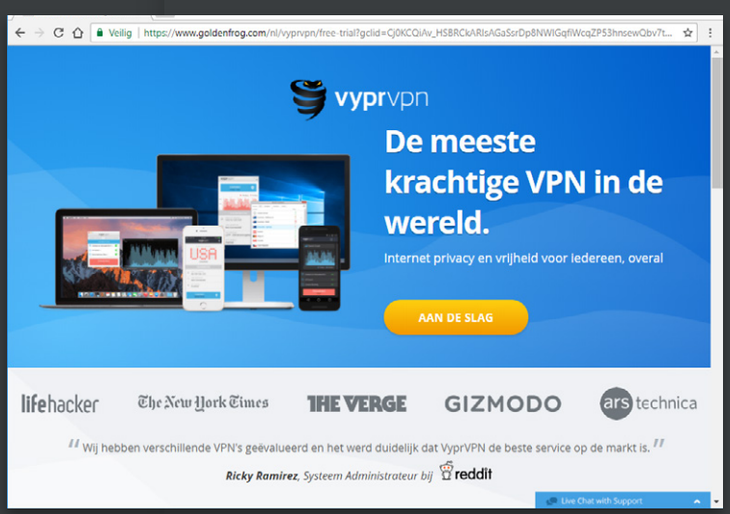
Stel vpn in op al je apparaten

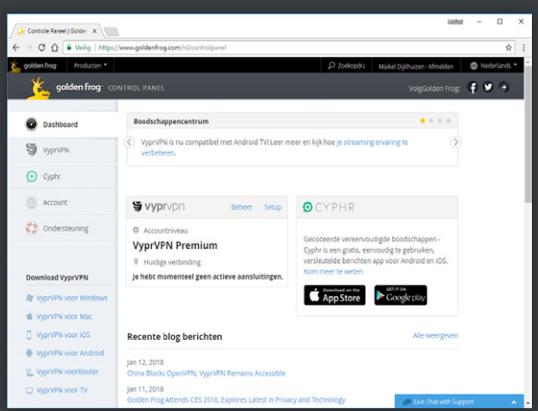
Met de naderende sleepwet speelt de overheid straks nog meer voor Big Brother dan het nu al doet. Zit je niet op pottenkijkers te wachten, dan maskeer je het dataverkeer eenvoudig met een vpn-dienst. Door via de server van de vpn-dienst te surfen, blijf je anoniem. In deze workshop leggen we uit hoe je zo'n beveiligde verbinding instelt op een computer, tablet, smartphone én router.

MAIKEL DIJKHUIZEN

1 Vpn-provider kiezen

Er zijn talloze vpn-providers op de markt, wat de keuze nu niet bepaald eenvoudiger maakt. Let naast een betaalbaar tarief vooral op de specificaties van de beoogde aanbieder. Voor deze workshop is het belangrijk dat er in elk geval ondersteuning is voor het betrouwbare OpenVPN-protocol. Je kunt dan namelijk gegarandeerd een vpn-verbinding op elke pc, laptop, tablet en smartphone realiseren. Zelfs geschikte routers voorzie je van een vpn-verbinding, zodat je in één klap het dataverkeer van alle netwerkapparatuur beveiligt. Geschikte vpn-providers zijn onder meer AirVPN, BlackVPN, CyberGhost, VyprVPN en ExpressVPN.





2 Aanmelden

Heb je eenmaal een geschikte vpn-aanbieder gevonden, dan is het zaak om jezelf te registreren. Sommige aanbieders hanteren diverse abonnementen, die onderling verschillen in het aantal serverlocaties en de hoeveelheid gelijktijdige verbindingen. Vul je persoonlijke gegevens in en geef aan op welke wijze je wilt betalen. Dat kan doorgaans via een creditcard, PayPal of bitcoin. Na aanmelding sturen de meeste aanbieders een bevestiging per e-mail. Als je het account bevestigt, heb je toegang tot een online bedieningspaneel. Naast betaalinformatie vind je hier vaak Engelstalige instructies om een vpn in te stellen.

Windows-client

In deze workshop gaan we aan de slag met de software OpenVPN om een vpn-verbinding voor een Windows-machine op te tuigen. Veel aanbieders hebben een eigen client voor Windows ontwikkeld. Als alternatief kun je die natuurlijk ook gebruiken. Na de installatie vul je de juiste inloggegevens in, waarna je de mogelijkheid hebt om de vpn-verbinding in te schakelen. Bij de serverlocatie bepaal je vanuit welk land je wilt surfen. Verder kies je ook het gewenste vpn-protocol. Naast OpenVPN heb je meestal keuze uit pptp (minder veilig) en l2tp/ipsec.



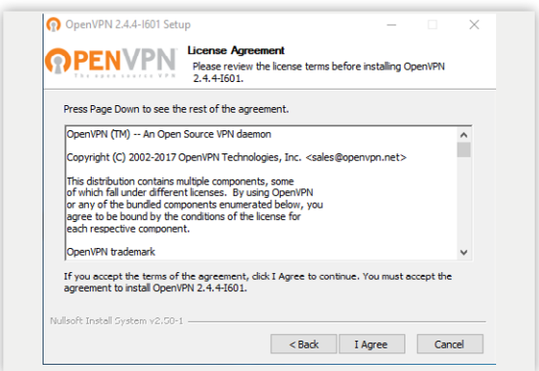
WINDOWS 10

3 Ovpn-bestand

Voor het instellen van een vpn-verbinding gebruiken we de gratis software OpenVPN. Je dient hiervoor een apart configuratiebestand bij de vpn-dienst op te halen, namelijk een zogeheten ovpn-bestand. De meeste vpn-aanbieders, waaronder VyprVPN, hebben een aparte webpagina ingericht waar je een zip-archief kunt downloaden. Na het uitpakken van dit zip-archief staan er vaak twee mappen voor je klaar. Hierbij heb je de keuze tussen 160bit- en 256bit-encryptie. Laatstgenoemde versleutelingsmethode is de veiligste optie. Open de map en je ziet dat er meerdere ovpn-bestanden voor verschillende landen beschikbaar zijn. Sommige vpn-aanbieders hebben als alternatief een online assistent waarmee je het gewenste ovpn-bestand kunt genereren, zoals CyberGhost.

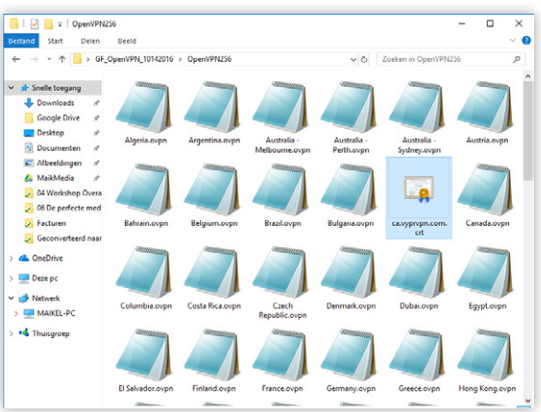
4 OpenVPN installeren

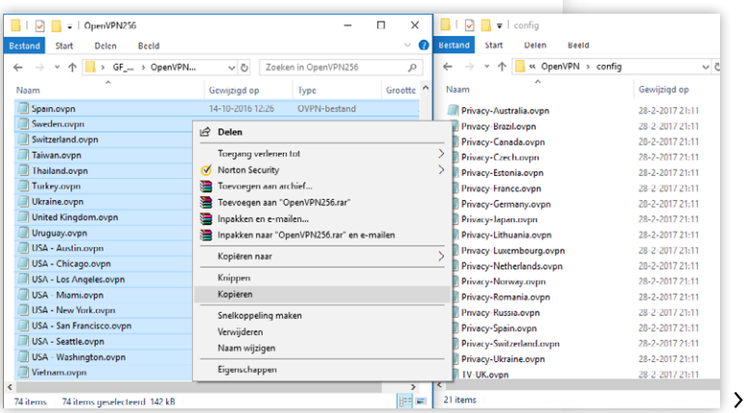
De website van de software OpenVPN is enigszins misleidend, want de downloadknop op de beginpagina leidt naar clientsoftware van een specifieke vpn-aanbieder. In deze workshop gaan we echter met de opensource-software van OpenVPN aan de slag. Die is compatibel met alle vpn-aanbieders die het OpenVPN-protocol ondersteunen. Surf naar de webpagina **www.tiny.cc/opvpn** en klik bij **Installer**, **Windows Vista and later** op de downloadlink. Na het openen van dit exe-bestand doorloop je enkele standaardinstellingen om de installatie in orde te maken. Vink hierbij voor de zekerheid alle installatie-onderdelen aan. Na afloop start je het programma nog niet op.



