twitter special



Juli 2015

JAARGANG 4

Secure Computing

Meer en meer wordt er gebruik gemaakt van Twitter. Nog geen Twitter account? In dit nummer leest u hoe dit te realiseren. Kunt u tijdens uw vakantie 'uw volgers' op de hoogte houden.

———————————-

In bijna elk artikel zijn hyperlinks opgenomen. Klik erop en u ziet meer informatie!

Veel lees(r)plezier

(NB: met Ctrl+ scrolwieltje kunt u de pagina vergroten en verkleinen. U kunt dus zelf uw leesbaar formaat kiezen.)



W.Bosgra Taakaccenthouder Digitale Criminaliteit Basisteam Enschede

Mijn geeltjes ? Kijk op compubuy.jouwpagina.nl



Snel index

Klik op een link voor snelle toegang tot het artikel.

Om terug te keren naar de snelindex klikt u onderaan de pagina op Index

Bronnen:

Security.nl, PCMweb, ZDnet, Webwereld, Comptable, Bits of Freedom, Cops in Cyberspace, De Digitale Revolutie, PCwereld, PCpro, Clikx, Pepermunt.net, PrivacyNieuws, HackInfo, HardwareInfo, Bright, Computerworld

De onderwereld van het internet: 7 waarheden

Slim pitabrood hackt je computer

10 tips om je privacy op social media te waarborgen

In 3 stappen een installatie-cd of usb-stick voor Windows 8.1

Hoe stel je NL-Alert in op je smartphone?

Rechter straft Facebook voor laksheid met illegale content

Foutje in toetsenbord: 600 miljoen Samsung-smartphones onveilig

Hoe werkt Twitter : basishandleiding

Mag je valse gegevens op een site invullen?

Wordt mij e-mail gemonitord?

Schatkist

Snapshots

Cops in Cyberspace

Handig

Wetsartikelen

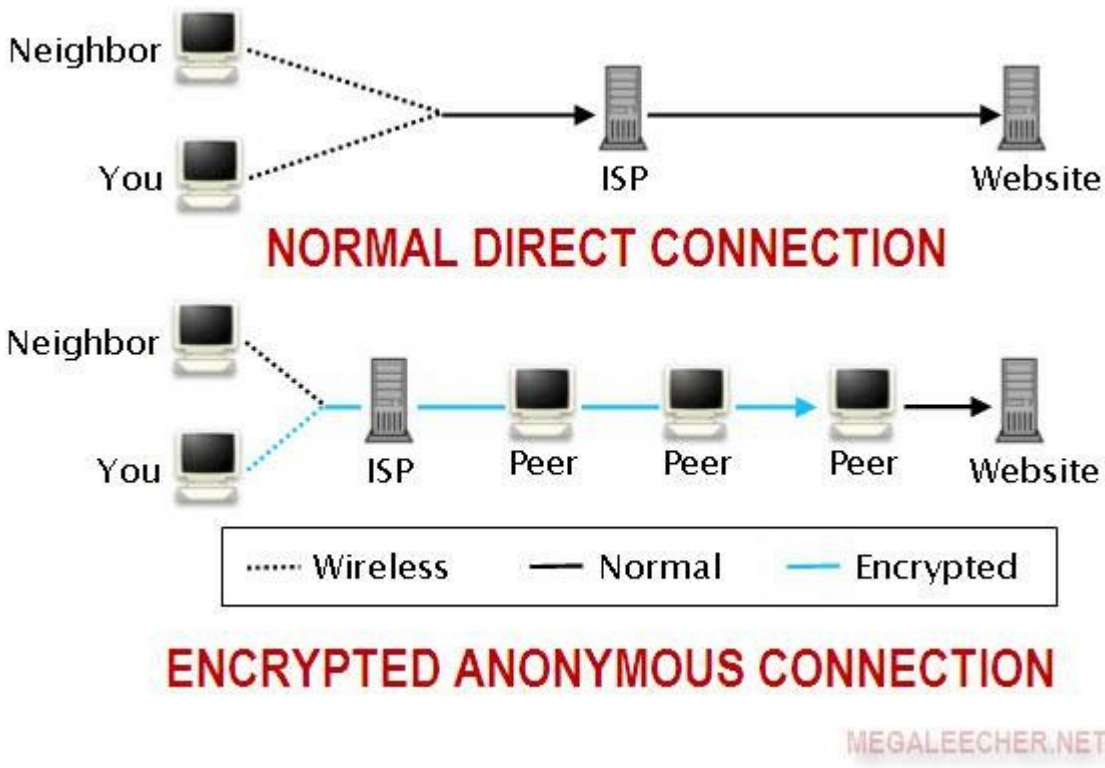
Het Deep Web of Dark Web kent vele donkere krochten waar je als internaut liever niet belandt. Maar ook in de schaduw zie je af en toe de zon.

De onderwereld van het internet: 7 waarheden

Nasa werkt op dit moment naarstig aan een Google-achtige zoekrobot die het Diepe Web moet gaan indexeren. Je vindt namelijk niet alles via je vertrouwde zoekmachine: vele gegevens zijn onbereikbaar omdat Google ze niet interessant genoeg vindt. Onder deze laag bevindt zich nog een diepere en meer duistere laag die we het Dark Web noemen.

Om deze laatste te kunnen bezoeken, heb je een gespecialiseerde browser nodig zoals TOR. The Onion Router werkt via een zogenaamd peer-to-peer (P2P) -netwerk waarbij andermans computer dient als een server die je signaal doorstuurt naar een volgende (anonieme) computer. Op deze manier kan je anoniem op het internet surfen en ben je letterlijk onnavolgbaar.

Het systeem was oorspronkelijk bedoeld om een stem te geven aan politieke dissidenten in landen met strenge regimes. Al snel sloeg de sfeer echter om en werd het een broeihaard voor the bad and the ugly. Toch is het niet allemaal kommer en kwel daarbeneden. Wij geven je zeven wistjedatjes mee.



Index

Bron: NU.nl

1. Het Diepe Web is gigantisch en er is niemand die er een volledig zicht op heeft

Er is niets zo vluchtig als het Diepe Web. Het weet zich steeds razendsnel aan te passen aan de noden van de dag, steeds met het doel om anonimiteit te verzekeren. Wie een crimineel hier bij zijn nekvel wil grijpen, zal ontzettend vroeg moeten opstaan.

2. 'De goeien' komen ook al eens langs

Ook vandaag vinden we tussen al het cybergespuis nog steeds mensen terug die het goed menen en het Diepe Web nodig hebben om hun boodschap uit te dragen. Alle informatie over de wantoestanden, diegenen waar we weet van hebben, in bijvoorbeeld Noord-Korea of China, verkrijgen we via dit verborgen net. Wees dus niet te snel met het veroordelen van deze sneaky surfers: ze kunnen het ook goed voorhebben met de mensen.

