

VEILIG ONLINE SHOPPEN



ANONIEM SURFEN

EN ZOEKEN

Veilige browsers
en zoekmachines

15 TIPS VOOR

VEILIG INLOGGEN

Maak de zwakste
schakel sterker

VEILIG ONLINE KERSTSHOPPEN?

Lees deze tien tips!

Fysiek naar een winkel gaan in de week vóór kerst is niet meer van deze tijd. Wie heeft er nu zin om door een drukke winkelstraat te struinen, winkel in en winkel uit voor dat ene cadeau? Anno 2017 koop je online! Veel makkelijker - maar bestel je kerstcadeau's wel veilig. Hier zijn 10 handige tips om dat te doen.

1

Gebruik een creditcard

Als het mogelijk is, reken je cadeau's dan af met een creditcard. Soms is dat wel wat duurder dan betalen met iDeal, maar met een Mastercard of Visa ben je wel altijd verzekerd als je iets online koopt. Bestelling niet geleverd, of stuk, en de webwinkel geeft geen gehoor? Dan kun je het bedrag via je creditcardmaatschappij meestal terugkrijgen. Bovendien geldt die verzekering tot wel een half jaar ná aankoop.

2

Schakel https in

Als je dat doet, zorg dan wel dat je je creditcardgegevens altijd versleuteld verstuurt. Let goed op het groene slotje bovenin de url-balk, waarmee je kunt zien of een website https gebruikt. Gebruik extensies voor je browser om dat te forceren als websites dat niet handmatig hebben ingeschakeld.

3

Zet een vpn aan

Om je verkeer te versleutelen kun je ook een **vpn gebruiken**. Daarmee wordt al je verstuurde data standaard versleuteld, zodat niemand met je mee kan kijken.

ken. Dat kost wel wat geld, maar een goede vpn hoeft helemaal niet duur te zijn. Al voor een paar tientjes per jaar kun je een goede vinden!

4

Gebruik een goed beveiligingspakket

Het is niet alleen belangrijk om je internetverbinding veilig te houden, maar ook je computer zelf. Met een goed **beveiligingspakket** voorkom je dat je computer wordt getroffen door virussen of ransomware. Bovendien zorg je daarmee ook dat je online bankzaken extra beveiligd zijn en dat je je transacties afschermt van pottenkijkers!

5

Geef niet teveel informatie weg

Winkeliers willen vaak nog wel eens meer informatie van je vragen dan strikt noodzakelijk. Een webshop heeft je echte verjaardag heus niet nodig voor het versturen van een pakketje, en een BSN mogen ze al helemaal niet vragen. Toch gebeuren zulke dingen nog regelmatig. Als je iets online koopt, vul dan al-





leen de nodige informatie in: je naam, je adres waar het pakket heen moet, en een emailadres voor de ontvangstbevestiging. Daarnaast ben je geboren op 01-01-1900, en is je telefoonnummer 06-12345678. Net zo makkelijk te onthouden!

6 Installeer een adblocker

Zeker tijdens het shoppen voor kerstcadeau's willen webwinkels maar wat graag weten waar je naar zoekt. Via agressieve tracking-cookies houden advertentienetwerken precies bij welke websites je bezoekt, en dat is op z'n minst vervelend te noemen. Gebruik een adblocker (zoals **uBlock Origin**) om advertenties tegen te houden, en addons of plugins zoals **Privacy Badger** of **Ghostery** om advertentie-trackers te blokkeren.

7 Surf incognito

Ondanks al die trackingblockers zijn er nog steeds cookies die er wel eens tussendoor glippen. Om dat te voorkomen kun je het beste altijd incognito browsen. Daarmee worden cookies, actieve logins en je surfgeschiedenis meteen gewist als je de browser sluit.

8 Gebruik een uniek wachtwoord

Als je verplicht een account moet aanmaken bij een webwinkel, gebruik dan een uniek wachtwoord dat je nergens anders gebruikt. Lastig te onthouden? Dat valt wel mee als je een wachtwoordmanager gebruikt! Maak gebruik van **Norton Identity safe**, **LastPass**, **1Password** of **KeePass** om automatisch unieke wachtwoorden te genereren en op te slaan.

9 Maak een 'wegwerpemailadres' aan

Eén van de vervelendste dingen aan webwinkels is dat heel veel je meteen aanmelden voor hun nieuwsbrief. Irritant, maar ook gevaarlijk: wat als de webshop ooit wordt gehackt en je emailadres op straat komt te liggen? Een goede maatregel om je emailadres privé te houden is om gebruik te maken van een tijdelijk emailadres. Met diensten zoals **TenMinuteMail**, **CrazyMailing** of **DropMail** maak je een tijdelijk emailadres aan waar je zo'n 10 minuten lang gebruik van kunt maken - genoeg om een cadeau te bestellen en de factuur te ontvangen. Let wel goed op dat je daarna géén toegang tot die inbox hebt, en dat je de ontvangstbevestiging, track-and-trace-code en factuur dus wel handmatig doorstuurt naar je echte emailadres. Als je het cadeau later wil ruilen of als er iets mis gaat met je bestelling heb je die informatie namelijk wel nodig!

10 Let op aanbiedingen die te mooi zijn om waar te zijn

Een oled-televisie voor slechts € 200,-, is dat een mooie deal, of toch niet? Net zoals alles in het leven geldt ook hier: als iets te mooi lijkt om waar te zijn, dan is het dat waarschijnlijk ook. Let daarom heel goed op of je niet in allerijl je creditcardgegevens op een neppe phishing-website invoert en je daarna al je geld kwijtraakt. Dat is sowieso makkelijk te voorkomen door een goede virus-scanner te gebruiken, maar gebruik verder je gezonde verstand als je online koopt; het ergste dat er dan kan gebeuren is dat je misschien een mooie aanbieding misloopt. Maar dan is tenminste niet je hele kerst in het water gevallen! ❗

SURFEN ZONDER POTTENKIJKERS

Onbespied op internet

Wie het internet opgaat, krijgt te maken met bedrijven die het niet zo nauw nemen met de privacy. Advertentiebedrijven bouwen profielen op met allerlei persoonlijke gegevens. Hoe voorkomt u dit soort praktijken? Met onze tips surft én zoekt u anoniem.

DIRKJAN VAN ITTERSUM

Veruit de meeste internetters gebruiken de browser Chrome. Die staat bekend als vlot en veilig, maar als het aankomt op privacy valt er wel wat op af te dingen. Chrome wordt ontwikkeld door Google. Dat bedrijf wil zoveel mogelijk informatie verzamelen over gebruikers om zo 'gerichte advertenties' te tonen. Chrome levert voor Google een goudmijn aan informatie op. Het bedrijf weet precies welke sites u bezoekt en welke zoektermen u gebruikt.

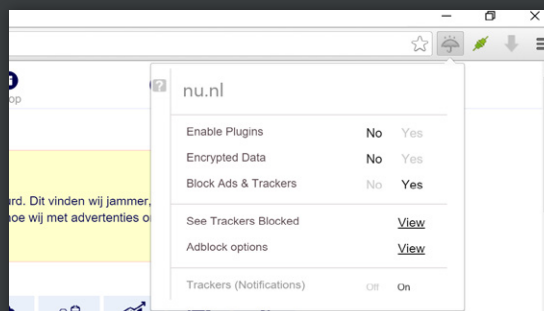
Er zijn gelukkig alternatieven. Van de grote browsers springt Firefox het meest in het oog. Er zijn veel instellingen om de privacy naar een hoger plan te tillen. Daar staat tegenover dat Firefox niet de snelste browser is. Ook met de beveiliging loopt het Firefox-team niet voorop. Ontwikkelaars werken nu pas aan een sandbox om een sessie volledig af te schermen van de rest van het systeem. Andere browsers gebruiken die technologie al veel langer.

Voor wie serieuze eisen stelt aan beveiliging en privacy is het de moeite waard om eens te kijken naar andere browsers die zich daar specifiek op richten. Er is inmiddels al behoorlijk wat keus in privacyvriendelijke browsers, kijk maar:

BROWSERS

Epic Browser

Dit is een prima keuze als u gewend bent aan Chrome, maar toch wat meer privacy wilt. Epic Browser (www.epicbrowser.com) is gebaseerd op Chromium, dezelfde opensource-broncode die ook aan de basis staat van Chrome. De aanvullingen van Google ontbreken, waardoor uw privacy beter is gewaarborgd. Epic Browser bevat een ingebouwde proxy waardoor het verkeer wordt omgeleid, bijvoorbeeld via pc's in Amerika, Duitsland of India. De surfessie is niet meer te herleiden naar uw computer. Ook wordt het verkeer versleuteld om af luisteren te voorkomen. Na het afsluiten van Epic Browser wordt de surfgeschiedenis gewist. Doordat advertenties, cookies en andere volgtechnieken worden geblokkeerd, staan nieuwsgierige adverteerders buitenspel. Het blokkeren van advertenties betekent ook dat websites sneller op het scherm staan. Pluspunt: u kunt per site advertenties toestaan om zo uw favoriete websites financieel te ondersteunen. Epic Browser kan overweg met extensies om de functionaliteit uit te breiden, maar het aantal beschikbare extensies is beperkt. Een slimme keuze, want slecht geprogrammeerde extensies vormen een veiligheidsrisico.

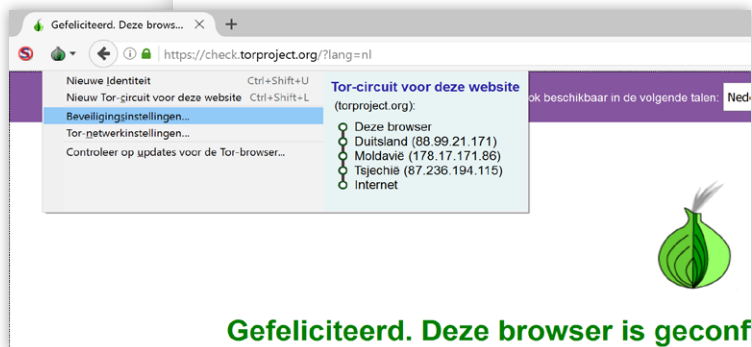


Met Epic Browser stelt u per website in of advertenties en plug-ins gebruikt mogen worden.

Tor Browser

De vermoedelijk beste bescherming biedt Tor Browser (www.torproject.org/projects/torbrowser.html.en). Internetverkeer gaat via Tor, een versleuteld netwerk dat is ontwikkeld met als doel volledig anoniem te kunnen communiceren. De data gaat langs diverse servers (zogenoemde 'nodes') die telkens alleen informatie krijgen over de vorige en de volgende server. Daardoor is bij de laatste node (de 'exitnode') niet meer bekend wat de herkomst van het verkeer was. Let op: om anoniem te blijven is het belangrijk dat een verbinding verloopt via ssl, anders heeft de exitnode wel toegang tot uw gegevens. Nadeel van Tor is dat de datasnelheid lager ligt, al blijkt uit een test dat YouTube-video's bekijken gewoon mogelijk is. Tor Browser is gebaseerd op Mozilla Firefox, maar er zijn allerlei extraatjes ingebouwd. Zo is er een knop om objecten op de pagina te blokkeren. Ook kunnen de beveiligingsinstellingen worden aangescherpt; u kunt bijvoorbeeld javascript uitschakelen. Houd er wel rekening mee dat bij de strengste beveiligingsinstellingen websites niet meer goed kunnen werken.

✓ Tor Browser laat zien via welke verbindingen het verkeer loopt.

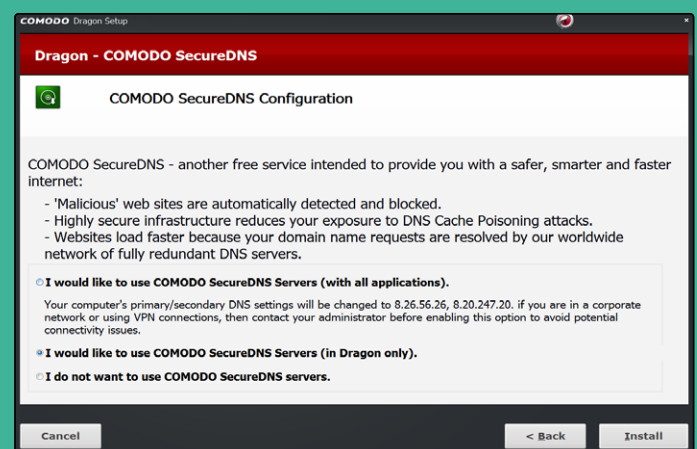


Dooble Web Browser

Dit is portable software: er hoeft dus niets te worden geïnstalleerd op de pc. Klikken op het exe-bestand volstaat om Dooble (<http://dooble.sourceforge.net>) te starten. De opensource-software is gebaseerd op de lichtgewicht-browser QtWeb. Dat veiligheid voorop staat, blijkt direct bij het opstarten: u wordt gevraagd om een wachtwoord in te stellen. Daarmee worden bladwijzers, cookies en andere onderdelen beschermd. Zolang u geen wachtwoord hebt ingesteld, gedraagt Dooble zich als het incognito-venster van Chrome: alles wordt verwijderd zodra de browser wordt afgesloten. Veel zaken staan standaard uit, zoals javascript en flash. Dat is heel veilig natuurlijk, maar daardoor ontbreken er wel veel zaken bij het surfen. Een video afspelen op YouTube bijvoorbeeld werkt niet. Dooble is alleen geschikt voor wie zoveel mogelijk veiligheid wil en daarbij voor lief neemt dat dit ten koste gaat van de gebruikerservaring. Wie een hogeresolutie-scherm heeft komt er bekaaid vanaf: Dooble kan daar niet goed mee overweg, waardoor pagina's verkleind worden weergegeven.

Comodo (Ice) Dragon

Beveiligingsbedrijf Comodo (www.comodo.com) maakt twee alternatieve browsers die zijn gericht op privacy. Comodo Dragon is gebaseerd op Chromium, terwijl Ice Dragon werkt met Firefox-code. Er zijn aanpassingen gedaan om te voorkomen dat gebruikers worden gevolgd. Ook is het mogelijk te kiezen voor een alternatieve dns-server die controleert of u wel op de juiste site zit. Het gaat om de dienst SecureDNS van Comodo zelf. Comodo kwam vorig jaar in opspraak toen een Google-ontwikkelaar fouten in de browser ontdekte, al zegt Comodo dat die inmiddels zijn opgelost.



Avira Scout

De naam Avira kent u misschien van de virusscanner, maar het beveiligingsbedrijf heeft ook een heuse browser (www.avira.com/en/avira-scout). Meteen bij het starten verschijnt het advies om verbinding te leggen via een vpn. Vermoedelijk is dat ook het verdienmodel achter de browser. De eerste (schamele) 500 MB dataverkeer is gratis. Voor 7,95 euro is er een onbeperkt abonnement. Overigens is Avira Scout ook zonder vpn te gebruiken, maar dan ontbreekt de extra beveiligde verbinding. Neemt niet weg dat er voldoende andere mogelijkheden zijn. Avira Scout is gebaseerd op Chromium, met wat extra functies. Zo controleert Avira de bezochte sites en blokkeert het toegang tot phishing-sites. Ook wordt er een ssl-verbinding gebruikt indien beschikbaar. Verder worden trackers geblokkeerd, zodat adverteerders u niet kunnen volgen. Het is best mogelijk om zelf deze mogelijkheden aan Google Chrome toe te voegen met behulp van extensies, maar het is handig dat Avira dit kant-en-klaar levert.

Opera

Deze browser is vermoedelijk de bekendste naam in de lijst. Opera (www.opera.com) bestaat al sinds 1996. Hoewel er een schare trouwe gebruikers is, heeft

Comodo wil graag dat u via de dienst SecureDNS surft.

Mobiele browsers

Privacy is niet alleen belangrijk op de desktop. Ook op smartphones en tablets is het zeker iets om rekening mee te houden. Er zijn verschillende mobiele browsers die uw privacy beschermen.

Lightning Browser (Android)

Deze lichtgewichtbrowser valt op door zijn snelheid. Wie een wat ouder toestel gebruikt zal hiervan profiteren. Door de app Orbot te installeren, kunt u met Lightning Browser surfen via het sterk versleutelde Tor-netwerk. Een adblocker ontbreekt, maar zit wel in de betaalde versie Lightning Browser + (1,66 euro).

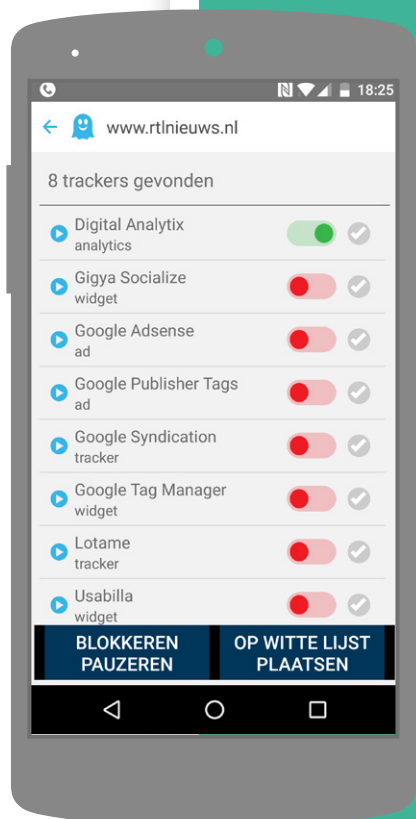
Firefox Focus (iOS)

Op de iPhone en iPad is Firefox Focus een browser die uitblinkt in privacy. Dat heeft alles te maken met de Spartaanse opzet. Er kan alleen een website worden bezocht; functies als bladwijzers, geschiedenis of het onthouden van wachtwoorden ontbreken. Bij het afsluiten van de app wordt meteen alles gewist. De browser blokkeert automatisch advertenties.

Ghostery Privacy Browser (iOS, Android)

Dit is een complete browser die voorkomt dat trackers uw surfgedrag in kaart brengen. Van iedere site verschijnt een overzicht van trackers. Ghostery geeft ook informatie over iedere tracker. Overigens is er ook een Ghostery-extensie voor desktopbrowsers.

◀ Ghostery toont een volledige lijst met trackers, inclusief informatie.



A browser for our friends

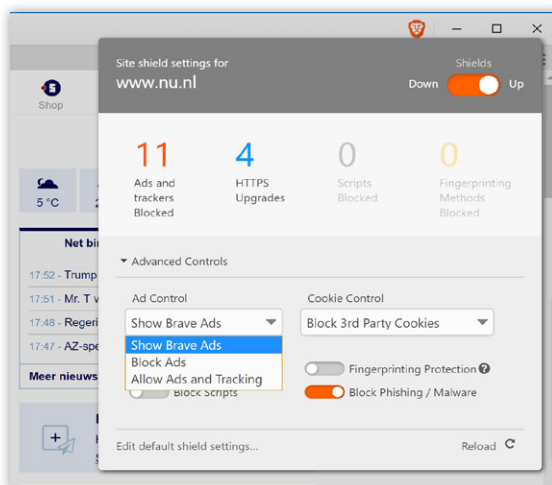
Vivaldi

De browser Opera is enige tijd geleden gestopt met het sociale netwerk My Opera. Twee oud-medewerkers van Opera waren ontevreden over deze koerswijziging. Zij ontwikkelden Vivaldi (<https://vivaldi.com>), een fraai ogende browser met de oude mogelijkheden van My Opera (inclusief webmail en weblogs).

de grote massa het programma nooit omarmd. Jammer, want het is prettige software. De nieuwste versie besteedt extra aandacht aan veiligheid en privacy. Zo is er een adblocker ingebouwd. Hij staat standaard uit, maar kan via de instellingen worden aangezet. Er is een witte lijst om een financieel duwtje te geven aan uw favoriete websites. Belangrijkste privacyoptie van Opera is wel het ingebouwde vpn. Daarmee gaat het surfen weliswaar wat trager, maar dankzij de versleuteling blijven surfgedrag, ip-adres en locatie wel geheim. Er geldt geen datalimiet voor het vpn.

Brave Browser

Een bijzonder geval is Brave Browser (www.brave.com). De browser gebruikt waar mogelijk ssl-verbindingen en voorkomt dat websites u volgen. Tot zover vrij gebruikelijke mogelijkheden, maar de ingebouwde adblocker valt op door een aparte functie. Het is namelijk mogelijk om advertenties te blokkeren, maar



◀ Brave Browser heeft de optie om gepersonaliseerde advertenties te vervangen door algemene advertenties.

ook om ze te vervangen door reclameboodschappen die Brave uitkiest. Het voordeel? Deze alternatieve banners worden niet geselecteerd op basis van een profiel. Brave wil de inkomsten doorsluizen naar bezochte websites. Brave Browser is gebaseerd op Chromium en is er niet alleen voor de desktop, maar ook voor smartphones en tablets (Android en iOS).