5 Ovpn-bestanden kopiëren

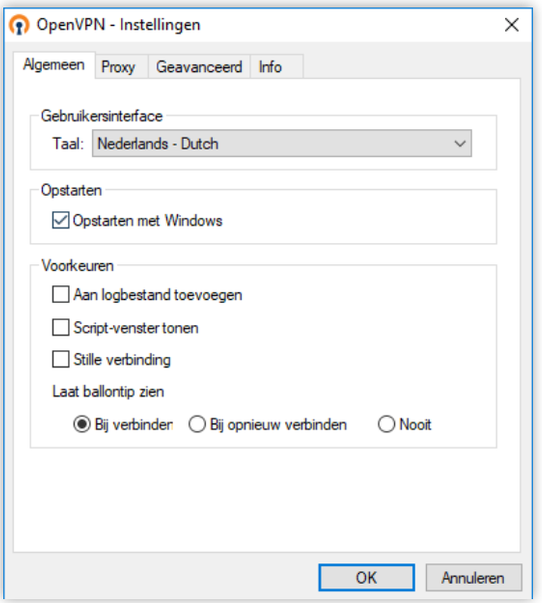
De ovpn-bestanden van je vpn-provider plaats je in een systeemmap van het programma OpenVPN. Open Windows Verkenner en ga naar C:\Program Files (x86)\OpenVPN of C:\Program Files\OpenVPN om de juiste locatie te openen. Heb je tijdens de installatie een andere locatie gekozen, dan zoek je zelf de juiste map op. Kies vervolgens voor de map **Config**. Aan deze bestandslocatie voeg je alle configuratiebestanden van je eigen vpn-provider toe. Mogelijk vraagt Windows om administrator-machtigingen. Klik in dat geval op **Doorgaan**. Je mag maximaal vijftig ovpn-bestanden toevoegen.





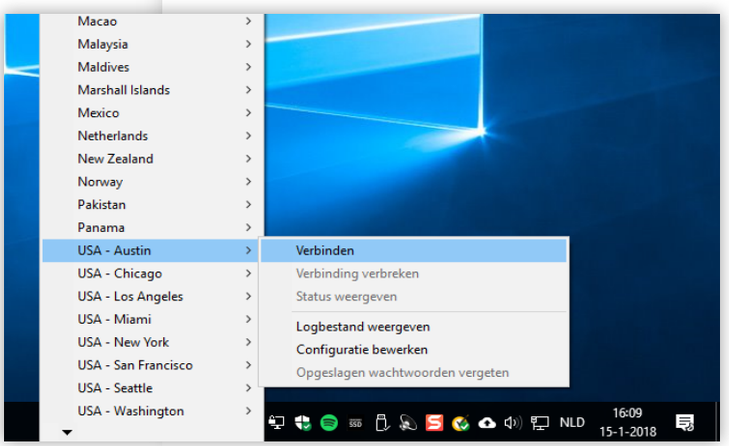
6 OpenVPN opstarten

Hoog tijd om met de software aan de slag te gaan. Navigeer in het startmenu naar OpenVPN en klik met de rechtermuisknop op **OpenVPN GUI**. Je kiest vervolgens voor **Meer / Als administrator uitvoeren** en bevestigt met **Ja**. Je ziet dat er rechtsonder in het systeemvak een extra pictogram is bijgekomen, namelijk een beeldscherm met een slotje. Wanneer je dit pictogram niet ziet, klik je eerst op het kleine pijltje **Verborgen pictogrammen weergeven**. Start je OpenVPN in het vervolg graag automatisch met Windows op? Klik met de rechtermuisknop op het systeemvakpictogram en kies voor **Instellingen**. Zet een vinkje voor **Opstarten met Windows** en bevestig met **OK**.



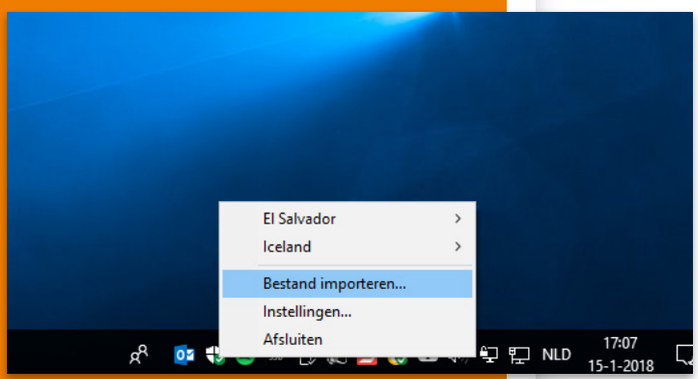
7 Vpn-server kiezen

Voor het kiezen van een vpn-server gebruik je het systeemvakpictogram. Klik erop met de rechtermuisknop en bekijk welke vpn-servers er beschikbaar zijn.



Later ovpn-bestand toevoegen

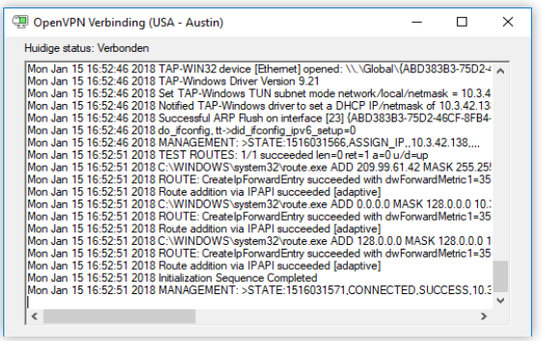
In deze workshop leggen we uit hoe je ovpn-bestanden naar de systeemmap van OpenVPN kopieert. Geen zin om in Windows Verkenner naar diepliggende bestandslocaties te graven? Je kunt een enkel ovpn-bestand ook naderhand toevoegen via de gebruikersinterface van OpenVPN. Start het programma op als administrator. Er verschijnt een melding dat er geen leesbare verbindingsprofielen zijn gevonden. Via **OK** klik je met de rechtermuisknop op het OpenVPN-pictogram. Je kiest nu voor **Bestand selecteren** en wijst een ovpn-bestand aan. Bevestig met **Openen**. De bijbehorende vpn-server is nu in het contextmenu van OpenVPN beschikbaar.



Zeker als je eerder meerdere ovpn-bestanden hebt toegevoegd, is de lijst wellicht lang. Bedenk goed via welk land je wilt surfen en ga er met de muisaanwijzer heen. Je kiest voor **Verbinden**, waarna je de juiste inloggegevens invult. Meestal zijn dat dezelfde inloggegevens die je tijdens de registratie bij je vpn-provider hebt opgegeven. Bij sommige aanbieders heb je misschien bij het genereren van een ovpn-bestand een aparte gebruikersnaam en wachtwoord aangemaakt. In dat geval vul je die in. Klik op **OK**.

8 Veilig surfen

Als OpenVPN een correcte vpn-verbinding heeft opgezet, kleurt het systeemvakpictogram groen. Afhankelijk van de gebruikte vpn-aanbieder is de internetverbinding nu mogelijk iets trager. Wil je graag weten welk (buitenlands) ip-adres je computer momenteel gebruikt? Ga met de muisaanwijzer op het OpenVPN-pictogram staan en de informatie verschijnt als ballontip in beeld. Verder staat ook aangegeven in welk land de vpn-server is gehuisvest.

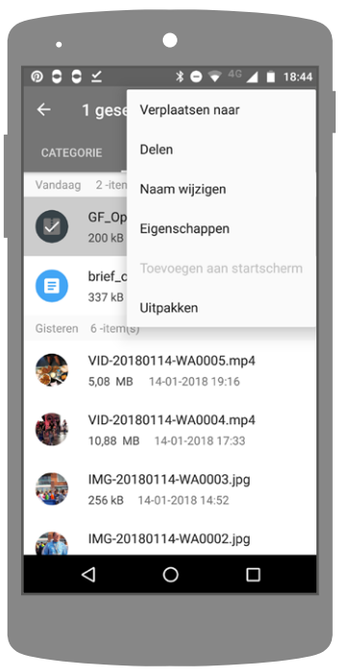


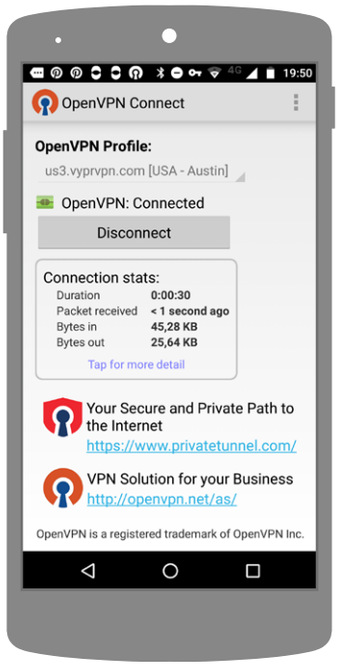
Wil je de vpn-verbinding weer afbreken? Dubbelklik op het pictogram om het venster met statusinformatie op te roepen. Kies daarna voor **Verbreken**.

ANDROID

9 Android

Ook een smartphone of tablet met Android voorzie je desgewenst van een vpn-verbinding. Allereerst is het een vereiste om de configuratiebestanden van je vpn-provider op je mobiele toestel te krijgen. In Android kan dat op meerdere manieren. De simpelste methode is om naar de downloadpagina van je vpn-provider te gaan, waarna je de benodigde ovpn-bestanden op je toestel bewaart. In het geval van een ziparchief open je de app Bestandsbeheer op het Android-toestel. Zoek het ziparchief op en selecteer dat bestand. Via het pictogram met de drie puntjes kies je voor **Uitpakken**. Nadat je de bestandslocatie hebt gekozen, sluit je af met **OK**.



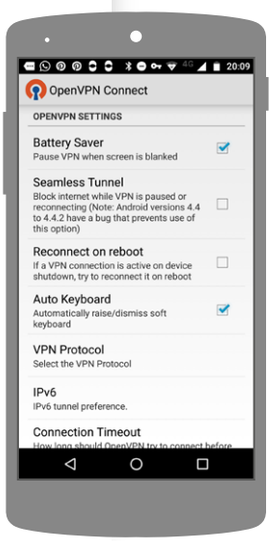


10 OpenVPN Connect

Je gebruikt OpenVPN Connect om verbinding met een vpn-server te maken. Download en installeer deze app vanuit de Play Store. Zodra je OpenVPN Connect opent, kom je in een Engelstalige gebruikersomgeving terecht. Tik rechtsboven op het pictogram met de drie puntjes en kies **Import / Import Profile from SD card**. Blader nu naar de locatie met configuratiebestanden en geef aan welk ovpn-bestand je wilt toevoegen. Via **Select** vul je daarna de inloggegevens van de vpn-provider in. Zet een vinkje voor **Save** wanneer je de inloggegevens wilt bewaren. Wanneer je het verbindingsverzoek accepteert, kies je voor **Continue**. De vpn-verbinding is nu actief.