3. Zij die zoeken naar drugs, willen gewoon een jointje roken

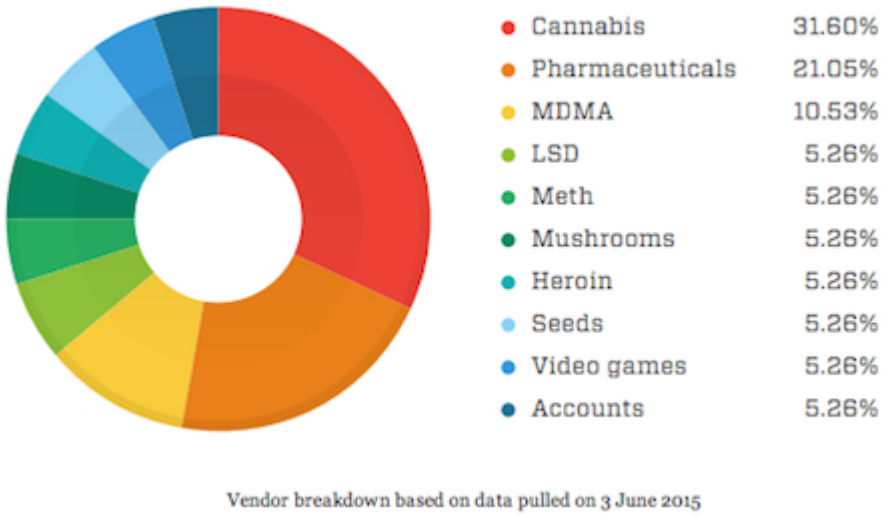
Het is een vaak gehoord verhaal: het Diepe Web is dé plaats om een harddrug te scoren. Toch blijken de meeste queesten gericht te zijn op softdrugs als cannabis. Methamfetamines en Heroïne beslaan samen slechts 10% van de verkochte waar.

4. Wie zoekt, die vindt

Harrods staat erom bekend dat het alles kan leveren, van olifanten tot Beyoncé. Op het Diepe Web vind je echter nog veel meer. Van drugs, over wapens, tot gebruikersaccounts. Zelfs moord vind je hier op bestelling. Je krijgt wel geen garantie dat je waar krijgt voor je geld.

5. Je bent nooit helemaal veilig op het Diepe Web, ook niet als crimineel

Het verborgen net mag dan wel bedoeld zijn om anoniem en ontraceerbaar te kunnen zijn, als je het te bont maakt, keert het zich tegen jou. Vele kinderpornosites en wapenmarkten zijn al gesloten omdat



Vendor breakdown based on data pulled on 3 June 2015

gebruikers, vaak geharde hackers, het welletjes vinden. Alle hoop is dus nog niet verloren.

6. Het Diepe Web kan Malware hosten

Door de verborgen natuur van TOR en andere diensten is het makkelijk voor hackers om je computer te besmetten met Malware. Gebruik je de speciale browsers, dan ben je immers verbonden met ontelbare andere computers die al eens iets kunnen doorgeven. Het gevaarlijke cryptovirus dat recent vele slachtoffers maakte, is er daar bijvoorbeeld eentje van. Dit soort Malware kan overigens zonder enig probleem je exacte locatie bepalen. Woon je in een rijk land, dan zal je automatisch veel meer losgeld moeten betalen.

7. Een criminele site platleggen lost niets op

Toen Silk Road offline werd gehaald, stond Silk Road 2.0 meteen klaar om de gestrande handelaars en klanten op te vangen. Beschouw het als een Lernaean Hydra: voor elk hoofd dat je afsnijdt, verschijnen er twee nieuwe in de plaats.



Index

Bron: NU.nl

De processor van je computer gebruikt verschillende voltages al naargelang de taken die de chip moet uitvoeren. De regulator die de voltages regelt, geeft daardoor ongewild elektromagnetische straling af, die varieert naargelang het voltage en dus de bewerkingen die de processor uitvoert.



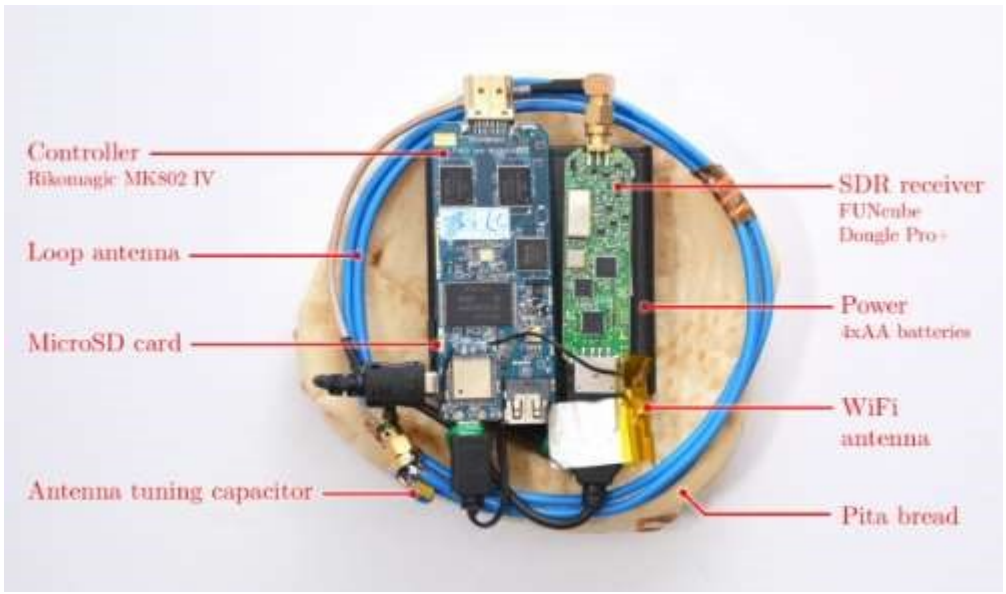
Slim pitabrood hackt je computer

De golven stralen in alle richtingen uit je computer, en ze kunnen eenvoudig opgepikt worden.

Kraakbare sleutel

Dat ontdekten onderzoekers van de universiteit van Tel Aviv. Ze bouwden een klein draagbaar toestel dat de golven ontvangt, waarna een computer ze kan interpreteren. Gevaarlijk, want zo is het mogelijk om een encryptiesleutel van een pc te ontfutselen. De researchers demonstreerde hun techniek door de sleutels van GnuPG buit te maken. GnuPG is een veelgebruikte gratis implementatie van de OpenPGP-standaard voor de beveiliging van data en communicatie.

Het Portable Instrument for Trace Aqcuisition (PITA) past niet toevallig in een pitabroodje. In de lokale kebabzaak is het met andere woorden in theorie een koud kunstje om de beveiligingssleutel van iemands laptop buit te maken.



In de winkel te koop

Het toestel in kwestie vereist een antenne, een radio-ontvanger van het kaliber dat je zo in de winkel kan kopen, een controller en een optionele wifi-verbinding of sd-kaart. Het pitabrood is niet essentieel en kan indien de omstandigheden daarom vragen vervangen worden door een smos van Subway.

Het kleine toestel heeft alles in huis om de elektromagnetische golven op te vangen, waarna de data ofwel wordt opgeslagen op de sd-kaart voor latere analyse, ofwel via wifi onmiddellijk naar de laptop van de aanvaller wordt gestuurd. In beide gevallen gebeurt de analyse van de data en het kraken van de eigenlijke sleutels op een andere computer.