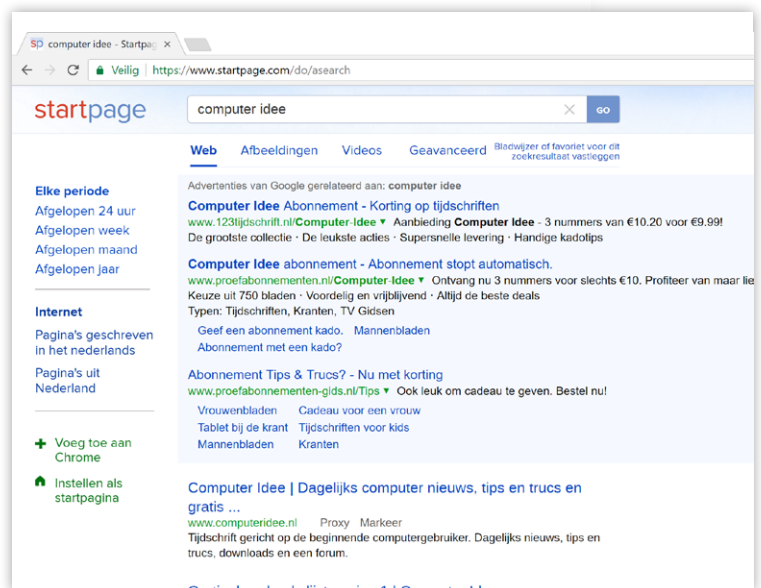
ZOEKMACHINES

Om uw privacy te beschermen is natuurlijk niet alleen de browser belangrijk. U geeft ook heel veel informatie prijs aan zoekmachines. Google bewaart al uw zoekopdrachten. Er zijn gelukkig steeds meer alternatieven, zoals deze:

DuckDuckGo

DuckDuckGo (www.duckduckgo.com) is de afgelopen jaren uitgegroeid tot een volwaardige site met prima zoekresultaten. In tegenstelling tot Google belooft DuckDuckGo geen profielen op te slaan. Zoekresultaten worden dus niet op de persoon aangepast. Ook op andere manieren zorgt DuckDuckGo voor een goede bescherming van uw privacy, bijvoorbeeld door geen informatie te versturen naar gevonden websites over uw zoekopdracht. Er is een Nederlandse versie van DuckDuckGo, maar met een muisklik schakelt u over naar de zoekresultaten voor China, Argentinië of Zuid-Afrika. Er is ook een app om te zoeken op smartphone of tablet.

➤ DuckDuckGo is de bekendste en wat ons betreft beste privacyvriendelijke zoekmachine.



Startpage

Dit is een initiatief van het Nederlandse bedrijf Ixquick. De zoekresultaten zijn prima in orde, want afkomstig van Google. Startpage (www.startpage.com) fungeert als een filter tussen de bezoeker en Google, waardoor de Amerikaanse zoekmachine niets te weten komt over de persoon die zoekt. Zo kunt u Google dus volledig anoniem gebruiken. Ixquick zelf slaat ook geen informatie over de bezoeker op. Handig is de optie om gevonden websites anoniem via een proxy te bezoeken. De website ziet dan niet uw ip-adres en kan ook geen cookies plaatsen. Javascript is via de proxy wel uitgeschakeld, waardoor veel sites niet goed werken.

Startpage plaatst advertenties van Google bij zoekresultaten, maar belooft dat Google geen informatie over de gebruiker ontvangt.



Yippy

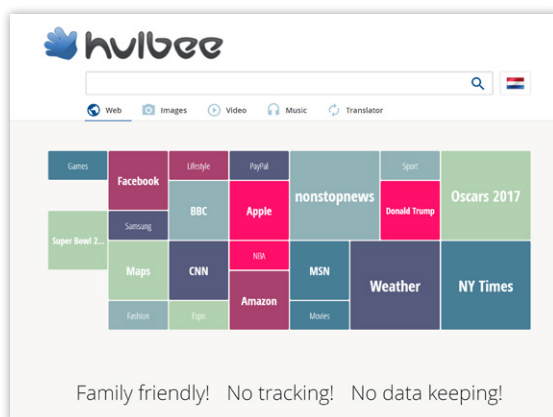
Net als Startpage belooft Yippy (www.yippy.com) optimale privacy voor de bezoeker, maar veel andere informatie geeft de website niet. In het verleden was het een metazoekmachine die zijn resultaten van bijvoorbeeld Google haalde. Tegenwoordig lijkt het erop dat Yippy zijn eigen webcrawler draait om het web te indexeren. Yippy bouwt geen profielen op van gebruikers, maar slaat wel zaken op als ip-adres en taal. In de privacyverklaring waarschuwt Yippy dat inwoners buiten de VS gevolgd kunnen worden door de Amerikaanse overheid. Handig is dat Yippy direct gerelateerde zoektermen in beeld toont. De zoekresultaten zijn bruikbaar, maar niet van het niveau dat we bij Google gewend zijn.

Hulbee

Het Zwitserse Hulbee (www.hulbee.com) gebruikt de zoekindex van Bing (Microsoft), maar werkt ook aan een eigen index. De zoekresultaten zijn in orde, mede dankzij de flinke sprongen die Bing de laatste tijd heeft gemaakt. Bijzonder is dat Hulbee gerelateerde zoektermen nadrukkelijk in beeld toont om zo de zoekresultaten te verbeteren. Zoektermen, ip-adressen en andere informatie over gebruikers worden niet opgeslagen, belooft Hulbee. Het gaat om een 'family-friendly' zoekmachine, dus links naar bijvoorbeeld naaktsites worden eruit gefilterd. De site verdient geld met het tonen van advertenties die aansluiten bij de ingevoerde zoektermen.

Oscobo

Deze Britse zoekmachine belooft geen enkele informatie over zijn gebruikers op te slaan. Oscobo (www.oscobo.com) heeft geen eigen crawler om het web in kaart te brengen, maar gebruikt de indexen van Bing en Yahoo. Omdat het bedrijf zich nadrukkelijk richt op de Britse markt, zijn de zoekresultaten daarop afgestemd. In de toekomst wil Oscobo verder uitbreiden naar andere Europese landen. Door advertenties te tonen bij de zoekresultaten wil het bedrijf geld verdienen. Hierbij wordt geen informatie over de bezoeker gebruikt: alleen de ingevoerde zoekopdracht dient als basis. ■



➤ Hulbee gebruikt opvallende blokken voor populaire en gerelateerde zoektermen.

DuckDuckGo als standaardzoekmachine

In de meeste browsers kunt u de zoekmachine eenvoudig wijzigen. DuckDuckGo is hierbij een prima keuze.

Voor **Firefox** heeft DuckDuckGo een add-on ontwikkeld.

➤ Start Firefox en ga naar

<https://addons.mozilla.org>.

➤ Zoek en installeer DuckDuckGo. De volledige naam van de add-on is DuckDuckGo Plus.

In **Chrome** wijzigt u de zoekmachine als volgt:

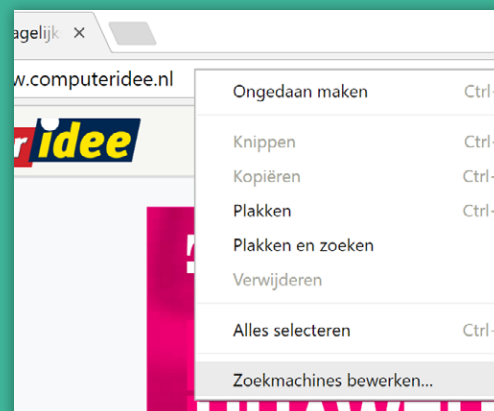
- Klik met de rechtermuisknop in de adresbalk (zie afbeelding).
- Kies voor Zoekmachine bewerken.
- Er verschijnt een lange lijst met zoekmachines en andere sites.
- Voeg DuckDuckGo toe door te klikken op 'Instellen als standaard'.
- Klik op Gereed.
- Een volgende keer dat u zoekt via de browserbalk zal DuckDuckGo worden gebruikt.

Ook de browser **Edge** kan DuckDuckGo gebruiken als standaardzoekmachine.

➤ Ga naar www.duckduckgo.com.

➤ Tik op Instellingen, Geavanceerde instellingen, Zoekprogramma wijzigen.

➤ Selecteer uit de lijst DuckDuckGo en kies 'Als standaard instellen'.



◀ Klik met rechts in de browserbalk om de zoekmachine te wijzigen.

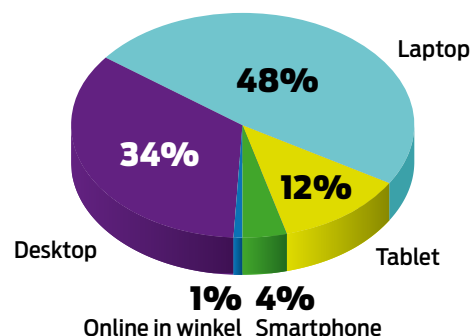
ONLINE SHOPPEN

populairder dan ooit!

Waren we een jaar of tien geleden nog extreem voorzichtig als het ging om het plaatsen van een bestelling op internet, inmiddels zijn we vaak eerder geneigd om een online aankoop te doen dan dat we de moeite nemen om naar een winkelcentrum te gaan. Maar wat kopen we eigenlijk online, en hoe?

MARTIN GIJZEMIJTER

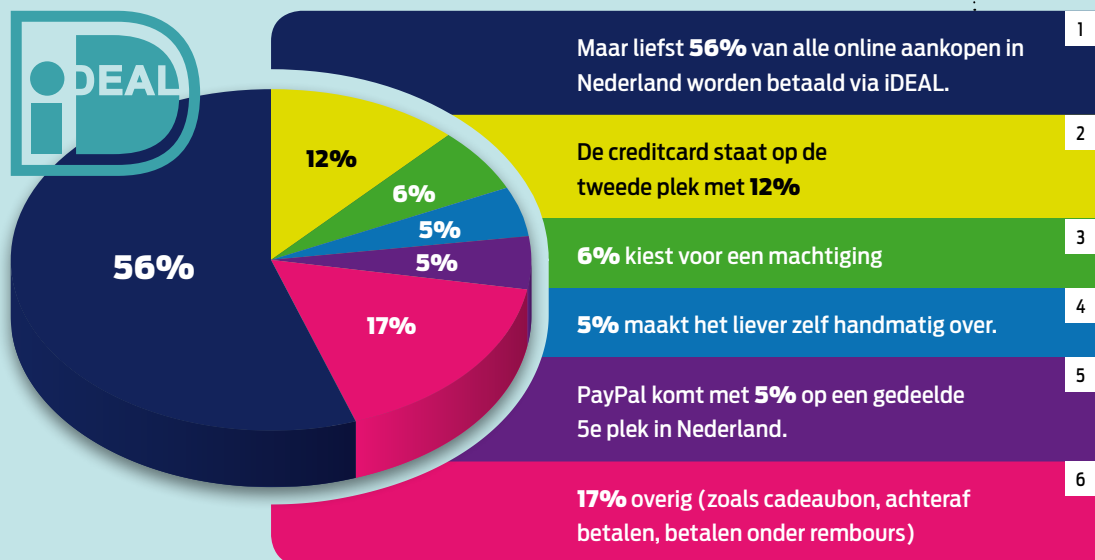
Verdeling online bestedingen naar apparaat



MAAR WAT KOPEN WE EIGENLIJK?

Hoe betalen we?

De enorme toename van de populariteit van online winkelen is niet in de laatste plaats te danken aan het feit dat men het betalen zo makkelijk en veilig heeft gemaakt.

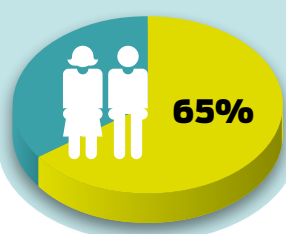


In de Verenigde Staten doet PayPal het een stuk beter, met een marktaandeel van **30%**. Indrukwekkend, aangezien het bedrijf daar ook concurrentie heeft van Apple Pay en Android Pay. Maar Amerika kent geen iDEAL-achtige betaalmethode.

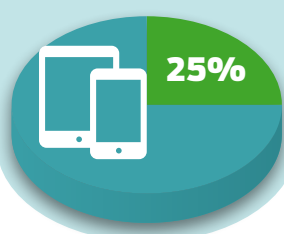
Hoe winkelen we?

Online winkelen is niet alleen voorbehouden aan jonge mensen. Maar liefst **65%** van de Nederlandse consumenten **boven de 55 jaar** verwacht de komende twee jaar steeds meer online te gaan shoppen.

NL-consumenten 55+ gaan meer shoppen



Shoppen via mobiel of tablet (55+)



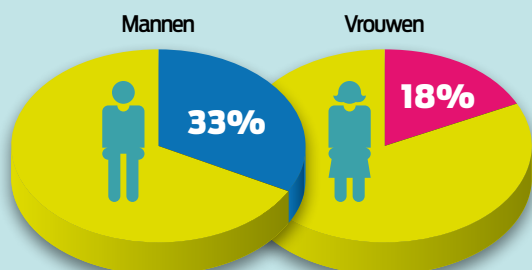
Voor deze doelgroep is **betaalgemak** het belangrijkste criterium, direct gevolgd door **betrouwbaarheid**. De doelgroep 55+ winkelt het liefst via de laptop of desktop. **Slechts 25 procent** geeft aan dit ook via de mobiele telefoon of tablet te doen.

Waar shoppen we?

De mogelijkheid om mobiel te winkelen zorgt er ook voor dat er veel meer plekken zijn waarop we dat doen. Voor de Nederlander is **het toilet** de favoriete plek om te winkelen op de smartphone. Ja, echt, dat blijkt uit onderzoek.



Maar liefst **33%** van de mannen die winkelen op de smartphone doet dat op het toilet. Onder vrouwen is dat aantal veel lager: **18%**



Een andere plek waarop graag gewinkeld wordt, is voor de televisie, **16%** geeft aan dat een reclameblok heeft geleid tot een mobiele aankoop.

Wat kopen we?

Kleding is wereldwijd het meest verkochte product.

In 2015 gaf **55%** van de online kopers aan een kledingstuk gekocht te hebben.

1ste

55%

Boeken en muziek staan op een tweede plek met **50%**

2de

50%

Opmerkelijk is dat elektronica met **37%** op de zesde plek staan.

6de

37%

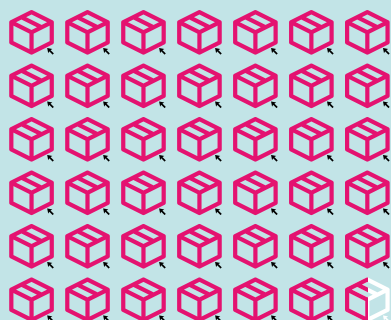
De dagelijkse boodschappen staan met **11%** op de 18e plek, maar de verwachting is dat dat percentage binnen nu en twee jaar behoorlijk zal exploderen.

18de

11%

aantal online aankopen

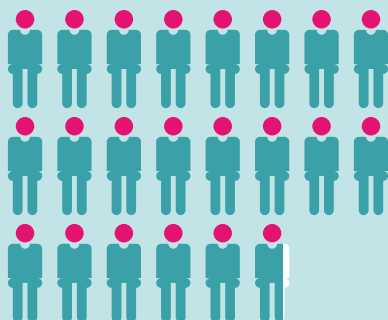
41,5 miljoen



1 miljoen

aantal online kopers

10,9 miljoen



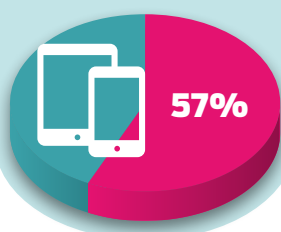
1 miljoen

VOOR DE NEDERLANDER IS HET TOILET DE FAVORIETE PLEK OM TE WINKELEN OP DE SMARTPHONE.

Online bestedingen
(excl. verzendkosten)

€ 4,54 miljard

Shoppen via mobiel of tablet (jongeren)



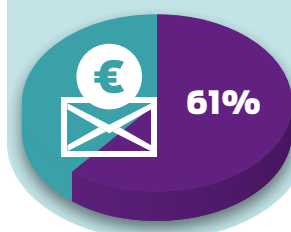
Jongeren vinden mobiel shoppen veel interessanter, **maar liefst 57%** geeft aan te shoppen via de smartphone of tablet.

Slechts 15% van de **doelgroep 18 tot 30 jaar** maakt zich druk om betrouwbaarheid van webwinkels. Zij storen zich vooral aan **verzendkosten**: 61% van hen ziet verzendkosten als een reden om niet te bestellen.

Zorgen over betrouwbaarheid



Verzendkosten als reden om niet te bestellen



VERKOOPPLAATJES

De beste foto's voor online verkopen

Wilt u online iets verkopen, bijvoorbeeld op Marktplaats of eBay? Dan zijn goede foto's heel belangrijk. Als u de tips in ons artikel volgt, kunnen die eigenlijk niet meer mislukken. Klik-klak-kassa!

KEES KRIK

Of u nu tweedehands spullen verkoopt of zelf-gemaakte producten aan de man of vrouw brengt, het is uitermate belangrijk dat u hier goed beeldmateriaal bij gebruikt. Foto's zijn het eerste wat mensen zien als ze op bijvoorbeeld Marktplaats, Etsy of uw eigen website rondsnoeien. Ze moeten meteen de aandacht trekken, bezoekers nieuwsgierig maken en ze aansporen om op uw product te klikken. Pas daarna lezen ze de beschrijving. Die moet natuurlijk ook prima in orde zijn en alle relevante informatie bieden, maar vooral de foto's zijn cruciaal. Ze laten zien hoe het product eruitziet en in welke staat het is. Ze bepalen of iemand op uw product klikt of verder kijkt en bij iemand anders gaat winkelen.

Zelf beeldmateriaal maken

Hoe komt u aan goed beeldmateriaal? Dat maakt u gewoon zelf met uw digitale camera of smartphone. Het is wel enorm belangrijk dat u foto's van voldoende kwaliteit maakt. Allereerst moet een foto technisch in orde zijn. Denk aan kleur, belichting en scherpte. Daarnaast moet het product zo goed mogelijk uit de verf komen. Schiet dus niet zomaar een paar plaat-

jes, maar neem er even goed de tijd voor en geef het de aandacht die het nodig heeft. Het hoeft gelukkig ook weer niet heel veel tijd te kosten en is zeker niet ingewikkeld.

Bij het fotograferen van producten is aandacht op grofweg drie vlakken nodig. Om een mooie foto te maken, hebt u allereerst goed licht nodig. Licht maakt of breekt een foto. Bij slecht licht is de technische kwaliteit van een foto meteen een stuk minder en het product dat u wilt aanprijzen ziet er minder aantrekkelijk uit. Niet doen dus. Daarnaast hebt u een geschikte plek nodig

✓ U hebt niet heel veel ruimte nodig om te fotograferen. Een stukje vloer of een tafeltje volstaat meestal wel.



om uw foto's te maken. U hoeft er gelukkig geen complete fotostudio voor in te richten: een rustig en opgeruimd hoekje is meer dan voldoende. Tot slot is het van belang om hetgeen u wilt verkopen er zo goed mogelijk uit te laten zien en het vervolgens zo gunstig mogelijk te fotograferen. Op al deze punten gaan wij in dit artikel uitgebreid in, zodat u binnen een mum van tijd foto's maakt waarmee u merkbaar beter verkoopt.

Geschikte plek

Het eerste wat u moet doen, is een goede plek vinden om foto's te maken. Als het overdag is, is een plekje in de buurt van een raam ideaal, omdat u zo gebruik kunt maken van natuurlijk daglicht. Dat zorgt al snel voor een mooi resultaat. Kies anders een plek in de buurt van een (schemer)lamp of bij een stopcontact waar u

➤ Mooie foto's voor de verkoop maakt u eenvoudig zelf met uw camera of smartphone.



er tijdelijk eentje neer kunt zetten. Afhankelijk van de grootte van het product kunt u een tafel of een plekje op de vloer gebruiken om een eenvoudige opstelling te maken. Maak die plek zo veel mogelijk rommelvrij. Een tip is om een product alvast neer te zetten of te leggen en vervolgens via uw camera te kijken wat er allemaal in beeld komt. Zo krijgt u een goed idee hoeveel vrije ruimte ongeveer nodig is. Let ook op wat er op de achtergrond te zien is, want dat leidt op een foto al snel af.

Achtergrond plaatsen

Bij voorwerpen die u plat neerlegt tijdens het fotograferen zal alleen uw zelfgekozen ondergrond te zien zijn. Maar is het iets wat u neerzet, dan komt al snel een deel van de omgeving op de foto. Dat staat niet zo mooi en leidt zelfs af, als daar allerlei rommel en het interieur van uw kamer te zien is. Dit is eenvoudig op te lossen door een eigen achtergrond te gebruiken. Plak bijvoorbeeld een groot vel papier op een stuk karton en plaats dat rechtop achter uw product. Leg er iets achter (bijvoorbeeld een stapeltje boeken) zodat het niet omvalt. U kunt ook een plaat kunststof in een kleur naar keuze kopen bij een bouwmarkt, of een rol behang met een rustig patroon of een mooie structuur uitkiezen. U kunt dat dan prima voor zowel de ondergrond als de achtergrond gebruiken.



> Als u meer naar voren fotografeert, is ineens uw kamer te zien. Dat staat niet mooi en verpest uw productfoto.

Passende ondergrond

Bij productfoto's wordt vaak een witte ondergrond gebruikt. Zo valt een voorwerp namelijk extra goed op. Een andere kleur gebruiken mag natuurlijk ook. Bij een wit product kunt u bijvoorbeeld beter een zwarte of in ieder geval een contrasterende ondergrond gebruiken. Want dan steekt het product beter af. Als ondergrond kunt u prima een lap stof, stuk behang of een tafelkleed gebruiken. Zorg dat het schoon is, trek het goed strak en leg eventueel iets zwaars op de hoekpunten zodat er zo min mogelijk lelijke kreukels te zien zijn. U kunt ook het tafelblad of de vloer zelf als ondergrond gebruiken als dat een mooie kleur of structuur heeft. Of u legt een plank met een mooie houtnerf neer. Iets creatiefs, bijvoorbeeld houtsnippers, kan ook, maar maak het niet te bont.