11 Batterijbesparing

Zodra je vanuit Android een vpn-verbinding opzet, verschijnt er bovenaan in de statusbalk een klein pictogram met een sleutel. In OpenVPN Connect tik je op **Tap for more detail** om het ip-adres en serverinformatie op te vragen. Een nadeel is dat de vpn-verbinding continu actief is, dus ook wanneer je het toestel niet gebruikt. De accu raakt hierdoor sneller leeg. Bij inactiviteit kun je de vpn-verbinding daarom beter even pauzeren. Tik rechtsboven op het pictogram met de drie puntjes. Via **Preferences** vink je de instelling **Battery Saver** in. Telkens wanneer je het mobiele toestel gebruikt, activeert OpenVPN Connect op de achtergrond de vpn-verbinding.



Mobiele app

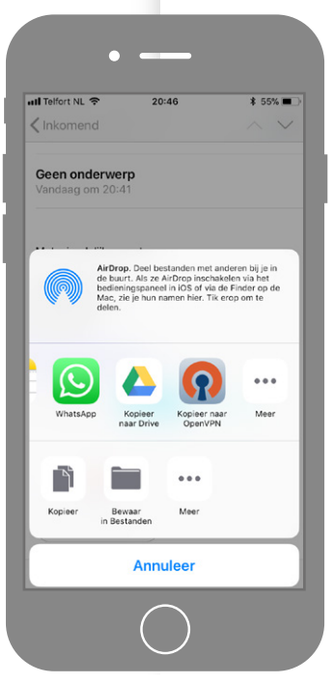
Nagenoeg elke grote vpn-aanbieder heeft voor iOS en Android een eigen mobiele app. Die kun je als alternatief voor OpenVPN Connect gebruiken. Typ in de App of Play Store maar eens de naam van je vpn-provider en installeer deze toepassing op je mobiele toestel. Na opgave van de inloggegevens kies je een vpn-server uit het gewenste land en pas je eventueel het vpn-protocol aan. In Android accepteer je het verbindingsverzoek. In iOS is het noodzakelijk om een vpn-configuratie toe te voegen. De meeste vpn-apps voeren dit proces automatisch uit, waardoor je niets handmatig hoeft te configureren.



iOS

12 Mailbijlage

OpenVPN Connect is ook beschikbaar voor iOS (iPhone en iPad). Je downloadt de app vanuit de App Store.



In tegenstelling tot Android is het toevoegen van een ovpn-bestand wel iets omslachtiger, aangezien je niet direct toegang hebt tot de mappenstructuur van iOS. Het heeft dus weinig zin om naar de downloadpagina van de vpn-aanbieder te surfen. De gemakkelijkste methode is door het configuratiebestand naar jezelf te mailen. Open de Mail-app en tik vervolgens op de bijlage. Kies daarna voor **Kopieer naar OpenVPN** om het ovpn-bestand te importeren. Hoewel dit erg vlot werkt, is er wel een klein risico op onderschepping.

13 Bestandsdeling iTunes

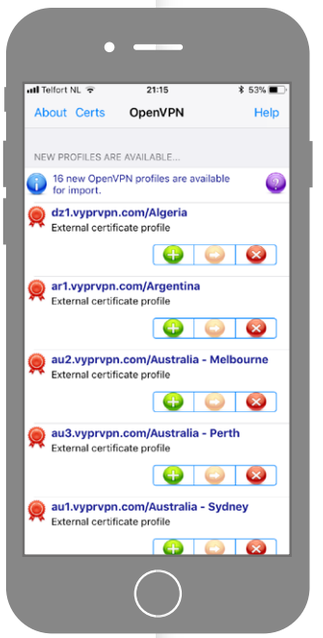
Wie meer veiligheid wenst, voegt de configuratiebestanden rechtstreeks via een usb-verbinding aan de iPhone



of iPad toe. Je gebruikt hiervoor iTunes (www.apple.com/nl/itunes/download). In dit programma open je de inhoud van je iOS-apparaat. Kies onder **Instellingen** voor **Bestandsdeling**. Alle apps waarnaar je documenten kunt overzetten verschijnen in beeld, waaronder dus in elk geval OpenVPN. Klik daarop en selecteer via **Bestand toevoegen** alle configuratiebestanden. Zodra je bevestigt met **Openen** en **Synchroniseren** hevelt iTunes de data over naar het mobiele Apple-apparaat.

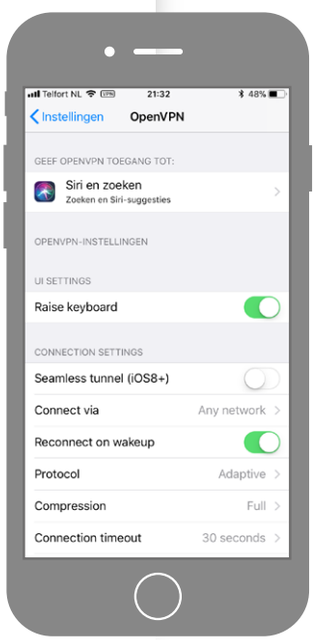
14 Vpn in iOS

Open OpenVPN Connect en bekijk welke configuratiebestanden er beschikbaar zijn. Het importeren van een ovpn-bestand is eenvoudig: tik op het plusteken. Via **Allow** geef je OpenVPN Connect toestemming om een vpn-configuratie aan het mobiele toestel toe te voegen. Log hiervoor in met je Apple-wachtwoord of vingerafdruk. Vanuit de apparaat-instellingen keer je automatisch terug naar de app. Je veegt indien nodig een stukje omlaag om de gebruikersnaam en het wachtwoord van de vpn-provider op te geven. Activeer de schakelaar achter **Save**. Gebruik de onderste schakelaar en kies **Yes** om de vpn-verbinding te activeren. In de statusbalk van iOS verschijnt het vpn-logo.



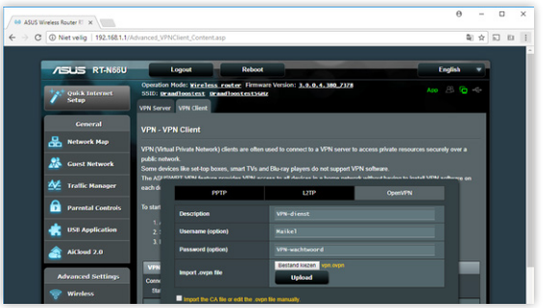
15 Instellingen

Op toestellen met Android open je binnen de app eenvoudig de instellingen van OpenVPN Connect, maar op een iPhone of iPad werkt dat anders. Tik vanuit het beginscherm van iOS op **Instellingen** en veeg een flink stuk omlaag. Via **OpenVPN** krijg je alle beschikbare opties te zien. Bij **Connect** geef je bijvoorbeeld aan dat



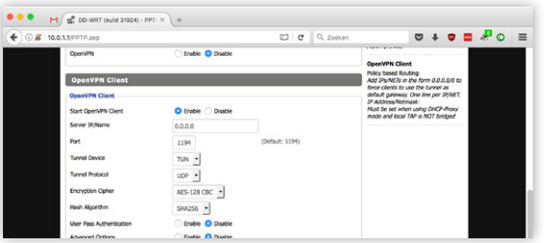
je alleen binnen een wifi-netwerk een vpn-verbinding wilt gebruiken. Verder stel je bij **Compression** de mate van compressie in om eventueel het dataverbruik te verminderen. Je past ook allerlei geavanceerde instellingen aan, al is het voor doorsneegebruikers verstandig om daar niet mee te rommelen.

ROUTER



16 Asuswrt

Sommige moderne routers kun je instellen als vpn-client. Aangezien al het dataverkeer via de vpn-server verloopt, gebruiken hiermee alle apparaten binnen het thuisnetwerk vpn. Denk bijvoorbeeld aan een Chromecast, smart-tv en gameconsole. Een voorbeeld is ASUS, dat veel van zijn routers voorziet van de firmware asuswrt. Hierin kun je een openvpn-client instellen. Typ in een browser het ip-adres van de router (meestal http://192.168.1.1) en log vervolgens in. Je navigeert dan achtereenvolgens naar **Advanced Settings / VPN / VPN Client**. Via **Add profile** heb je op het tabblad **OpenVPN** de gelegenheid om met **Upload** een ovpn-bestand toe te voegen. Na het invullen van een beschrijving en de inloggegevens bevestig je met **OK**. Klik in de vpn-serverlijst als laatste op **Activate**.