Hongerige hackers

De Israëlische onderzoekers waarschuwden GNuPG al voor de kwetsbaarheid, en die zou intussen verholpen zijn. Het pitabrood toont desalniettemin aan dat je laptop heel wat data prijs geeft door gewoon te werken, zelfs wanneer Bluetooth en Wifi zijn uitgeschakeld. Staat er gevoelige en versleutelde data op je pc, pas dan in het vervolg op voor duistere figuren met verdachte voedingswaren en laptops.

Index

Bron: Clickx

Mensen maken zich zorgen over hun online privacy. En terecht. Vooral op social media is het oppassen geblazen, omdat juist daar je gedrag, beslissingen en interesses van waarde zijn voor adverteerders. En ook P&O-afdelingen checken steeds vaker je Facebookprofiel.

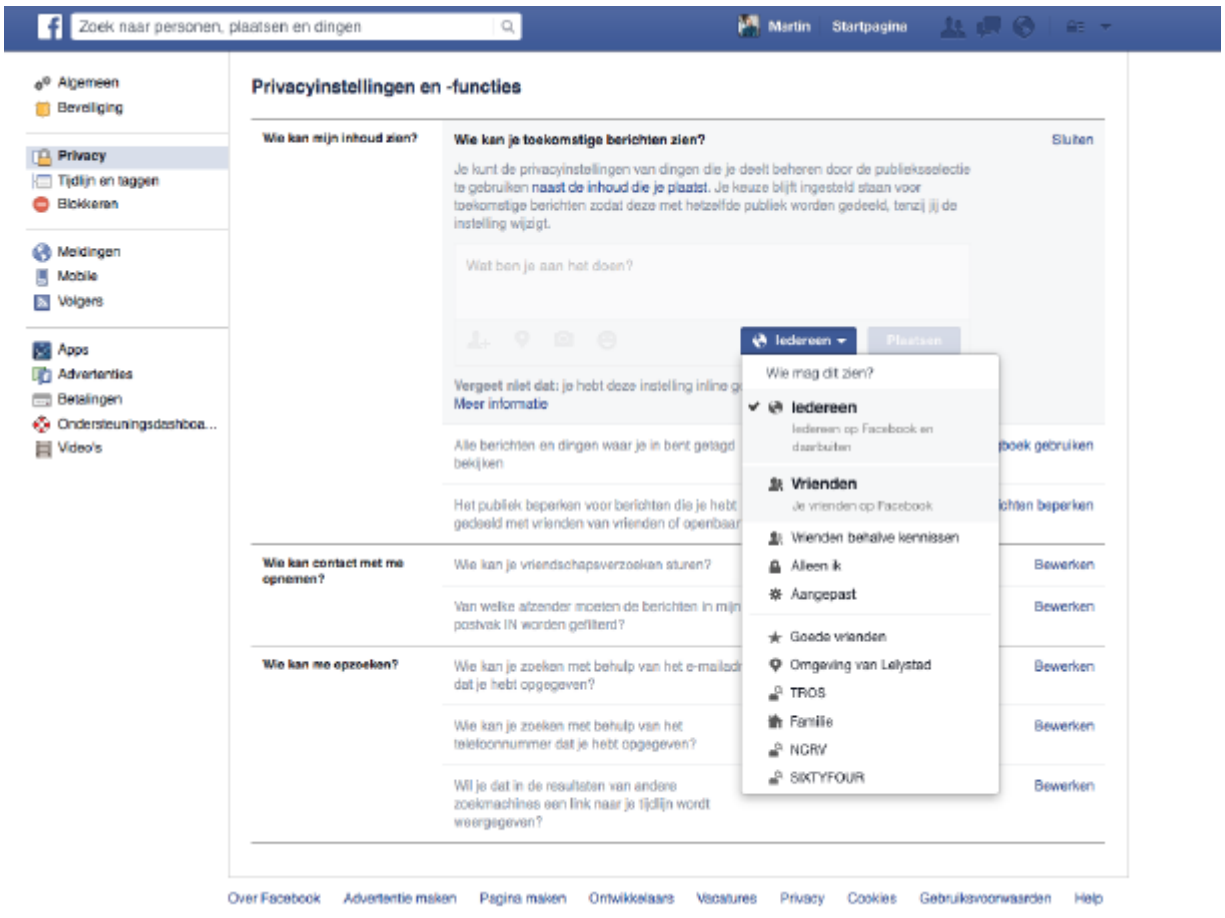
10 tips om je privacy op social media te waarborgen

Facebook

Tip 01: Inhoud bekijken

We beginnen direct met de instelling die het belangrijkst is: wie kan en mag zien wat jij op Facebook plaatst? Het effect hiervan heb je ongetwijfeld zelf wel eens gemerkt wanneer je op het profiel van een ander klikte, maar een vrijwel lege pagina kreeg voorgeschoteld. Zo iemand heeft aangegeven dat personen die geen Facebook-vrienden met hem of haar zijn, niets mogen zien van wat er op de pagina wordt geplaatst. Dit kun je zelf ook heel eenvoudig instellen.

Klik rechtsboven op het pijltje naar beneden (naast het pictogram met het slotje) en vervolgens op Instellingen / Privacy. Het pictogram met het slotje bevat overigens snelkoppelingen naar privacy-instellingen, maar omdat we graag alles op één plek aanpassen navigeren we via Instellingen. Naast Wie kan je toekomstige berichten zien? klik je op Bewerken. Je hebt hier flink wat opties. Je kunt ervoor kiezen om alles aan iedereen te laten zien, alleen aan vrienden of aan een specifieke doelgroep. Let op: dit is alleen van toepassing op toekomstige berichten. Wil je ook berichten uit het verleden afschermen, klik dan op Eerdere berichten beperken.



