



Secure Computing

Nieuwsbrief Januari 2013

W.Bosgra taakaccenthouder digitale criminaliteit

In dit nummer:

Voorspellingen voor 2013

USB sneller verwijderen

Voicemail via Facebook

Browser plug-ins

Anti-virus Boot-cd's

Data verbergen

Schijf nog gezond?

en .. Windows 8 !!

Nieuw jaar, nieuwe layout

Ook dit jaar hoop ik jullie als lezer weer te verblijden met het nodige digitale nieuws. Wederom zal deze nieuwsbrief bestaan uit noodzakelijke info, waarin veiligheid voorop staat. Uiteraard ook uit onderwerpen waar je het nodige voordeel en plezier uit kunt halen.

Er is gekozen voor een nieuwe layout, waardoor de structuur van de pagina's grotendeels met elkaar overeenkomt.. Ik hoop dat dit de leesbaarheid ten goede komt.. Tevens zal worden getracht nog meer interactie met informatie op het internet te bewerkstelligen.

Laat maar weten wat jullie er van vinden!

Gr,

W.B

E-mail? [klik hier](#) !



De cloud wordt complexer, wetgeving houdt ze op

Bedrijven zullen steeds meer op de cloud vertrouwen om BYOD-medewerkers te scheiden van gevoelige bedrijfsgegevens. De cloud is niet langer gewone opslag, het is een krachtige machine en die kracht zal vanaf 2013 steeds meer benut worden.

Praktische bezwaren en wetten over clouddata zullen hun hoogtepunt bereiken alms de EU terug naar de tekentafel moet met nieuwe gegevensbeschermingsregels die allicht een impact zullen hebben om meer dan de 27 EU-landen. Problemen over waar de clouddata opgeslagen worden en wie toegang heeft tot de gegevens blijven de grote struikelblokken, maar oplossingen zouden wel eens lang op zich kunnen laten wachten.



ANONYMOUS

We are Legion. We do not Forgive.
We do not Forget. Expect us.

Voorspellingen 2013: maatschappelijke trends

Anonymous en Wikileaks gaan weer van zich laten horen, terwijl technologiebedrijven proberen om opkomende markten aan te boren. In 2013 wordt de cloud nog complexer en meer gereguleerd.

Anonymous en Wikileaks veren op, hacktivisme op hoger Niveau

Wikileaks heeft een vrij stil jaar achter de rug, ondanks (of dank zij) het huisarrest dat Julian Assange beleeft in de Ecuadoriaanse ambassade in Londen.

Anonymous is een bezig bijtje gebleven. Ze hebben bedrijven platgelegd waarvan het onethisch handelen vermoedt, leggen beveiligingslekken in netwerken bloot en hebben vooral heel veel lol in alles wat ze doen. Het hackingcollectief werkt voor de mensen en legt illegale gedragingen en activiteiten bloot.

Wikileaks van Assange heeft al beloofd om meer lekken te openbaren met een blijvend effect op overheden en de private sector. Buiten Wikileaks blijven Anonymous en aanverwanten beveiligingslekken manipuleren 'for the lulz' en groeit de mogelijkheid dat overheden deze hackers gaat inzetten om er zelf voordeel aan te doen.

Cyberwapens zullen een effectieve methode blijven om fysieke schade aan te richten met computercode zoals Stuxnet, Flame en Duqu. Waar geleide raketten en tactische militaire operaties ooit het meeste schade aanrichtten, zullen de 'onbekende' overheden anoniem regionale doelwitten aanvallen, wat een probleem is voor de nationale veiligheid.

Techreuzen richten zich op China en BRIC-landen voor herstel

Brazilië, Rusland, India en China, de zogenaamde BRIC-landen, hebben potentieel voor bedrijfsuitbreidingen. Amazon heeft al zijn vleugels uitgespreid in Brazilië, net zoals Microsoft. Lenovo probeert hard om een lokale pc-fabriek neer te poten in het land.

Nu markten in de ontwikkelde wereld zo goed als verzadigd zijn, willen bedrijven uitbreiden. Maar ze worden daarbij gehinderd door importtaksen. Daarom gaan bedrijven zich ook echt vestigen in de BRIC-landen om toegang te krijgen tot al het geld dat er rondgaat.

Het zal wel niet makkelijk zijn, want lokale wetgeving maakt het moeilijk en de overheden van de opkomende landen hebben de bedrijven nog niet de hand gereikt. De doorbraak kan er in 2013 komen.

Microsoft test: herken jij alle nep-virusscan- ners?

Vorig jaar werd er op vele miljoenen Windows-computers scareware aangetroffen, vaak in de vorm van nep-virusscanners.

De programma's laten gebruikers geloven dat hun pc besmet is en ze voor het verwijderen van de malware moeten betalen.

Vaak doet scareware zich voor als beveiligingssoftware van bekende aanbieders. Reden voor Microsoft om op Facebook een test te plaatsen.

Deelnemers krijgen 10 afbeeldingen te zien waarbij ze moeten aangeven of het om echte of valse software gaat.

"Een deel van de reden dat valse beveiligingsprogramma's zo succesvol zijn, is dat ze erg overtuigend zijn. Denk jij dat je het verschil tussen een echt en een vals beveiligingsprogramma kunt herkennen?", vraagt Microsofts Tim Rains, directeur Trustworthy Computing.

Ga [hier](#) naar de test!

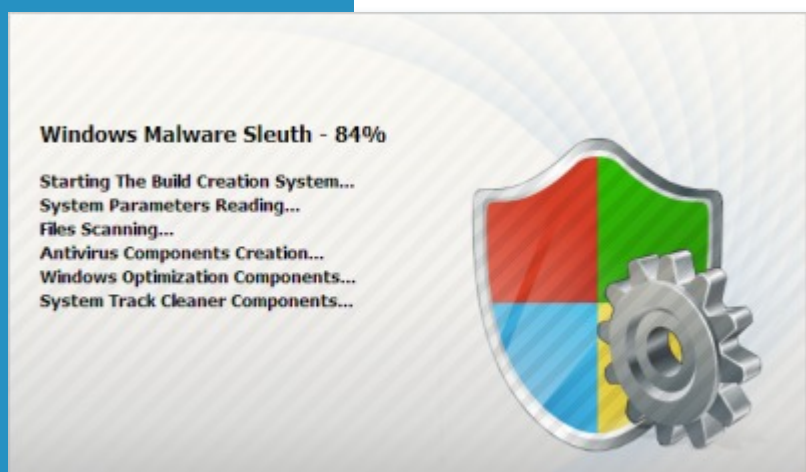
Nigerianen gaan strijd aan met internetscammers

Een Nigeriaans bedrijf is een online wiki gestart waarbij internetgebruikers sleutelwoorden en zinnen kunnen toevoegen die in scam e-mails worden gebruikt. Deze sleutelwoorden kunnen vervolgens virusscanners helpen bij het detecteren van Nigeriaanse 419 scam-berichten, die grote hoeveelheden geld beloven. Slachtoffers worden bij deze 'advance fee scams' verleid om eerst zelf te betalen.

De [Wayopedia-database](#) wordt door het vanuit Lagos opererende Co Creation Hub onderhouden. Veel van de Nigeriaanse scammers zijn jonge Nigerianen met een opleiding maar zonder werk of vooruitzichten. "De meeste cybercriminelen zijn tussen de 22 en 29 jaar en hoog opgeleid", aldus Joshua Oyeniyi Aransiola, socioloog aan de Obafemi Awolowo Universiteit in het Nigeriaanse Ile-Ife.

Volgens Bosun Tijani, mede-oprichter van Co Creation Hub, is een deel van de oplossing om scammers te overtuigen dat er wel degelijk kansen zijn om als softwareontwikkelaar aan de slag te gaan. "Zodra deze mensen zien dat ze een toekomst als softwareontwikkelaar hebben, helpt dat bij het oplossen van het probleem", aldus Tijani. "Scammen is niet eenvoudig, deze jongens werken hard."

Het probleem heeft echter ook gevolgen voor legitieme Nigeriaanse IT-bedrijven, die extra moeite moeten doen om internationale partners te overtuigen dat ze serieus zijn. Zo is PayPal, dat in 190 landen beschikbaar is, nog steeds niet beschikbaar voor Nigerianen.



Regels

De leidraad omvat verschillende regels die tot het op verantwoorde wijze melden van beveiligingslekken moeten leiden. Hackers mogen de volgende maatregelen of activiteiten niet toepassen:

Het hacken van systemen via social engineering.

Het plaatsen van een backdoor in informatiesystemen.

Het verder uitnutten van een kwetsbaarheid dan noodzakelijk om de kwetsbaarheid vast te stellen.

Het kopiëren, wijzigen of verwijderen van gegevens van het systeem te kopiëren.

Het aanbrengen van veranderingen in het systeem.

Het herhaaldelijk toegang tot het systeem verkrijgen of de toegang te delen met anderen.

Het via "bruteforce" verkrijgen van van toegang tot systemen.

Daarnaast is het aan beide partijen om te bepalen of de kwetsbaarheid openbaar wordt gemaakt. In het geval een kwetsbaarheid wordt gevonden, zou die volgens de leidraad binnen een bepaalde tijd moeten worden opgelost. Voor een softwarematige kwetsbaarheid wordt 60 dagen aangeraden, terwijl voor problemen in hardware 6 maanden wordt geadviseerd.