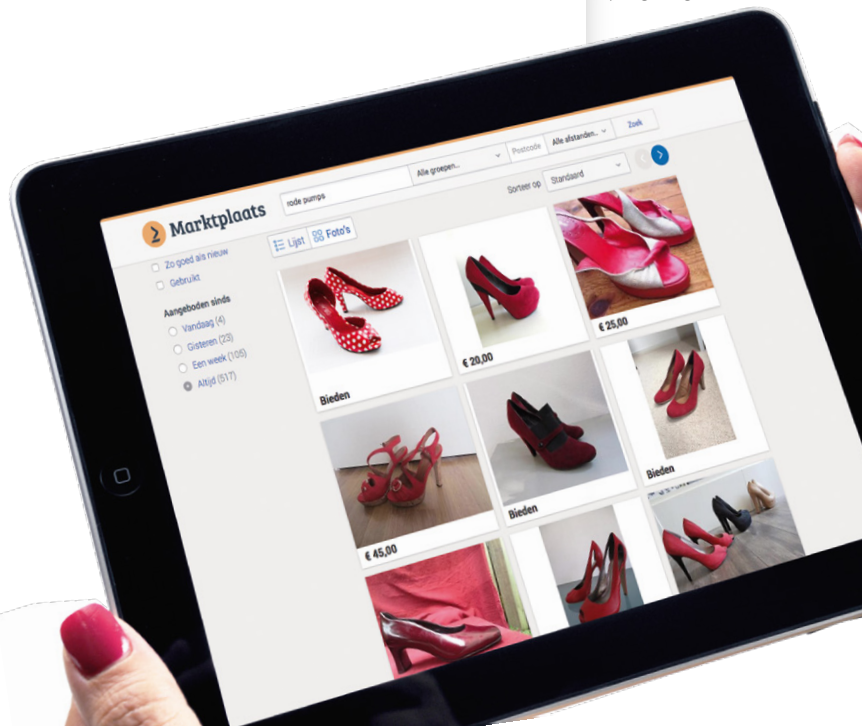
De juiste hoek vinden

Dan is het tijd om het product verkoopklaar te maken. Voordat u het op de foto zet, maakt u het eerst zo goed mogelijk schoon. Een stoffig of zelfs vies product ziet er natuurlijk niet echt aantrekkelijk uit op een foto. Daar schrikt u potentiële kopers alleen maar mee af. Stof het dus goed af, haal vingerafdrukken van bijvoorbeeld een schermpje af en haal vuil weg uit naden en kieren. Vervolgens legt of zet u het product neer op de plek die u hebt voorbereid. Bekijk het ongeveer vanaf ooghoogte voor een goede indruk hoe het straks op de foto komt. Draai het product om een hoek te vinden waarop het optimaal in beeld is. Meestal is het een goed idee om een product niet pal van voren te fotograferen, maar meer vanuit een hoekpunt, bijvoorbeeld in een hoek van vijfenveertig graden.

^ Een effen of rustige ondergrond werkt het beste.



< Vanuit een hoek fotograferen levert een spannender beeld op en een beter zicht op het product. Recht van voren ziet alles er wat platgeslagen uit.



Op die manier krijgt u een dynamischer, spannender beeld en is behalve de voorzijde meteen ook een zijkant te zien. Door tegelijkertijd vanaf iets hoger te fotograferen, komt ook de bovenzijde in beeld. U ziet nu ineens drie zijden, wat veel meer diepte aan de foto geeft en hem interessanter maakt om naar te kijken. U hebt vast meerdere foto's nodig, dus zoek ook nog een paar andere interessante standen op. Draai altijd het product in plaats van dat u er met zelf met uw camera of telefoon omheen beweegt, want anders blijft uw eigen ondergrond en achtergrond het beeld niet goed vullen.

Het beste licht

Goed licht is essentieel voor mooie foto's. Bij een raam hebt u overdag voldoende licht van hoge kwaliteit, zelfs als het bewolkt is. Voorkom wel dat u pal tegen al te fel raamlicht in fotografeert, want productfotografie bij sterk tegenlicht is lastig. Hier hebt u vooral mee te maken als u nagenoeg recht naar voren en dus naar het raam toe fotografeert. Ga er dan liever met uw rug naartoe zitten, dus met het te fotograferen product voor u en de gekozen achtergrond daar weer achter. Het licht schijnt dan goed over het product heen. Gaat het om

iets wat u neerlegt of neerzet en vervolgens (schuin) van boven fotografeert? Dan speelt dit probleem meestal niet. Sluit op een zonnige dag wel de vitrage als u die hebt, anders kan het licht iets te fel zijn. Is het bewolkt, dan mag de vitrage gerust open blijven.

Is het avond of kunt u niet bij een raam fotograferen, dan is er kunstlicht nodig. Het beste kunt u een lamp schuin achter u plaatsen, zodat het licht over de voorzijde van het product strijkt, maar wel iets van boven komt. Twee lichtbronnen, aan beide zijden



Tussen ondergrond en achtergrond

Gebruikt u een eigen achtergrond? Dan zal er een naad te zien zijn tussen de ondergrond en de achtergrond. Dat is niet zo heel erg, maar mocht u zich er toch aan storen, dan kunt u het met een trucje eenvoudig wegwerken. Gebruik een doek van voldoende lengte als ondergrond en laat het achter uw product met een mooie boog omhoog uit beeld verdwijnen. U kunt ook een rol behang met een mooie kleur of een leuk patroon gebruiken. Zet het behang of de lap stof vast aan iets wat u erachter neerzet, zoals een flinke stapel boeken. Doordat er nu een mooie bocht in zit, gaat de ondergrond naadloos over in de achtergrond.



^ Laat de ondergrond met een mooie boog omhoog gaan, dan is er geen scheiding met de achtergrond te zien.

achter u, kan ook: dan hebt u minder last van schaduwwerking. Een stukje van het product mag best deels in schaduwen gehuld blijven, zolang het maar niet storend is of afleidt. Speel met de opstelling van de lamp(en) om te kijken wat het beste effect geeft. Maak het liefst een stel testfoto's, want een camera ziet de dingen heel anders dan u met het blote oog. En of u nu zonlicht of lamplicht gebruikt, let er altijd op dat uw eigen schaduw niet over het product valt of ergens in beeld te zien is. In dat geval lost een iets ander standpunt het probleem snel weer op.

Natuurlijke kleuren

Met lamplicht is het altijd iets lastiger om de juiste kleuren in foto's te krijgen. Terwijl dit wel belangrijk is: het product moet er natuurlijk wel uitzien zoals het in het echt is. Bij kunstlicht kan dit alsnog door de witbalans op de camera anders in te stellen via het menu of een knop. Probeer het eerst met de automatisch gekozen witbalans en anders met de stand die een gloeilamp als symbool heeft. Niet tevreden? Probeer gerust alle andere witbalansstanden tot

^ Bij een raam is voldoende daglicht om goede foto's te maken.

✓ Kunstlicht gebruiken kan natuurlijk ook.



de meest realistische kleuren op het camerascherm verschijnen. Gebruikt u daglicht, dan is dit een stuk eenvoudiger: de camera doet het dan meestal automatisch goed.



> Bij lamplicht kan een foto te geel of oranje worden. Stel dan een andere witbalans in.

Reflecties

Bevat een product reflecterende delen, dan is daar al snel de weerspiegeling van de lichtbron op te zien. Ook bent u mogelijk zelf te zien, samen met uw camera. Dit is vaak op te lossen door een iets ander standpunt in te nemen of de lamp een stukje te verplaatsen. Wat ook kan, is het lamplicht door een heel dunne witte doek laten schijnen. Laat iemand zo'n doek op korte afstand van de lamp houden (nooit ertegenaan wegens brandgevaar!). Hoe groter het witte oppervlak, hoe meer het licht verspreid wordt. De lamp zelf is dan vrijwel niet meer te zien en daarnaast worden schaduwen lichter gemaakt en zijn ze ook nog eens mooier om te zien.



> Door een dunne stof te gebruiken is de felle pit van de lamp verdwenen en zien schaduwen er minder donker en mooier uit.

Huis in de verkoop

Ook uw huis kunt u als een product zien zodra u het wilt verkopen of verhuren. Ruim weer eerst alle troep op voordat u begint met fotograferen. Plaats overvloedige spullen desnoods tijdelijk in een andere ruimte. Laat een kamer er zo neutraal mogelijk uitzien, dus met zo min mogelijk persoonlijke spullen erin – dus ook geen familiefoto's of verwaald speelgoed. Plaats een paar mooie accessoires zoals een vaas met bloemen, een mooi schilderij of een paar kaarsen, om de ruimte er gezellig uit te laten zien. Zet tafels en stoelen netjes recht. Een beetje speels mag best, zolang het maar niet slordig of rommelig oogt. Fotografeer liefst vanuit de hoeken van de kamer. Dat spreekt meer dan wanneer u recht de kamer inkijkt. Schakel eventueel wat verlichting in om extra sfeer toe te voegen, maar let op dat de ruimte er niet te gelig of oranje van wordt. Zorg dat rechte lijnen ook echt recht op de foto komen. Denk aan de muren en het plafond. Werk het liefst vanaf statief, want dan kunt u alles zorgvuldig uitlijnen. Hebt u buitenfoto's nodig? Kies een tijdstip op een mooie zonnige dag waarop veel mensen van huis zijn, zodat de straat niet vol geparkeerde auto's staat.

Camera of smartphone

Fotograferen kan met een camera, maar ook met uw smartphone. Zoom met een telefoon liever niet in, omdat een smartphone (op een zeldzame uitzondering na) geen echte zoomlens heeft. Fotografeer ook niet van extreem dichtbij, want dan vervormt het beeld en dat is niet bevorderend voor de verkoop. Mocht uw achtergrond te smal zijn waardoor langs de randen van de foto een stukje kamer te zien is, dan knipt u dat er achteraf in een fotobewerker eenvoudig weer vanaf. Let er verder op dat de camera of telefoon goed op het product scherpstelt en niet op bijvoorbeeld de ondergrond of de achtergrond. Houd het toestel tot slot volledig stil en druk rustig af, om bewegingsonscherpte te voorkomen.

U kunt gewoon een automatische stand gebruiken. De camera of telefoon regelt dan alles voor u. Kiezen voor de portretstand of de macrostand kan vaak ook nog, omdat deze standen bedoeld zijn om iets van redelijk dichtbij te fotograferen. Mocht de foto te donker worden, gebruik dan belichtingscompensatie (meestal een knop met een plus-minteken en anders een menuoptie) van bijvoorbeeld +1 of +2 om de volgende opname lichter te maken. Is de foto te licht, dan corrigeert u dit met -1 of -2. Zorg er verder voor dat de flitser is uitgeschakeld. Natuurlijk daglicht of gewoon kunstlicht toont namelijk mooier in een productfoto. Beschikt u over een statief of een ministatief, gebruik dan dat om scherpere foto's te maken. 📷

✓ Foto's maken kan met ook met uw smartphone.



REKENINGEN DELEN

Zo voorkom je dat jij altijd betaalt

Natuurlijk kun je ook in een restaurant iedereen voor zich laten betalen. Dan heb ik nog een nieuw intro voor je voor het artikel 'Rekeningen delen': We eten steeds vaker buiten de deur en daarmee wordt er heel wat geld uitgegeven in de vele horecagelegenheden die ons land rijk is. Gezellig om met vrienden en familie van een hapje en een drankje te genieten, maar het is natuurlijk niet zo fijn als jij telkens de rekening voor je kiezen krijgt. Tijd om daar een einde aan te maken.

MARTIN GIJZEMIJTER

Natuurlijk kun je ook op een terrasje iedereen voor zich laten betalen. Maar in de praktijk betaalt meestal één iemand, dat is makkelijker. En daar gaat het vaak mis ... om geld vragen is niet fijn, zeker niet als je iemand meerdere keren moet helpen herinneren dat hij je nog wat verschuldigd is. Bovendien moet je dat dan ook allemaal gaan bijhouden. Gelukkig zijn er tegenwoordig heel veel apps en manieren die je kunnen helpen. We lichten er een paar voor je uit.

1 We all pay

De app We all pay, die alleen beschikbaar is voor de iPhone, is niet gelieerd aan een bank of financiële instelling. Dit is vooral een handige – en gratis – oplossing om snel in kaart te brengen wie welk bedrag aan wie moet betalen. De app werkt eenvoudig. Zodra je de

app start, kun je een rekening toevoegen. Aangezien deze app niet verbonden is aan een financiële instelling wordt hier geen rekeningnummer bedoeld, maar een rekeningmoment/bonnetje. In ons voorbeeld voegen we een lunch met drie personen toe. Geef aan wie er aanwezig waren, oftewel wie er allemaal dienen te betalen. Vergeet niet om jezelf hier ook toe te voegen. In het tabblad **Betalingen** bovenin druk je vervolgens op **Nieuwe betaling**. Daar geef je aan wie er betaald heeft en waar het precies om ging — als bijvoorbeeld de een de parkeerkosten en de ander het eten en drinken betaald heeft. Specificeer het totaalbedrag dat is betaald en kies onderin wie er moeten bijdragen. Je kunt dus iemand uitschakelen die niet hoeft mee te betalen, handig als je dit als cadeau voor iemand deed. Tot slot druk je op **Oplossing**, waarna er een overzicht wordt getoond van wie precies wat moet betalen aan wie. Druk op **Stuur email** om een bericht te verzenden naar de betrokken personen om ze te laten weten hoeveel ze moeten betalen. Helaas houdt de functionaliteit van de app hier wel op, je kunt niet bijhouden wie er een betaling heeft voldaan.

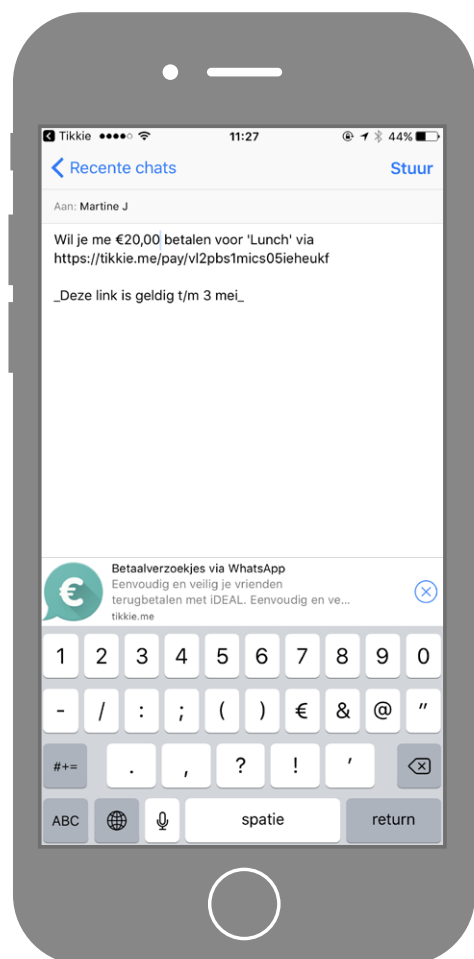
2 Tikkie

Ook Tikkie is een app die je in staat stelt om een rekening te delen, maar dan wel met de mogelijkheid om via iDeal te betalen. De app kan dit, omdat hij gemaakt is door een bank

✓ 01 We all pay is een supersnelle manier om een rekening te verdelen, maar biedt geen betaalmogelijkheid.



(ABN Amro), waarvoor een dergelijke functionaliteit uiteraard eenvoudig te implementeren is. Wanneer je Tikkie hebt gedownload (voor iOS of Android) en gestart, dan moet je je naam, telefoonnummer en bankrekeningnummer opgeven (dat laatste is uiteraard omdat de app wil weten waar het geld naartoe gestort moet worden). Vervolgens kun je aangeven dat je een melding (pushbericht) wilt ontvangen wanneer iemand een rekening betaald heeft. Om een betaalverzoek te starten, druk je op het plusteken rechtsonder. Opvallend is dat je bij deze app het rekenwerk zelf moet doen. Stel dat de rekening 60 euro was en je deelt hem gelijkmatig met z'n drieën, dan vul je 20 euro in en druk je op **Volgende**. Je kunt nu een beschrijving opgeven van de gebeurtenis waarvoor betaald moet worden (maximaal 35 tekens) en vervolgens kun je onderin drukken op **Deel via WhatsApp**. Door op de puntjes daarnaast te drukken kun je ook delen via andere kanalen, zoals Facebook Messenger, sms enzovoort. Vervolgens wordt er een bericht gestuurd met daarin het bedrag, de beschrijving en een betaallink. Wanneer de ontvanger hierop drukt, kan hij/zij direct via iDeal betalen. Het nadeel van deze app is dat je het versturen van een verzoek dus voor iedere persoon afzonderlijk moet doen.



> 02 Tikkie stelt je in staat om via iDeal te betalen, maar je dient wel iedere persoon apart een verzoek te sturen.

Verdienmodel

Het is natuurlijk fantastisch dat je rekeningen zo eenvoudig kunt delen, maar voor niets gaat de zon op. Waar verdienen dit soort apps eigenlijk hun geld aan? Het antwoord daarop is lastig te geven, omdat het verschilt per aanbieder. Aanvankelijk werd beweerd dat banken het geld een aantal dagen vasthielden om zo te profiteren van de rente, maar daarvoor hebben we geen enkel bewijs kunnen vinden. Banken laten hier dan ook niet veel over los, met uitzondering van ABN Amro, dat aangeeft niets aan de app te verdienen – sterker nog, er geldt op te verliezen. Het gebruik van de app levert de bank echter wel nuttige inzichten op over het betaalgedrag van consumenten, dus indirect heeft de bank daar natuurlijk wel veel aan. Daarnaast loopt er nu een test waarbij bedrijven Tikkie (ABN) kunnen gebruiken om klanten extra's aan te bieden (bijvoorbeeld extra beenruimte vlak voor een vlucht). Het gebrek aan een verdienmodel is overigens wel merkbaar aan het feit dat een aantal partijen, waaronder Rabobank en ING, na een jaar al de handdoek in de ring hebben gegooid.

✓ Vooralsnog lijkt er geen verdienmodel te zitten aan dit soort apps.

Hoe werkt Tikkie bij Transavia?

1 Stuur een berichtje via WhatsApp



Laat ons via WhatsApp weten welk product je wilt (bij)boeken. Dit kunnen de volgende producten zijn.

- Ruimbagage
- Speciale bagage
- Stoelen

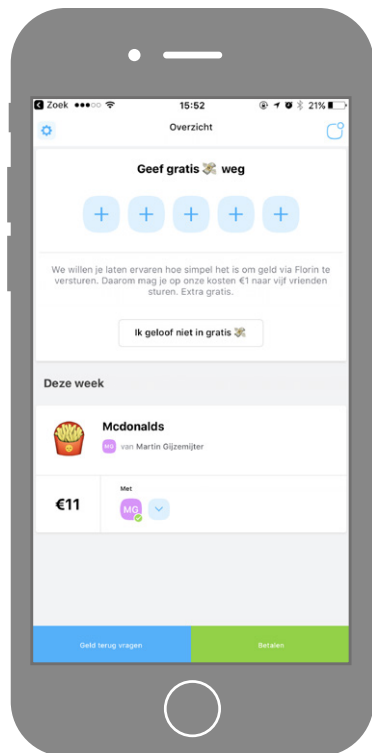
Je kunt ons een WhatsApp-berichtje sturen via: +31613533850

Tip: geef meteen je boekingsnummer door, dan kunnen we je sneller helpen.

3 Florin

Deze app is niet gemaakt door een bank, maar door een aantal jonge ondernemers die een front willen vormen tegen banken. Helemaal zonder de banken kunnen ze niet, want ze hebben iDeal nodig voor de werking van deze app, maar het is natuurlijk wel interessant dat er ook een app is die niet in handen is van een van de grote banken. Wanneer je de app hebt gedownload (Android of iOS) en een account hebt aangemaakt met alle bijbehorende gegevens,

kun je direct van start door te drukken op **Geld terug vragen**. Voeg vervolgens de contactpersonen toe aan wie je het verzoek wilt sturen (Florin werkt via je telefoonnummer), kies een pictogram en vul een omschrijving in. Geef in welk bedrag je terug wilt vragen, voeg eventueel een foto toe (van de gebeurtenis of van 'n smekende blik met puppy-ogen) en druk op **Versturen**. Het bedrag wordt nu automatisch verdeeld tussen de personen, waarbij je de verdeelsleutel eenvoudig kunt wijzigen. Druk nogmaals op **Versturen** en de aanvraag wordt verstuurd per sms, of je kiest een andere app zoals WhatsApp. De ontvanger krijgt nu een bericht met betaallink en kan direct betalen.