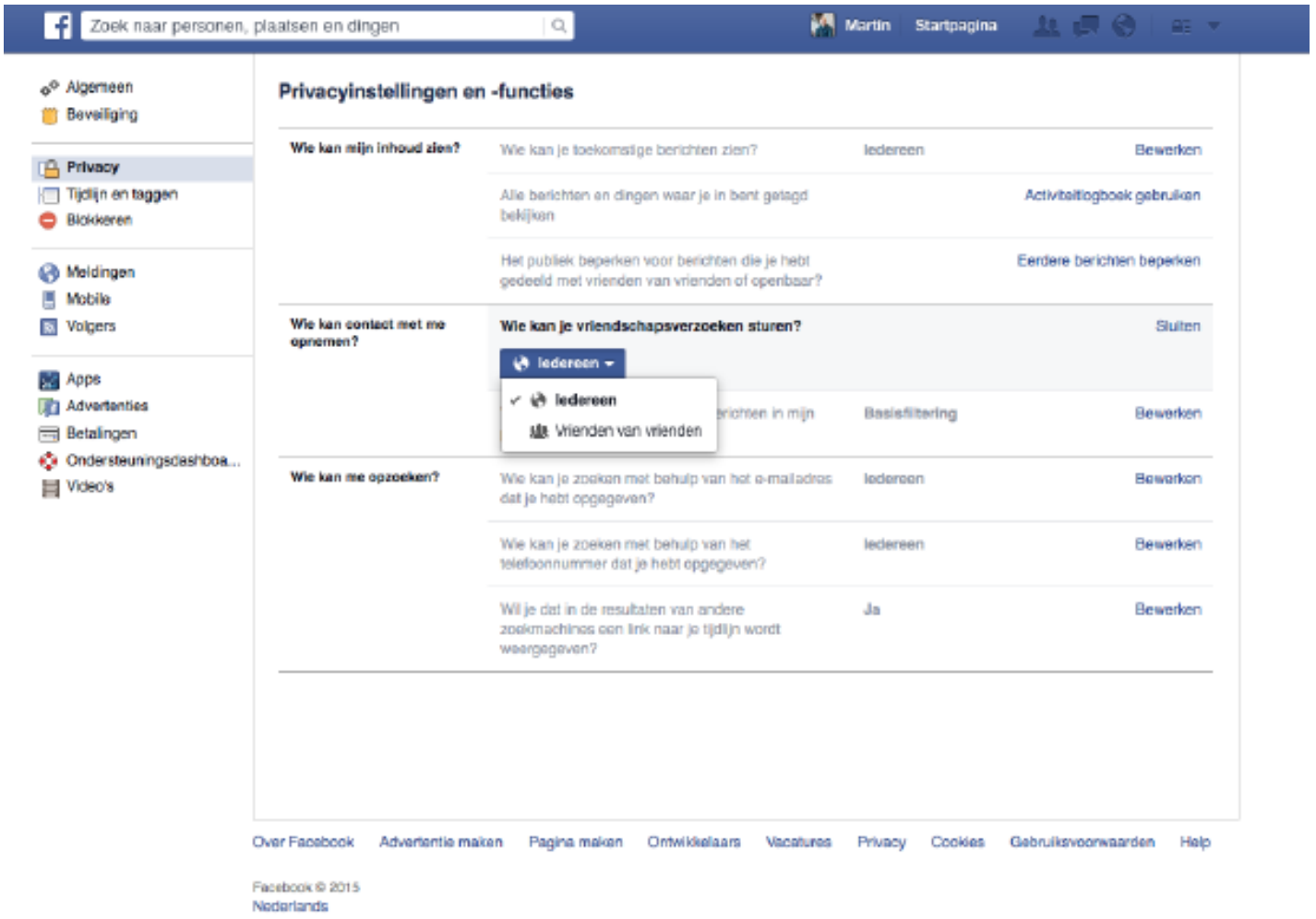
Tip 02: Contact opnemen

Wanneer je populariteit op social media (en wellicht ook in de echte wereld) toeneemt, is het mogelijk dat het aantal vriendschapsverzoeken ineens de spuigaten uitloopt. Dat kan ook het geval zijn wanneer je plotseling in het vizier van spammers terecht bent gekomen. Vervelend, want die vriendschapsverzoeken komen voortdurend in beeld en kunnen ervoor zorgen dat je door de bomen het bos niet meer ziet. Voor je het weet, weiger je mensen die je nu juist wél had willen accepteren.

Index

Bron: ComputerTotaal

Onder het kopje Wie kan contact met me opnemen? heb je twee opties: Iedereen en Vrienden van vrienden. Dat laatste is een veilige optie, omdat je dan alleen kunt worden toegevoegd door mensen die vrienden zijn van je huidige Facebook-vrienden en dan treedt er direct een soort sociale controle in werking. Daarnaast kun je ook voorkomen dat je berichtenbox in Facebook volloopt met spamberichten, door onder het kopje Wie kan contact met me opnemen? te klikken op Bewerken naast Basisfiltering en te kiezen voor Strikte filtering. Berichten die niet van je vrienden afkomstig zijn, komen dan in het postvak Overig terecht.



Tip 03: Wie kan je opzoeken?

Je weet nu hoe je kunt voorkomen dat iemand de inhoud van je Facebook-pagina ziet, maar wat als je überhaupt niet wilt dat iemand je op Facebook kan vinden? Bijvoorbeeld omdat je een schooljuf of -meester bent die niet wil worden toegevoegd door leerlingen of omdat je een andere openbare functie hebt die het onhandig maakt om op Facebook te worden gevonden. Of gewoon omdat je daar geen zin in hebt, want waarom zou je een reden nodig hebben?

Onder Instellingen / Privacy kun je onder het kopje Wie kan me opzoeken? aangeven dat iedereen je kan vinden aan de hand van je e-mailadres of telefoonnummer, of alleen je vrienden of vrienden van vrienden. Opmerkelijk genoeg is de optie Niemand hier niet aanwezig. Onderin kun je tot slot nog aangeven of je tijdlijn mag worden weergegeven in de resultaten van bijvoorbeeld Google.