Overheid onthult richtlijnen voor hackers

De overheid heeft richtlijnen voor ethische hackers geopenbaard die op verantwoorde wijze lekken willen melden. Er is echter geen garantie dat hackers die zich aan deze regels houden niet vervolgd worden. Minister Opstelten van Veiligheid en Justitie beloofde de Kamer vorig jaar een richtlijn voor responsible disclosure. Het gaat dan om regels omtrent het vinden en rapporteren van lekken.

De nu gepresenteerde leidraad geldt niet alleen voor ethische hackers, maar ook voor bedrijven. Concreet betekent dit dat een organisatie publiekelijk het beleid voor responsible disclosure uitdraagt.

De organisatie en melder maken daarnaast afspraken over de termijn waarop de kwetsbaarheid verholpen zal zijn, de wijze waarop zij met elkaar zullen communiceren en over eventuele openbaarmaking en het verder inlichten van de ICT-security-community.

Lering

"Zo kunnen ook anderen lering kunnen trekken uit de kwetsbaarheid waar het om gaat. Als een organisatie eenmaal beleid heeft op dit gebied moet ook duidelijk zijn hoe zij met aangiftes omgaat en dat er geen aangifte wordt gedaan als de melder volgens afspraken heeft gehandeld."

Er zijn echter geen glasharde garanties dat een hacker niet vervolgd zal worden. Volgens de nu naar de Kamer gestuurde brief blijft de zelfstandige bevoegdheid van het Openbaar Ministerie bestaan om eventueel tot vervolging over te gaan wanneer het vermoeden bestaat dat er strafbare feiten zijn gepleegd.

Vrijbrief

Wil van Gemert, Directeur Cyber Security van de Nationaal Coördinator Terrorismebestrijding en Veiligheid, laat weten dat het geen vrijbrief voor het hacken van andermans systemen is.

"Dit is geen vrijbrief om maar te doen wat je wilt, het is een kader waarmee je als bedrijf, als je het van tevoren kenbaar maakt, duidelijk maakt dat je geïnteresseerd bent om te weten wat voor kwetsbaarheden je hebt en dat je die op verantwoorde wijze gemeld wilt zien en daar op een normale manier mee omgaat."



EC onthult cybercrime-centrum in Den Haag

Eurocommissaris Cecilia Malmström zal in Den Haag het Europees cybercrimecentrum onthullen.

Het European Cybercrime Centre (EC3) wordt op 9 januari aan de pers gepresenteerd, de officiële ingebruikname vindt op 11 januari plaats.

Het centrum is ondergebracht bij Europol, dat zich al in Den Haag bevindt. Het EC3 moet de gevaarlijkste cybercrimedreigingen en cybercriminele-organisaties in kaart brengen.

Ook zal het centrum lidstaten bij het uitvoeren van cybercrime-onderzoeken ondersteunen. "De komst van een Europees cybercrimecentrum zal een mijlpaal zijn in de strijd van de EU tegen cybercrime", aldus Europol-directeur Rob Wainwright.

Volgens Wainwright zal het centrum Europese overheden, bedrijven en burgers het gereedschap bieden om cybercrime aan te pakken.

Anti-virus boot cd's

Soms is het nodig om een computer vanaf een ander medium en buiten Windows om te scannen. In dit soort gevallen biedt een boot cd uitkomst.

De meeste anti-virus boot cd's starten een Linux distributie en laden vervolgens de virusscanner. De volgende stap is het downloaden van de laatste updates, waarna het scannen kan beginnen.

- [AVG Rescue CD](#)
- [Avira AntiVir Rescue System](#)
- [Dr Web Live Bootable Antivirus CD](#)
- [F-Secure Rescue CD](#)
- [Kaspersky Rescue CD](#)

Online scanners

Het installeren van een tweede virusscanner wordt over het algemeen afgeraden. Voor wie toch een 'second opinion' wil, kan een online scan uitkomst bieden.

- [ESET Online Scanner](#)
- [F-Secure Online Scanner](#)
- [Trend Micro HouseCall](#)
- [Bitdefender Online Virus Scanner](#)



'Hoe je weet dat je smartphone is gehackt'

Mobiele malware voor met name het Android-besturingssysteem kende een grote groei in 2012, maar hoe weet je nu dat je smartphone of tablet besmet is geraakt door een kwaadaardige applicatie? Beveiligingsbedrijf Lookout heeft een lijstje van vijf punten gemaakt waarmee smartphone-eigenaren kunnen controleren of hun toestel geïnfecteerd is. Een eerste aanwijzing is het snel leeglopen van de accu.

Doordat kwaadaardige apps continu in de achtergrond draaien, zal het toestel veel eerder leeg raken dan normaal. Een tweede herkenningpunt is het versturen en ontvangen van vreemde sms-berichten. Een andere aanwijzing zijn vreemde of onbekende kosten op de telefoonrekening.

Ook internationale telefoongesprekken kunnen een aanwijzing van een besmet toestel zijn. Als laatste punt waarschuwt Lookout voor telefoons 'die gek doen', bijvoorbeeld apps die niet goed openen of werken, of uit zichzelf worden geopend.

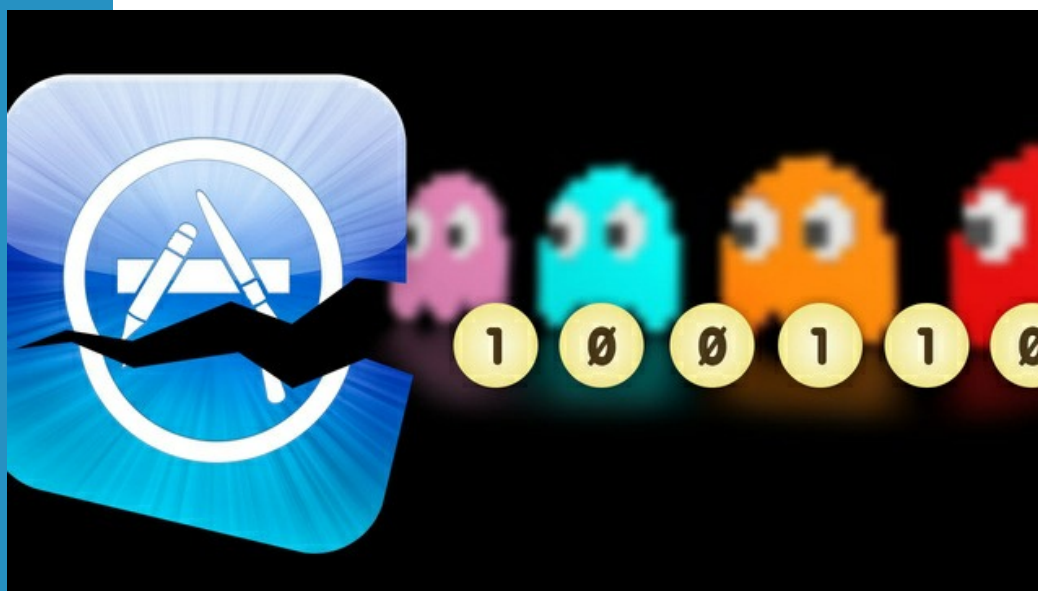
Om mobiele malware te voorkomen wordt geadviseerd de software op het toestel up-to-date te houden en voorzichtig te zijn met App Stores van derden. "Het is altijd beter om bij bekende merken langs te gaan, en blijf bij de Google Play Store, Apple App Store en de Amazon.com app store", aldus het beveiligingsbedrijf.

Browser plugins

Veel malware wordt tegenwoordig via de browser verspreid. Verschillende anti-virusbedrijven bieden dan ook plugins aan die links, downloads en websites scannen.

Plugins zijn er voor Internet Explorer (IE), Firefox (FF), Opera (OP) en Google Chrome (GC).

- [BitDefender QuickScan \(GC\)](#)
- [Dr Web \(IE/FF/OP\)](#)
- [G Data CloudSecurity \(IE/FF\)](#)
- [Prevx SafeOnline](#)
- [Team Cymru's MHR \(FF\)](#)
- [Trend Micro Browser Guard](#)
- [Trusteer Rapport](#)



Half miljoen wifi-routers lek

Het wifi-wachtwoord van minstens een half miljoen routers, waaronder modellen van KPN, UPC en Ziggo, is nog steeds te kraken. Het wifilek is al bekend sinds eind 2011, maar het probleem is nog steeds niet opgelost.

Het lek zit in routers van KPN (Experia ZTE H220N), Ziggo (Ubee evw3200) en de Horizon mediabox van UPC.

Ook sommige routers uit de losse verkoop zijn lek zoals de Linksys E1000 en E2000.

Kwaadwillenden kunnen makkelijk misbruik maken van het lek, waardoor ze toegang krijgen tot het netwerk en de computer kunnen overnemen. Daarvoor moeten de hackers wel in de buurt van het wifi-netwerk zijn.

Hoe gezond is je schijf?

Je harde schijf is wellicht het belangrijkste onderdeel van je pc – je programma's en gegevens, weet je wel – en tegelijk is het ook een van de meest kwetsbare componenten. Je houdt dus maar beter de gezondheid van je schijf in de gaten. Of liever: je láát dat doen, door een tool als [GsmartControl](#).