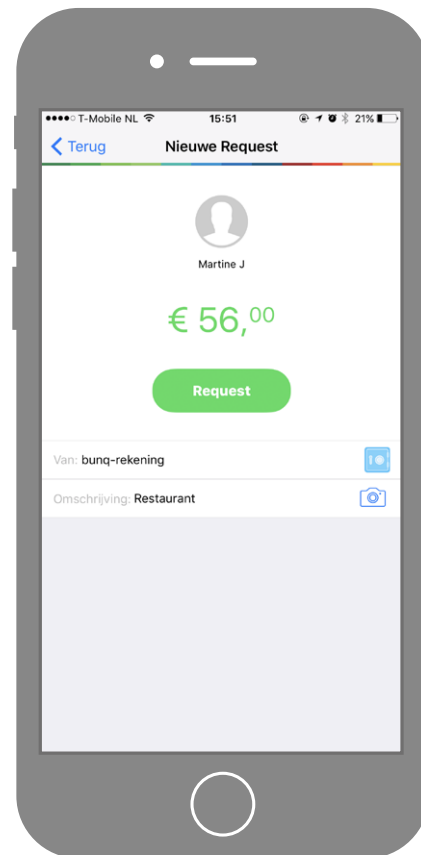


> 03 Florin werkt ook met iDeal, maar is niet in handen van een bank, knap!

4 Bunq

De bijnaam van Bunq is Bank of the Free. Dit heeft te maken met het feit dat de financiële instelling achter de app niets te maken heeft met alle grote banken en daardoor onafhankelijker is. In tegenstelling tot de andere apps is Bunq niet zomaar een betaalverzoekjesdienst, maar een daadwerkelijke bankrekening waar je geld op kunt storten en vanaf kunt halen. Er wordt dan ook best wat aan je gevraagd wanneer je een account aanmaakt. Je kunt je betaalverzoeken alleen sturen aan mensen die ook Bunq hebben. In principe is het versturen van een betaalverzoek heel eenvoudig: je drukt onderin op **Request** en kiest een contactpersoon en geeft aan hoeveel je van deze persoon krijgt en waarom. Deze krijgt dan in zijn/

haar Bunq-app het betaalverzoek binnen. Betalen kan alleen met saldo op je Bunq-rekening, dus niet met iDeal. Als beide partijen een Bunq-rekening met een bepaald bedrag erop hebben, dan is dit een best handige en snelle methode. Wat nog een leuke optie is, is dat je ook kunt betalen door je vingers te scannen met je camera. Heeft één van de twee geen Bunq, dan werkt dit niet. Vind je Bunq erg fijn en wil je je Bunq-rekening omzetten in een 'echte' bankrekening dan kan dat, maar dan moet je wel extra gegevens zoals een identiteitsbewijs afgeven.



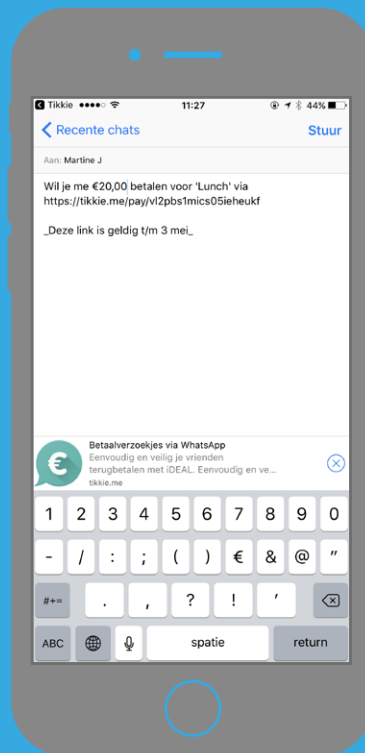
< 04 Bunq is niet zomaar een appje, maar een compleet functionerende bankrekening.

Tik geen vreemden

Hoewel het versturen van betaalverzoeken via dit soort apps ontzettend makkelijk en gebruiksvriendelijk is, kleeft er natuurlijk ook een risico aan. Kwaadwillenden kunnen uiteraard ook dit soort verzoekjes sturen via dergelijke apps en het is dus belangrijk om goed op te letten wie je een bezoeker heeft gestuurd, waarvoor precies en voor welk bedrag. Het is niet zo dat je nu bang hoeft te zijn om dit soort apps te gebruiken, maar zoals altijd: blij waakzaam en voldoe niet altijd zomaar aan verzoekjes.

Communicatie

Het is fijn dat er apps bestaan waarmee je een rekening die je betaalt hebt, later kunt vereffenen met anderen. Al betekent het feit dat jij zo'n app moet gebruiken natuurlijk dat jij vaak degene bent die rekeningen betaalt. Om ruzies of irritaties binnen de vriendenkring te voorkomen, is het wel handig om goed te communiceren over dát je de rekening gaat delen, en hoe je dat gaat doen. Uit ervaring kunnen we je vertellen dat als je na een paar drankjes of een lunch zegt: "Ik betaal wel even" en daarna onaangekondigd een berichtje stuurt voor het delen van de rekening, dat bij anderen voor verbazing kan zorgen. Hoe terecht het ook is dat je de rekening wilt delen, geldzaken blijven een gevoelig onderwerp. Het blijft gênant dat het nodig is, maar introduceer even de app én je plan om de rekening te delen voor of tijdens de gebeurtenis die geld kost, zodat het niet als een verrassing komt.

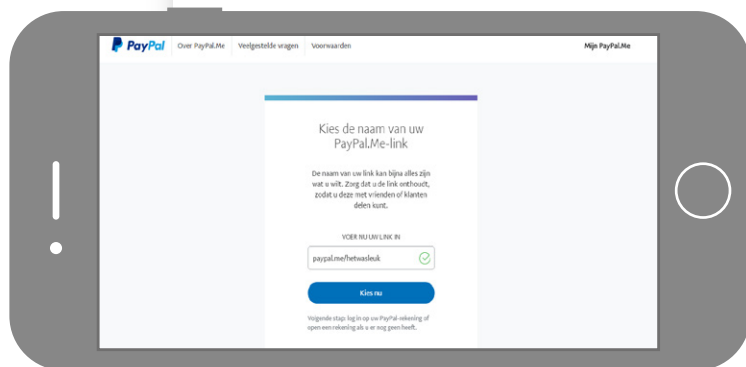


◀ Denk goed na hoe je het verzoek brengt, anders leidt het alsnog tot conflict.

5 PayPal.me

Deze optie is een beetje een vreemde eend in de bijt, omdat het geen app is die je gebruikt, maar een website. PayPal.me is een soort verlengstuk van PayPal, dat je in staat stelt om geld te vragen met behulp van een link. Je gaat hiervoor naar www.paypal.me en bedenkt het woord waaruit je link moet bestaan, bijvoorbeeld hetwasleuk. De link die je genereert wordt dan www.paypal.me/hetwasleuk. Zodra je klikt op **Kies nu**, dien je in te loggen bij PayPal om de link te koppelen aan je account. Het enige dat je nu nog hoeft te doen is de link te sturen naar de mensen aan wie je geld terug wilt vragen, waarna zij direct kunnen betalen. Nadeel? Je moet zelf de bedragen berekenen en mensen kunnen alleen betalen als ze zelf ook een PayPal-rekening hebben.

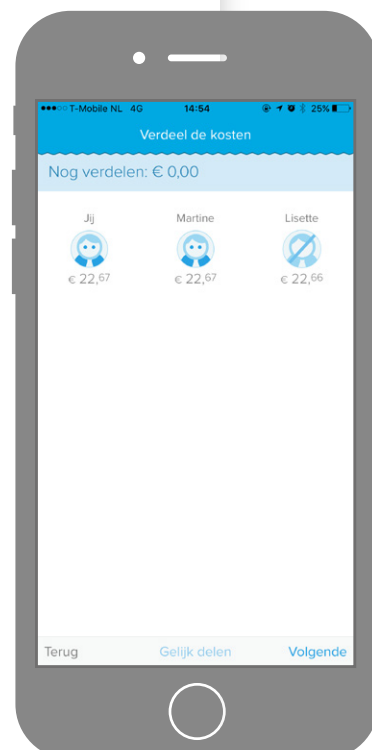
✓ 05 Geen zin om te werken met apps? Met PayPal.me deel je gewoon een betaallink.



6 Sjaak

We betwijfelen of het de reden is dat deze app zo genoemd is, maar als je altijd moet betalen, dan ben je behoorlijk de Sjaak. Het is dan ook niet meer dan gepast dat Sjaak je hierbij gaat helpen. Wanneer je de app (Android en iOS) start, moet je ook hier je naam, telefoonnummer en IBAN opgeven. Vervolgens dien je een groep aan te maken van de mensen met wie je een activiteit hebt uitgevoerd waarvoor betaald moet worden, waarin je uit je adresboek de contactpersonen toevoegt. Wanneer je de groep hebt gemaakt, druk je op **Tijdljn**, waarna je drukt op **Bon toevoegen**. Je geeft nu aan hoeveel geld er is betaald en hoe je dat wilt verdelen tussen jezelf en de mensen van wie je geld krijgt. Sjaak kan dat zelf berekenen of je past zelf een verdeling toe. Vervolgens krijgen de betrokkenen een betaalverzoek. Daarbij is het wel belangrijk dat de andere partijen

✓ 06 Bunq is niet zomaar een appje, maar een compleet functionerende bankrekening.



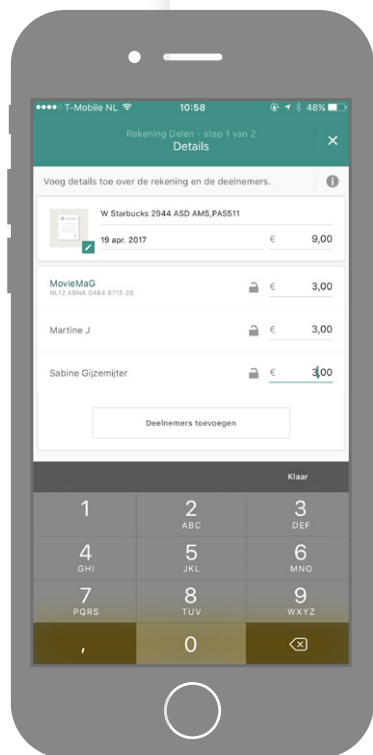
ook Sjaak hebben. Het enige dat niet zo fijn is aan de app, is dat je de betaling zelf moet regelen; je krijgt geen iDeal-link of iets dergelijks. Dat zou de app wat ons betreft trouwens perfect maken (maar we begrijpen dat dat lastig is bij een gratis app).

7

De bank

Naast losse apps die je kunt installeren om een rekening te delen, kun je bij een deel van de banken

terecht bij de eigen app van de bank. Dit kan onder andere bij ING met het Betaalverzoek, en bij ABN Amro met Rekening delen. We beschrijven de manier in de ABN-app. Tijdens het betalen van de rekening zelf hoeft je nergens rekening mee te houden. Wanneer je de transactie hebt voltooid, zal deze verschijnen in het transactieoverzicht van de bank. Log je vervolgens in op de app (in het geval van ABN Amro) en druk je op de betreffende transactie, dan zie je onder in beeld de optie **Rekening delen**. Wanneer je hierop drukt, dan kun je deelnemers toevoegen, oftewel, de mensen met wie je het bedrag wilt delen. Wanneer je deelnemers toevoegt (je heb hiervoor hun naam en e-mailadres nodig), wordt



het bedrag automatisch verdeeld over het aantal personen. Je kunt het bedrag van een specifieke persoon aanpassen, waarna het restant verdeeld zal worden tussen de rest. Druk op **Volgende** wanneer je tevreden bent met de verdeling. Je kunt nu een persoonlijk bericht toevoegen, dat wordt de inhoud van de e-mail. Deze inhoud zal, samen met de informatie over het te betalen bedrag, worden verzonden zodra je drukt op **Verzenden**. De betaling zal overigens handmatig moeten worden gedaan en kan niet, zoals bij de Tikkie-app, via iDeal.

8

Continuïteit

De markt rond het delen van rekeningen (of sociaal betalen zoals het ook wordt genoemd) is nogal een dynamische. De ene na de andere app duikt op, met wisselend succes. Tegen de tijd dat dit artikel verschijnt, zijn er ongetwijfeld apps verschenen die wij nog niet hebben beschreven. Apps verdwijnen ook regelmatig. Zo bleken apps als Twyp (ING) en Grppy (Rabo) geen lang leven beschoren. Voordat je op een nieuwe app duikt, is het dus verstandig om de kat uit de boom te kijken, zodat je kunt lezen wat de ervaringen van anderen zijn. Als je het niet erg vindt om tijd te investeren in een app die er misschien over een tijdje niet meer is, kun je er natuurlijk voor kiezen om een 'early adopter' te zijn (die zijn immers ook nodig wil een platform ooit van de grond komen). Staar je in ieder geval niet blind op grote merken achter dergelijke apps: zowel ING als Rabo hebben laten zien net zo makkelijk weer te stoppen als de dienst niet bevalt. ■

07 Banken bieden zelf ook de mogelijkheid om rekeningen te delen.

[Naar ING.nl](#)

ING Nieuws

[Nieuws- en persberichten](#)
[Perscontact](#)
[Beeldmateriaal](#)
[Agenda](#)
[Feiten en cijfers](#)
[ING Directie](#)

Twyp neemt afscheid van Nederland

Amsterdam, 21-11-2016 09:00

Twyp stopt per 15 december 2016 in Nederland. Twyp is een mobiele app waarmee gebruikers snel en makkelijk geld aan elkaar kunnen overmaken via hun contactenlijst. De app werd in januari 2016 door ING in Nederland gelanceerd, een paar maanden na de lancering in Spanje. Uit de ervaringen van Nederlandse Twyp-gebruikers blijkt dat het gebruiken van een aparte betaalapp, die niet gekoppeld is aan je betaalrekening, onvoldoende toegevoegde waarde biedt. In Spanje is Twyp van ING met ruim 300.000 gebruikers succesvol en blijft de app in de markt.

Innoveren is experimenteren
ING werkt continu aan vernieuwingen die aansluiten bij de behoefte van klanten. Daarbij hoort het experimenteren met nieuwe innovaties zoals Twyp en het stapsgewijs verbeteren op basis van feedback van gebruikers. Innoveren betekent het verder ontwikkelen van succesvolle innovaties, maar ook stoppen met producten en diensten die onvoldoende aansluiten bij de behoefte van klanten.

Twyp in Spanje succesvol
Twyp is eind vorig jaar als eerste geïntroduceerd in Spanje, daar is de app met ruim 300.000 enthousiaste gebruikers succesvol. De Spaanse markt voor mobiel bankieren is anders dan in Nederland. Zo hebben mobiel bankieren apps in Spanje minder functionaliteiten dan de Nederlandse apps. Twyp blijft daarom in Spanje bestaan en wordt daar verder doorontwikkeld. Recent heeft ING in Spanje Twyp Cash geïntroduceerd waarmee in ruim 3500 winkels en tankstations betaald kan worden.

Bankieren makkelijk maken
ING wil bankieren zo makkelijk mogelijk maken voor haar klanten. De ING Mobiel Bankieren App wordt goed gewaardeerd door klanten en er worden voortdurend nieuwe functionaliteiten aan de app toegevoegd zoals recent het betaalverzoek. Hiermee kunnen klanten van ING en andere Nederlandse banken elkaar snel onderling (terug)betalen via onder andere WhatsApp, sms en e-mail. Daardoor is een aparte app, die niet gekoppeld is aan je betaalrekening, voor onderlinge betalingen niet nodig.

Contact voor de media
 Eva Hersbach
 +31 651301832
eva.hersbach@ing.nl

08 Kijk wel goed naar de beschikbare partijen, er zijn er namelijk ook alweer veel gestopt.

VOORKOMEN IS BETER DAN GENEZEN

Blijf ransomware voor

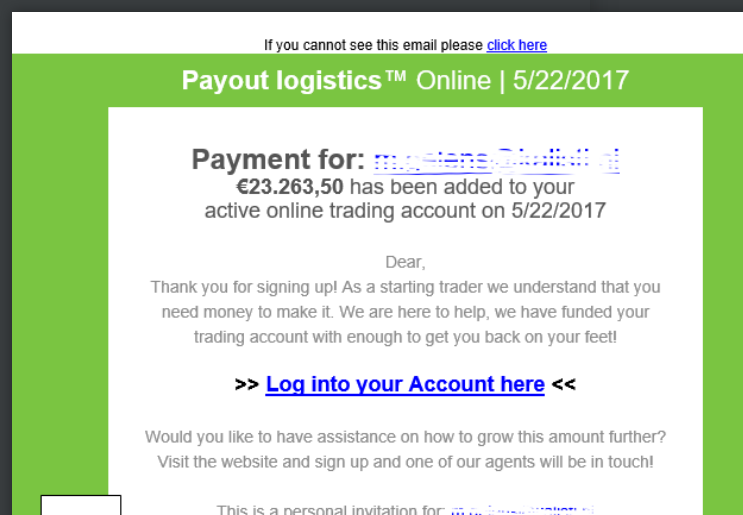
Met de WannaCry malware-aanval van afgelopen voorjaar staat ransomware helemaal in de belangstelling. Malwarebesmettingen die bestanden gijzelen en losgeld eisen, zijn al een tijd zeer populair bij criminelen. Het kost beveiligers moeite om computers automatisch tegen deze aanvallen te beschermen. We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

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



1

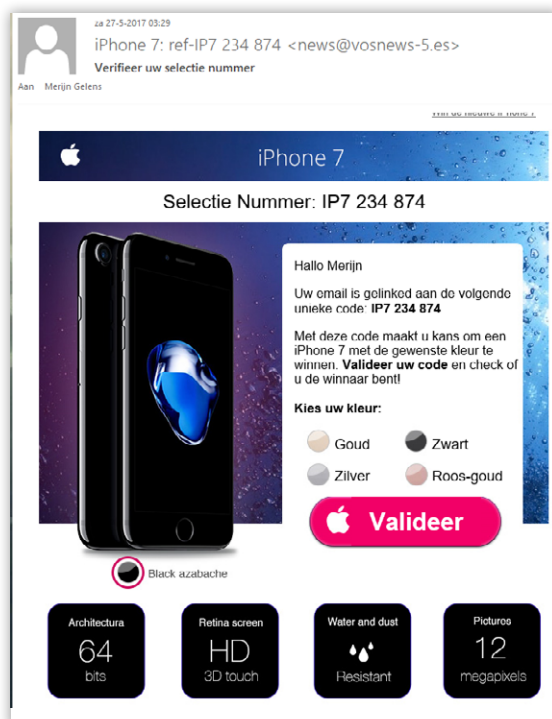
Blijf scherp

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 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.

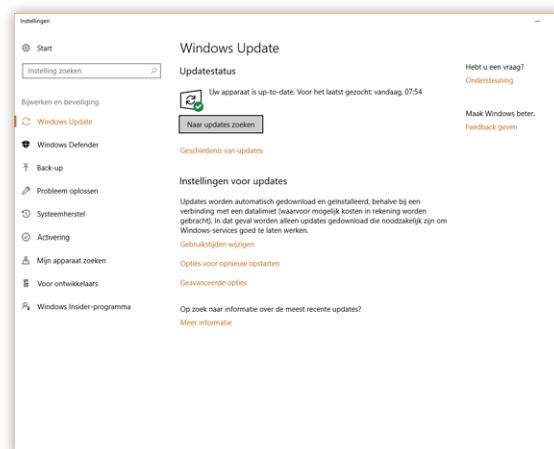
speelt die overweging niet mee. Gebruik dus de automatische updates die Microsoft voor Windows en Office beschikbaar stelt. De installatie en de mogelijke herstart die nodig is kan irritant zijn, maar deze ergernis weegt niet op tegen de gevolgen die het alternatief kan hebben. Door Microsoft-software 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.

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



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)

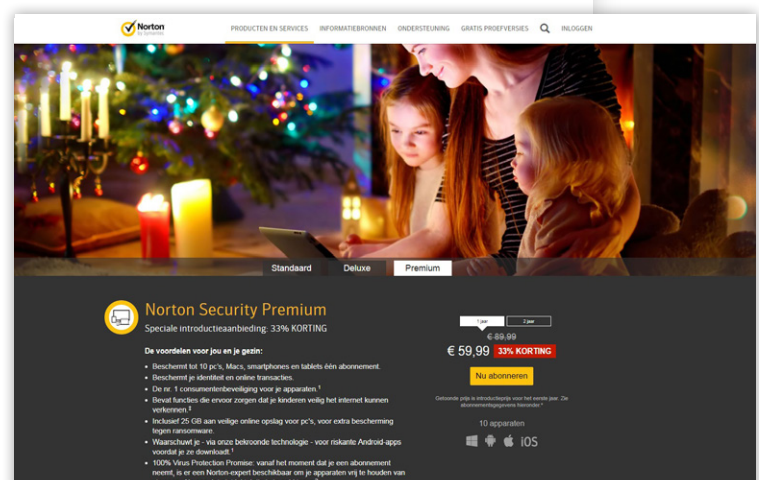


< 02 Maak gebruik van de automatische updates om zwakke plekken in je systeem automatisch te dichtten.