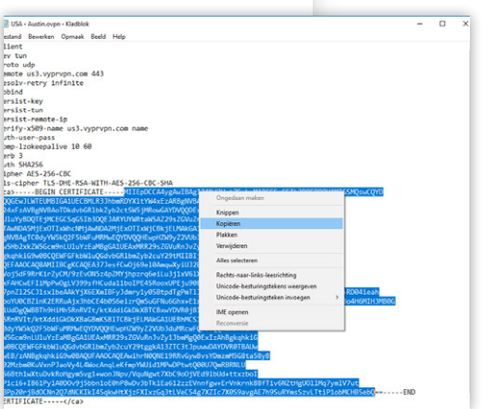


17 Dd-wrt

Wie geluk heeft, kan zijn router 'flashen' met de alternatieve firmware dd-wrt. Via het OpenVPN-protocol stel je dan een vpn-verbinding voor je complete thuisnetwerk in. Log in op het bedieningspaneel van je router en navigeer naar **Services / VPN**. Vervolgens selecteer je **Enable** achter **Start OpenVPN Client**. Vul nu zo veel mogelijk eigenschappen van de vpn-server in, zoals de servernaam, het poortnummer (meestal 1194 of 443), de versleutelingsmethode en de inloggegevens. Hoe je aan alle gevraagde informatie komt, lees je in de volgende stap.

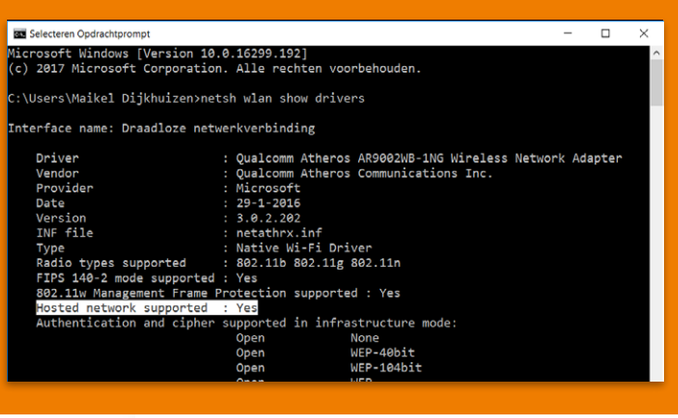
18 Kladblok

Dd-wrt wil nogal wat gegevens over de vpn-server weten. De juiste informatie tref je aan in het betreffende ovpn-bestand. Open dit bestand in Kladblok en klik bovenaan op **Opmaak / Automatische terugloop**. Je vindt tussen de codes <ca> en </ca> het ca-certificaat. Die kopieer je naar dd-wrt. Gebruik hiervoor het veld bij **CA Cert in DD-WRT**. Ook de velden bij **Public Client Cert** en **Private Client Key** vul je indien nodig op deze wijze in, al zijn de gegevens wellicht in aparte configuratiebestanden van de vpn-provider beschikbaar. Als alles in ingevuld, klik je op **Save / Apply Settings**. Ga naar **Status / OpenVPN** om de vpn-verbinding te controleren.



Mobiele app

Nagenoeg elke grote vpn-aanbieder heeft voor iOS en Android een eigen mobiele app. Die kun je als alternatief voor OpenVPN Connect gebruiken. Typ in de App of Play Store maar eens de naam van je vpn-provider en installeer deze toepassing op je mobiele toestel. Na opgave van de inloggegevens kies je een vpn-server uit het gewenste land en pas je eventueel het vpn-protocol aan. In Android accepteer je het verbindingsverzoek. In iOS is het noodzakelijk om een vpn-configuratie toe te voegen. De meeste vpn-apps voeren dit proces automatisch uit, waardoor je niets handmatig hoeft te configureren.



BACK-UPPEN IS MAKKELIJKER DAN U DENKT!

Wees de ramp voor

U zult zien: precies op het moment dat uw computer het begeeft, hebt u geen back-up van uw gegevens! Tegenwoordig is het maken van back-ups echt geen lastige klus meer, dus wees dit doemscenario voor ...

MARK GAMBLE

Back-upsoftware is lang niet zo ingewikkeld als vaak wordt gedacht. Bovendien hoeft u er niet de hoofdprijs voor te betalen. Veel fabrikanten stellen namelijk een gratis versie van een betaald pakket beschikbaar. Soms kunt u de software dan maar een bepaalde periode gebruiken, maar bij Aomei Backupper werkt dat eigenlijk op een vriendelijkere manier: de software kunt u onbeperkt gebruiken, maar bepaalde opties zijn alleen toegankelijk als u de professionele versie aanschaft.

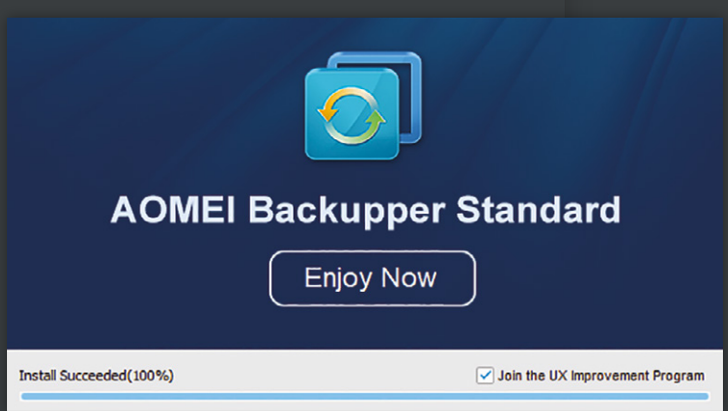
De gratis versie van Aomei Back-upper biedt voldoende opties voor het maken van een volledige systeem-back-up van uw Windows-partitie. Het programma maakt daarbij dan een volledig snapshot, met daarin het complete Windows-systeem, alle bijbehorende programma's en uw documenten. De software vindt u op www.backup-utility.com/free-backup-software.html. Kies daar voor de knop Download Freeware. De download is ongeveer 85 MB groot.

Kies tijdens de installatie voor de taal Engels, klik op de knop OK en vervolgens op Install Now. Desgewenst kunt u nog een andere locatie opgeven, maar de standaard Program Files-map voldoet prima. De installatie verloopt snel en na afloop wordt er automatisch een webpagina geopend met meer informatie, zodat u eventueel de Engelstalige hulp kunt lezen.

U kunt het programma nu direct starten met de knop Enjoy Now, maar rechts onderin staat nog een vinkje ingeschakeld met de tekst 'Join the UX Improvement Program'. Hiermee geeft u de maker van Aomei Backupper toestemming om alles wat u met de software doet, op te slaan en te gebruiken om de software verder te verbeteren. Helaas kunt u nergens precies zien wat dat allemaal inhoudt, dus om uw privacy te beschermen, kunt u die optie beter uitschakelen.

Hoofdscherm

Vanuit het hoofdscherm hebt u direct toegang tot de back-up-opties van Aomei Backupper. Let wel: dit is de gratis versie waarin niet alle functies beschikbaar zijn! De opties die voor thuisgebruik het handigst zijn, kunt



Zet het vinkje uit bij Join the UX Improvement Program als u niet wilt dat de software bijhoudt wat u doet.

u echter wel gewoon gebruiken. Die nemen we dan ook met u door.
Onder de knop Backup vindt u de interessantste opties terug, namelijk die voor het maken van back-ups. Zo kunt u een kopie van uw Windows-systeemschrijf maken, waarbij dan zowel de bootpartitie als de Windows-partitie zelf worden geback-upt. U kunt de back-up-taak bovenin een naam geven bij het veld Task Name, bijvoorbeeld Systeemback-up van Windows. Het programma selecteert automatisch de juiste partities, u hoeft alleen nog een locatie op te geven waar het back-upbestand moet worden opgeslagen. Dat doet u bij Step 2. Dat mag in principe iedere locatie zijn, zoals een externe harde schijf of een netwerkstation, zolang er maar genoeg schijfruimte vrij is. Een echte back-up hoort natuurlijk sowieso op een locatie los van uw eigen computer te worden opgeslagen; het is dus onverstandig om de back-up op te slaan op de harde schijf van de computer waarvan u een back-up maakt! Een back-up kunt u eenvoudig opslaan naar een nas die u aan een schijfletter van Windows gekoppeld hebt. Als uw nas niet via een schijfletter is gekoppeld, kunt u ook de directe maplocatie opgeven, bijvoorbeeld \\NAS\MAP, waarbij NAS de naam is van uw nas in het netwerk en MAP de naam van de map op die nas waar u toegang tot hebt. Indien dat nodig is, moet u ook nog een gebruikersnaam en wachtwoord invoeren.

Systeemback-up maken

De omvang van de back-up is ongeveer even groot als de ruimte die de bestanden innemen op de partities. De bootpartitie van Windows 10 is standaard zo'n 500 MB groot; daar telt u dan nog de ingenomen ruimte op de C-schijf bij op. U weet dan ongeveer hoeveel ruimte u nodig hebt voor de com-plete systeemback-up. Op ons testsysteem duurde het maken van de back-up met een totale grootte van 65 GB zo'n dertig minuten.



Een systeemback-up van uw Windows-partitie maken gaat eenvoudig.