GSmartControl, dat zich zowat op alle mogelijke platformen laat installeren en eigenlijk weinig meer is dan een GUI voor de opdrachtregeltool smartctl, lijst eerst alle gedetecteerde schijven op en geeft meteen al een indicatie over de algemene gezondheidstoestand van de schijven. Voorwaarde is wel dat de schijf voorziet in zogenoemde S.M.A.R.T-data (Self-Monitoring, Analysis and Reporting Technology) – wat bij nagenoeg alle schijven het geval is. Mocht je toch geen S.M.A.R.T.-data doorkrijgen, ga dan na of die functie wel in het systeem-BIOS is geactiveerd.

Door de gewenste schijf aan te klikken krijg je dan veel meer gedetailleerde informatie te zien. Wanneer je namelijk het tabblad Attributes opent, toont GsmartControl je alle gedetecteerde S.M.A.R.T-attributen, inclusief de ideale waarden, de drempelwaarden en de vastgestelde waarden. Behoorlijk technisch, dat wel, maar als je de muispijl even boven zo'n attribuut of waarde houdt, krijg je nuttige feedback.

Maar er is meer. Op het tabblad Error log vind je de vijf meest recente problemen opgelijst die de controller met de schijf heeft vastgesteld. Ook dat kan je inzicht geven in de betrouwbaarheid van de schijf.

Ten slotte kan je nog een tweetal zelftests laten uitvoeren: een snelle zelftest (circa 2 minuten) en een uitgebreide zelftest (die ruwweg anderhalf uur in beslag kan nemen, afhankelijk ook van het schijftype en –capaciteit). Deze tests zijn op geen manier destructief voor je data. Dat neemt niet weg dat zo'n zware test behoorlijk beslag legt op je schijf en, bij een onbetrouwbaar exemplaar misschien net de fatale slag toebrengt. Vooraf een back-up maken van je gegevens is dus wel aangewezen. Na afloop van de tests vind je dan een gedetailleerd rapport terug op het tabblad Self-test logs.



Telefoneren via Facebook

's Werelds grootste sociale netwerk is in Canada gestart met het aanbieden van gratis online telefoongesprekken.

Andere gebruikers kunnen sinds deze week gesproken berichten naar elkaar versturen via Facebook Messenger. Zij dienen hiervoor een update van de Messenger app voor iOS of Android binnen te halen.

Om een gesproken bericht naar een Facebookvriend te sturen, moeten gebruikers op het '+' teken drukken naast het venster waarin je een boodschap kunt schrijven. Vervolgens houd je de opname knop vast terwijl je praat. Als je klaar bent laat je de knop los waarna de boodschap automatisch wordt verzonden.

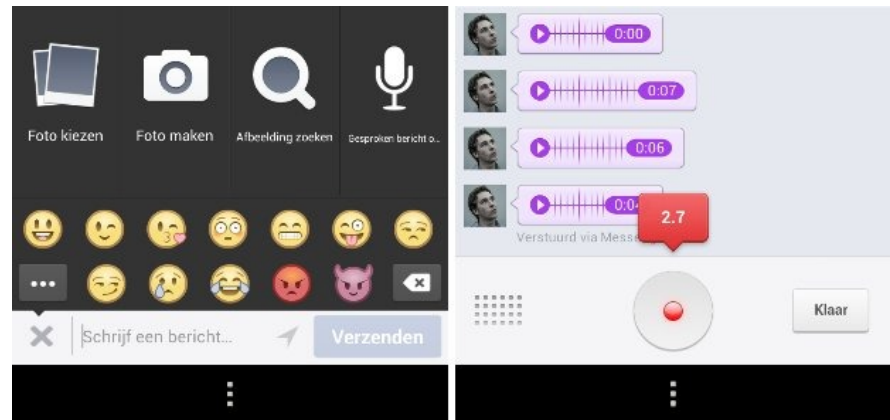
Het is afwachten of de nieuwe functie aanslaat onder gebruikers. Het inspreken van voicemail is binnen de telefonie al geruime tijd op zijn retour, in plaats daarvan sturen mensen elkaar berichten via diensten als Whatsapp.

De telefoniedienst waarvan Canadese gebruikers gebruik kunnen maken werkt op eenzelfde wijze als Skype. Vooralsnog spreekt Facebook over een test.

Voicemails sturen met Facebook Messenger

Facebook heeft 4 januari jl. de Messenger app voor Android en iOS van een update voorzien. De meest opmerkelijke toevoeging is de mogelijkheid om voicemails naar je contacten te versturen.

Om een voicemail te versturen, druk je op het plusteken links van het vak waar je normaal gezien je bericht zou typen. Naast de mogelijkheid om een afbeelding te versturen, kan je hier vanaf nu ook kiezen om een gesproken bericht op te nemen.



Houd de rode opnameknop ingedrukt terwijl je je bericht opneemt, en laat hem weer los om de opname te versturen. Wil je de opname annuleren, dan volstaat het om je vinger van de knop te schuiven.

Je contact kan de voicemails zowel via de Messenger app als via de website van Facebook beluisteren. De gewone Facebook app geeft wel een melding bij een nieuw gesproken bericht, maar verwijst je door naar de Messenger app om het af te spelen.

De vernieuwde Facebook Messenger app is beschikbaar in de Apple App Store en de Google Play Store.



Slachtoffer?

Wanneer je het slachtoffer bent geworden van een delict dat middels internet is gepleegd dan is het noodzaak om de informatie over dit delict vast te leggen. Informatie op het internet is zeer vergankelijk. Probeer zoveel mogelijk gegevens vast te leggen. Dit kunt je doen door:

- De datum en tijd van het feit of opeenvolgende feiten te noteren;

- De betreffende Internetpagina('s) waarop het bericht staat op te slaan als bestand;

- Eén of meerdere afdrucken op papier te maken van de betreffende Internet pagina('s) waarop het bericht is geplaatst die als testbaar belastend bewijsmiddel kunnen dienen;

- Is afdrucken niet (meteen) mogelijk, kan dit ook door schermkopieën te maken. Dit kan door de Print Scrn-toets

- Gebruik desnoods een digitale camera om de situatie op het scherm vast te leggen.

- het internetadres (URL) van de relevante pagina's te noteren. Deze is te vinden bovenin het scherm van de gebruikte internet browser (meestal beginnend met http://);

- De naam (meestal nickname) van de persoon die het bericht heeft geplaatst;

- De datum en tijdstip (indien aanwezig) wanneer bericht is geplaatst;

- Het e-mailadres (indien aanwezig) van de persoon die het bericht heeft geplaatst. Het e-mailadres staat op sommige fora gewoon vermeld. Op andere fora is het e-mailadres als link te vinden achter in een soort menu wat te vinden is binnen het 'persoonlijke' gedeelte van de gebruiker die het bericht heeft geplaatst.

Data verbergen

Iedere gebruiker heeft wel ergens gegevens opgeslagen die hij liever niet met anderen deelt. Recht op privacy, heet dat. Nu kan je dergelijke data onder Windows wel in je eigen profielmap opslaan, maar echt veilig is dat niet. [Wise Folder Hider](#) pakt het anders aan: die maakt je gegevens onzichtbaar, ook als je bijvoorbeeld via een ander besturingssysteem opstart.

Na de installatie (die je vriendelijk vraagt of je nog meer gratis software wil downloaden - neen, dus?) moet je logischerwijze eerst een 'master password' invullen. Onthoud dat wachtwoord goed, want het is de enige manier om gegevens die je straks gaat verbergen, te benaderen.

Vervolgens verschijnt het hoofdvenster van Wise Folder Hider. Van hieruit kan je dan specifieke mappen of bestanden verbergen. Die kan je gewoon naar het hoofdvenster verslepen of je klikt hier een knop aan en bladert zelf naar de gewenste gegevensbestanden.

Zolang je bij Wise Folder Hider bent aangemeld, krijg je vanuit dit venster probleemloos toegang tot 'verborgen' bestanden. Zodra je je bij de tool afmeldt, blijken die gegevens onzichtbaar en dus automatisch ook ontoegankelijk. Deze truc kan je trouwens ook met een usb-stick uithalen.

Je kan deze beveiliging echter nog doordrijven. Elk item dat je op deze manier verborgen hebt – beschermd door het hoofdwachtwoord dus – kan je nog van een bijkomend wachtwoord voorzien, specifiek voor dat item.

Via de kleine Menu-knop en de rubriek Languages is het programma ook Nederlandstalig te maken.

De beste manier om data af te schermen blijft hoe dan ook (stevige) encryptie, maar het moet gezegd: ook met Wise Folder Hider geef je de meeste onverlaten ongetwijfeld al het nakijken.



Usb sneller verwijderen

Werken met usb-sticks is handig. Maar het feit dat Windows wil dat je de gegevensdragers eerst veilig verwijdert in Windows voordat je ze daadwerkelijk uit de usb-poort kunt trekken, zorgt ervoor dat je er niet zo snel mee kunt werken als je wellicht zou willen. Gelukkig is daar een oplossing voor, je kunt de belemmering voor het snel verwijderen namelijk uitschakelen.