3 Installeer beveiligingssoftware

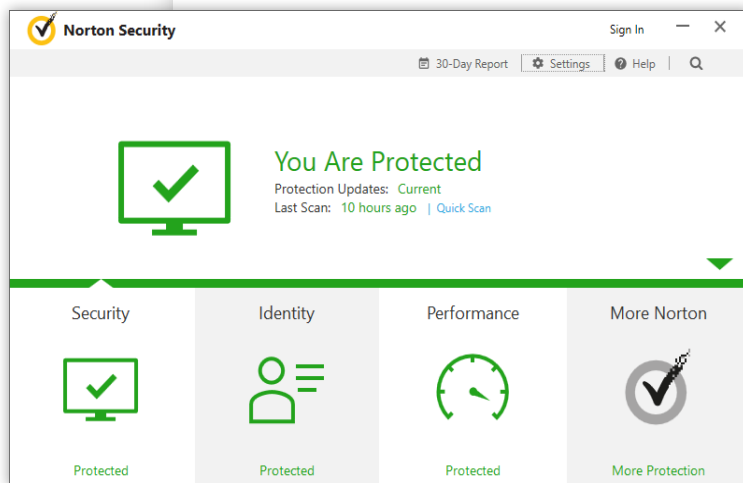
Een beveiligingspakket is onmisbaar op iedere computer. Alle beveiligingssoftware, van de ingebouwde gratis scanner van Windows Defender tot het meest kostbare zakelijke pakket, scant op bekende dreigingen en herkent gedragspatronen van toepassingen. Dat voorkomt dat je slachtoffer wordt van een (variant op een) bekende aanval. Bescherming tegen ransomware vraagt om specifieke extra bescherming die niet ieder-

> 03 Sommige beveiligingspakketten hebben speciale bescherming tegen aanvallen met ransomware.



✓ 03 Naast je applicaties en besturingssysteem is het zeer verstandig om te zorgen dat je beveiligingssoftware up-to-date is.

een 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 aangeropen 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.

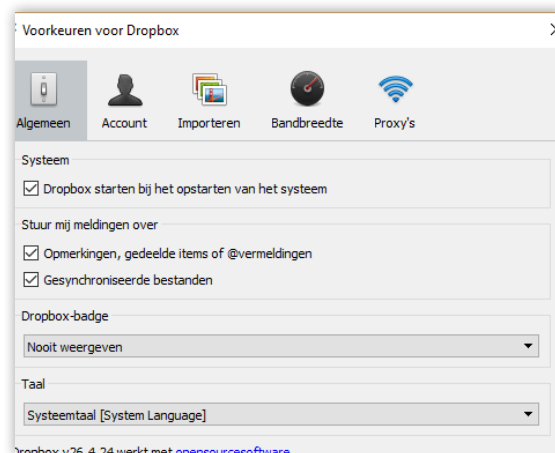


4 Onveilige back-ups

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,

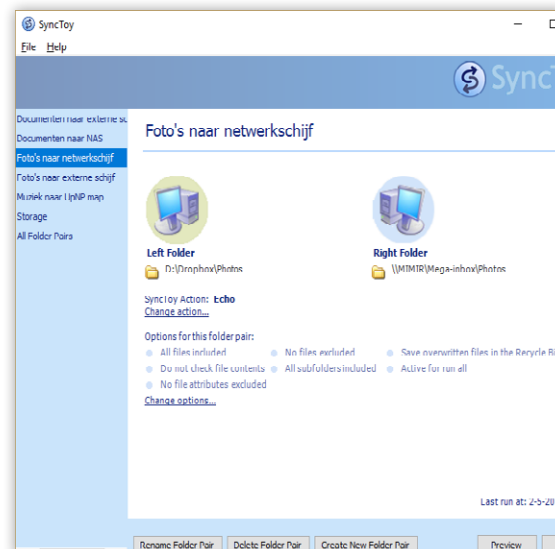
Misbruik van gelekte NSA-informatie

Vorig jaar bracht een hackersgroep met de naam ShadowBrokers 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.



< 04 Cloudopslag zoals Dropbox is geen goede back-uplocatie als je je tegen ransomware wilt beschermen.

dan zou je met versiebeheer kunnen teruggrijpen naar een niet-versleutelde versie. Helaas zijn er ook varianten ransomware die de schaduwkopieën beschadigen.



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

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.



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 schaad 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 beveiliging redding bieden.

Norton Security	STANDAARD	DELUXE	PREMIUM
	Aanbevolen voor gezinnen		
1 jaar	2 jaar	1 jaar	2 jaar
€59,99	€79,99	€89,99	
€29,99	€49,99	€59,99	
50% KORTING	37% KORTING	33% KORTING	
Nu abonneren	Nu abonneren	Nu abonneren	
Getoonde prijs is de prijs voor het eerste jaarabonnement. Zie abonnementsgegevens hieronder.*			
1 pc, 1 Mac of 1 mobiel apparaat	5 apparaten	10 apparaten	
> Voordelen weergeven	> Voordelen weergeven	> Voordelen weergeven	

HOUD GESPUIS BUITEN

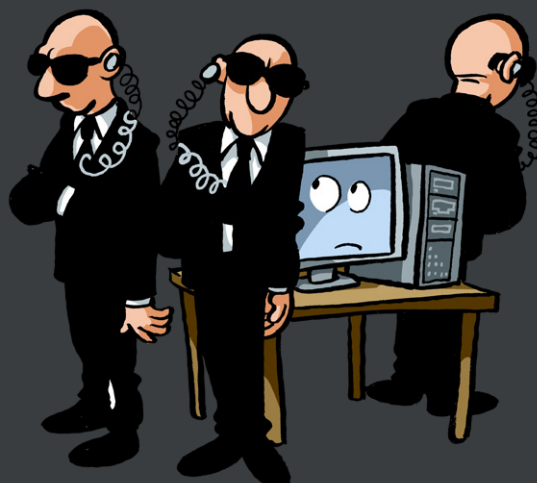
Van ransomware tot digitale spionnen

Het liefst wilt u natuurlijk voorkomen dat u slachtoffer wordt van criminelen die u via ransomware afpersen of uw systeem kapen. Recent is er zelfs in het journaal aandacht besteed aan een grote wereldwijde aanval. We helpen u met software die daadwerkelijk beschermt tegen datadieven.

DIRK SCHOofs

RansomFree

Ransomware is het type malware dat de bestanden op uw pc versleutelt zodat u er niet meer bij kunt. De criminelen eisen losgeld voordat ze de sleutel vrijgeven waarmee u uw gegevens kunt ontsleutelen. Als ze zich aan hun woord houden tenminste, en daar bent u nooit zeker van. RansomFree (<https://ransomfree.cybereason.com>) is een toeltje van Cybereason dat uw systeem bewaakt tegen ransomware. De installatie

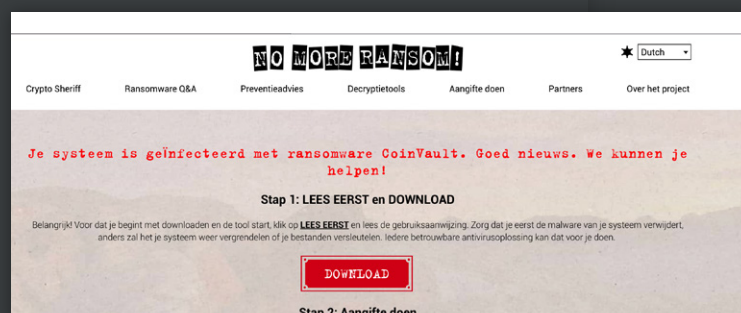


heeft niet veel om het lijf, het programma gebruikt nauwelijks pc-kracht. In feite slaapt RansomFree tot het ransomware op heterdaad betrapt. Wanneer software zich gedraagt als ransomware, ontvangt de gebruiker een waarschuwing en zal het de versleuteling van zijn bestanden blokkeren. Bij een foute detectie kan de gebruiker beslissen het proces toch toe te laten. De tool onthoudt uw keuze en zal deze ransomware opnieuw automatisch tegenhouden wanneer die de volgende keer de kop opsteekt. De makers beweren dat RansomFree in 99% (lees: veel, maar niet alle) van de gevallen afdoende werkt en dat deze pro-tection zelfs de bedreiging van WannaCry of WCry voorkomt.

No more ransom!

No More Ransom (www.nomoreransom.org) is een initiatief van de Nederlandse politie, Europol en enkele grote softwaremerken. Het Centrum voor Cybersecurity houdt een lijst bij van decryptiesleutels om uw bestanden mee te ontsleutelen. Helaas is er nog niet voor iedere versie van ransomware een sleutel beschikbaar, maar wanneer u de oplossing hier toch in de lijst aantreft, kunt u echt opgelucht adem halen. Op de website vindt u 'Crypto Sheriff', een applicatie die ontwikkeld is om de ransomware te herkennen die uw systeem aantast. Daartoe laadt u een versleuteld bestand naar 'Crypto Sheriff' zodat die meteen nakijkt of er een decryptie-

✓ We hebben geluk: Crypto Sheriff heeft de sleutel voor de ransomware waarmee onze computer besmet is



oplossing beschikbaar is. U kunt ook het websiteadres opgeven dat te zien is op het vergrendelscherm dat door de ransomware getoond wordt. Tenslotte helpt deze site om aangifte te doen bij de politie, want het gaat tenslotte wel om een combinatie van misdrijven: afpersing, computersabotage, computervredebreuk én het plaatsen van aftapapparatuur.

ScanCircle

De cyberaanval van half mei maakte misbruik van een lek in het Windows-besturingssysteem. Dat lek was door Microsoft wel al gedicht in een recente update. Een belangrijke manier om ransomware te voorkomen is dus zorgen dat alle software up-to-date is, waaronder het besturingssysteem, de internetbrowser, de browserplug-ins en de populaire programma's. ScanCircle (www.scancircle.com/nl) kijkt uw computer na van top tot teen. U ontvangt eerst een algemene veiligheidsscore en daaronder leest u in vijf tabbladen hoe u het systeem kunt verbeteren. De linkerbalk met de adviezen is belangrijk (de rest van de pagina bestaat uit reclame voor onder andere computerbedrijven in de buurt). Bij deze adviezen staat in de meeste gevallen de link waarmee u de update binnenhaalt. U kunt ook met de muisaanwijzer over de items in de adviezen gaan: u leest dan in het tekstvak hoe u het probleem kunt oplossen.

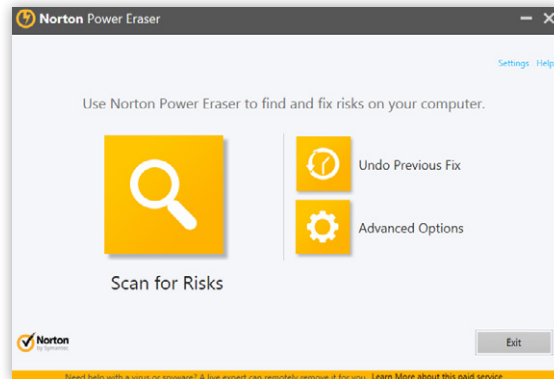


> Nadat u de adviezen hebt gevolgd, kunt u een nieuwe scan uitvoeren om de nieuwe resultaten te vergelijken met de oude.

Norton Power Eraser

Opent uw browser na het opstarten een startpagina die u helemaal niet hebt opgegeven? Of springt hij tijdens het surfen onverwacht naar een dubieuze site? Waarschijnlijk zit u met een browserkaper opge-zadeld. Een browserhijacker richt zich speciaal op internetbrowsers. Dit levert de verspreider advertentie-inkomsten op, want het aantal bezoekers wordt hiermee kunstmatig opgekrikt. Bovendien doen deze kapers graag dienst als spion en zenden ze vaak informatie over uw surfgedrag door.

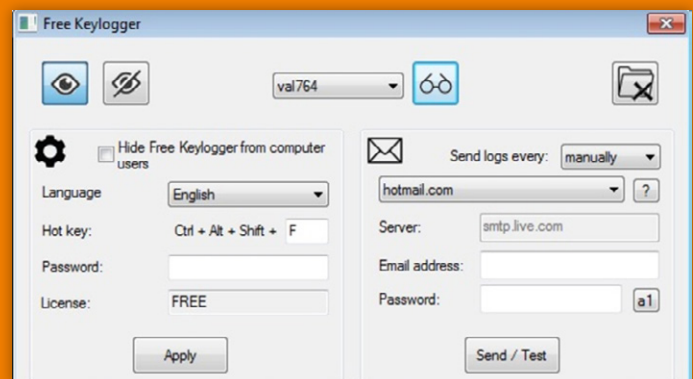
Norton Power Eraser (<https://security.symantec.com/nbrt/npe.aspx>) is een gratis tool die erin gespecialiseerd is dit soort rotzooi te verwijderen. In het programma klikt u op de knop Unwanted Application Scan en daarna volgt u de instructies om de kaper(s) te verwijderen.



< Let op, want Norton Power Eraser is een agressief virus-verwijderingsprogramma, dat soms legitieme programma's markeert voor verwijdering.

Keyloggers

Een keylogger is een piepklein programma dat stiekem op een pc wordt geplaatst. Vanaf dan werkt de keylogger als recorder. Hij neemt iedere toets die de gebruiker indrukt op en stuurt alle deze informatie naar een pc op afstand. In de sommige gevallen is dat de computer van een hacker die op die manier uw wachtwoorden en vitale gegevens als creditcard-gegevens gewoon in het logboek leest. Gek genoeg valt deze software in Verenigde Staten onder de noemer 'software for parental control', een programma voor ouderlijk toezicht. Ouders kunnen hiermee volgen wat zoon- of dochterlief op hun computer doet, maar partners kunnen hiermee ook elkaar bespioneren.



> Bepaal hoe vaak de keylogger het logboek van alle toetsaanslagen stiekem naar een bepaald e-mailadres moet verzenden.

Ghostpress

Met Ghostpress (<https://hendrik.tf/ghostpress.html>) bent u de keyloggers een stap voor. De tool verbergt namelijk uw toetsaanslagen voor deze spionnen. Het gaat om een bijzonder bescheiden en eenvoudig programma. U hoeft zelfs niets te installeren, het Ghostpress-spookje

zit voortaan in het systeemvak. Met de rechtermuisknop kunt u het programma op het bureaublad oproepen. Vandaar is de bediening de eenvoud zelve: klik op de groene knop om de bescherming te starten en op de rode knop om Ghostpress te stoppen. In de instellingen kunt u de vertragingsscherm activeren waardoor een keylogger een gebruiker niet langer herkent aan diens typische typstijl. En met de optie 'Hook-overschrijving' voorkomt u dat de keylogger Ghostpress zou passeren.

Prey

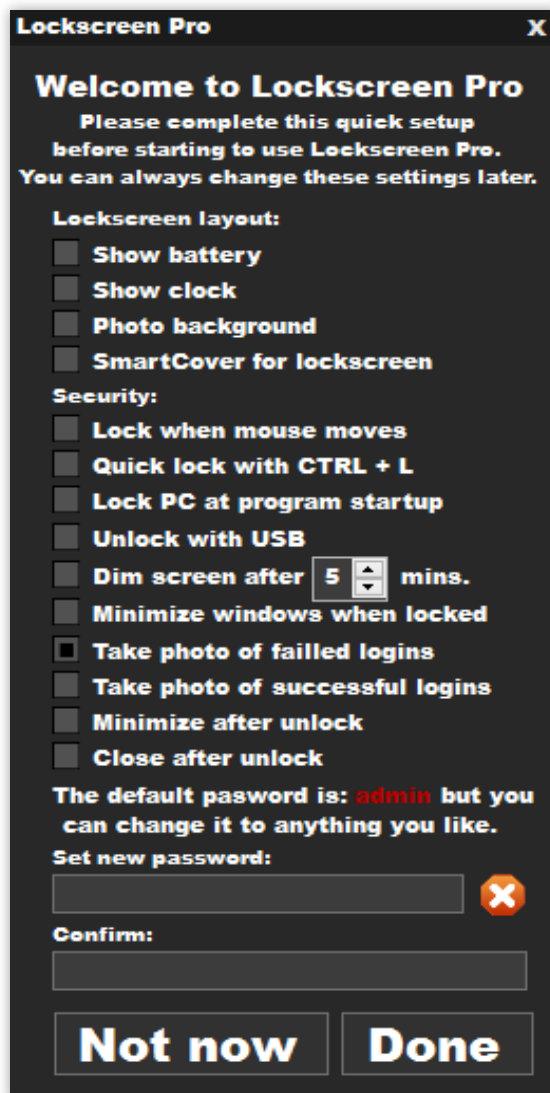
Bang dat uw laptop, tablet of smartphone wordt gestolen? Of gebeurt het vaak dat u niet meer weet of u het toestel op kantoor of in de sportclub hebt achtergelaten? Met het gratis anti-diefstal programma Prey (www.preyproject.com) maakt u geruisloos contact met het apparaat wanneer het verbinding maakt met het internet. U leest de locatie, het programma verstuurt een schermafbeelding wanneer de dief bijvoorbeeld zijn Facebook opent, u maakt een foto op afstand van de dief, u verwijdert eigen wachtwoorden, laat hard geluid afspelen of blokkeert het besturingssysteem. Prey werkt op macOS, Windows, Android en iOS. U kunt met de gratis versie tot drie apparaten beheren. Een betaald Prey Pro-account (15 dollar per maand) maakt altijd gebruik van een versleutelde verbinding via het https-protocol en kan meer dan drie apparaten bedienen en meer dan twintig rapporten bewaren. Daarnaast is het mogelijk om tien zones op een landkaart

af te bakenen (geofencing) waarbij u een notificatie van Prey ontvangt zodra uw apparaat binnen of buiten deze zone(s) komt.

Lockscreen pro

De meeste indringers in computersystemen zijn geen duistere types met bivakmutsen die op afstand uw bestanden proberen te bekijken. Heel vaak gaat het om huisgenoten, collega's of medewerkers die een ongezonde vorm van nieuwsgierigheid aan de dag leggen. Met Lockscreen Pro (<https://sourceforge.net/projects/lockscreenpro>) vergrendelt u uw pc met één muisklik. Vanaf dat moment komt u op het beveiligingsscherm waarop, als u dat wilt, ook de batterijstand te zien is. Uit de naam zou u kunnen afleiden dat het om een betaald programma gaat, maar dat is niet het geval. Uiteraard opent het systeem weer met het juiste wachtwoord. Leuk is dat u Lockscreen Pro kunt opdragen om met de webcam een foto te nemen van iemand die probeert in te loggen. Bovendien kunt u een usb-stick gebruiken als sleutel van uw pc of laptop.

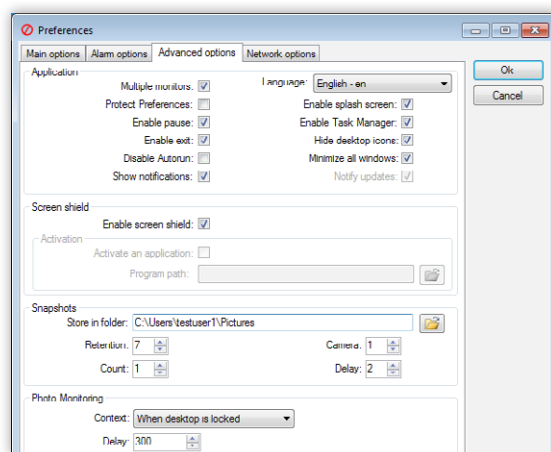
✓ Welke acties verwachten we van Prey om deze iPad Mini terug te vinden?



◀ Wanneer iemand een mislukte poging doet om in te loggen, zal de laptop automatisch een foto van deze persoon nemen.

Predator

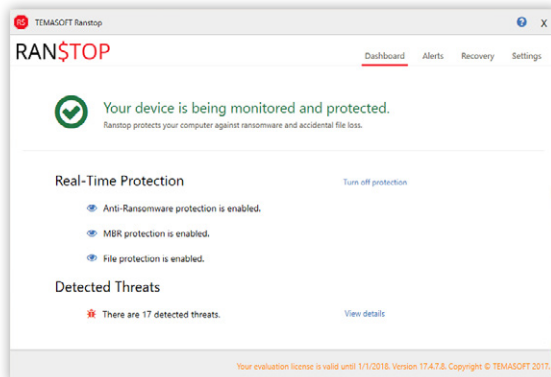
Gebruik een geprepareerde usb-stick als toegangssleutel voor uw systeem. De bedoeling van de makers van Predator (www.predator-usb.com) is uw computer beter te beveiligen bij een korte afwezigheid. Nadat u inlogt, controleert de software of de usb-stick in uw pc steekt. Is dat zo, dan kunt u beginnen. Is dat niet het geval, dan zal het veiligheidssysteem de muis en het toetsenbord deactiveren en het systeem afsluiten. Wanneer u de usb-stick bent vergeten, kunt u gelukkig nog bij uw bestanden met een wachtwoord. Bij de opties is het mogelijk regelmatig te laten controleren of de stick nog aanwezig is. Predator bestaat in een gratis en een betaalde versie.



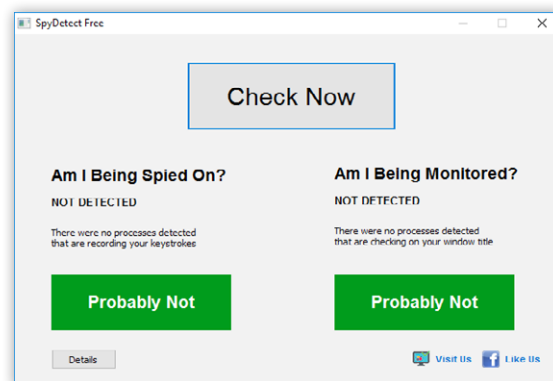
> Ook Predator kunt u foto's laten nemen van de persoon die probeert in te loggen.