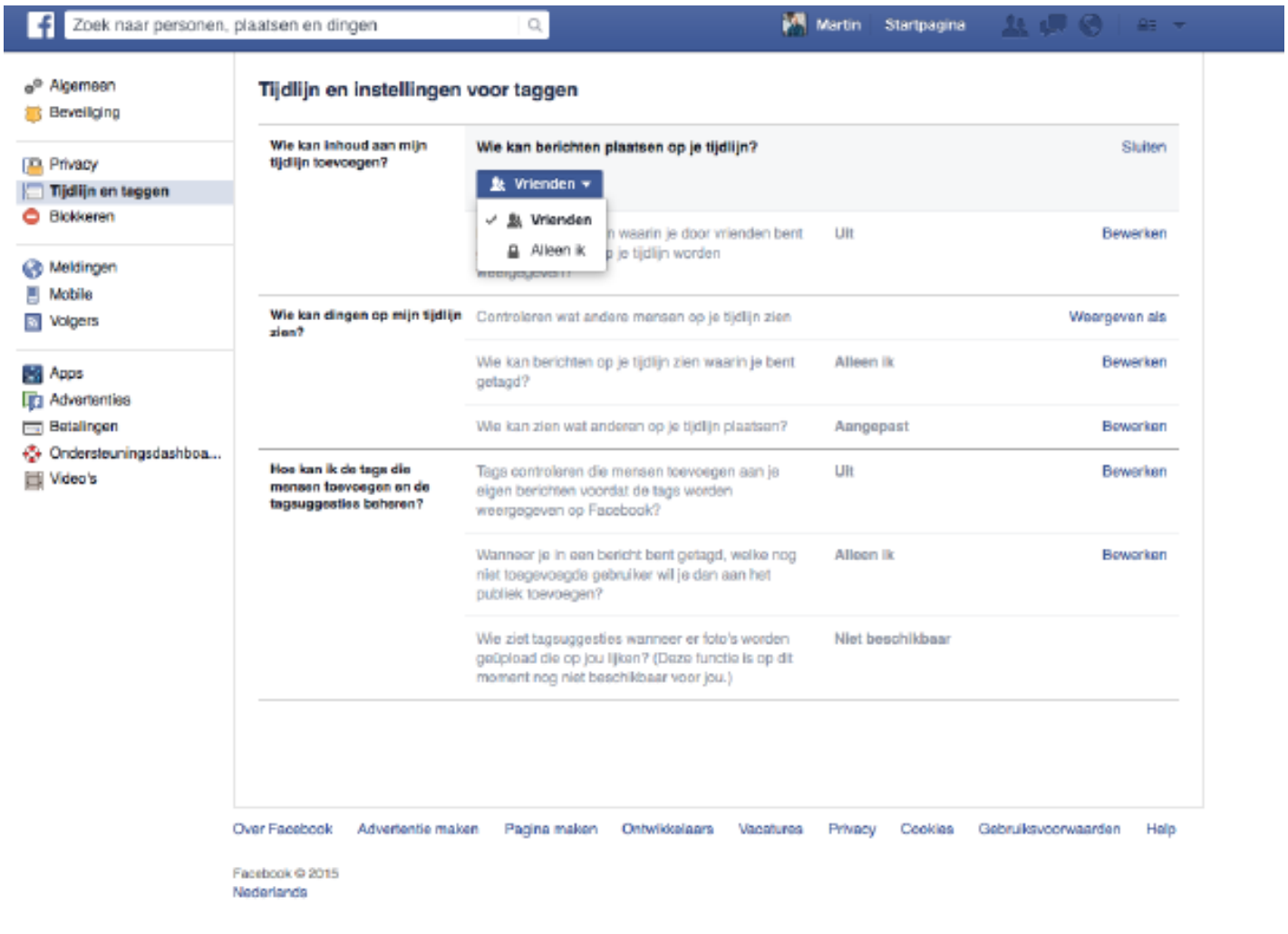
Tip 04: Tijdlijn en taggen

Je hebt nu onder andere afgekaderd wat de zichtbaarheid is van dingen die je zelf op Facebook plaatst, maar hoe zit het met anderen? Een leuke, maar ook opdringerige functie van Facebook is namelijk de mogelijkheid om een bericht op de tijdlijn van een ander te plaatsen. Dit kan erg vervelend zijn wanneer je je ziek hebt gemeld en een vriend je doodleuk tagt in een foto waarop jullie samen op een terrasje zitten, om maar een voorbeeld te noemen. Gelukkig kun je dit reguleren door in Instellingen te klikken opTijdlijn en taggen. Door bij Wie kan berichten plaatsen op je Tijdlijn? te kiezen voor Alleen ikhoef je je over taggende vrienden geen zorgen meer te maken.

Index

Bron: ComputerTotaal

Vind je dat iets te ver gaan, dan kun je direct daaronder de mogelijkheid inschakelen om berichten eerst goed te keuren voordat ze op je tijdlijn worden geplaatst. Vervolgens kun je in dit menu ook nog bepalen wie de berichten die door anderen op je tijdlijn worden geplaatst, of waarin je wordt getagd, kunnen zien. Zo hou je de volledige controle en zorg je ervoor dat anderen je niet onbedoeld in de problemen brengen (en maak je het mogelijk om iemand te verrassen zonder dat een ander de pret voortijdig bederft).



Tip 05: Apps

Je hebt ongetwijfeld wel eens ingelogd op een website met behulp van een Facebook-account, waarbij je die website toestemming hebt gegeven om bepaalde gegevens van Facebook te gebruiken. Dat kan niet altijd kwaad, maar op den duur zijn er wel heel veel websites die de vrije beschikking hebben over je gegevens, en dat is niet de bedoeling. Het kan daarom absoluut geen kwaad om eens in de zoveel tijd te klikken op Instellingen / Appsom te zien welke apps op dit moment toegang tot je persoonlijke gegevens hebben.



Als hier apps tussen staan die je al een tijd (of misschien wel nooit) hebt gebruikt, dan is het aan te raden om deze te verwijderen. Immers, hoe minder mensen toegang hebben tot je gegevens, hoe beter, en als je de website of app ooit nog eens gebruikt, log je gewoon opnieuw in met Facebook. Beweeg je muis over de app die je wilt verwijderen en druk op het kruisje. Facebook vraagt vervolgens of je het zeker weet, waarna je klikt op Verwijderen. De melding die je krijgt - dat het bedrijf in kwestie je gegevens wellicht niet verwijdert - is een goede reminder aan het feit dat je moet oppassen wie je toegang verleent.

Index

Bron: ComputerTotaal

Tip 06: Advertenties

En dan de optie waar eind vorig jaar zoveel paniek om was: advertenties. Door te klikken op Instellingen / Advertenties kun je precies aangeven op wat voor manier je al dan niet wilt deelnemen aan het advertentienetwerk van Facebook. De optie waar zoveel angst voor was eind vorig jaar, was de mogelijkheid voor Facebook om je foto's in advertenties te gebruiken. Druk op Bewerken naast de optie Externe sites en kies voor Niemand, en je persoonlijke gegevens worden aan niemand getoond in de vorm van een advertentie.

Wat Facebook al jaren doet, is advertenties aan je tonen van bijvoorbeeld pagina's, waarbij wordt aangegeven wie van je vrienden die pagina al 'liken'. Als jij niet in dit soort advertenties wilt worden opgenomen, dan kun je dat ook uitschakelen. Klik bij Advertenties en vrienden op Bewerken en kies voor Niemand in plaats van Alleen mijn vrienden. Je wordt nu niet meer 'gebruikt' voor dit soort advertenties. Overigens raden we je aan om deze instellingen eens in de zoveel tijd door te lopen, omdat Facebook regelmatig veranderingen doorvoert.