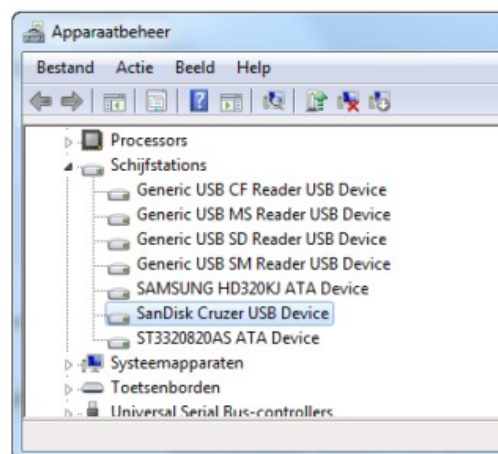
01 Usb-stick plaatsen

Het is eigenlijk niet de bedoeling dat je een usb-stick zomaar uit de usb-poort trekt zonder deze eerst veilig te verwijderen. Dit komt doordat Windows gebruikmaakt van schrijfcache: Windows gebruikt het geheugen om schrijfopdrachten te verzamelen die een fractie later worden uitgevoerd op het verwisselbare medium.

Dit is bedoeld om langzamere stations te versnellen. Het nadeel is uiteraard dat, wanneer je een station verwijdert terwijl er nog weggeschreven wordt, de data niet meer kan worden weggeschreven. Schakel je schrijfcache uit, dan kun je dus wel direct de usb-stick verwijderen.

Schrijfcache is echter iets dat je niet globaal uitzet, maar uitschakelt per afzonderlijk usb-apparaat. Plaats daarom de usb-stick (of sticks) waarvoor je schrijfcache wilt uitschakelen. Overigens zorgt het uitschakelen van deze functie ervoor dat het schrijven naar het verwisselbare medium iets langzamer zal gaan, maar in werkelijkheid zijn deze verschillen tegenwoordig vaak verwaarloosbaar. Daarbij is de handeling uiteraard niet onomkeerbaar, dus merk je toch aanzienlijke snelheidsverschillen, dan zet je de schrijfcache gewoon weer aan.

Schrijfcache is een optie die je per apparaat afzonderlijk instelt, dus zorg ervoor dat je de juiste usb-stick in de pc plaatst.



Usb sneller verwijderen (2)

03 Verantwoord werken

Het is fijn dat je nu niet meer telkens allerlei stappen hoeft te doorlopen voordat je een usb-stick uit de usb-poort mag trekken, maar dat wil niet zeggen dat je nu als een bezetene sticks kunt gaan wisselen zonder erbij na te denken.

Trek je echter een usb-stick uit de usb-poort terwijl Windows nog aan het schrijven is, dan is er wel een kans dat je de stick daarmee onleesbaar maakt.

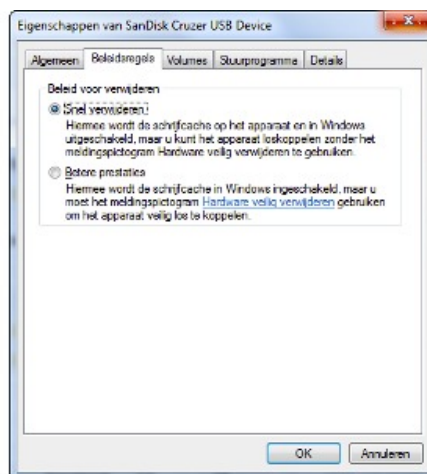
Het gaat dan vaak om een beschadigd indexbestand dat met behulp van software meestal wel weer te repareren is, maar zo'n grap kost je doorgaans enorm veel tijd. De reden dat we schrijfcache uitschakelen is juist dat we tijd willen winnen, niet verliezen. Wanneer je een usb-stick uit het poortje wilt trekken, kun je dus het beste twee of drie seconden wachten, zodat je zeker weet dat Windows klaar is.

02 Instelling aanpassen

Open de Windows Verkenner en klik met de rechtermuisknop op Computer en vervolgens op Eigenschappen. In het venster dat verschijnt, klik je op Apparaatbeheer (dit is het Configuratiescherm, dus klikken op Start / Configuratiescherm kan ook) en zoek je naar het kopje Schijfstations.

Wanneer je klikt op dit kopje, zie je tussen de apparaten de naam van de usb-stick(s) staan die met de computer is of zijn verbonden. Dubbelklik op het apparaat, waarna er een venster Eigenschappen verschijnt. In dit venster klik je op het tabblad Beleidsregels. Hier zie je twee opties: Snel verwijderen en Betere prestaties.

Wanneer Betere prestaties is geselecteerd, moet je apparaten veilig verwijderen voordat je ze daadwerkelijk mag loskoppelen. Snel verwijderen is de optie waarnaar we op zoek zijn. Afhankelijk van het apparaat kan het zijn dat Snel verwijderen al standaard is geselecteerd. Kies de gewenste instelling en klik op OK. Herhaal deze stap voor alle usb-sticks waar je sneller mee wilt kunnen werken.



Je kunt aangeven of je de usb-stick snel wilt verwijderen of gaat voor betere prestaties.



Experimenteel, maar slimmer en sneller zoeken met Google

Google is aan het experimenteren hoe je het beste kan zoeken. Als je inlogt op je google-account en dan naar de volgende url gaat, kan je aan een van de experimenten meedoen:

<http://www.google.com/experimental/index.html>

Hier kan je kiezen uit voorkeursites, zodat deze hoger eindigen in je zoekresultaten. Of zoeken met behulp van een tijdlijn, zodat je alleen resultaten krijgt van bepaalde jaren. Sneller door je zoekresultaten heen bladeren met behulp van sneltoetsen! Of zoeken met een wereldkaart naast je resultaten, waarop direct alle locaties komen te staan :)

Helaas valt alles nog in beta, en alles is dus experimenteel, en helaas kan je maar aan 1 experiment tegelijk mee doen. Maar toch is het handig, zonder dat je daarvoor firefox plugins hoeft te installeren.

Beter zoeken met Google

Zoekopdracht specificeren

Hoe specifieker u de zoekopdracht formuleert, hoe beter de zoekresultaten worden. Dat geldt niet alleen voor de zoekwoorden die u gebruikt, er zijn veel meer trucjes die u kunt toepassen om tot goede resultaten te komen.

AND Deze term is niet nodig bij Google. Standaard worden alle woorden die u intypt meegenomen.

OR Wilt u niet dat alle termen worden meegenomen, maar hoeft slechts één ervan op een pagina voor te komen, gebruik dan OR, in hoofdletters. Bijvoorbeeld: notebook OR laptop

Minteken (-) Een minteken voor een woord (direct eraan vast) betekent dat u dit woord niet wilt meenemen in de zoekresultaten. Bijvoorbeeld: computer linux -windows

Plusteken (+) Een plusteken voor een woord (direct eraan vast) kan twee dingen doen. Ten eerste kunt u voorkeur aangeven bij meerdere zoekwoorden. Bijvoorbeeld: computer installatie +windows. Ten tweede kunt u voorkomen dat veelgebruikte woorden (en, het, hoe, waar) niet meegenomen worden. Bijvoorbeeld: windows 7 +en office 2003

Sterretje (*) Het sterretje gebruikt u wanneer u een deel van het zoekresultaat wilt laten invullen door Google, het is dus een 'wildcard'. Bijvoorbeeld: microsoft * 7

Tilde (~) De tilde gebruikt u wanneer u wilt zoeken op het woord (computer), én op vergelijkbare woorden (laptop). Bijvoorbeeld: ~computer

Aanhalingstekens (" ") Aanhalingstekens gebruikt u wanneer u naar een hele zin of een bepaald zinsdeel wilt zoeken. Bijvoorbeeld: "bestanden overzetten van pc naar mac"

Aanhalingstekens plus sterretje (" * ") Wilt u zoeken op een zinsdeel, maar weet u niet alle woorden exact, dan kunt u de aanhalingstekens gebruiken in combinatie met een ster. Bijvoorbeeld: "bestanden overzetten * mac"

Intitle: Wilt u dat uw zoekwoord in de titel van de pagina van de website voorkomt, dan gebruikt u intitle: met het zoekwoord direct eraan vast. Bijvoorbeeld: intitle:computer

Inurl: Wanneer u inurl: gebruikt, toont Google alleen websites waarin het woord in de url voorkomt. Bijvoorbeeld: inurl:computer

Site: Om binnen een site te zoeken, gebruikt u site:. Dit is ook erg handig als een site geen (goede) zoekfunctie heeft. Bijvoorbeeld: site:www.computertotaal.nl windows

Define: Weten wat een begrip betekent? Met define: zoekt Google de definitie voor u op, meestal wordt Wikipedia als informatiebron gebruikt. Bijvoorbeeld: define:videokaart

Related: Met de operator related: zoekt u naar gerelateerde websites. Bijvoorbeeld: related:www.computertotaal.nl

Filetype: De operator filetype: zorgt dat er alleen op een bepaald bestandstype wordt gezocht. Wilt u meerdere bestandstypen meenemen, gebruik dan OR tussen de verschillende bestandstypen. Bijvoorbeeld: filetype:doc OR filetype:pdf handleiding



Tips voor Windows 8

01 Vastmaken aan Start

In Windows 8 heb je tot in tegenstelling met de andere Windows versies een Microsoft account nodig.

Met dit account moet je inloggen op je computer. Wat hiervan eigenlijk het nut is weten we niet echt, we weten wel dan Microsoft door het gebruik hiervan naar cloud wil toe werken.