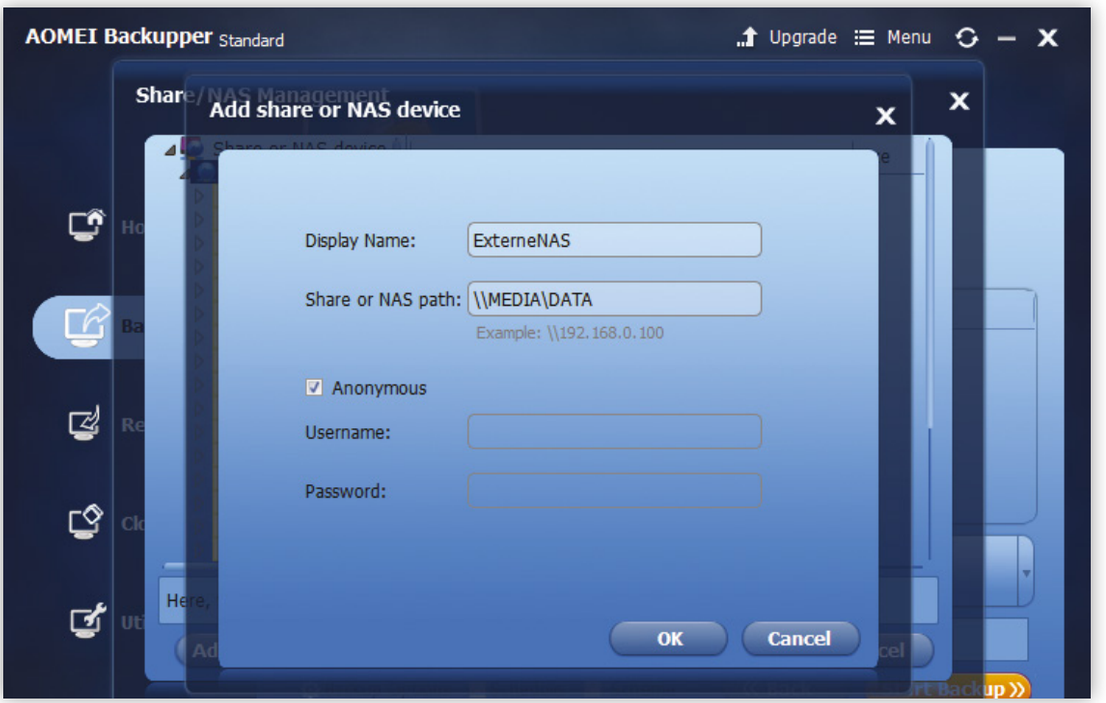
Na afloop is de back-up opgeslagen in een enkel bestand dat de naam heeft die u eerder hebt opgegeven. De extensie is .afi. In dat bestand zijn alle partities en losse bestanden alsmede de bestandstabel opgenomen.
U krijgt in Aomei Backupper netjes een melding te zien dat de back-up is voltooid. De inhoud kunt u meteen bekijken doordat u de gemaakte back-up direct kunt koppelen aan Windows Verkenner. Via de knop Advanced op het hoofdvenster en Explore Image bij een geselecteerde back-up koppelt Aomei Backupper de gemaakte back-up aan een schijfletter. In de verkenner zelf kunt u dan gewoon door de back-up bladeren alsof het een gewone schijf is. U hebt zelfs de keuze welke driveletter(s) u aan het back-up-image wilt toekennen.
U hoeft zich overigens geen zorgen te maken dat u de back-up 'stukmaakt', want het gekoppelde back-upbestand is ingesteld als alleen lezen. U kunt dus geen bestanden (per ongeluk) uit die back-up verwijderen of aanpassen, maar alleen zien welke bestanden er in de back-up zijn opgenomen.

Gratis met wat beperkingen

Hoewel de gratis versie van Aomei Backupper veel mogelijkheden biedt voor het maken en terugzetten van back-ups, is een aantal functies alleen beschikbaar in de betaalde versie. Zo is het in de gratis versie bijvoorbeeld niet mogelijk om een kloon (exacte kopie) van uw systeempartitie te maken en die naar een andere computer te kopiëren. Zo'n functie kan handig zijn als u meerdere computers van eenzelfde Windows-installatie wilt voorzien, met alle programma's en drivers inbegrepen. Voor thuisgebruik is dat wellicht wat minder interessant. Daarnaast kunt u niet meerdere back-ups samenvoegen in een enkele back-up en u kunt ook geen bootable usb-stick of dvd maken. Bestanden filteren kan ook niet. Tot slot kan deze gratis versie van Aomei Backupper niet overweg met dynamische schijven, maar bij thuissituaties komt dat sowieso weinig voor. Functies die u in de gratis versie niet kunt gebruiken, worden aangeduid met een tekst 'Pro'. Als u wel alle functies van Aomei Backupper wilt gebruiken, betaalt u 58 euro. Voor dat bedrag mag u de software op twee computers gebruiken en hebt u recht op 'levenslang' gratis support en updates.



Als een bepaalde functie niet beschikbaar is in de gratis versie, krijgt u daar een melding van.



› Geef het pad naar de nas op als u die niet aan een schijfletter van Windows hebt gekoppeld.

Herstellen

Het terugzetten van de systeemback-up is eveneens een fluitje van een cent, dat kan direct vanuit Windows. Het programma geeft netjes een overzicht van de partities die worden teruggezet en naar welke plek op de harde schijf dat gebeurt.

Voor het terugzetten moet de computer wel opnieuw worden opgestart. U krijgt daarbij de keuze welk bootsysteem daarvoor gebruikt moet worden: een Linux-systeem of een Windows PE-bootable-systeem. In principe maakt het niet zoveel uit welke optie u kiest, maar wij hebben gemerkt dat de Linux-versie net even wat vlotter werkt. Wees niet bang, u hebt geen kennis van Linux nodig om een back-up terug te zetten: u hoeft alleen een keer op een knop te klikken om het herstel te bevestigen.

Back-uptypes

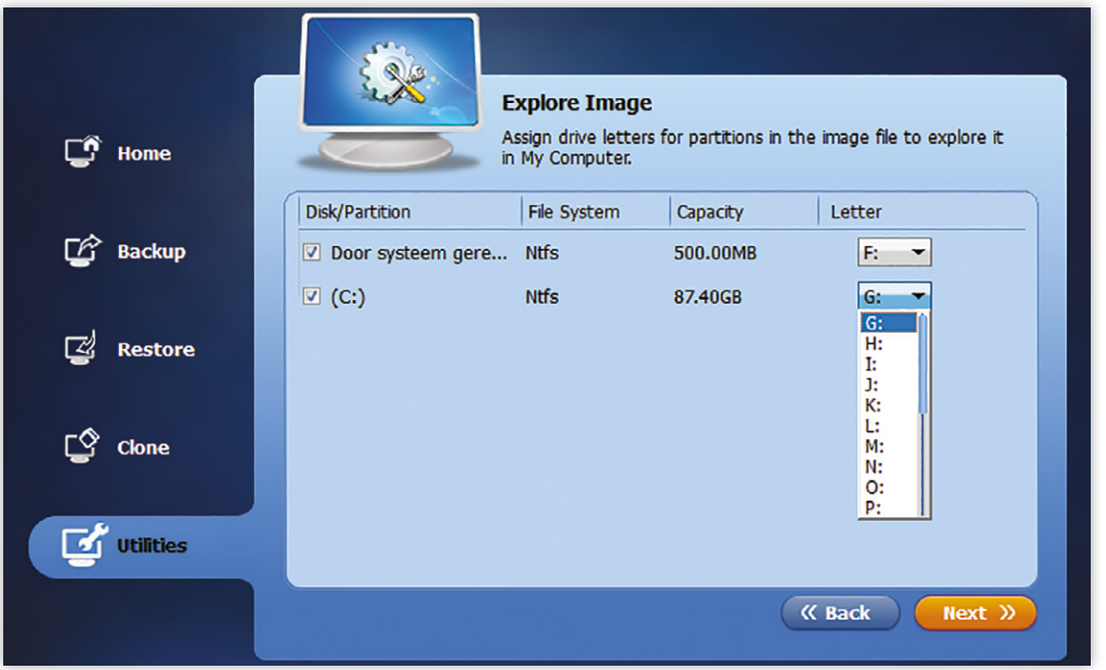
Het kan in sommige gevallen – bijvoorbeeld bij een crash van uw computer – handig zijn om een back-up van uw systeempartitie achter de hand te hebben. Nog belangrijker echter is het regelmatig back-uppen van uw persoonlijke bestanden. Windows en uw programma's kunt u relatief eenvoudig opnieuw installeren, maar uw dierbare foto's kunt u maar één keer maken. Om die reden zijn 'normale' back-ups van uiterst belang. Ook hiermee kan Aomei Backupper u helpen. U kunt namelijk diverse soorten back-ups maken: een complete back-up van een enkele partitie, bijvoorbeeld uw data-partitie; een back-up van alle partities (dus een kopie van uw hele schijf, inclusief alle partities) of back-ups van losse bestanden en mappen. En in dat laatste geval kunt u ook nog kiezen voor synchronisatie, waarbij alle bestanden telkens automatisch worden bijgewerkt. Bij al die soorten back-ups kunt u bovendien ook schema's instellen, zodat Aomei Backupper automatisch op de door u ingestelde tijden de gegevens voor u wegschrijft zonder dat u er omkijken naar hebt.



› Het back-uppen verloopt vlotjes.

Bestandsback-up

Om een normale back-up van bestanden op uw harde schijf te maken, gaat u vanuit het hoofdscherm naar Backup en kiest u daar voor File Backup. Bij Step 1 kiest u welke mappen en/of bestanden u in de back-up wilt hebben, via de knoppen Add File of Add Folder. Bij het back-uppen van een map kunt u er ook nog voor kiezen om alle submappen in de back-up op te nemen.