Ranstop

Zorg dat alle systeemupdates zijn uitgevoerd en installeer een behoorlijk antivirusproduct om een ransomware-aanval af te slaan. Pas wanneer die twee factoren in orde zijn, kunt u nog een gespecialiseerd anti-ransomware-product installeren voor extra veiligheid. Terasoft Ranstop (www.terasoft.com/ranstop-anti-ransomware) is een commercieel product dat automatisch ransomware-aanvallen voorkomt en blokkeert. Het werkt met een 'Protection engine' en een 'File recovery engine'. Het isoleert besmette pc's van het netwerk zodat de besmetting zich niet kan uitbreiden. Bovendien start Ranstop het herstelproces op basis van back-ups. Een licentie voor één machine kost 29 dollar (ongeveer 26 euro) op jaarbasis.



> Ranstop biedt realtime bescherming, en herstelt eventuele besmette bestanden via hun back-up.



Spydetect free

Wordt u bespioneerd? Of wordt u constant in de gaten gehouden? De twee vragen lijken hetzelfde, maar SpyDetect Free (www.worktime.com/spydetectfree) maakt een onderscheid. In het eerste geval zoekt deze gratis software naar keyloggers of hooks op uw toetsenbord. Zoals gezegd wordt dit soort malware vooral door huisgenoten of collega's op uw computer gesmokkeld. Op de vraag of u ook in de gaten wordt gehouden, zal SpyDetect Free de lopende processen nakijken. Het gaat na of daar processen bijzitten die uw computeractiviteiten registreren. Het gebruik van deze tool is al even eenvoudig als de installatie. Er is één knop, Check Now. Is het antwoord op beide vragen Probably Not, dan hoeft u zich weinig zorgen te maken. Verschijnt er toch een rode knop, klik dan op Details om meer informatie te krijgen over het probleem. SpyDetect Free is een nuttige tool die u geen euro kost, waarbij u niets hoeft te installeren én u kunt het portable vanaf een usb-stick laten werken. :

< Oef, we worden niet gevolgd en niet bespioneerd.



15

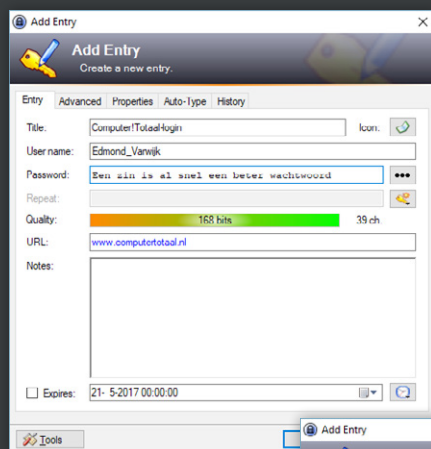
KEER VEILIG(ER) INLOGGEN

Maak de zwakste schakel sterker

Overheidszaken, bankrekeningen, mailverkeer, cloudbestanden, beheerde apparaten ... Als je er zo over nadenkt heb je best veel achter een inlog zitten.

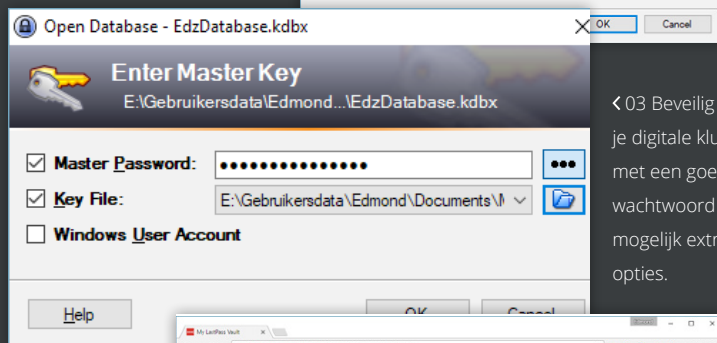
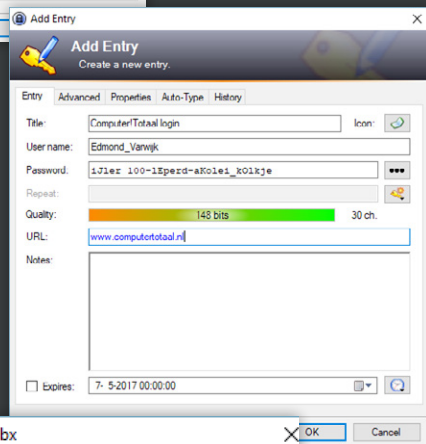
Intussen hoeven we niet meer uit te leggen dat je voor een veilig en uniek wachtwoord dient te zorgen. Maar er zijn andere zaken om in acht te nemen, zaken waarmee je het inloggen veiliger én makkelijker kunt maken. En dat hoeft helemaal niet altijd te betekenen dat het meer moeite kost.

EDMOND VARWIJK



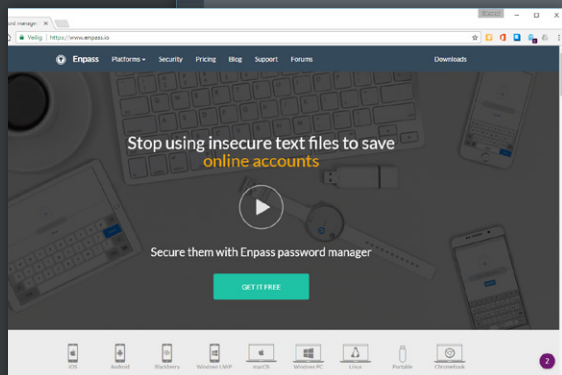
< 01 Een zin is makkelijker te onthouden dan alleen een wachtwoord.

> 02 Met een dobbelsteen en een woordenlijst vorm je een goed onthoudbare wachtwoord(on) zin



< 03 Beveilig je digitale kluis met een goed wachtwoord en mogelijk extra opties.

> 04 Bij een noodgeval kun je een vertrouwde persoon toegang tot jouw digitale kluis geven.



< 05 Enpass ondersteunt een groot aantal platformen met echte apps en applicaties.

1 Beter lang dan complex

De sterkte van een wachtwoord geeft aan hoe snel het geraden kan worden. Het is de functie van lengte x complexiteit x onvoorspelbaarheid. Omdat lange wachtwoorden moeilijk te onthouden zijn, wordt er vaak gegooid met de 96 tekens op het toetsenbord. Maar hackers raden geen wachtwoorden: ze gebruiken de computer en daarvoor maakt het niet uit of er een letter, hoofdletter, leesteken of cijfer staat. Voor een computer wordt het vooral lastiger als een wachtwoord langer is: elke extra positie maakt het wachtwoord exponentieel sterker. Een lange zin is daardoor beter dan een cryptisch wachtwoord, ook om te onthouden.

2 Entropie

Met alleen een wachtwoordzin ben je er nog niet: computers zijn namelijk goed in het herkennen van woorden. Kies daarom niet voor spaties, maar streepjes of komma's. Een dictionary-attack, waarbij het woordenboek woord voor woord wordt gebruikt, is dan kansloos. Gebruik ook entropie. Entropie is de hoeveelheid wanorde in het wachtwoord. Een zin als 'Ik woon in een huis' is erg voorspelbaar, terwijl 'ijler 100 leperd akolei kolkje' ook te onthouden én minder kwetsbaar is. Zo'n onzin-zin maak je met Diceware. Je selecteert de woorden door telkens vijf keer met een dobbelsteen te gooien. Diceware vind je op www.tiny.cc/dice.

3 Offline versus online

Gebruik geen pen en papier, maar een wachtwoordmanager: een versleutelde digitale kluis beveiligd met een sterk hoofdwachtwoord. Er zijn offline en online wacht-

woordmanagers, zie ook pagina 46. Bij een offline versie staan de applicatie en kluis op de pc, bij een online wachtwoordmanager draait alles in de browser via de cloud. Beide hebben voor- en nadelen. Offline heb je de gegevens slechts op één apparaat en ben je kwetsbaar bij malware. Online biedt standaard apparaatsynchronisatie, maar je moet wel de clouddienst vertrouwen en hopen dat deze niet gehackt wordt.

4 Noodgevallen

LastPass (www.lastpass.com) is een online wachtwoordmanager. Op de pc gebruik je de browser om je wachtwoorden te gebruiken. LastPass integreert met alle bekende browsers en vult dan de inloggegevens automatisch voor je in als je een site bezoekt. Doordat de wachtwoordkluis in de cloud staat, is deze altijd toegankelijk. Er zijn ook mobiele apps. LastPass biedt enkele leuke extra's. Zo kan het de kwaliteit van jouw wachtwoorden beoordelen en kun je log-ins tijdelijk delen. Voor noodgevallen kun je anderen (tijdelijk) toegang verlenen tot je kluis.

5 Mengvorm

Enpass van www.enpass.io is een offline wachtwoordmanager, met synchronisatie en apps. Enpass biedt je de mogelijkheid de lokale digitale kluis via de cloud te synchroniseren. Bij elke wijziging wordt de hele versleutelde kluis gekopieerd, dus niet alleen de wijziging. Zo gaat er dus nooit een niet-versleuteld wachtwoord over het internet. Je kunt zelf de clouddienst selecteren die je hiervoor gebruikt: Dropbox, Google Drive, OneDrive, Box, Map en elke vorm van WebDAV inclusief ownCloud. Enpass is gratis op Windows en macOS, voor de app betaal je een klein bedrag.

6 Hergebruik

Veel datalekken worden veroorzaakt door wachtwoordhergebruik bij meerdere websites en diensten. Nadat een site gekraakt wordt, kunnen hackers de gegevens hergebruiken. Dé oplossing hiervoor is overal een uniek wachtwoord gebruiken, maar dat is met het grote aantal plekken waar je moet inloggen niet te doen. Minimaliseer het risico van hergebruik door het wachtwoord toch telkens op details te veranderen of gebruik een wachtwoordmanager. Op <https://haveibeenpwned.com> kun je zoeken of jouw inloggegevens bij een van de laatste grote datalekken zijn buitgemaakt. Pas ze in dat geval zeker aan voor de betreffende site én alle plekken waar je hetzelfde wachtwoord gebruikt.

7 Wachtwoordreset

Ben je een wachtwoord kwijt, dan bieden veel online diensten de mogelijkheid het te resetten. Vaak moet je dan eerst een paar vragen beantwoorden, vragen waarvan je bij de registratie lang daarvoor zelf de antwoorden hebt gegeven. Noteer dus ook die vragen én de antwoorden in de wachtwoordmanager én bedenk dat een beetje hacker via Google al snel ook weet waar je moeder is geboren of wat je favoriete voetbalclub is. Ga je voor echt veilig, geef dan op elke controlevraag bewust een foutief antwoord – maar vergeet niet het opgeven antwoord, liefst met de vraag, te noteren!

8 2fa

Een belangrijke stap om het inloggen veiliger te maken, is het toevoegen van een tweede factor voor de authenticatie. Naast het

wachtwoord wordt er dan nog een bewijs gevraagd. Dat kan een pas zijn die je hebt zoals bij de pinautomaat, maar ook een sms-code. Andere bekende vormen van een tweede factor voor authenticatie zijn een vingerafdruk of een iris-scan. Steeds meer smartphones zijn tegenwoordig uitgerust met een vingerafdrucscanner, dus vooral van deze mogelijkheid zal steeds vaker gebruik worden gemaakt. Nadeel is dat je afhankelijk bent van de aanbieder van de dienst. Die bepaalt of en zo ja, welke vormen van multifactor-authenticatie worden toegestaan.

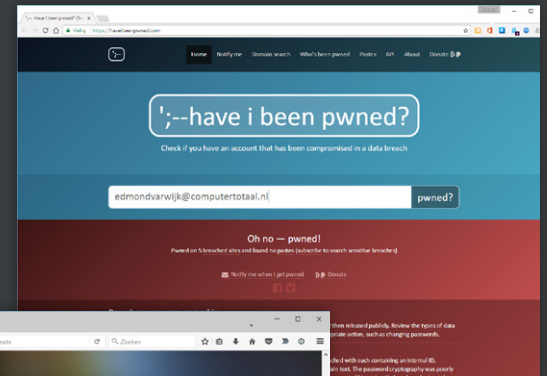
9 Veiliger en handiger DigiD

Om in te loggen op overheidssites gebruik je DigiD. Deze bijzonder gevoelige gegevens wil je goed beveiligen. Standaard bestaat DigiD uit een gebruikersnaam en een wachtwoord, optioneel kun je een sms-code toevoegen. Je kunt deze ook verplichten. Nog handiger gaat het met de DigiD-app. Installeer de app op de smartphone en log in op www.digid.nl. Ga naar **Inlogmethoden** en volg de stappen voor **DigiD-app activeren**. Als de registratie is voltooid, kun je inloggen door de qr-code op de DigiD-site te scannen.

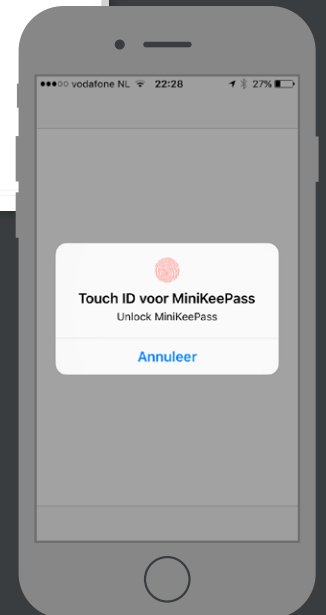
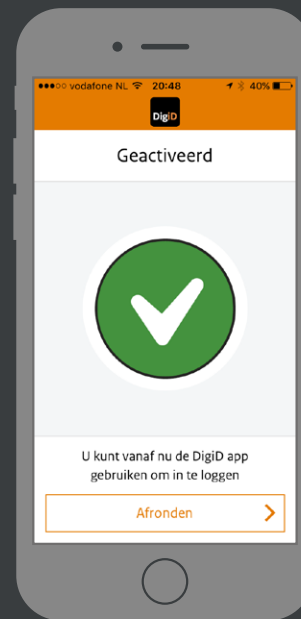
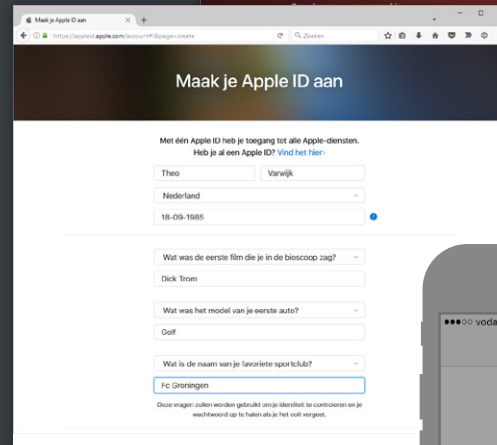
10 Browserintegratie

Gebruik je een wachtwoordmanager, laat die dan niet alleen je inloggegevens bewaren, maar ze ook invullen. Dat maakt veilig inloggen makkelijker. Elke wachtwoordmanager kan dat, maar er zijn verschillen. Bij KeePass kun je een soort log-in scripten, maar dit werkt onhandig. Makkelijker zijn Enpass en LastPass. Deze twee hebben browserplug-ins, die – zodra je de website of online dienst opent – de juiste gegevens uit de beveiligde kluis halen en invullen.

> 06 Controleer of jouw wachtwoord geraakt is door een datalek.

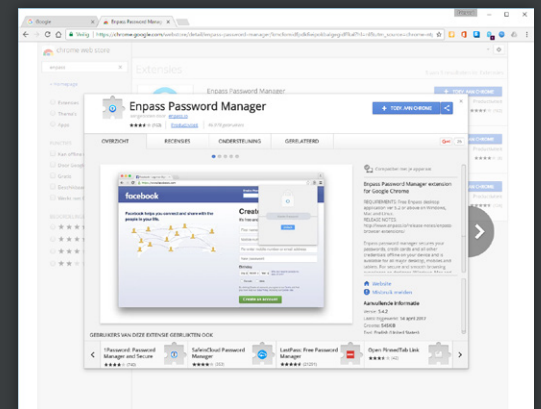


< 07 De antwoorden op controlevragen zijn vaak zo gevonden.



< 09 Maak inloggen met je DigiD veiliger met de app.

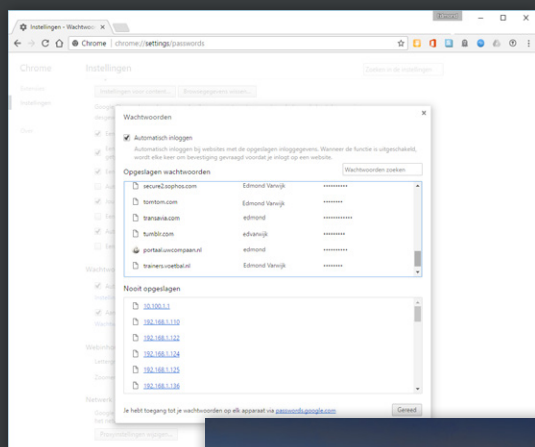
> 08 KeePass laat zich extra beveiligen met de vingerafdrucscanner op de iPhone.



> 10 Integreer de wachtwoordmanager in de browser door een extensie te installeren.

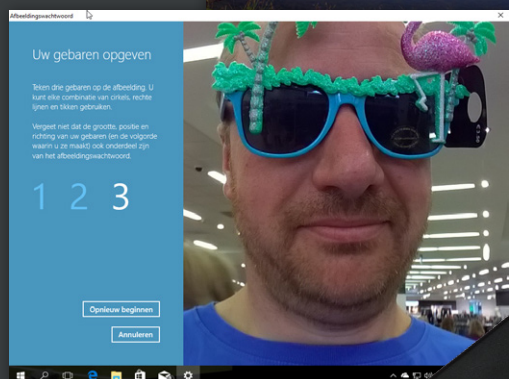
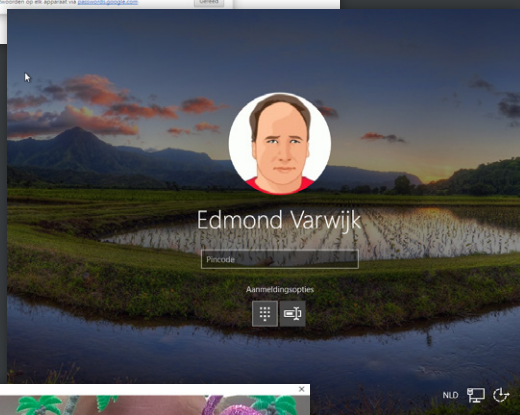
SPECIAL

Veilig inloggen



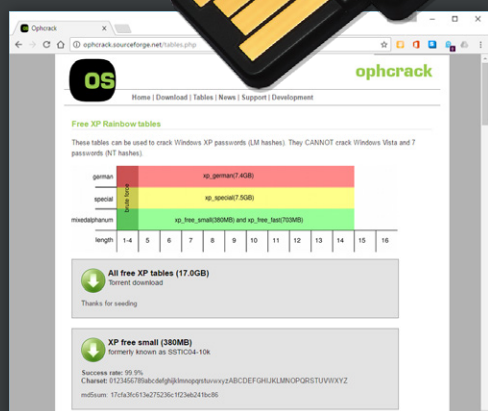
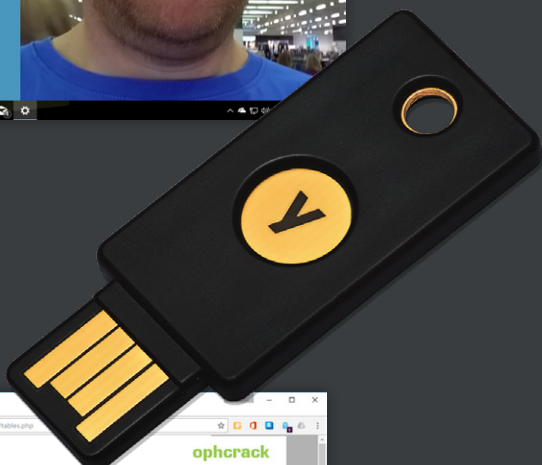
11 Gebruik je de wachtwoordmanager van de browser, schoon dan regelmatig de digitale kluis op.

12 Inloggen met een pincode, met het wachtwoord veilig in de tpm-kluis op het moederbord.



13 Een afbeeldingswachtwoord is vooral handig in combinatie met een aanraakscherm.

14 Beveilig je Facebook-login met een Yubikey als tweede factor.



15 Gratis rainbowtables zijn meestal minder uitgebreid en voor oudere versleutelingen.

11 Browsermanager

Steeds meer browsers bieden een wachtwoordmanager, zoals ook Chrome. Log je in op een website, dan vraagt Chrome je of het inloggegevens voor je zal bewaren. Ben je ingelogd in Chrome, dan synchroniseer je de wachtwoorden tussen al je Chrome-apparaten, zoals je smartphone. De opgeslagen wachtwoorden beheren doe je via **Chrome / Instellingen / Geavanceerde instellingen weergeven / Wachtwoorden beheren** of online via <https://passwords.google.com>.

12 Pincode

Windows 10 kent ook nieuwe inlogmethodes. Zo kun je in plaats van met een wachtwoord ook met een pincode inloggen. Dat lijkt minder veilig, maar is het niet. Op de achtergrond blijft het wachtwoord actief, het zit alleen veilig opgeborgen in de tpm-chip (Trusted Platform Module) op het moederbord. Als je de pincode intypt, wordt het wachtwoord uit de kluis gehaald en word je ingelogd zonder dat je het wachtwoord echt hebt ingetypt, en dat is veiliger. Door op elk apparaat een andere pincode te kiezen, kun je toch op al die apparaten je Microsoft-account met hetzelfde wachtwoord gebruiken. Overstappen op een pin gaat via **Start / Instellingen / Accounts / Aanmeldingsopties / Pincode**.