Wanneer je meerdere Windows 8 computers hebt, zullen je internet instellingen, favorieten, andere instellingen, thema's, apps, foto's en eventueel ook bestanden worden gesynchroniseerd.

Items op je bureaublad, zoals mappen en de Prullenbak, kun je vastmaken aan het Windows 8-startscherm. Zo heb je altijd snel toegang tot de locaties via een eigen tegel. Klik met de rechtermuisknop op het pictogram en kies voor Vastmaken aan Start. Het item is direct beschikbaar op het Startscherm. Heb je je later bedacht? Klik met rechts op de tegel op het Startscherm en kies voor Losmaken van Start (je vindt deze optie in de balk onderin). Via dezelfde balk kun je het item ook vastmaken aan de taakbalk. Kies voor Aan taakbalk vastmaken.

02 Startscherm indelen

Er bestaan verschillende mogelijkheden om de indeling van het Startscherm aan te passen. Zo wordt er onderscheid gemaakt tussen enkele en dubbele tegels. Een dubbele tegel neemt twee kolommen in. Je kunt een dubbele tegel eenvoudig smaller maken: klik erop met rechts en kies in de balk onderin voor Kleiner maken. Je kunt de tegel later altijd weer vergroten door er met rechts op te klikken en te kiezen voor Groter maken.

03 Groeperen

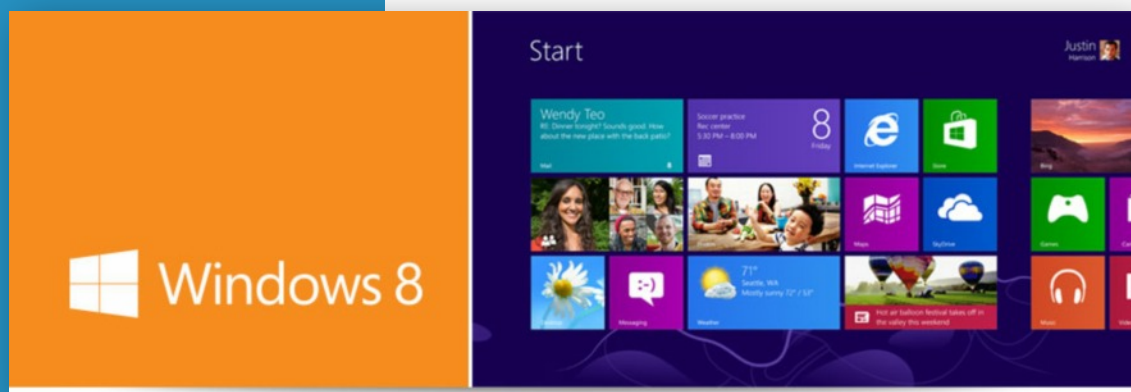
Er zit maar weinig structuur in het Startscherm. Dat kan beter, bijvoorbeeld door je applicaties te groeperen. Zo kun je bijvoorbeeld aparte groepen maken voor games, zakelijke software en andere hulpprogramma's. Plaats eerst alle tegels bij elkaar waarmee je één groep wilt maken. Klik op het minusteken rechtsonder in het scherm, zodat je uitzoomt. Hierna kun je de groep een passende naam geven. Klik erop met rechts en kies Naam aan groep geven. Een vak verschijnt, waarin je de groepsnaam kunt opgeven. Prettig is dat je later kunt uitzoomen binnen het Startscherm, waardoor de groepen zichtbaar worden.

04 Live-tegels

Apps die ervoor geschikt zijn, kunnen informatie in de tegel tonen. Dit worden live-tegels genoemd. De tegel van de Berichten-app toont bijvoorbeeld de meest recente e-mail, terwijl de tegel van de Weer-app het actuele weer toont. De informatie op de tegels wordt regelmatig vernieuwd. Wil je niet dat een specifieke tegel live-informatie toont? Klik erop met rechts en kies Live-tegel uitschakelen. Voortaan wordt alleen de naam van de app getoond.

05 App-meldingen onder controle

Apps kunnen allerhande meldingen geven. Bijvoorbeeld zodra je een nieuw Facebook-bericht binnenkrijgt of wanneer een belangrijk nieuwsbericht voorbijkomt. Standaard mogen alle apps meldingen tonen, maar je kunt zelf aangeven van welke apps



Tips voor Windows 8 (2)

Windows 8 beschikt over een Fast Startup functie, waarmee je de computer verbazend snel kan opstarten.

De Fast Startup functie, ook wel hybrid boot of hybrid Shutdown genoemd, zorgt ervoor dat Windows 8 nog sneller kan opstarten dan in de normale opstart modus. De techniek werkt als volgt: wanneer de computer wordt afgesloten, wordt alle systeem informatie, de kernel sessies en de drivers opgeslagen in het "hiberfil.sys" bestand.

Dit is het bestand wat ook wordt gebruikt om alle bestanden op te slaan, wanneer de computer in sluimerstand staat, maar bij sluimerstand worden alle bestanden van het RAM-geheugen opgeslagen, waardoor het bestand dan tot wel 4 GB en zelfs meer groter kan worden, bij de Fast Startup Functie is dit niet het geval, omdat dan enkel de systeem informatie wordt opgeslagen in dit bestand en de andere programma's en tools die nog draaien gewoon worden afgesloten.

Wanneer de computer dan terug opgestart, worden deze bestanden gewoon terug snel naar het RAM-geheugen geladen en moeten ze dus niet opnieuw worden geladen en opgebouwd, wat als resultaat heeft dat de computer 30% tot 70% sneller opstart. Microsoft laat ook nog weten dat het nog sneller gaat wanneer je een moederbord hebt met "UEFI". Normaal gezien is deze functie standaard al ingeschakeld in Windows 8.

07 Geen app-meldingen meer

Wil je helemaal geen meldingen van apps meer ontvangen? Je kunt de functie volledig uitschakelen, zodat er geen meldingen meer worden getoond. In het onderdeel Pc-instellingen ga je naar Meldingen. In de sectie Meldingen (aan de rechterkant van het scherm) zet je de schuif uit bij App-meldingen weergeven. Je kunt er ook voor kiezen om de app-meldingen nog wel weer te geven, maar niet meer op het vergrendelingsscherm. Zet dan de schuif op Uit bij App-meldingen weergeven op vergrendelingsscherm. Wil je geen geluiden horen, maar wel nog meldingen zien? Zet de schuif op Uit, bij Meldingsgeluiden afspelen.

08 Tweede beeldscherm

Via de rechterbalk kun je het bureaublad eenvoudig uitbreiden naar een extern scherm. Handig als je bijvoorbeeld een presentatie houdt of een film wilt kijken. Open de Charms-balk en klik op Apparaten. Een overzicht van randapparaten verschijnt. Klik nu op Tweede scherm. Vervolgens kun je beelden tonen op een aangesloten scherm. Je kunt hierbij kiezen om het bureaublad te dupliceren, het uit te breiden (zodat je werkoppervlak groter wordt) en alleen het tweede scherm te gebruiken. Wil je het tweede scherm niet meer gebruiken, kies dan voor Alleen computerscherm.

09 Geen persoonlijke gegevens

De dynamische tegels van het Startscherm geven diverse informatie weer. Denk aan de koersen van de Aandelen-app, het laatste nieuws van de Nieuws-app en de updates binnen uw sociale netwerk. Als u hierop geen prijs stelt en even geen persoonlijke informatie wilt zien, dan kunt u ervoor kiezen om de persoonlijke gegevens te wissen. In het Startscherm roept u de balk aan de zijkant op. Kies Instellingen. Bovendien de balk kiest u voor Tegels / Gegevens verwijderen.

10 Navigeren met het toetsenbord

Natuurlijk, het Startscherm is duidelijk ontwikkeld met touch-apparaten (zoals een tablet) in het achterhoofd. Toch kom je met het toetsenbord en de muis ook een heel eind. Om vooruit en achteruit te rollen, kun je het muiswiel gebruiken. Om in één keer naar het einde van de lijst met tegels te bladeren, druk je op de End-toets op het toetsenbord. Druk op de Home-toets om in één keer naar het begin van de lijst te rollen. Wil je in- of juist uitzoomen op een lijst, bijvoorbeeld als deze omvangrijk is geworden, dan rol je met het muiswiel terwijl je de Shift-toets houdt ingedrukt.

11 Verkenner-Lint

Windows Verkenner is voortaan voorzien van een Lint, zoals je mogelijk al kent van Office. Het Lint biedt plaats aan veelgebruikte bestandsopties, zoals knippen, kopiëren en naam wijzigen, maar kent ook contextgerelateerde opties. Open je een bibliotheek, dan verschijnt de extra tab Hulpprogramma's voor bibliotheken. Klik hierop om de bibliotheek te beheren en de bibliotheek te optimaliseren voor specifieke inhoud. Zo kun je de bibliotheekinhoud optimaliseren voor documenten, muziek, afbeeldingen en video's. Via de knop Opslaglocatie instellen, kun je aangeven welke map standaard moet worden gebruikt voor het opslaan van foto's. Ook is er de tab Opties voor muziek of Opties voor video. Op deze tab vind je de mogelijkheden om media af te spelen en aan een afspeellijst toe te voegen.



Tips voor Windows 8 (3)

Windows 8 video:

- [Introductie](#)
- [review](#)
- [Start menu](#)
- [Bureaublad en Verkenner](#)
- [Store en Apps](#)

Hoe weet ik of mijn oude computer nog wel geschikt is voor Windows 8?