Index

Bron: ComputerTotaal

Twitter

Tip 07: Fototags

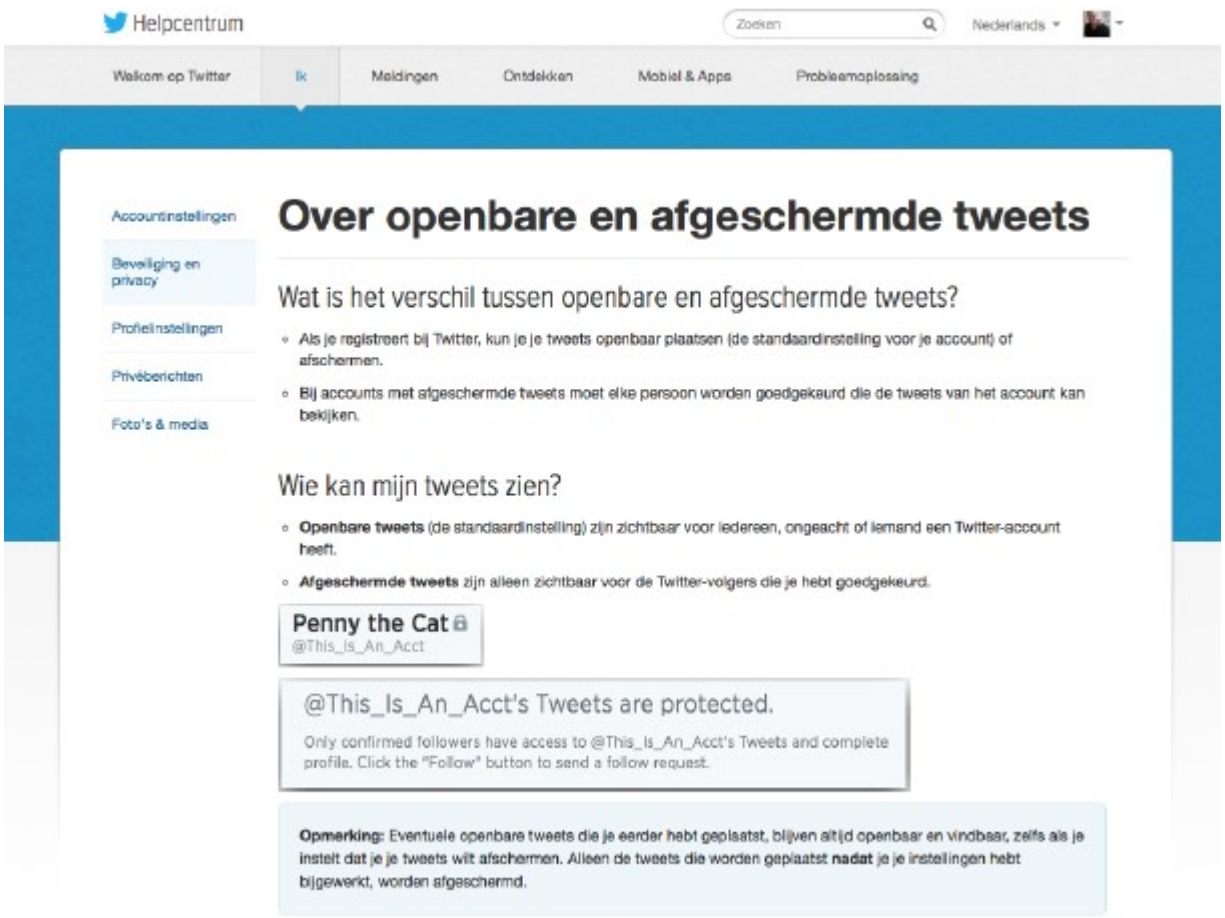
Op Twitter is doorgaans veel minder persoonlijke informatie te vinden dan op Facebook, maar dat wil niet zeggen dat je zomaar alles open moet laten staan. Immers, ook Twitter kan je in de problemen brengen als je te veel deelt met mensen die dat niets aangaat.
Log in op Twitter, klik rechtsboven op je profielfoto en vervolgens op Instellingen /Beveiliging en privacy. Het kopje Beveiliging slaan we over, omdat dit heeft te maken met het beschermen van je account tegen hackers, en niet zozeer met privacy. Onder het kopjePrivacy zie je de optie Fototaggen.

Deze optie is vergelijkbaar met het taggen in Facebook en ook hier kun je bepalen of mensen je mogen taggen in een foto of niet. Hier heb je echter niet de keuze om een tag eerst goed te keuren, je kunt alleen kiezen voor Iedereen mag mij taggen in foto's, Alleen personen die ik volg mogen mij taggen in foto's en Niemand mag mij taggen in foto's. Als je het écht veilig wilt maken, kies je uiteraard voor de laatste optie.



Tip 08: Afschermen

De volgende optie, Mijn tweets afschermen, is er eentje waarover je goed moet nadenken. Net als bij Facebook kun je er namelijk voor zorgen dat mensen die jij niet volgt op Twitter, de inhoud van je profiel en je tweets niet kunnen zien. Dat klinkt heel veilig en dat is het ook, je moet je alleen wel realiseren dat de aard van Twitter anders is dan die van Facebook. Waar Facebook vooral draait om vriendschappen, volgen mensen op Twitter je vooral op basis van gedeelde interesses. Het afschermen van je account is prima en veilig, maar als het je doel is om op korte termijn een flink aantal volgers aan je te binden, dan is het afschermen van je account wellicht niet de juiste keuze (immers, een vreemde die je tweets niet kan zien, zal je ook niet gaan volgen). Een optie om even goed over na te denken dus.