13 Afbeeldingswachtwoord

Behalve met een pincode kun je met een tekening inloggen in Windows 10. Vooral handig wanneer jouw computer touchscreen heeft. Je typt dan geen wachtwoord of pincode, maar maakt een paar bewegingen op het beeld. Eventueel kies je een foto die als achtergrond dient. Een aanraakscherm is trouwens niet nodig, het kan ook

met de muis. Net als de pincode uit tip 12 maakt het afbeeldingswachtwoord het mogelijk eenzelfde moeilijk wachtwoord op meerdere apparaten te gebruiken.

14 Yubikey

De Yubikey is een usb-stick voor tweefactor-authenticatie. De sleutel wordt gebruikt om de toegang tot computers en apparaten te beveiligen, maar ook applicaties als Keepass en diensten als Facebook, Google of LastPass. Raak de sensor boven op de Yubikey aan en een signaal wordt afgegeven aan de pc. Dit kan een bevestiging zijn dat jij dat apparaat hebt, maar bijvoorbeeld ook een reeks tekens die je gebruikt om je wachtwoord heel sterk te maken. De Yubikey heeft een hogere leercurve en ook niet elk of apparaat is ermee compatibel. Zorg ervoor dat je altijd een kopie van de Yubikey hebt én een mogelijkheid om bij problemen je account te resetten. Meer info via www.yubico.com.

15 Zelf wachtwoorden kraken

De populairste technieken om wachtwoorden te kraken zijn 'brute force' en 'rainbowtables'. Bij de eerste worden domweg alle mogelijke combinaties van cijfers, letters en leestekens geprobeerd tot het wachtwoord is gevonden. Dit duurt lang, maar is 100% trefzeker. Rainbowtables zijn sneller. Een rainbowtable is een tabel met alle bekende woorden en de hashes (de versleutelde vorm van mogelijke wachtwoorden). Laad rainbowtables en hashes in Ophcrack, een opensource-wachtwoordkraker, en al snel rollen de wachtwoorden eruit. Test je wachtwoorden zelf, Ophcrack is gratis te downloaden via <http://ophcrack.sourceforge.net>.

GEHACKT? GEÏNFECTEERD?

Preventie en eerste hulp

Hackers zouden maar wat graag je accounts kraken om zo toegang te krijgen tot privacygevoelige data, en om allerlei malafide scripts en dito software uit te voeren op jouw pc. Tijd om je hier zo goed mogelijk tegen te wapenen. En als je al slachtoffer geworden bent, laten we je weten hoe je hier zo goed mogelijk op reageert.

TOON VAN DAELE

WAT GAAN WE DOEN?



We gaan eerst na hoe je kunt uitvissen of één van je online accounts werd gehackt, vervolgens wat je in dat geval het beste kunt doen en hoe je zoiets voortaan kunt voorkomen. Daarna is het de beurt aan onze computer: hoe weet je of je pc gehackt is, wat staat je dan te doen en welke voorzorgsmaatregelen kun je in het vervolg nemen?

ONLINE ACCOUNTS

1

Ben ik gehackt?

Het is al vaker gebeurd dat internetdiensten, inclusief grote spelers als LinkedIn, Dropbox en Adobe, het slachtoffer van hackers zijn geworden. Daarbij verkregen hackers telkens vele miljoenen datarecords, met daarin gebruikersgegevens als namen, e-mailadressen, wachtwoorden en zelfs creditcardnummers. Een bezoekje aan www.haveibeenpwnd.com/pwnedwebsites, met een lijst van tientallen inbraken, is ontluisterend. Bestaat je e-mailadres al wat langer, dan is de kans groot dat ook jouw gegevens bij zo'n inbraak werden buitgemaakt. Dat vis je snel uit door je e-mailadres in te vullen op www.leakedsource.com en op www.haveibeenpwnd.com, beide databases bevatten een paar miljard gehackte accounts. Bij deze laatste kun je via de link **Notify me when I get pwned** na een gratis registratie aangeven dat je een bericht wilt ontvangen zodra bekend wordt dat jouw adres is buitgemaakt.

Verification complete

All done, you'll be sent an email if this address gets pwned in future, below is your existing exposure

Oh no — pwned!

Pwned on 3 breached sites and found no pastes (subscribe to search sensitive breaches)

Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.



Adobe: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, encrypted password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Compromised data: Email addresses, Password hints, Passwords, Usernames



Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Compromised data: Email addresses, Passwords

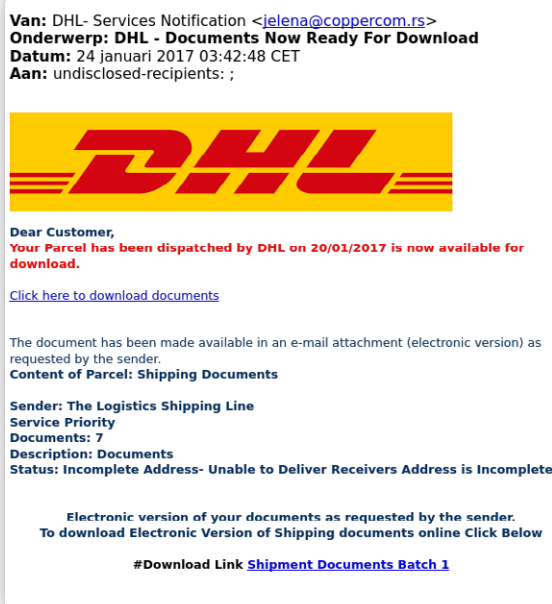


LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

<01 Ook het e-mailadres van ondergetekende werd buitgemaakt bij een hack – tot 3x toe zelfs.

2 Symptomen

Dat je e-mailadres niet voorkomt in de in tip 1 vermelde databases, geeft je natuurlijk geen garantie dat één van je accounts intussen niet toch bij een hack betrokken is geraakt. Gewetensvolle webservices brengen zelf hun leden op de hoogte zodra ze een inbraak hebben vastgesteld, maar daar kun je niet zomaar van uitgaan. Je moet dus ook altijd zelf alert blijven. Symptomen die erop wijzen dat één van jouw online accounts echt gehackt is, kunnen divers zijn. Een paar mogelijke tekenen: je kunt plotseling zelf niet meer inloggen bij je account (omdat je wachtwoord 'onjuist' is), er worden uit jouw naam vreemde berichten gepost, je verneemt van kennissen dat ze geregeld mails ontvangen die van jou afkomstig lijken te zijn, of je ontvangt zelf spam- en phishing-mails die je heel correct met je naam en soms zelfs met je adres aanspreken. Of erger nog: je merkt dat er geld van je rekening is afgegaan voor online bestellingen waar je zelf niets van weet.



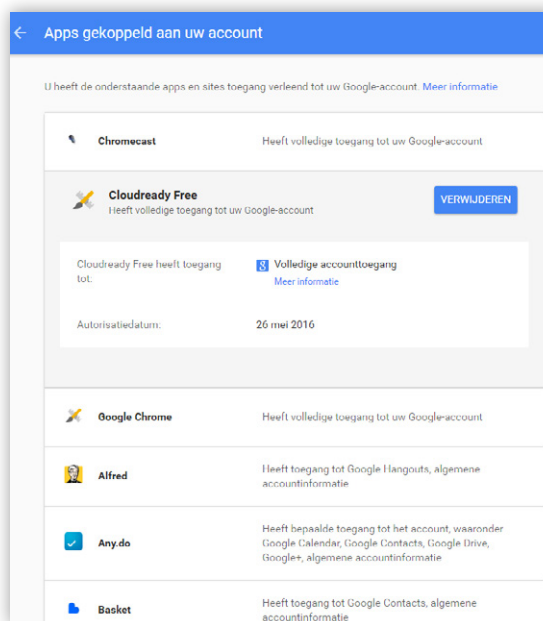
> 02 Net echt, maar toch: een phishing-mail!

De kans is reëel dat je e-mailadres ooit al werd gehackt

3 Snel reageren

Vermoed je dat één van je accounts is gehackt, dan is het zaak zo snel mogelijk je wachtwoord bij die dienst te wijzigen. Gebruik je hetzelfde wachtwoord nog bij andere diensten – wat geen goed idee is (zie ook tip

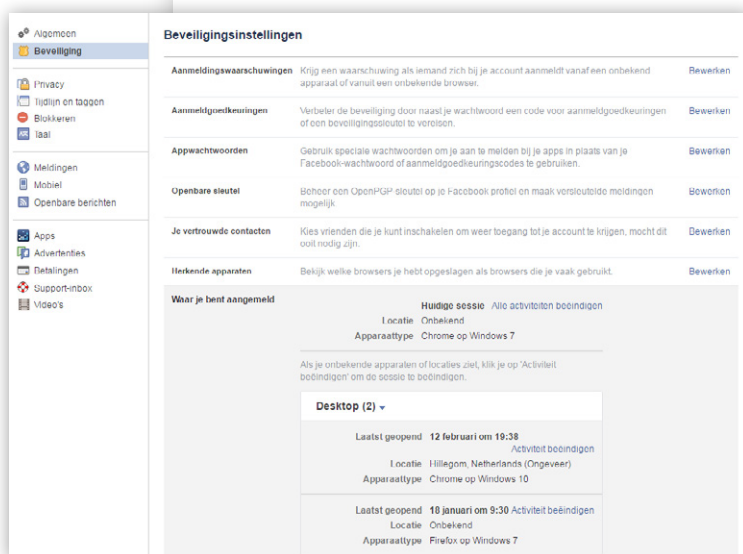
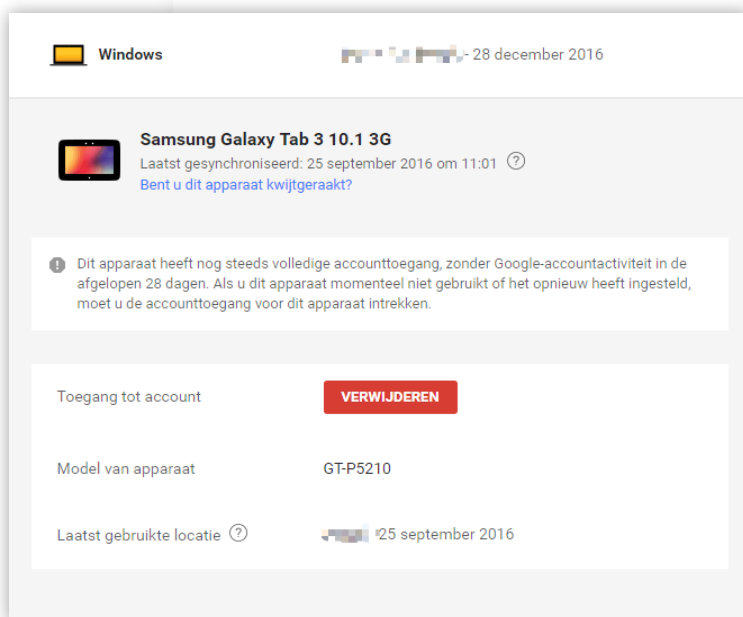
5) – dan moet je het wachtwoord daar ook aanpassen. Dat geldt eveneens voor het antwoord op de eventuele veiligheidsvraag, zoals 'Wat is de naam van je eerste huisdier'. Immers, het risico bestaat dat je die vraag op dezelfde manier bij een andere dienst hebt beantwoord, zodat de hackers mogelijk langs die weg een wachtwoordwijziging in jouw naam kunnen aanvragen. Vermijd trouwens altijd antwoorden die men via sociale media makkelijk te weten kan komen. Ga bovendien uit van een 'worst case scenario': alle gegevens via dat account beschikbaar waren, zijn in handen van hackers. Hoort daar een creditcardnummer bij, dan laat je die kaart het best meteen blokkeren. Op www.creditcardacties.nl/creditcard-blokkeren vind je een lijst met telefoonnummers om precies dat te doen bij diverse organisaties. Ga tevens na of je de gehackte service toestemming had gegeven om andere diensten te benaderen. In dat geval trek je die permissie meteen in. Voor Google bijvoorbeeld doe je dat vanaf <https://myaccount.google.com/permissions>, en voor Facebook via <https://www.facebook.com/settings/?tab=applications>. Op de site <https://mypermissions.org> vind je directe links naar de permissie-pagina's van de grootste websites.



< 03 Voor je het goed en wel beseft, hebben tientallen andere services toegang tot gegevens uit je Google-account.

4 Gebeurtenissenlogs

Heel wat webservices houden logs bij van de belangrijkste gebeurtenissen van je account, met name rond het aanmelden. We raden je aan deze logs regelmatig te controleren, zeker wanneer je vermoedt dat een van je accounts werd gehackt. Bij Google vind je deze informatie via <https://myaccount.google.com>, waar je achtereenvolgens **Inloggen en beveiliging** / **Apparaatactiviteit en meldingen** / **Apparaten controle-**



04 Onder meer Google en Facebook houden netjes bij vanaf welke apparaten je account is benaderd.

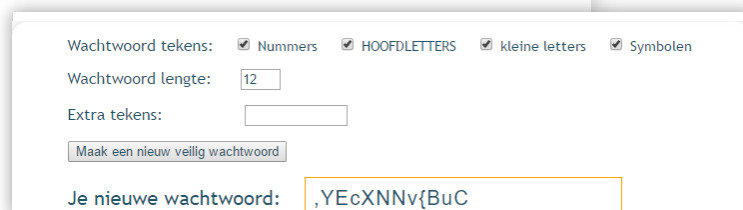
ren opent. Je krijgt een overzicht van apparaten die zich de afgelopen 28 dagen bij jouw account hebben aangemeld. Klik zo'n apparaat aan om meer details te krijgen, zodat je bijvoorbeeld ziet welke browser voor de aanmelding werd gebruikt. Klik hier ook op **Instellingen beheren**, en laat een e-mail en sms aan jou versturen bij **Kritieke beveiligingsrisico's, bijvoorbeeld als een hacker uw wachtwoord heeft en probeert in te loggen op uw account**. Ook Facebook houdt zo'n logboek bij. Meld je aan, klik op het pijltje rechtsboven en kies **Instellingen / Beveiliging / Waar je bent aangemeld**. Klik op **Alle activiteiten beëindigen** als je inderdaad merkt dat er iets niet koosjer is. Ga tevens na bij **Aanmeldingswaarschuwingen** of je echt hebt geselecteerd dat je een melding wilt ontvangen wanneer iemand zich vanaf een onbekend apparaat of browser bij je account aanmeldt.

5 Wachtwoordrecycling

In de vorige tips hebben we ons vooral gefocust op 'eerste hulp bij mogelijke hacking'. Maar voorkomen is beter dan genezen, dus geven we je nu graag enkele tips mee waarmee je het hackers moeilijker maakt om hun slag te slaan. Belangrijk is in elk geval dat je geen wachtwoorden 'recyclet', waarmee we bedoelen dat je niet voor verschillende accounts hetzelfde wachtwoord gebruikt. Het zal niet de eerste keer zijn dat iemand een account creëert voor een gastenboek van een of andere hobbyclub, om dan te vernemen dat die gastenboek-software exploits bevatte. Gevolg: je account wordt gehackt en als je hetzelfde wachtwoord ook voor andere diensten hebt gebruikt, kunnen de hackers ook die accounts benaderen!

Gebruik dus verschillende wachtwoorden en het liefst ook nog eens lange, complexe en niet (zomaar) te raden wachtwoorden. Dat verzwaart in veel gevallen de inspanningen van de hackers om je wachtwoord te weten te komen wanneer ze in een database hebben ingebroken (zie ook het kader 'Hashing').

05 Lange, complexe wachtwoorden, bij voorkeur met een random generator.



Zorg dat je een melding ontvangt wanneer iemand zich vanaf een onbekend apparaat aanmeldt

6 Tweestapsverificatie

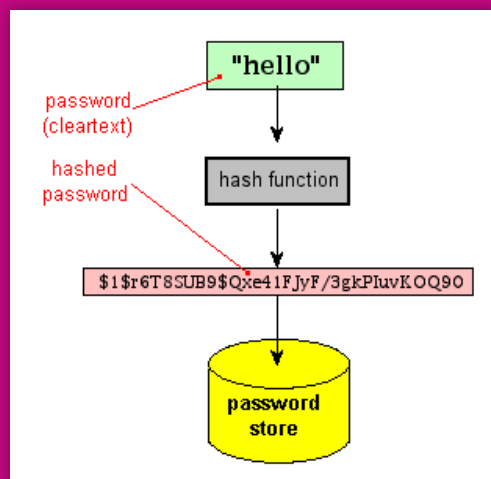
Verschillende, complexe wachtwoorden zijn al een flinke stap in de goede richting, maar idealiter maak je waar mogelijk ook nog gebruik van tweestapsverificatie. Dat houdt in dat je naast een wachtwoord nog een andere code nodig hebt, die niet op dezelfde computer wordt gegenereerd als waarop je je aanmeldt. Deze code krijg je door- gaans via sms of een app. Zelfs als je wachtwoord is gekraakt of je pc is gehackt, kunnen hackers zich dan nog niet aanmelden omdat ze die extra code niet hebben. Heel wat bedrijven en services bieden intussen zo'n dubbele verificatiemethode aan,

waaronder Google, Facebook, LinkedIn, Microsoft en WhatsApp. Wanneer je naar iets als **two factor authentication [naam service]** googelt, beland je al snel op de webpagina waar je de tweestapsverificatie voor die dienst kunt instellen. Voor Google kan dat via <https://myaccount.google.com> / **Inloggen en beveiliging / Authenticatie in twee stappen**. Voor Facebook kan het via **Instellingen / Veiligheid / Aanmeldgoedkeuringen**.

Een handige app voor mobiele apparaten die met de tweestapsverificatie van heel wat bekende diensten overweg kan, is het gratis Authy. Die is beschikbaar voor zowel iOS als Android. Op www.authy.com/learn-more vind je alvast alle nodige instructies terug, voor zowel Google, Gmail, Dropbox als Facebook.

Hashing

Webservices die zichzelf en de veiligheid van hun gebruikers serieus nemen, zullen wachtwoorden nooit in leesbare vorm opslaan in een database. De meeste diensten berekenen hiervan een 'hash' en slaan die op in plaats van het wachtwoord zelf. Zo'n hash is een 'string' die met behulp van cryptografische algoritmes uit het wachtwoord wordt berekend, maar wel zo dat het wachtwoord niet uit de hash kan worden afgeleid. Om de wachtwoorden op basis van de gestolen hashes te vinden, moeten hackers dan zelf hashes berekenen van mogelijke wachtwoorden en de resultaten telkens toetsen aan de database. Bij lange, complexe wachtwoorden is dat nagenoeg onbegonnen werk en kan het vele jaren duren voor ze de hash in de database gevonden hebben en dus je wachtwoord gekraakt hebben.



> In de regel worden wachtwoorden niet in leesbare vorm in een database bewaard.

7

Wachtwoordstelsysteem

In tip 5 hebben we al het belang aangegeven van verschillende en liefst ook complexe wachtwoorden. Het wordt dan natuurlijk wel een hele klus om al je wachtwoorden te onthouden, maar daar zijn gelukkig hulpmiddelen voor. Er zijn bijvoorbeeld wachtwoordssystemen die het makkelijker maken om je wachtwoorden voor de diverse diensten terug te vinden. Je kunt weliswaar je eigen systeem bedenken, maar op www.passwordcard.org/nl vind je een kant-en-klaar ontwerp. Telkens als je deze pagina bezoekt, wordt een andere, unieke wachtwoordkaart gegenereerd, ter grootte van een creditcard. We raden aan om een vinkje te plaatsen bij **aanvinken om symbolen toe te voegen**. De kaart druk je bij voorkeur af op een kleurenprinter en lamineer je. Bij de kaart hoort ook een code van 16 tekens die je op een veilige plaats bewaart: verlies je ooit je kaart, dan kun je op basis van deze code weer dezelfde kaart laten genereren op de site. Vervolgens kies je voor elke service een specifiek symbool en een kleur. Stel, je kiest voor Dropbox het symbool \$ en de kleur groen, dan kom je, althans in onze voorbeeldkaart, uit op de letter M. Als je nou voor jezelf de richting 'rechts' had ingesteld en je werkt met wachtwoorden

Nummer

Dit is het nummer van uw kaart. Bewaar het op een veilige plaats! Als u een verloren kaart opnieuw wilt genereren, tik dan hier het nummer in en druk op Enter:

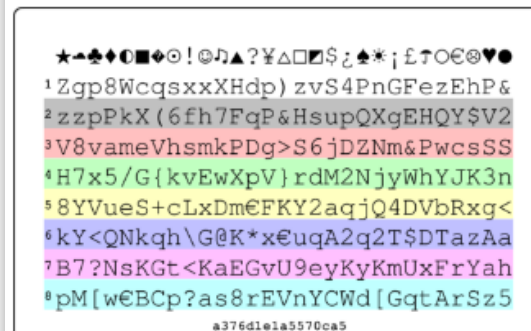
a376d1e1a5570ca5

Opties

- ☐ aanvinken voor een gebied met alleen cijfers.
- ☒ aanvinken om symbolen toe te voegen.

Kaart

Dit is uw PasswordCard:



Printen

Klik hier om deze pagina te printen: [Print](#)

van tien tekens, dan wordt je Dropbox-wachtwoord: M2NjyWhYJK.