Voor een goede werking van Windows 8 is het van belang dat alle hardware door Windows 8 wordt ondersteund.

Dit is zelf te controleren door naar <http://www.windows.com> te gaan en daar de 'Upgrade assistent' een controle uit te laten voeren.

Deze assistent zoekt uit of de computer voldoet aan de minimale systeemeisen en of voor alle componenten en aangesloten randapparatuur de stuurprogramma's beschikbaar zijn.

12 Weg met het Lint

Ben je niet gecharmeerd van het Lint van Windows Verkenner? Je kunt het Lint ook minimaliseren, door te klikken op het pijltje dat je rechtsboven in het venster aantreft. De eerstvolgende keer dat je weer een Verkenner-venster opent, is het niet meer aanwezig.

13 Werkbalk Snelle toegang

Linksboven in het Verkenner-venster zit de werkbalk Snelle toegang verscholen. Deze geeft opties weer die vaak worden gebruikt in Verkenner. Denk hierbij aan het maken van een nieuwe map, het oproepen van de bestandseigenschappen en het geven van een nieuwe naam aan de map. Je kunt de functies van de werkbalk Snelle toegang aanpassen. Klik op de pijl naast de werkbalk (linksboven in het venster). Een menu verschijnt. Kies hier welke onderdelen in de werkbalk moeten worden opgenomen. Je kunt ook de plaats van de werkbalk aanpassen (via de optie Onder het lint weergeven).

14 Snel schermafbeeldingen maken

Een slimme, maar verborgen optie in Windows 8: snel een schermafbeelding maken. Met de PrintScreen-toets (ook wel aangeduid met PrtScn) maakte je in vorige Windows-versies snel een schermafbeelding van het scherm. Gebruik je nu de toetsencombinatie Windows-toets+PrintScreen, dan zal het scherm even knippen en wordt de gemaakte schermafbeelding automatisch opgeslagen in de map Afbeeldingen\Schermopnamen.

15 Andere oriëntatie

Maak je gebruik van een tablet? Je kunt de schermoriëntatie van de tablet eenvoudig wisselen tussen landschapsmodus en portretmodus. Druk op de Windows-toets+O. Het scherm wordt omgedraaid.

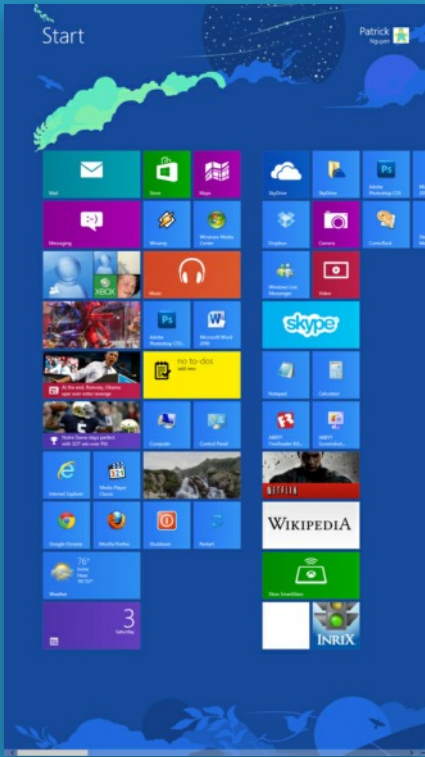
16 Heimwee

Het nieuwe Startscherm en de afwezigheid van het menu Start is even wennen. Kun je er maar niet aan wennen? Verschillende softwaremakers spelen hier slim op in en brengen software uit waarmee u een 'klassieke' Windows-omgeving kunt nabootsen. Met RetroUI kunt u schakelen tussen de oude en de nieuwe Windows-omgeving. U vindt het programma via <http://retroui.com>. Nadat je het hebt geïnstalleerd, wordt het bureaublad van Windows standaard geopend bij het laden van Windows. Je kunt verder zelf bepalen of andere 'nieuwe' onderdelen (zoals de Charms-balk en opdrachtenbalk) wel of niet kunnen worden gebruikt. Je kunt de software zeven dagen proberen, daarna betaal je zo'n vier euro.

17 Sociale netwerken koppelen

In Windows 8 is veel aandacht besteed aan de koppeling met sociale netwerken. Zodra je sociale netwerkaccounts aan Windows hebt gekoppeld, worden dingen als statusupdates en contactinformatie op verschillende plaatsen in het besturingssysteem getoond. Het koppelen van de accounts moet nog wel gebeuren. In het Startscherm kies je voor Personen. Links in het venster zie je welke accounts je kunt koppelen. Bijvoorbeeld: Twitter-contactpersonen, Exchange-contactpersonen en Google-contactpersonen. Klik op Alles weergeven in Instellingen. Hierna kun je ook andere diensten koppelen, zoals Hotmail.





Er zijn een hoop fabrikanten die binnenkort zullen komen met een Windows 8 tablet of die eraan bezig zijn.

De lancering van Windows 8 is alweer even geleden en hoewel vele mensen en zelfs grote fabrikanten schrik hadden dat het geen succes ging zijn, blijkt het dit toch te zijn.

Hierdoor gaan vele fabrikanten dan toch verder met het maken van Windows 8 tablets, er zijn al reeds enkele op de markt zoals de Samsung Ativ Tab, maar ook andere fabrikanten, zoals Nokia en Lenevo en nog enkele anderen gaan er nu eentje maken.

Het Windows 8 tablet van Nokia zal onthult worden in februari 2013 en het betreft een tien inch tablet met een Qualcomm processor die draait op Windows RT. Het feit dat Nokia nu ook zijn eigen Windows 8 tablet gaat lanceren is goed nieuws, want eerder dit jaar had het bedrijf een financieel niet zo goede situatie.

Tips voor Windows 8 (4)

18 Sociale netwerken beheren

Het aantal instelmogelijkheden voor je sociale netwerken is vanuit Windows zelf relatief beperkt. Online kun je flink meer opties aanpassen en hebt je meer controle over je account. In de Personen-app druk je op Windows-toets+I om het instellingenvenster te openen. Kies het account. Klik vervolgens op Dit account online beheren. Een webpagina met extra opties wordt geopend.

19 Direct updates zien

Als je jouw sociale netwerken aan Windows hebt gekoppeld, kun je direct reageren op en communiceren met contactpersonen. In het Startscherm kies je voor Personen. Klik op de contactpersoon met wie je wil communiceren. De persoonlijke pagina (met zaken als updates en foto's) wordt geladen. Links zie je de contactmogelijkheden. Zo kun je direct een Facebook-bericht schrijven en een e-mail sturen. Klik achtereenvolgens op Profiel weergeven / Meer details, als je aanvullende (contact)gegevens wilt zien.

20 Berichten uitbreiden

Via de Berichten-app kun je met je vrienden communiceren via verschillende kanalen. Zo kun je de app koppelen aan Messenger en Facebook. Het koppelen gaat relatief eenvoudig. Open de Berichten-app en druk op Windows-toets+I. Kies Accounts. Een overzicht van bestaande koppelingen verschijnt. Klik op Een account toevoegen. Selecteer het account dat je wilt toevoegen en geef de vereiste aanmeldingsgegevens op om het netwerk te koppelen met de Berichten-app. Bestaande netwerken kun je beheren door erop te klikken.

21 Contactpersonen filteren

De Personen-app laat je contactpersonen zien van verschillende kanalen, waaronder Hotmail, Facebook en LinkedIn. Ook andere bronnen, zoals Outlook en Google, kun je toevoegen. Dit betekent echter niet dat je altijd alle contactpersonen hoeft te bekijken. Je kunt namelijk zelf opgeven welke lijsten je wilt zien en welke lijsten je wilt verbergen. Prettig hierbij is dat de personen nog wel in de zoekresultaten worden getoond, ook als de lijst is verborgen. Open de Personen-app en open de instellingenbalk. Kies voor Opties / Mijn lijst met contactpersonen filteren. Haal de vinkjes weg naast de lijsten die je niet wilt tonen. De lijsten worden direct verborgen, maar de zoekresultaten blijven gelijk.

22 Aangepaste sorteervolgorde

Standaard worden contactpersonen in de Personen-app gesorteerd op voornaam. Vooral bij omvangrijke lijsten kan het handig zijn juist te sorteren op achternaam. Je kunt de sorteervolgorde aanpassen. In de Personen-app open je de instellingenbalk. Ga naar Opties. Zet de schuif op aan bij de optie Mijn contactpersonen sorteren op achternaam.

23 Alle apps tonen

Benieuwd naar alle applicaties die op de pc aanwezig zijn? Er zijn twee manieren waarop je dit overzicht kunt oproepen. In het Startscherm van Windows klik je met de rechtermuiskop op een leeg gedeelte. In de balk onderin klik je op Alle apps. Het overzicht verschijnt. Liever het toetsenbord? Druk op Windows-toets+Q. Deze toetsencombinatie kun je ook gebruiken als je op het bureaublad werkt.

24 Apps verwijderen

Het verwijderen van apps gaat sneller dan met bureaubladsoftware. Klik met rechts op de tegel van de app. Kies voor Installatie ongedaan maken. Je kunt de app ook verbergen, als je deze niet wilt verwijderen, maar ook niet prominent in beeld wilt hebben. Klik erop met rechts en kies Losmaken van Start. De app is dan alleen zichtbaar als je ernaar zoekt via de zoekfunctie.