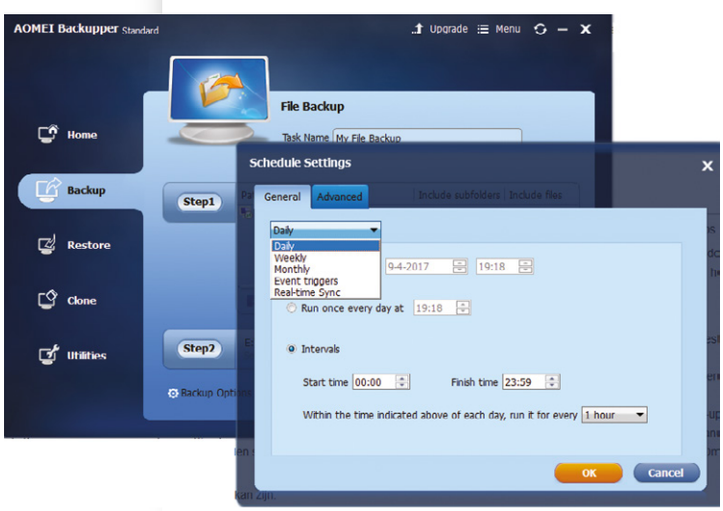


U kunt de inhoud van de gemaakte back-up bekijken door er een schijfletter aan te koppelen.

Het filteren op bepaalde bestandstypes kan niet: die functionaliteit
is voorbehouden aan betalende gebruikers (zie ook het kader Gratis met wat beperkingen).
Hebt u alle bestanden en mappen geselecteerd? Dan kunt u bij Step 2 de locatie van de back-up opgeven. Ook hier geldt dat dit de harde schijf mag zijn, een externe usb-schijf of een netwerkstation. Ook handig: door op het (vrij kleine) knopje Schedule te klikken, kunt u automatische back-ups instellen. Hiermee kunt u dus opgeven of de back-up dagelijks, wekelijks of maandelijks moet worden uitgevoerd. En als u klikt op Intervals is het zelfs mogelijk om dit ieder uur te doen. Op het tabblad Advanced kunt u zelfs nog bepalen of u er een incrementele, differentiële of een complete back-up van wilt maken.
Hebt u de instellingen voor de back-up naar wens aangepast, dan kunt u op de knop Start Backup klikken. Let op, als u een back-upschema hebt gemaakt, dan zal de back-up pas worden gemaakt als de opgegeven tijd en dag is bereikt. Is een back-up succesvol of zijn er juist problemen? Het is mogelijk om daar een e-mailnotificatie van te ontvangen.



Stel een schema in om Aomei Backupper automatisch te laten back-uppen.



U kunt nog veel meer instellen, zoals automatische e-mailnotificaties als een back-up gelukt of mislukt is.

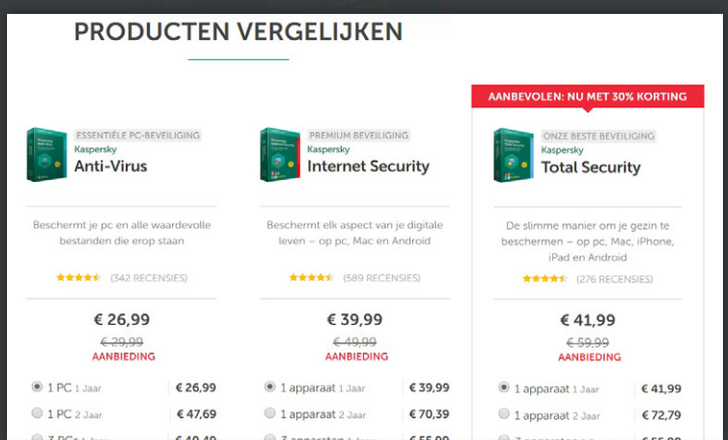
Op de achtergrond

Als u eenmaal back-upschema's hebt ingesteld, dan kunt u die altijd terugvinden op het startscherm van Aomei Backupper. Het programma hoeft niet op de voorgrond te draaien om back-ups te maken, dus u merkt er weinig van. Het programma installeert zich namelijk als een vaste service in het besturingssysteem, waardoor de back-ups altijd zullen worden gemaakt zonder dat u de interface van het programma open hoeft te hebben.

KIES JE ANTIVIRUS OF INTERNET SECURITY



Dat malwarebescherming op je pc nog altijd noodzakelijker dan ooit is, mag duidelijk zijn. Veel beveiligingsbedrijven bieden naast antivirus ook uitgebreidere pakketten aan, zoals Internet Security of nóg uitgebreidere Total Security. Is deze beveiliging de meerprijs waard?



Verschillende soorten beveiliging, maar wat is de slimste (en veiligste) keuze?

Zoals de naam al weggeeft, bevat antivirussoftware beveiliging die malware moet voorkomen en (als malware toch heeft toe kunnen slaan) genezen. PC's zijn een kwetsbaar en geliefd doelwit voor malwaremakers, die graag zichtbaar of juist onzichtbaar toe willen slaan. Met ransomware bijvoorbeeld, die je systeem gijzelt en een betaling in Bitcoin eist. Zonder dat je het door hebt kan malware echter ook toeslaan, bijvoorbeeld om je systeem op te nemen in een botnet (dat bijvoorbeeld gebruikt wordt om met ddos-aanvallen banken plat te leggen met een enorme hoeveelheid dataverkeer), of als spyware om zo stiekem inlog- en betaalgegevens te kapen. Zelfs Windowsmaker Microsoft heeft ingezien dat malwarebescherming noodzakelijk is en rust Windows sinds Windows 8 standaard uit met Windows Defender. Dat scheelt alvast in de beveiliging. Dit antivirusprogramma behaalt echter wisselende resultaten in tests en is wel erg basaal. Wie een betrouwbaardere beschermer zoekt is beter af bij **Kaspersky**, dat met Kaspersky Anti-Virus een beter alternatief biedt om je pc malwarevrij te houden.



Windows 8 en Windows 10 zijn standaard voorzien van een virusscanner, maar is deze veilig genoeg?

Internet Security

Voor een meerprijs bieden Kaspersky en andere malwarebestrijders ook Internet Security-pakketten aan. Meer beveiliging dan de antivirus die we kennen, maar waartegen eigenlijk? En is dit zijn meerprijs waard? Het idee achter Internet Security is om je naast tegen malware, ook te beschermen tegen andere online bedreigingen. Want helaas is malware niet de enige boosdoener voor je pc. Het aanbod van extra's en de kwaliteit hiervan verschilt per aanbieder. Zo is Kaspers-



Diefstalbeveiliging: denk eraan voordat het te laat is!

ky's Internet Security bijvoorbeeld uitgerust met een browser-omgeving die gemaakt is om veilig te kunnen internetbankieren of andere betaalzaken te regelen.

Phishing

Een andere aanhoudende bedreiging is phishing, waarbij je met nepmailtjes of nagemaakte sites verleid wordt om in te loggen of andere persoonsgegevens achter te laten. Wat identiteitsdiefstal, of zelfs hacks tot gevolg kan hebben. Je moet er niet aan denken dat anderen zo je Facebook kapen, inloggen bij je bank of zelfs een telefoonabonnement op jouw naam afsluiten om zo dure betaalnummers te bellen. Internet Security beschermt hier ook tegen, door phishingsites te herkennen en blokkeren.

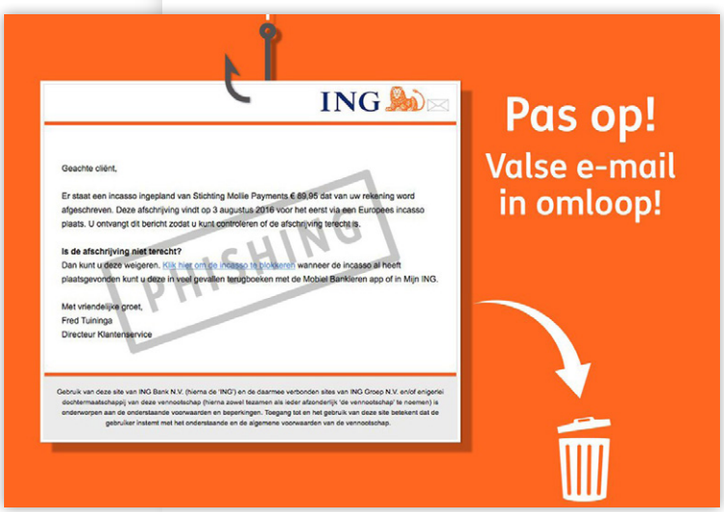
Phishing is helaas geen onbekend fenomeen. Een andere vorm van datadiefstal waar minder mensen mee bekend zijn, zijn open draadloze netwerken, waar je vaak mee verbindt als je op een mobiel apparaat werkt. Wanneer je verbinding maakt met een draadloos netwerk, kan iedereen die met hetzelfde netwerk verbonden is jouw dataverkeer inzien. Van bezochte internetpagina's tot verstuurde mailtjes. Zelfs als het open netwerk een inlogpagina laadt nadat je ermee verbindt. Kaspersky's Internet Security zorgt er ook voor dat dit verkeer op een open netwerk afgeschermd wordt.

Veilig voor kinderen

Kaspersky Internet Security beschikt ook over ouderlijk toezicht, waardoor je je (klein)kinderen ook achter de pc kunt laten zetten. Net als de zojuist genoemde phishingsites worden ook andere sites geblokkeerd in ingestelde categorieën, zoals geweld en seks. Ook kun je met accounts ingeven wie wat mag doen en zien op de pc en op welke tijden.