Een alternatief is natuurlijk een heuse wachtwoordmanager, die je wachtwoorden achter een sterk masterwachtwoord in een versleutelde database bewaart. Browsers als Firefox en Chrome hebben zelf zo'n beheermodule aan boord, maar je kunt ook terecht bij diensten als LastPass (www.lastpass.com) en het gratis opensourceprogramma KeePass (www.KEEPASS.INFO).

COMPUTER

8 Mogelijke symptomen

Hackers kunnen je niet alleen belagen door in te breken op je online accounts, maar ook door rechtstreeks op je pc in te breken. Dat gebeurt doorgaans via een of andere vorm van malware. Vaak is dat een phishing-mail of een bericht op sociale media met een link naar een malafide site. Of je surft ongemerkt naar een geïnfecteerde site en die plaatst automatisch malware op je pc (een zogeheten drive-by-download). Net zoals bij een hack van een online account, is het echter niet altijd meteen duidelijk dat je computer het slachtoffer van malware of hackers is. Je moet als gebruiker dus altijd een beetje op je hoede zijn en oog hebben voor bepaalde symptomen. Dat kan bijvoorbeeld een verhoogde schijfactiviteit zijn of meer netwerkverkeer. Het kan ook gebeuren dat programma's vaker vastlopen. Of dat bepaalde services, zoals je firewall of antivirus, niet meer werken. Dan wel dat je sommige sites, zoals die van antivirusproducenten, niet langer kunt bereiken. Of je vrienden klagen dat ze plots van jouw adres spamberichten ontvangen. Dat kunnen

▼ 08 Even surfen naar een malafide site kan al volstaan om malware binnen te krijgen.

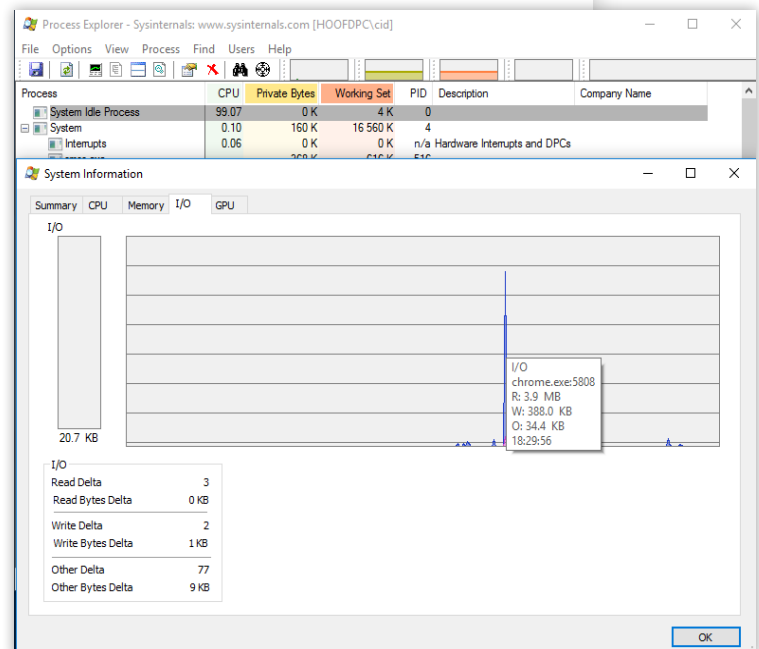
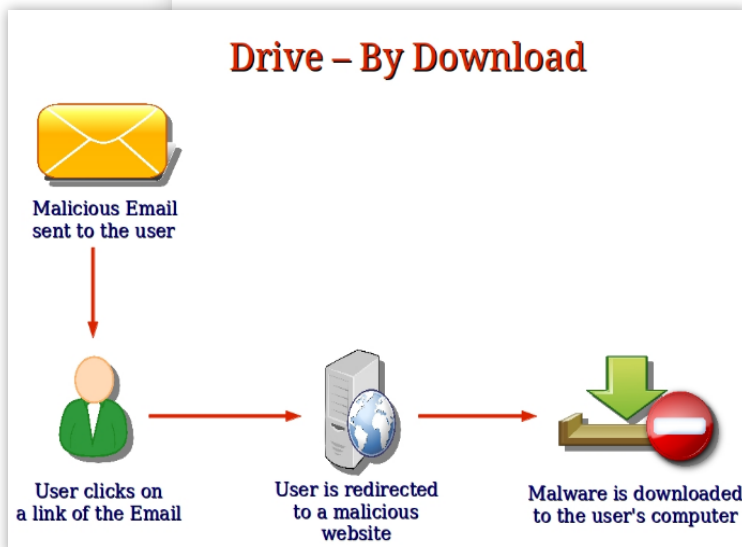
allemaal indicaties zijn dat je pc het slachtoffer is geworden van malware of een hack, maar verdere analyse moet uitsluitend geven. In de tips hierna geven we je alvast enkele nuttige tips en tools mee.

9 Schijfactiviteit

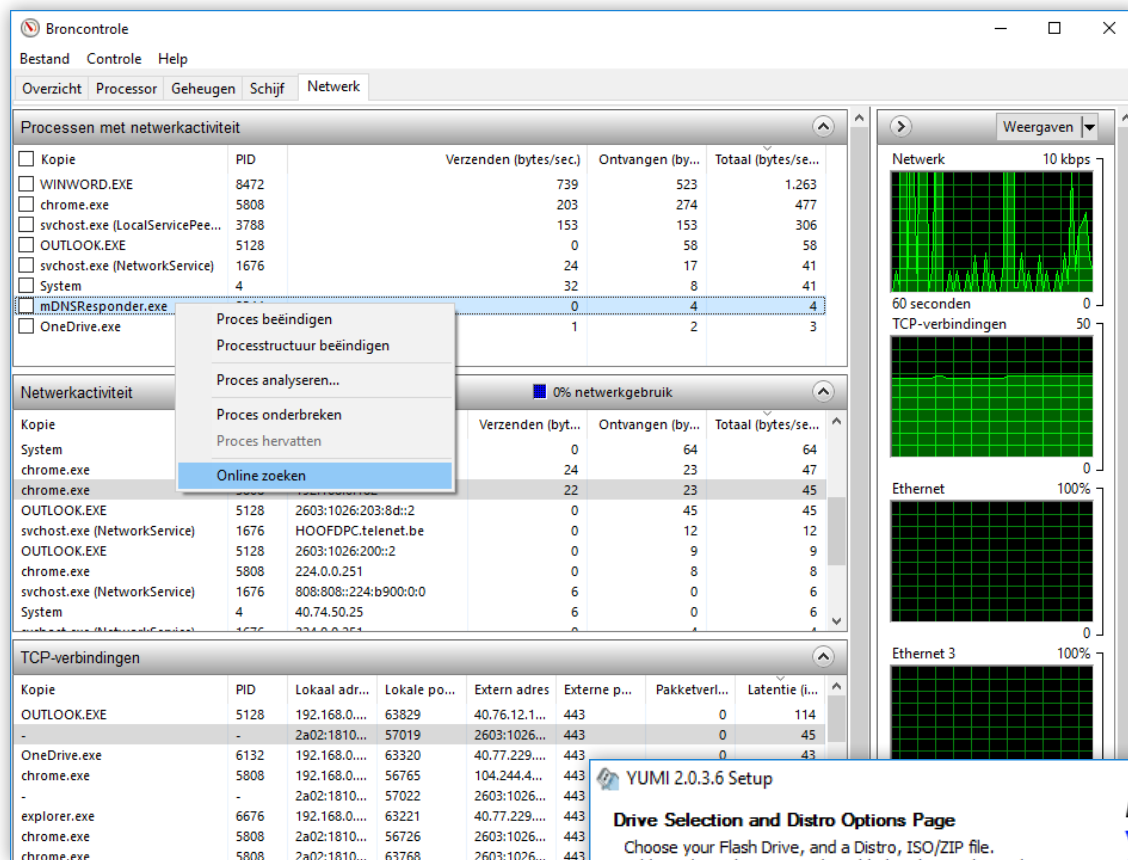
Stel je een ongewoon drukke schijfactiviteit vast, dan is het Windows Taakbeheer een goed vertrekpunt voor nader onderzoek. Dat roep je op met Ctrl+Shift+Esc. Klik (in Windows 10) op **Meer details**, open het tabblad **Processen** en klik de kolomtitel **Schijf** aan: alle actieve processen worden dan gesorteerd op de hoeveelheid schijfactiviteit die ze veroorzaken. Via het menu **Beeld / Bijwerksnelheid** kun je de verversingsfrequentie aanpassen of stopzetten. Sommige processen laten zich verder uitvouwen door het kleine pijltje aan te klikken. Klik een procesnaam met de rechtermuisknop aan en kies **Bestandslocatie openen**. Wellicht volstaan de naam en de locatie al om je duidelijk te maken of het om betrouwbare software gaat. Uiteraard kun je deze informatie ook nog googelen. Een handig alternatief is ProcessLibrary (www.processlibrary.com/directory): een online database met een beschrijving van circa 140.000 processen, weliswaar niet helemaal up-to-date. In de meeste gevallen krijgt een proces ook een 'security rating' mee, wat een bruikbare indicatie kan zijn.

Het Taakbeheer geeft je dus een actueel overzicht van de actieve processen en hun schijfgebruik. Voor een iets uitgebreider overzicht kun je een gratis tool als Process Explorer inzetten (www.tiny.cc/procx). Start het programma op en klik bovenaan het mini-

▼ 09 Process Explorer is één van de beste tools om (verdachte) procesactiviteit bloot te leggen.



> 10 De Windows broncontrole geeft al een aardig idee van je netwerkactiviteit.

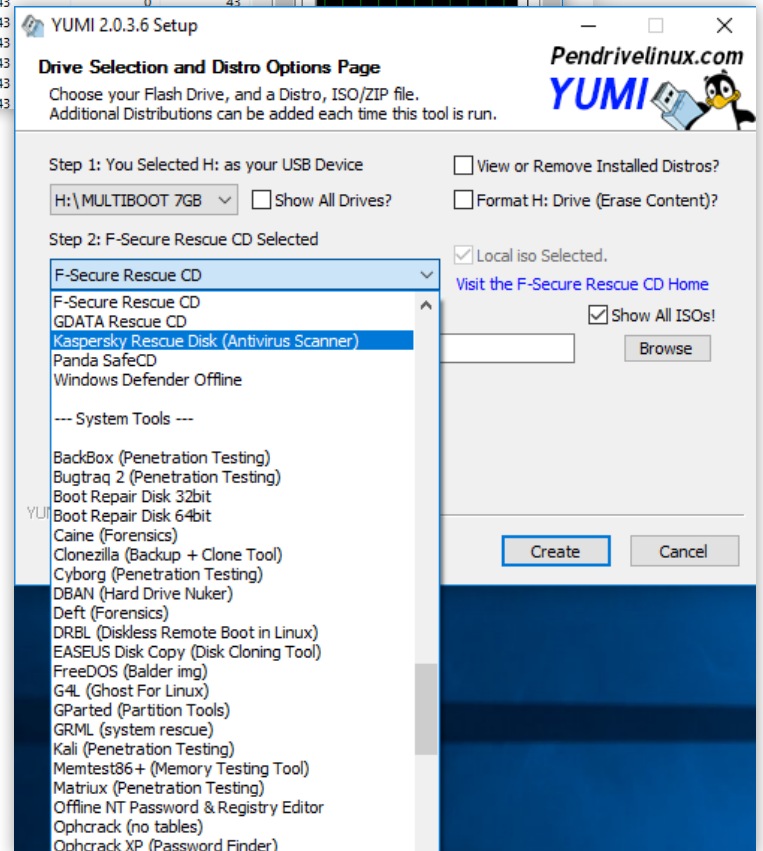


grafiekje met de naam I/O aan. Deze grafiek kun je verbreden om verder in de tijd terug te gaan. Houd de muisaanwijzer boven een piek om het achterliggende proces te kennen.

Je krijgt te zien hoeveel bytes elk proces ontvangt en verstuurt

10 Netwerkactiviteit

Lichten de ledjes van je switch of router op alsof het kerstmis was, zelfs wanneer je zelf geen internet- of netwerkactiviteit genereert, dan vergt dat nader onderzoek. Ook hier kan Windows Taakbeheer je eerste toevlucht zijn. Open het tabblad **Prestaties** en klik onderaan op **Broncontrole**. Er verschijnt een nieuw venster waar je het tabblad **Netwerk** opent (merk trouwens op dat je hier ook het tabblad **Schijf** vindt, met per proces een overzicht van de schijfactiviteit van de laatste minuut). Voor nog meer informatie klik je de drie grijze balken aan: **Netwerkactiviteit**, **TCP-verbindingen** en **Listener-poorten**. Je krijgt nu onder meer te zien te zien hoeveel bytes elk proces



ontvangt en verstuurt, met welke adressen verbindingen worden gelegd en over welke poort zo'n connectie gaat. Klik een verdacht item (in het bovenste paneel) met de rechtermuisknop aan en kies **Online zoeken** om via het internet meer informatie over het proces bij elkaar te sprokkelen.

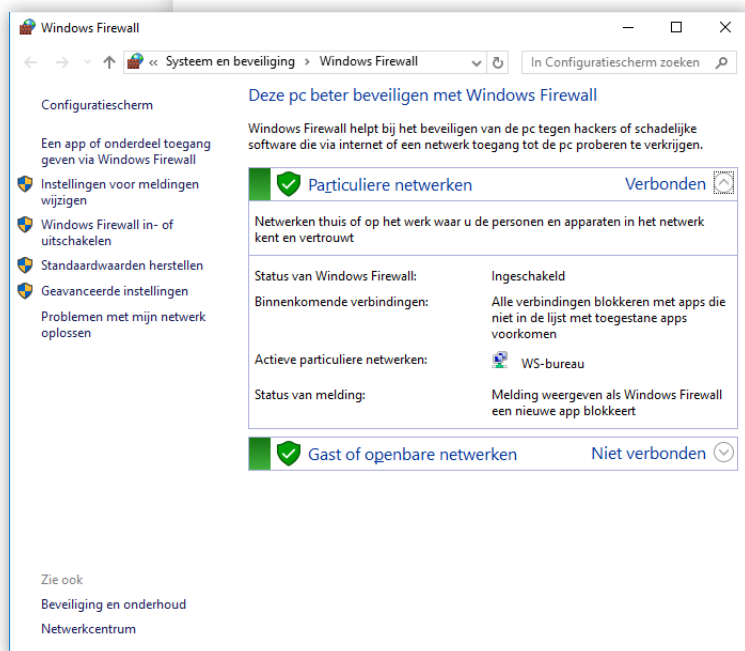
✓ 11 Een live antivirusmedium heb je zo samengesteld met YUMI.

11 Malwarecheck

Natuurlijk, lang niet alle malware geeft zich prijs door een merkbaar verhoogde schijf- of netwerkactiviteit. Vermoed je toch een infectie – omwille van andere symptomen: zie ook tip 8 – dan doe je er goed aan een grondige antivirusscan uit te voeren. Aangezien je eigen antivirusprogramma blijkbaar niet aan de alarmbel heeft getrokken, haal je er het best een 'second opinion' bij. Een degelijke tool is alvast Malwarebytes Anti-Malware (<https://nl.malwarebytes.com>). Voor een handmatig gestarte scan voldoet de gratis versie prima. Vindt ook deze tool niets en vermoed je nog altijd een infectie, dan raden we je aan het met een live antivirusmedium te proberen. Je start je systeem dan op vanaf een usb-stick of dvd, waardoor malware die zich bijvoorbeeld diep in Windows heeft genesteld, geen kans krijgt. Een uitstekende tool om zo'n medium aan te maken is het gratis YUMI (www.tiny.cc/yumiboot). Start dit portable programma op, verwijs naar je lege usb-stick, selecteer bij **Step 2** in de rubriek **Antivirus Tools** een geschikt antivirusprogramma als **Kaspersky** of **Bitdefender**. Plaats een vinkje bij **Download Link** en haal het bijhorende iso-bestand op. Start het kopieerproces met **Create**. Na afloop kun je eventueel nog meer antivirustools op dezelfde stick zetten.

Heb je last van hardnekkige adware, browsertoolbars en andere ongein, dan is het gratis AdwCleaner (www.tiny.cc/adwc) een prima opschoontool. We raden je echter wel aan vooraf een systeemherstelpunt te maken en de tool niet te draaien tenzij je echt hinder van pop-upadvertenties of toolbars ondervindt.

✓ 12 Een firewall houdt alvast wat tegen, maar je moet hem natuurlijk wel activeren.



12 Preventie

We gaan ervan uit dat je eventuele malware intussen hebt kunnen opsporen en verwijderen en dat je nu meer dan ooit overtuigd bent dat je zulke rotzooi voortaan liever niet op je pc krijgt. Dat vraagt vanzelfsprekend om de nodige preventiemaatregelen, en die spreken eigenlijk voor zich. Zorg om te beginnen voor up-to-date beveiligingstools. Dat kan een all-in-one suite zijn, maar zorg in elk geval voor antivirus, antimalware, antispyware en een firewall. De Windows-firewall kan volstaan, maar ga wel even na of die is ingeschakeld: klik op **Start**, zoek naar **firewall** en kies **Status van firewall controleren**. Houd tevens je besturingssysteem en je programma's, zoals browsers en plug-ins, altijd goed up-to-date. Dat houdt dus in dat je Windows Update moet inschakelen. In Windows 10 zijn (beveiligings) updates eenvoudigweg al verplicht en moet je heel wat moeite doen, wil je die toch blokkeren. Verder is het belangrijk dat je je gezonde verstand gebruikt in combinatie met een dosis gezond wantrouwen. Open dus geen mails die er verdacht uitzien, klik nooit zomaar wat links aan in e-mails of in berichten op sociale media, en haal al je downloads eerst door de antivirusservice www.virustotal.com.

13 Back-ups

Ook het maken van (zo goed als) malwarebestendige back-ups mag je rustig tot de afdeling preventie rekenen. Immers, wie nonchalant omspringt met zijn databack-ups en het slachtoffer wordt van bijvoorbeeld gijzelsoftware (ransomware) riskeert al zijn gegevens te verliezen, ook die in de back-ups! Idealiter zorg je voor verschillende back-upversies en koppel je telkens het back-upmedium fysiek los van je computer zodra de back-up is gemaakt. Is dit laatste geen optie, zorg er dan voor dat het account waarmee je je bij Windows aanmeldt, standaard geen toegang heeft tot het back-upmedium. Zoiets krijg je eenvoudig voor elkaar door een gedeelde map (bijvoorbeeld op een nas) van de juiste machtigingen te voorzien en met die machtigingen volautomatisch back-ups van je systeem op die map te laten wegschrijven. We tonen je eerst hoe je die gedeelde map correct instelt. Als voorbeeld nemen we een Synology-nas, maar de aanpak is vergelijkbaar bij andere producenten. Open de webinterface van je nas en ga naar het **Configuratiescherm**. Open de rubriek **Gebruiker**, klik op **Maken** en kies een gepaste naam, wij gaan voor **backupper**. Geef die een sterk wachtwoord mee. Ga vervolgens naar de rubriek **Gedeelde map** en creëer de map voor

✓ 13 Alleen de back-upgebruiker krijgt (schrijf)rechten op je back-up-map.

◀ 13 Creëer een gebruiker uitsluitend voor je back-upoperaties.

Naam	Geen toegang	Lezen/schrijven	Alleen-lezen	Aangepast
admin	☐	☐	☐	☐
backupper	☐	☒	☐	☐
ben	☐	☐	☐	☐
guest	☐	☐	☐	☐
ina	☐	☐	☐	☐
sarah	☐	☐	☐	☐
toon	☐	☐	☐	☐

je back-ups. Op het tabblad **Machtigingen** verleen je voor die map lees- en schrijfrechten aan de zonet gemaakte gebruiker (backupper).

14 Back-ups: Veeam

Een schitterende en bovendien gratis tool om volautomatisch back-ups van je schijf te laten maken is Veeam Endpoint Backup (www.tiny.cc/veb), dat je na registratie kunt downloaden en installeren. Start het programma op en kies **Configure Backup**. Idealiter kies je hier voor **Entire computer**. De eerste keer levert dat weliswaar een fiks back-upbestand op, maar de daaropvolgende back-ups nemen alleen nog maar de gewijzigde data mee en zijn dus heel wat zuiniger met je opslagruimte. In het volgende venster duid je de **Shared folder** aan, waarna je het correcte pad naar je gedeelde map invult (een UNC-pad als \\<nas>\\<map>) en een vinkje plaatst bij **This share requires access credentials**. Vul de gebruikersnaam en het wachtwoord voor de share in. Klik op **Populate** om te checken of de map

Gezond verstand en gezond wantrouwen zijn meer dan wenselijk

wel bereikbaar is. Geef tevens aan hoelang je de back-ups wilt bewaren (standaard veertien dagen). Een venster verder duid je de gewenste back-upfrequentie of -timing aan. Leg alles vast met **Save** en **Finish** en controleer meteen met **Backup Now** of alles naar behoren functioneert. We hopen natuurlijk dat je nooit slachtoffer van een hack wordt, maar met een goede back-up ben je in elk geval niet al je bestanden kwijt. 📁

✓ 14 Je moet Veeam het juiste account-ID meegeven voor de back-up tool aan de slag kan.