Tips voor Windows 8 (5)

Windows 8 heeft 2012 afgesloten met een marktaandeel van 1,6 %.

Vorige maand raakte het marktaandeel van Windows 8 niet hoger dan 1%, gelukkig is er ondertussen toch verandering in gekomen.

Op dit moment staat het marktaandeel namelijk op 1,64%. Dat lijkt niet veel, maar we spreken toch van een succesvolle groei. Vermits het besturingssysteem eind oktober is gelanceerd en in november pas echt verkrijgbaar was op de markt. Bovendien staat het besturingssysteem met zijn 1,64% niet meer laatste in de rangorde, het heeft namelijk Linux voorbij gestoken dat nu laatste staat met z'n 1,21%.

Vergeleken met Linux dat al jaren op de markt is, is het marktaandeel van Windows 8 dus al heel groot, want Windows 8 is nog maar drie maanden op de markt en Linux gaat al jaren mee.

De grote koploper blijft nog steeds Windows 7 met 44,9%, als tweede staat Windows XP, vervolgens Mac OS X en als vierde Windows Vista met 5,6%.

Dat de lancering van Windows 8 is gelukt kunnen we dus nog niet echt zeggen, maar dat het besturingssysteem aardig opweg is kunnen we zeker en vast concluderen.

25 Ruimte opvragen

Elke app neemt ruimte in. Als opslagruimte beperkt is, is het handig te achterhalen hoeveel ruimte zij in beslag nemen. In het onderdeel Pc-instellingen kies je voor Algemeen. Klik op de knop Appgrootte bekijken. Een overzicht van apps (en de bijbehorende ruimte) verschijnt. Op basis hiervan kun je bepalen welke onderdelen niet meer interessant zijn.

26 Direct delen

Vanuit veel Windows 8-apps kun je direct onderdelen delen, zonder dat je hiervoor een app hoeft te starten. Heb je bijvoorbeeld foto's die je via de SkyDrive-app bekijkt? Je kunt deze direct delen via e-mail of sociale netwerken. Open de map die je wilt delen en open de Charms-balk. Kies Delen. Vervolgens kies je een van de kanalen die je voor het delen wilt gebruiken, bijvoorbeeld E-mail of Personen.

27 Nooit meer sluiten

Apps in Windows 8 hoeven niet te worden afgesloten. Zodra ze enige tijd niet worden gebruikt, komen ze in een sluimerstand terecht. Je kunt de app snel weer oproepen als dat nodig is, maar in de sluimerstand wordt een minimaal beslag gelegd op de systeembronnen. Soms kan het handig zijn om een app alsnog expliciet af te sluiten. Je kunt hiervoor drukken op Ctrl+F4. Nog handiger is met de muis bovenin het venster te zweven (waardoor deze verandert in een handje) en dan de app naar de onderkant van het scherm te schuiven: ook hiermee sluit je de app af. Ook handig voor touch-apparaten: veeg de app naar beneden.

28 Geen automatische updates

Standaard haalt Windows automatisch de nieuwste updates voor je apps binnen. Wil je hierover zelf controle houden? Je kunt het standaardgedrag aanpassen. Open de Windows Store en roep de instellingenbalk op (Windows-toets+I). Kies App-updates. Zet de schuif op Uit bij de optie Automatisch updates downloaden voor mijn apps. Je kunt later altijd handmatig controleren op de beschikbaarheid van apps. Klik op Controleren op updates.

29 Licenties beheren

Apps die je in de Windows Store koopt, kun je op meerdere computers installeren. Het is toegestaan om de app op maximaal vijf pc's te installeren. Windows houdt bij op welke computers de apps zijn geïnstalleerd. Een overzicht hiervan kun je opvragen via de Windows Store. Open het instellingenvenster (Windows-toets+I) en ga naar Uw account. In de sectie Uw pc's, zie je op welke pc's de apps zijn geïnstalleerd. Je kunt de pc die je gebruikt verwijderen uit de licentielijst. Hiermee komt een positie vrij. Klik op de knop Verwijderen en klik hierna op Bevestigen.

30 Volwaardige browser

De app-versie van Internet Explorer (die je via het Startscherm kunt openen) is voldoende voor het bezoeken van websites. Kom je echter een website tegen die je liever bezoekt met de vertrouwde bureaubladversie van Internet Explorer? Klik met rechts op een leeg gedeelte. In de balk onderin kies je voor Hulpprogramma's / voor pagina's / Op het bureaublad weergeven. De bureaubladversie van Internet Explorer wordt geopend en de pagina wordt geladen.



Windows® 8

In de Europese richtlijn inzake elektronische handel wordt daarom onderscheid gemaakt tussen het opslaan van informatie (caching en hosting) en het doorgeven van informatie, dat mere conduit genoemd wordt.

Wanneer er sprake is van onrechtmatige informatie die verwijderd moet worden van een server van een hostingprovider, dan zal die provider aan een verzoek van de officier of rechter-commissaris gehoor moeten geven.

Wanneer de informatie zich echter op een andere server bevindt, en er dus sprake is van mere conduit, dan zal de provider die informatie niet ontoegankelijk maken. In dat laatste geval kunnen bij de internetprovider wel de NAW-gegevens van de betreffende klant opgevraagd worden, zodat de eisende partij zich rechtstreeks tot de klant kan richten.

Om die procedure eenvoudiger en duidelijker te maken, heeft internetprovider XS4ALL als eerste in februari 2007 een procedure voor klachten over uitingen op internet gepubliceerd. In navolging daarvan heeft een groot aantal Nederlandse providers, samenwerkend in het programma Samen tegen Cybercrime, op 2 oktober 2008 een Gedragscode Notice-and-Take-Down[2] gepubliceerd, waarin beschreven staat hoe geklaagd kan worden over uitingen op internet en hoe met klachten wordt omgegaan.



Internetprovider

Een internetprovider of internetaanbieder (Engels: internet service provider of ISP) is een organisatie of persoon die diensten levert op of via het internet. Dit kan zowel de verbinding van een gebruiker aan het internet zijn, alsook diensten die de gebruiker via het internet kan gebruiken.

De verschillende diensten die een internetprovider aanbiedt zijn hieronder uitgewerkt.

Een (Internet) Access Provider of IAP is een organisatie of persoon die aan particulieren en/of bedrijven faciliteiten biedt om een vaste computer of een mobiel apparaat verbinding te laten maken met het Internet. Dit kan op verschillende methoden: bijvoorbeeld via inbellen, ADSL, kabelinternet of via UMTS of wifi.

Internet service provider

Een Internet Service Provider of ISP is een bedrijf dat via het internet aan klanten een eigen e-mailadres aanbiedt, de mogelijkheid geeft een eigen site op het World Wide Web te maken, en vaak om daar gegevens via FTP toegankelijk te maken. Vaak biedt een ISP ook een nieuwsserver voor Usenet.

In de volksmond wordt vaak ISP gezegd als de Access provider wordt bedoeld. Meestal bieden Access providers ook allerlei diensten aan die hen tot ISP maken. Steeds vaker worden de genoemde diensten op het internet door grote bedrijven als Microsoft, Google en Yahoo! gratis aangeboden.

Internet hosting provider

Een internethostingprovider of een IHP is een ISP die diensten levert voor het toegankelijk maken van een internet domeinnaam en webhosting (het maken van een eigen website).

Provideraansprakelijkheid

Omdat internetproviders vaak servers beheren waarop niet zichzelf, maar hun klanten informatie kunnen plaatsen, was in het verleden onduidelijk wie nu verantwoordelijk was voor onrechtmatige informatie op een bepaalde website: de beheerder van de webserver of degene die de informatie op de website beheert. Dit is kort uitgelegd het vraagstuk van de provideraansprakelijkheid.

Artikel 54a van het Nederlandse Wetboek van Strafrecht luidt:

Een tussenpersoon die een telecommunicatiedienst verleent bestaande in de doorgifte of opslag van gegevens die van een ander afkomstig zijn, wordt als zodanig niet vervolgd indien hij voldoet aan een bevel van de officier van justitie, na schriftelijke machtiging op vordering van de officier van justitie te verlenen door de rechter-commissaris, om alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om de gegevens ontoegankelijk te maken.

Dit betekent dat een internetprovider in beginsel niet verantwoordelijk is voor de informatie die haar klanten online plaatsen, mits de provider informatie ontoegankelijk maakt wanneer de officier van justitie of de rechter-commissaris dit bevelen.

Dat klinkt redelijk, maar is in de praktijk niet zo eenvoudig: Wanneer het informatie betreft op een webserver van een provider, dan kan die provider de informatie simpelweg verwijderen. Maar wanneer het informatie betreft op een server die eigendom is van de klant, en waar de internetprovider dus alleen zorg draagt voor de internetverbinding, dan ligt dat minder eenvoudig. In zo'n geval kan de provider de informatie niet van de server verwijderen: de enige maatregel die de provider zou kunnen nemen, is de internetverbinding verbreken. Maar daarmee zou ook alle andere informatie op de betreffende server, ontoegankelijk worden.