Extra's

Internet Security is vooral voor je Windows-apparaat belangrijke extra beveiliging. Maar je licentie werkt op vrijwel al je apparatuur. Zo is je Mac (die even kwetsbaar is als je pc) tegen dezelfde gevaren beschermd en desgewenst zijn er apps voor iOS en Android die je (onder andere) waarschuwen voor onbeveiligde draadloze netwerken. Vooral als je je bedenkt dat het naast uitgebreide bescherming ook beveiliging biedt tegen diefstal van bijvoorbeeld je laptop, tablet of smartphone. Via de browser (van een ander apparaat natuurlijk) spoor je de locatie op van je verloren apparaat. Bovendien kun je deze ook op afstand beheren, om het apparaat terug te vinden of zelfs de inhoud te wissen, zodat je belangrijke mailtjes, foto's en de andere hoogstpersoonlijke gegevens niet zomaar in handen van een ander vallen. Voor ieder mobiel apparaat is goede diefstalbeveiliging eigenlijk onmisbaar.



Bij phishing denk je al gauw aan ouderwetse imitatiemailtjes, maar er wordt op meerdere manieren naar je gegevens gehengeld.

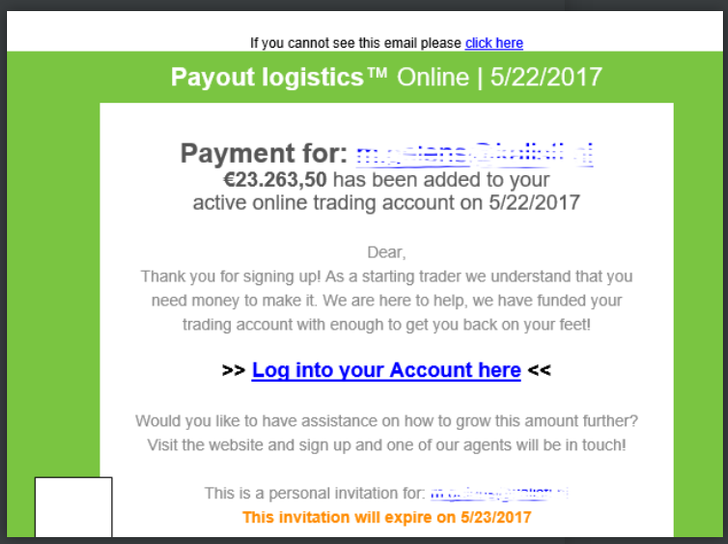
VOORKOMEN IS BETER DAN GENEZEN

Blijf ransomware voor

Met de WannaCry malware-aanval van afgelopen voorjaar staat ransomware helemaal in de belangstelling. Malwarebesmettingen die bestanden gijzelen en losgeld eisen, zijn al een tijd zeer populair bij criminelen. Het kost beveiligers moeite om computers automatisch tegen deze aanvallen te beschermen. We kijken wat je zelf kunt doen om ransomware voor te blijven.

MERIJN GELENS

Virussen, wormen, spyware en andere aanvallen op besturingssystemen worden samengevat onder de naam malware. Dat bestaat uit grofweg uit twee delen: een vector en een payload. De vector is de manier waarop de malware zich verspreidt. Denk daarbij onder meer aan een website die bij bezoek ongewenste code plaatst (drive-by-download), software die zich automatisch via het internet/netwerk verspreidt (worm) of code die zich in een gewenste toepassing verstopt (virus). Een malwarevariant kan verschillende vectoren hebben. Naast de vector is er een payload: datgene wat de malware doet. In het geval van ransomware (ook vaak cryptomalware genoemd) versleutelt het bestanden of het hele systeem en eist het losgeld. De eerste geregistreerde ransomware-aanval werd in 1989 uitgevoerd met behulp van geïnfecteerde floppydisks. Een aids-onderzoeker verspreidde 20.000 floppy's onder medeonderzoekers in meer dan 90 landen. De malware activeerde pas nadat een computer 90 keer herstart was. Deze aanval kreeg, vanwege zijn oorsprong, de naam AIDS Trojan. Ransomware is vooral de laatste tijd een zeer populaire payload. Reden om stappen te nemen zodat je zelf een besmetting kunt voorkomen.


If you cannot see this email please click here

Payout logistics™ Online | 5/22/2017

Payment for: [redacted]
€23.263,50 has been added to your active online trading account on 5/22/2017

Dear,
Thank you for signing up! As a starting trader we understand that you need money to make it. We are here to help, we have funded your trading account with enough to get you back on your feet!

>> Log into your Account here <<

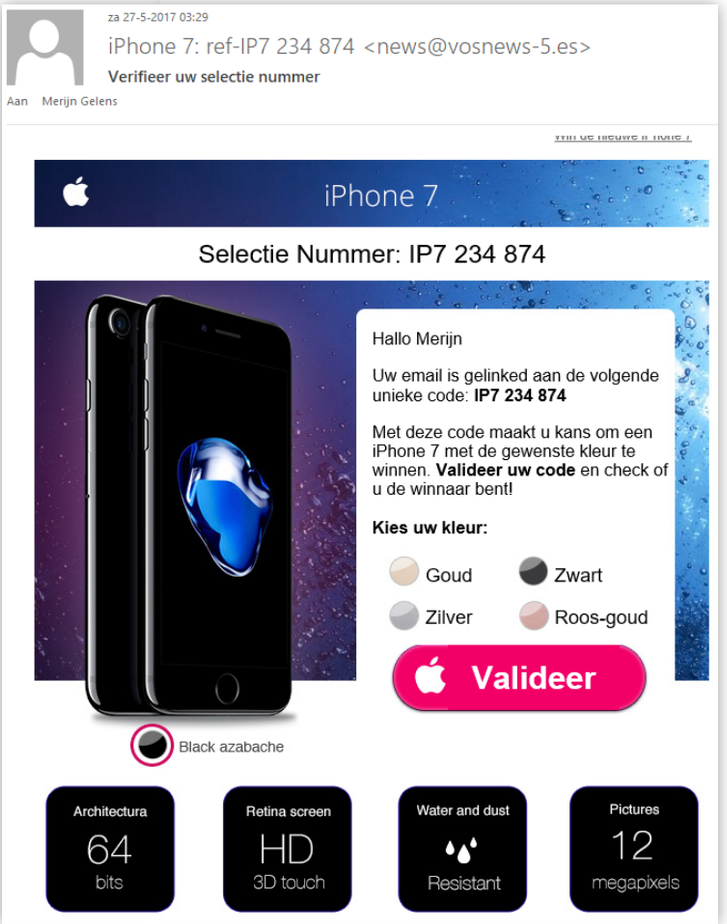
Would you like to have assistance on how to grow this amount further? Visit the website and sign up and one of our agents will be in touch!

This is a personal invitation for: [redacted]
This invitation will expire on 5/23/2017

1 Blijf scherp

De meest gebruikte manier van malware infecteren is door middel van een e-mail met daarin een 'rekening' of link naar een malafide website. Een flink deel van deze mails is eenvoudig herkenbaar omdat ze niet aan jou geadresseerd zijn, vol spelfouten staan of van een zeer raar mailadres afkomen (de bank gebruikt altijd

^ 01 Veel besmettingen met malware zijn eenvoudig te voorkomen door verdachte e-mail direct te wissen. >



01 Win je een prijsvraag waar je niet eens aan deelnam? Het is waarschijnlijker dat de 'valideer'-link naar een malafide website verwijst.



02 Maak gebruik van de automatische updates om zwakke plekken in je systeem automatisch te dichten.

zijn eigen domein voor mail!). Wie zijn nieuwsgierigheid niet kan bedwingen (en volgens de cijfers van beveiligers zijn dat een hoop mensen), infecteert zijn systeem. Met proactieve scans probeert antivirussoftware mensen tegen zichzelf te beschermen. Mail en links worden centraal in de gaten gehouden en bij een mogelijke dreiging geblokkeerd. Maar voor die dreiging geconstateerd wordt, vallen er al enkele slachtoffers. Die eerste slachtoffers fungeren als digitale kanarie in de kolenmijn. Door scherp te blijven voorkom je niet iedere besmetting, maar verlaag je wel je kans om die rol te vervullen.

2 Automatische updates

Het is niet zo eenvoudig om op een modern besturingssysteem ongewenste activiteit uit te voeren. Om zichzelf te installeren, misbruikt malware fouten in code. Daarbij hebben de criminelen achter de malware een voorkeur voor veelgebruikte software. Want hoe meer gebruikers een softwarepakket op de computer hebben staan, hoe groter de kans natuurlijk is dat de malware zijn slag kan slaan. Door fouten bij ontdekking snel te herstellen, bieden softwareleveranciers extra bescherming. Dat vereist wel dat die patches worden uitgevoerd. De besmetting met WannaCry (zie kader) was vooral succesvol bij grotere organisaties omdat systeembeheerders daar patches met vertraging doorvoeren om de stabiliteit van de systemen te bewaken. Voor thuis(-kantoor) speelt die overweging niet mee. Gebruik dus de automatische updates die Microsoft voor Windows en Office beschikbaar stelt. De installatie en de mogelijke herstart die nodig is kan irritant zijn, maar deze ergernis weegt niet op tegen de gevolgen die het alternatief kan hebben. Door Microsoft-software up-to-date te houden, sluit je een groot deel van de risico's al uit. Dat weten criminelen maar al te goed. Daarom wordt tegenwoordig steeds vaker gemikt op zwaktes in andere veelgebruikte software. Adobe Reader, browsers en Java Runtime Environment vormen een top drie die extra aandacht vraagt. Houd applicaties in deze top drie up-to-date met (bij voorkeur) automatische updates.