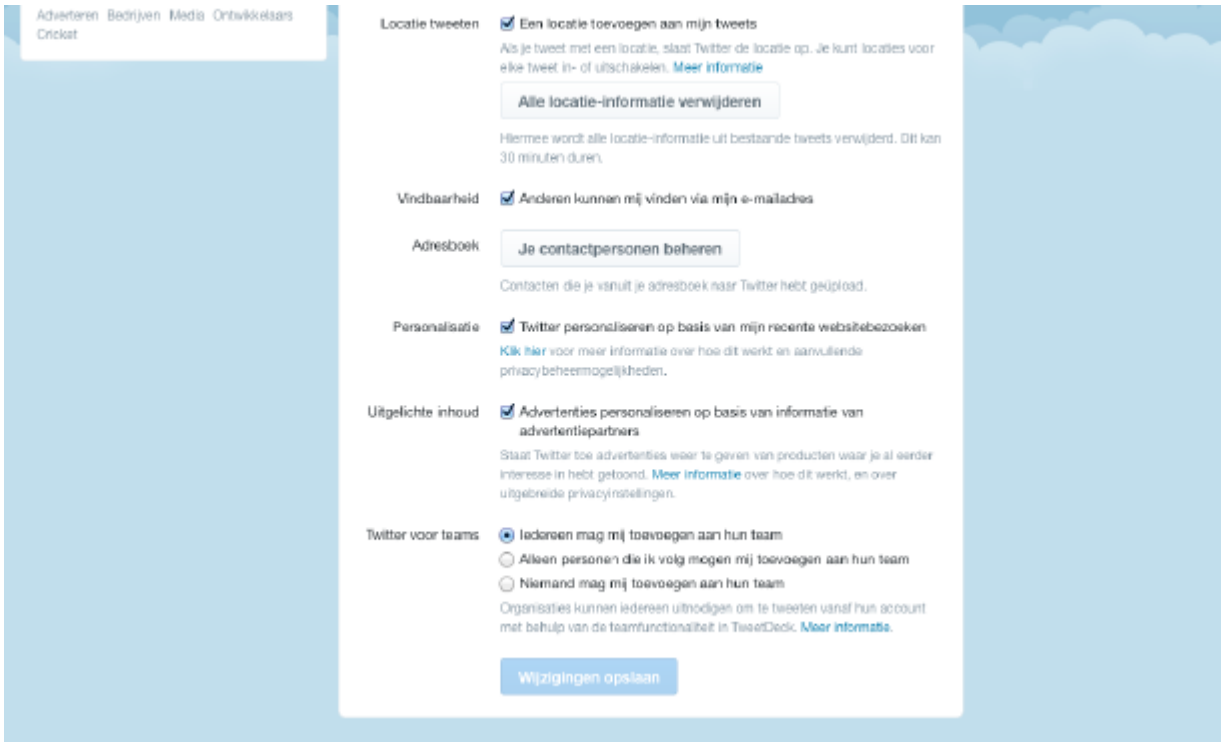
Index

Bron: ComputerTotaal

Tip 09: Locatie

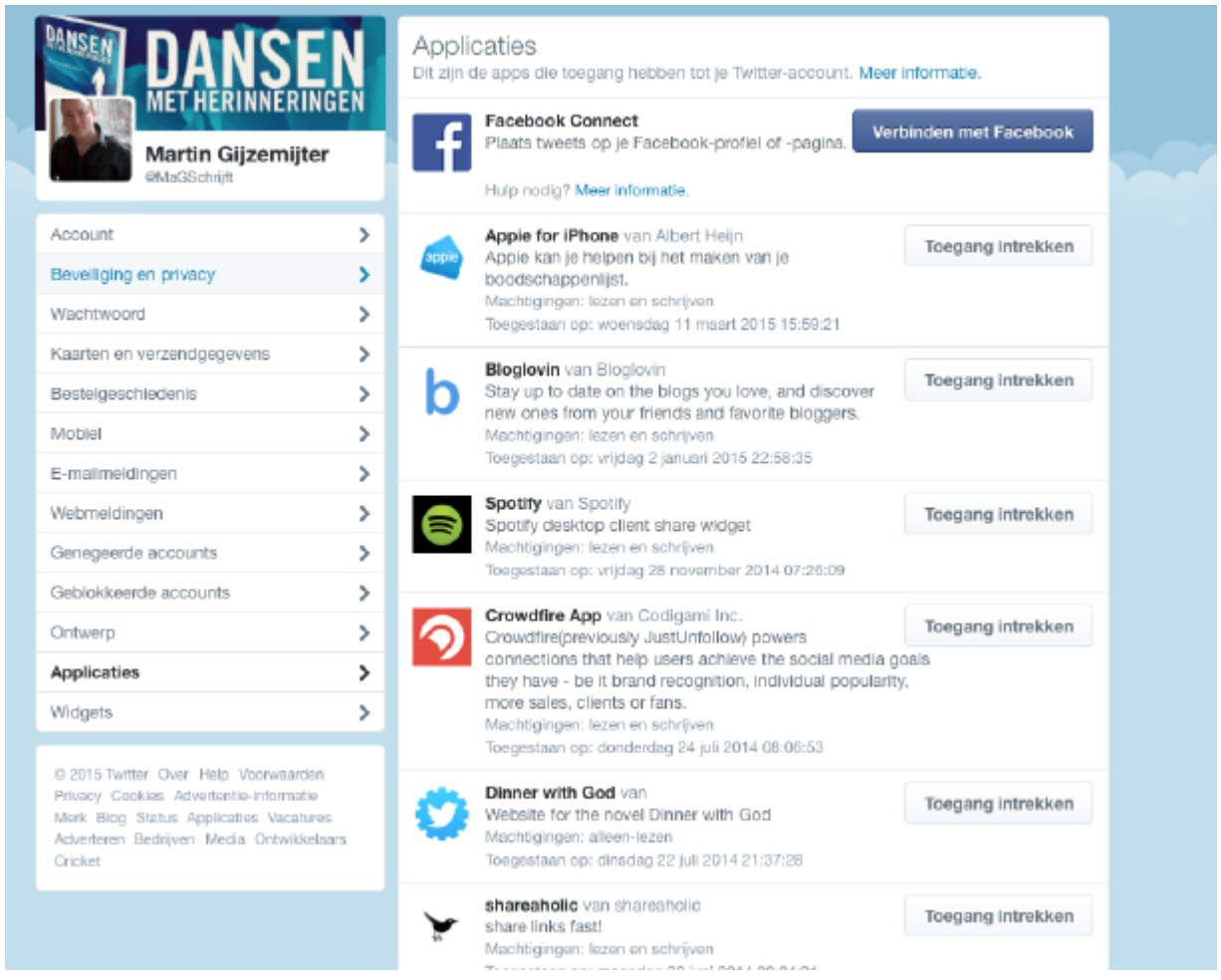
Twitter maakt het mogelijk om standaard een locatie toe te voegen aan je tweets, bijvoorbeeld wanneer je tweet vanaf je mobiele telefoon. Hartstikke leuk en handig, maar ook heel gevaarlijk. Denk er alleen maar even aan dat je een foto tweet van je zoon of dochter in de speeltuin en er staat vervolgens doodleuk bij waar deze speeltuin zich bevindt. Er zijn vele gevallen bekend van kwaadwillenden die deze informatie daadwerkelijk hebben misbruikt om slachtoffers te maken. Dat wil je uiteraard vermijden. Verwijder het vinkje bij Een locatie toevoegen aan mijn tweets, om deze informatie voortaan achterwege te laten. Een klik op de knop Alle locatie-informatie verwijderen past dit ook toe op al je tweets uit het verleden.

Daarnaast kun je net als bij Facebook uitschakelen dat mensen je kunnen vinden door op je e-mailadres te zoeken. Een andere overeenkomst met Facebook is dat Twitter je advertenties voorschotelt op basis van je surf- en tweetgedrag. Dit kun je eveneens eenvoudig uitschakelen door de vinkjes te verwijderen bij de opties Personalisatie en Uitgelichte inhoud.



Tip 10: Apps

Tot slot is er nog een vergelijking te maken tussen Facebook en Twitter, want ook Twitter biedt de mogelijkheid tot het koppelen van apps (oftewel de mogelijkheid om met je Twitter-account in te loggen op websites van derden). Hoewel hierbij wederom geldt dat er op Twitter doorgaans minder gevoelige informatie (in je profiel) staat dan bij Facebook (meer dan een url, een profielnaam en een e-mailadres hoef je niet in te vullen), wil dat wederom niet zeggen dat zomaar iedereen toegang moet hebben tot die informatie. Klik op het tabblad Applicaties in Instellingen om te bekijken welke apps toegang hebben tot je Twitter-informatie. Klik vervolgens op de knop Toegang intrekken achter de apps die je niet langer aan je account wilt hebben gekoppeld. Wees niet bang om verkeerd te klikken, je kunt een website/app net zo makkelijk opnieuw toegang geven.



Index

Bron: NU.nl

Computers worden niet meer geleverd met originele installatiemedia. Gelukkig kun je deze eenvoudig maken en dat is handig om achter de hand te hebben als het ooit misgaat. Lees hoe je installatiemedia voor Windows 8.1 legaal downloadt en herstelmedia aanmaakt.

In 3 stappen een installatie-cd of usb-stick voor Windows 8.1

Stap 1: Herstelmedia

Om dit artikel te volgen heb je een computer nodig met Windows 8.1 en een lege usb-stick van 4 GB. Het is mogelijk om de installatiemedia op een dvd te branden, maar een usb-stickaanmaken is eenvoudiger. Plaats een lege usb-stick van minimaal 4 GB. Sommige sticks van 4 GB worden geweigerd omdat er te weinig ruimte beschikbaar zou zijn. Gebruik in dat geval een 8 GB usb-stick.