Maar dat is slechts de persoonlijke kant. Verschillende identiteiten bij meerdere diensten stellen me in staat per dienst te beperken wat ze van me mogen weten. Mijn bank hoeft niets te weten van bankrekeningen elders en al helemaal geen rekening te houden met m'n muziekvoorkeur of waar ik mijn boodschappen doe. Natuurlijk lekt deze informatie wel tussen leveranciers en is er een hele industrie ontstaan om me meer gericht producten te laten kopen.

Ook verzekeraars willen alles van me weten om hun risico zo klein mogelijk te houden. Sommige werkgevers willen zoveel mogelijk van hun werknemers weten. Hoe meer online diensten we gebruiken - en die kant gaat het steeds sterker op - hoe meer sporen we achterlaten die op een gegeven moment in een database belanden.

Databases kunnen zich tegen je keren

Sommige diensten, waaronder Facebook en Google Now, verleiden mensen ertoe hun activiteiten in de dienst op te slaan, waardoor een enkel profiel al snel een compleet beeld van je geeft. De belofte is dat de intelligente software voor jou gaat bedenken wat jij zou willen doen, maar dat 'cadeautje' staat in schril contrast met hetgeen de diensten over jou beschikbaar hebben - ze zouden je compleet kunnen buitensluiten. (De Europese Unie begrijpt dit, de Verenigde Staten helaas nog niet.)

Gelukkig zijn opsporingsdiensten nog niet zo ver als in series als CSI. Ze kunnen nog niet snel een profiel van je opstellen en direct zien waar je overal geweest bent, maar dankzij forensische technieken en toegang tot bank- en telecomgegevens komen ze een heel eind. Maar zodra meer van jouw eigenschappen gelinkt worden via een gedeelde identiteit, wordt de kans op zulke politiestaatscenario's steeds groter - het zijn niet alleen de criminelen die dan makkelijk in de gaten kunnen worden gehouden.

De gevaren van een enkele identiteit

Dienstverleners op internet streven al jaren naar single sign-on (SSO), maar houden daarbij te weinig rekening met nuances en privacy.

Word jij ook zo moe van het constant wisselen tussen verschillende loginnamen en wachtwoorden voor alle sites, computers en apps die je dagelijks gebruikt? Ik wel. Ik heb vijf verschillende identiteiten en wachtwoorden voor werk en een dozijn voor internetbankieren, online winkelen en de diensten die ik via internet gebruik. Voor mij zijn het er teveel om te kunnen onthouden.

Omdat het probleem voor velen geldt, probeert de industrie het idee '1 ID voor alle diensten' uit te voeren. Een paar jaren geleden probeerde RSA het fundament te leggen voor een single sign-on die door alle leveranciers gebruikt zou kunnen worden, een soort DNS-register voor identiteiten. De poging van RSA mislukte omdat niemand de RSA een vergoeding wilde betalen voor iedere opgeslagen ID. En het idee van een enkele bibliotheek was eng: Het zou een geweldig interessant doelwit voor hackers vormen. (Deze angst bleek later gegrond aangezien RSA niet kon voorkomen dat zijn eigen SecurID ten prooi viel aan hackers.)

'Facebook is niet te vertrouwen'

Vandaag is het panacee het gebruik van OpenID of Facebook om je overal in te kunnen loggen. OpenID bestaat al jaren, maar wordt nog lang niet altijd toegepast. En het vertrouwen op Facebook is zowel lachwekkend als eng te noemen: Facebook schendt stelselmatig de privacy van gebruikers en zou met niets belangrijks vertrouwt mogen worden.

Stel dat er wel een vertrouwde entiteit zou bestaan waarmee je een identiteitsbeheerder en validator zou kunnen gebruiken, een soort BSN waar iedere website mee uit de voeten kan, zouden we die dan allemaal moeten gebruiken?

Zulke systemen zijn ronduit gevaarlijk. Neem gefingeerde en gestolen BSN-gegevens. Een enkele ID lokt hetzelfde misbruik uit - zodra je enige identiteit gestolen of gehackt wordt, ben je het haasje. Je kunt niet langer bewijzen wie je bent. Als je denkt dat herstel van identiteitsdiefstal al lastig is, maak je borst dan maar nat bij diefstal van je enkele identiteit.

Daarnaast is identiteit meer dan een gebruikersnaam, wachtwoord of biometrische scan. Hoewel we allemaal als individu door het even gaan, kennen we meerdere identiteiten. Ik ben iemand anders bij m'n verzekeraar, bij Ziggo, bij Essent enz. Ja natuurlijk ben ik fysiek dezelfde figuur, maar iedere entiteit heeft een andere doelstelling en andere context. Ik pas me daarop aan.



China: vader probeert zoon in game te doden

14 januari 2013

In Xi'an, China heeft de vader van een verslaafde gamer 'huurmoordenaars' ingehuurd die zoonlief moeten helpen bij zijn spelverslaving. De werkloze zoon, Feng (23), zou beter een baan kunnen zoeken, vond pa. Maar Feng zei de tijd te willen nemen om geschikt werk te vinden. Zijn vader huurde vervolgens gamers in die Feng in het internetspel om zeep moesten brengen. Zonder succes: 'spelen boeit me niet, ik zoek niet zomaar een baan', aldus Feng. Gaming is big business in China: zo'n 150 miljoen Chinezen besteedden in 2012 gezamenlijk 770 miljoen euro aan online computerspellen. Zeker nu steeds meer Chinezen thuis een internetcomputer hebben en niet meer naar een internetcafé hoeven. In Nederland zou 2% van de kinderen een gameverslaving hebben.

Man uitgeleverd na kinderporno op SkyDrive

14 januari 2013

Nederland heeft een Amerikaan uitgeleverd wegens seksueel misbruik van minderjarigen. Christopher Robinette (43, woonachtig in Amsterdam) werd eind december op het vliegtuig gezet. De man zou zich tussen januari 2003 en juli 2009 schuldig hebben aan het misbruik, zowel in de VS, Mexico, Costa Rica als in Nederland. Hij liep tegen de lamp toen bleek dat hij kinderpornografische afbeeldingen op zijn Microsoft SkyDrive account plaatste. Microsoft zelf vond de plaatjes met het programma PhotoDNA dat online geplaatste afbeeldingen automatisch scant. Volgens Justitie in de VS werkten de politie Amsterdam, het KLPD en de FBI aan de zaak mee.

VS: tieners drogeren ouders om internet

9 januari 2013

In Rocklin, California zijn twee tienermeisjes opgepakt die een slaapmiddel hadden gestopt in de milkshakes van de ouders van een van hen. De meisjes, 15 en 16, mochten tot 22 uur 's avonds op internet maar vonden dat kennelijk te kort. De ouders dronken slechts een deel van de shake, vonden dat er een raar smaakje aan zat maar vielen toch binnen een uur in slaap. Ze werden pas de volgende ochtend wakker. Een test bevestigde dat ze waren gedrogeerd waarop de ouders hun dochter op het politiebureau afleverden.

Theatervoorstelling politie over online seksueel misbruik

9 januari 2013

Politie Noord heeft samen met theatermaker Dominic van Vree een voorstelling gemaakt om jongeren en ouders te waarschuwen voor online seksueel misbruik. Volgens Monique van der Geest, teamchef recherche bij de nieuwe politie-eenheid Noord Nederland, vindt grooming vaak op geraffineerde wijze plaats onder valse voorwendselen. Ze wil daarom het onderwerp bespreekbaar maken. De voorstelling lets dat niemand weet is geschikt voor ouders van kinderen in groep 7 en 8 en voor leerlingen in het voortgezet onderwijs. 14 februari is de premiere, in Drachten. Als het een succes wordt, volgt mogelijk landelijk uitrol.

Facebook en Twitter helpen agent bij opsporing

7 januari 2013

Voor de een is het nieuws, voor de ander (al lang) niet meer. Dat de politie bij het opsporen gebruikt maakt van sociale media, kwam weer eens in de krant, dit keer naar aanleiding van de opening van het nieuwe Real Time Intelligence Centre (RTIC) in Noord-Nederland. Bij het RTIC worden onder meer foto's van verdachten van facebook, twitter en andere sociale media gekoppeld aan de politiesystemen. Volgens RTIC-chef Albert Veenstra is de hoofdtaak 'zo veel mogelijk relevante informatie te vinden die op dat moment nodig is voor het werk op straat'. Profielfoto's van facebook kunnen bijvoorbeeld snel naar de wijkagent gestuurd worden. Maar volgens universitair docent strafrecht Nico Kwakman (Rijksuniversiteit Groningen) moet de politie hier 'terughoudend' mee omgaan en eerst opsporingsmiddelen gebruiken die minder inbreuk maken op de privacy. Hij geeft toe dat er 'juridisch weinig tegen in te brengen' is. Het gaat immers om gegevens die mensen zelf achterlaten op sociale media. En dus werd de twitteraar die schreef dat de boerderij van Jasper S. in vlammen moest opgaan, na een klein uur opgespoord.



Dit magazine verschijnt maandelijks.

De inhoud bestaat uit verzameld werk uit openbare internetbronnen.

Voor zover mogelijk zal de bron worden vermeld.

Gebruikte bronnen voor dit nummer:

Webwereld
Security.nl
Ixquick
Voelspriet
Zdnet
De Waarschuwingsdienst
Europol

Opmerkingen kunt u mailen naar [de redacteur](#).