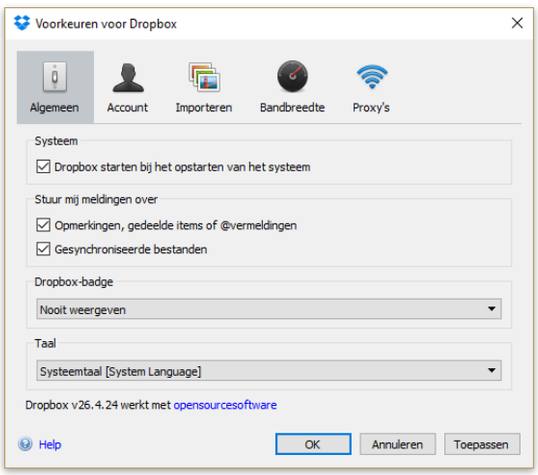
3 Installeer beveiligingssoftware

Een beveiligingspakket is onmisbaar op iedere computer. Alle beveiligingssoftware, van de ingebouwde gratis scanner van Windows Defender tot het meest kostbare zakelijke pakket, scant op bekende drei-

Misbruik van gelekte NSA-informatie

Vorig jaar bracht een hackersgroep met de naam Shadow-Brokers naar buiten dat het de hand had weten te leggen op hack-gereedschappen van de Amerikaanse veiligheidsdienst NSA. Na enkele stukken code te lekken, werd losgeld in Bitcoin geëist. Anders zou de groep onder meer een aantal voor Microsoft nog onbekende fouten in Windows (0-day-exploits) publiek maken. Er is niet betaald. Microsoft wist in maart de meeste 0-days te patchen. ShadowBrokers maakte op 16 april alle exploits publiek. Twee weken later werd WannaCry gelanceerd op basis van één van deze zwaktes.

gingen en herkent gedragspatronen van toepassingen. Dat voorkomt dat je slachtoffer wordt van een (variant op een) bekende aanval. Bescherming tegen ransomware vraagt om specifieke extra bescherming die niet iedereen biedt. Er zijn twee onderdelen in een beveiligingspakket die bij nieuwe varianten kunnen proberen om problemen te voorkomen. Allereerst 'exploit protection', dat het gedrag van applicaties in de gaten houdt en ingrijpt als een toepassing ineens abnormale acties neemt. Gaat Flash Player bijvoorbeeld ineens naar een bestand schrijven waar het niets mee te maken heeft, dan grijpt de beveiliging in. Daarmee kan een onbekende aanval, puur op basis van gedrag, gestopt worden. Enkele beveiligingsbedrijven bieden ook nog specifieke 'ransomware protection' aan. Dit onderdeel houdt in de gaten of de computer encryptietaken gaat uitvoeren. Worden deze taken aangeroepen door een niet geautoriseerde applicatie, dan grijpt de scanner in. Let bij keuze van een beveiligingspakket op of deze opties geboden worden. Alle extra bescherming is uiteindelijk mooi meegenomen.



› 04 Cloud-opslag zoals Dropbox is geen goede back-uplocatie als je je tegen ransomware wilt beschermen.

4 Onveilige back-ups

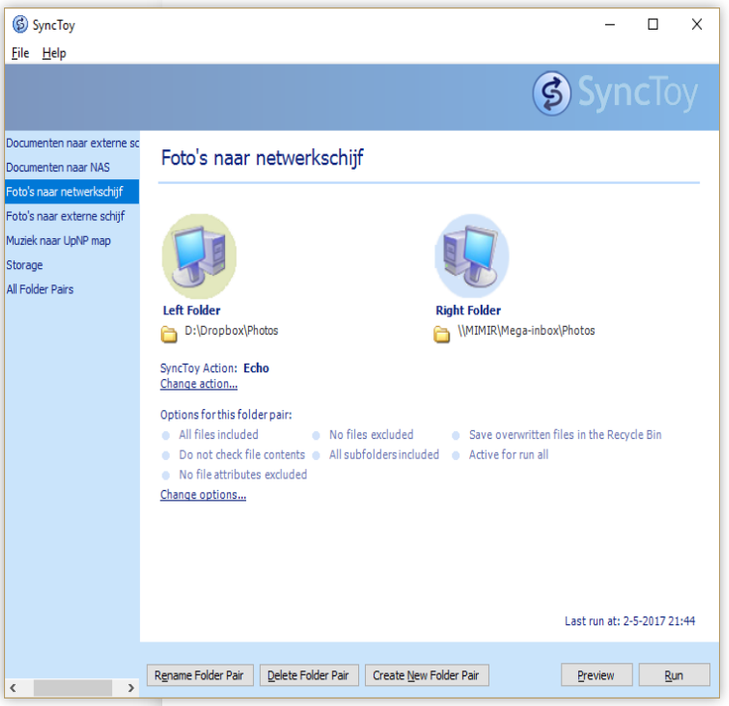
Hoe meer maatregelen je neemt, des te kleiner de kans is dat het misgaat. Maar die kans blijft wel altijd bestaan. Het beste verweer tegen ransomware is dan ook een betrouwbare back-up. Bestanden die veilig op een tweede locatie benaderbaar zijn, kun je niet gijzelen. Een back-up opzetten om je tegen ransomware te beschermen vraagt extra aandacht. Er zijn venijnige varianten in omloop die alle bereikbare bestanden versleutelen. Dat betekent dat je back-up op de nas geen soelaas kan bieden. Ook zijn er varianten die bestanden in de cloud meenemen in de aanval. Hier gaat het volgende principe op: als je er zelf eenvoudig (zonder wachtwoord) bij kunt, geldt dat ook voor een ongewenste 'bezoeker'. Houd daar rekening mee bij het plannen van de back-up. Verschillende back-up-systemen werken met versiebeheer. Zo biedt Windows Volume Shadow Copy bijvoorbeeld toegang tot oudere versies van een bestand. Is de laatste versie ongewenst versleuteld, dan zou je met versiebeheer kunnen teruggrijpen naar een niet-versleutelde versie. Helaas zijn er ook varianten ransomware die de schaduwkopieën beschadigen.

WannaCry

De ransomware-aanval met de naam WannaCry was in mei groot nieuws. Wat deze aanval bijzonder maakt, is de schaal van de infectie. Dat kwam door de gebruikte vector. In eerste instantie verspreidt WannaCry zich via een phishingmail, maar na infectie gedraagt het zich als worm en besmet het andere computers in het lokale (wifi- en lan-)netwerk. WannaCry wist zichzelf snel te verspreiden bij grotere organisaties omdat computers daar achterlopen met patches. Eén infectie was genoeg om alle andere computers in het netwerk te infecteren. Een technisch mankement in WannaCry beperkte de schade: de code bevatte verwijzingen naar een webadres. Een beveiligingsanalist die routinematig deze url claimde, ontdekte dat de verspreiding van WannaCry daarna stopte. Klaarblijkelijk was het adres een zogenaamde 'killswitch' waarmee de makers infectie konden stoppen. Ondanks de killswitch wist WannaCry meer dan 200.000 computers te infecteren. Betaling van het losgeld werd in Bitcoin geëist. Omdat Bitcoin-transacties voor iedereen te volgen zijn, is te zien hoeveel de daders verdiend hebben. WannaCry kwam met iets meer dan tweehonderd betalingen op een opbrengst van omgerekend 64.000 euro. De aandacht voor deze malware maakt het voor de verspreiders overigens lastig om de Bitcoins om te zetten naar andere valuta.



De WannaCry-ransomware kreeg veel aandacht omdat het zich razendsnel wist te verspreiden.



05 Met een gratis gereedschap als SyncToy kun je eenvoudig goede externe back-ups maken.

5 Maak veilige back-ups

De enige betrouwbare manier om te beschermen tegen ransomware is daarom met een back-up die na synchronisatie weer offline gehaald wordt. Voor thuis is daarbij een externe harde schijf het meest voor de hand liggende middel. Diverse programma's kunnen je helpen om naar een externe schijf te back-uppen, bijvoorbeeld de gratis tool SyncToy. Koppel je externe schijf na gebruik los en maak een schema om regelmatig de back-up te updaten. Vergeet niet om na ingebruikname van de back-upschijf te testen of je bestanden tijdens de back-up ook echt weggeschreven zijn. Niets is zo frustrerend als pas ná een ramp ontdekken dat je trouw gemaakte back-ups niet werken.

6 Eerste hulp bij ransomware

We schreven het al: hoeveel maatregelen je ook neemt, een besmetting met malware kan iedereen overkomen. Als je computer op slot schiet met een boodschap equivalent aan: 'betalen of anders', raak dan niet in paniek. Er is mogelijk nog redding te vinden. Betaal om te beginnen nooit. Hiermee moedig je criminelen aan en je hebt geen enkele garantie dat je je gegevens ook terugkrijgt. Haal de computer van het netwerk en maak een notitie van de melding (wat staat er op het scherm?). Gebruik die notitie op een schoon en veilig systeem om te zoeken naar decryptie- en ontsmettingsmogelijkheden. Beveiligingsbedrijven bieden, waar mogelijk, toepassingen om gekaapte systemen te redden (decryption tools). Is er voor je besmetting geen gereedschap voorhanden, neem dan contact op met de ondersteuning van je beveiligingsbedrijf. Soms zijn er nog maatregelen te nemen en baat het niet, dan schaadt het niet. Valt ook deze optie weg, maak dan je systeem schoon en gebruik je back-up. Let op: scan je systeem eerst voordat je de back-up koppelt. Het zou een beetje jammer zijn om op de valreep ook je reservebestanden te infecteren.



06 Als je onverhoopt toch besmet raakt, kan een bezoek aan de site van een beveiliger redding bieden.