Stap 2: Downloaden

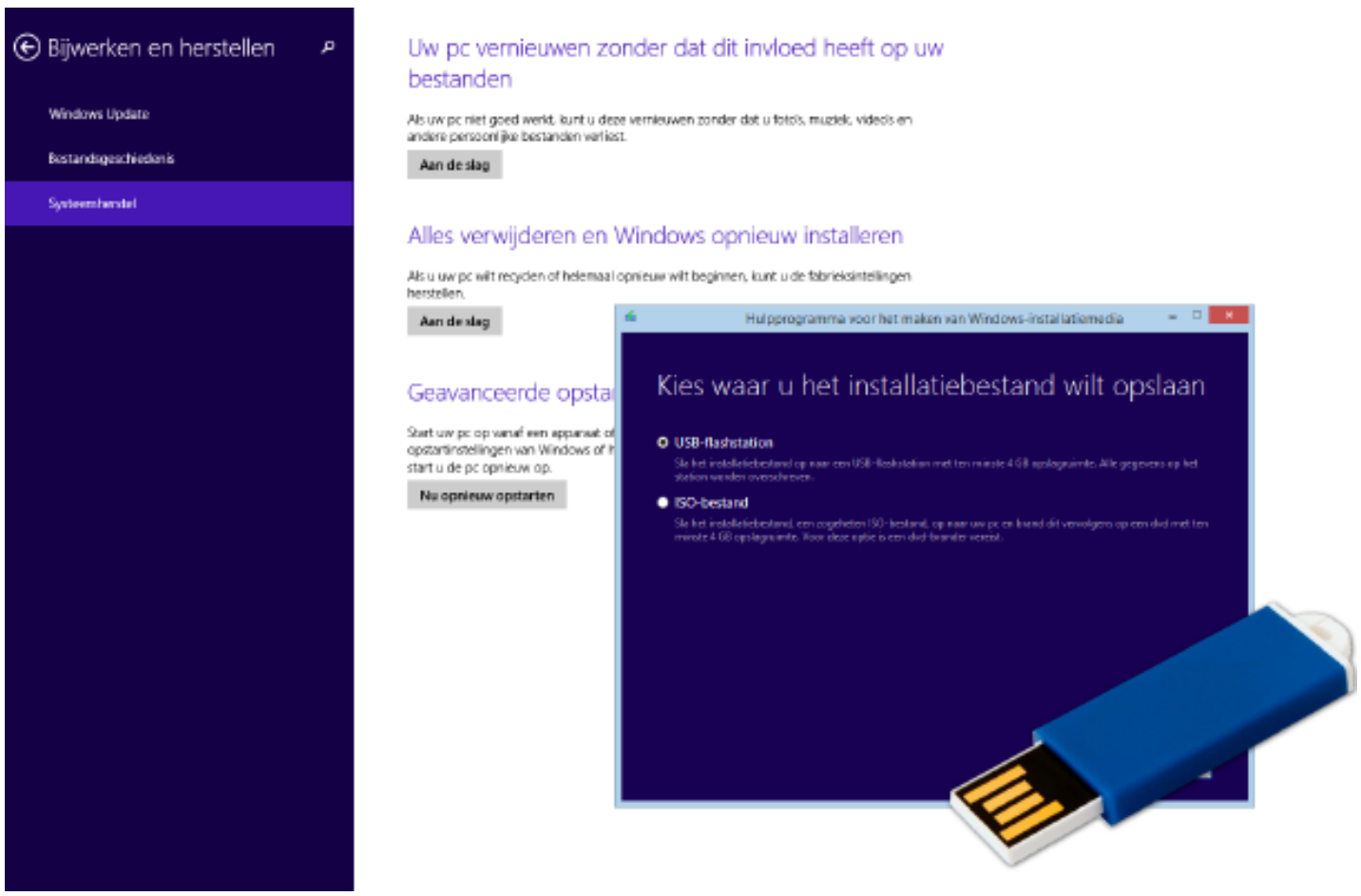
Ga naar de website van Microsoft en klik op Medium maken. Er wordt een bestand binnengehaald dat je moet opstarten. Kies de gewenste taal (Nederlands), editie (Windows 8.1) en architectuur (32-bit of 64-bit). Als je dit laatste niet weet, gebruik dan de toetscombinatie Windows-toets+Pause. Achter Type systeem vind je de aanduiding 32-bits besturingssysteem of 64-bits besturingssysteem.

Geef aan dat je een usb-flashstation wilt aanmaken en wijs de schijfletter van de usb-stick aan. Het programma haalt de installatiebestanden binnen en zet deze op je stick. Dit proces kan veel tijd in beslag nemen. Schrijf na afloop op de stick Windows 8.1 herstelmedia en bewaar deze bij je computerspullen.

Stap 3: Windows herstellen

Om Windows ooit te herstellen kun je de usb-stick gebruiken. Als Windows nog correct opstart, is er een eenvoudigere manier. Open Charms-balk en ga naar Instellingen / Pc-instellingen wijzigen / Bijwerken en herstellen / Systeemherstel.

De eerste optie is het veiligst en heet Uw pc vernieuwen zonder dat dit invloed heeft op uw bestanden. Het besturingssysteem wordt hiermee vernieuwd, maar je bestanden en instellingen blijven ongewijzigd. Met Alles verwijderen en Windows opnieuw installeren wordt Windows opnieuw geïnstalleerd. Hierbij wordt mogelijk om de usb-herstelmedia gevraagd. Als je kiest voor Geavanceerde opstartopties zal je computer opnieuw opstarten en krijg je vergelijkbare hersteloptie voorgeschoteld. Ook kun je hiermee eventuele systeemherstelpunten terug laten zetten.



Index

Bron: ComputerTotaal

NL-Alert is een waarschuwingssysteem van de Nederlandse overheid. Het wordt ingezet tijdens rampen, zoals overstromingen, brand, of erg heftig noodweer. Het systeem is bedoeld om burgers in een bepaald gebied te waarschuwen om zich kunnen voorbereiden door bijvoorbeeld ramen en deuren te sluiten.

Hoe stel je NL-Alert in op je smartphone?

NL-Alert werd in 2012 geïntroduceerd, en is sindsdien al meer dan 30 keer ingezet.

Het systeem stuurt een tekstbericht als er iets aan de hand is, met daarin informatie over de ramp én wat je eraan kunt doen. Het gaat daarbij niet om een sms-bericht, maar om een tekstbericht dat via cell broadcast wordt verstuurd. Cell broadcast is dezelfde technologie als sms, maar werkt op een andere frequentie en kan naar een grote groep mensen in één keer worden gestuurd. Op die manier wordt het netwerk niet overbelast wanneer er in één keer veel berichten worden verstuurd.

Niet via 4G

Een groot nadeel van NL-Alert-berichten is dat ze niet worden gestuurd als je op een 4G/LTE-netwerk zit. Als je telefoon automatisch gebruik maakt van het beste netwerk, en als je abonnement 4G heeft, dan krijg je het bericht niet binnen.

De providers hebben de plicht om hun netwerken geschikt te maken om NL-Alerts te ontvangen. Dat moet vóór 1 december 2015 rond zijn. KPN is daar inmiddels mee klaar, dat is inmiddels begonnen met de uitrol van NL Alerts op 4G. Andere providers moeten daar nog mee komen, maar er bestaat dus een grote kans dat jij vanmiddag het bericht niet binnen krijgt.

Instellen op Android:

Op de meeste moderne apparaten is NL-Alert standaard al ingesteld. Dat heeft te maken met je besturingssysteem. Op Android 5 (Lollipop), maar ook op het oudere Android 4.4 en 4.3 staan de controleberichten meestal standaard aan.

Je kunt dat controleren door naar je 'Instellingen' te gaan, en bij 'Draadloos en netwerken' op 'Meer' te klikken. Daar kun je onderaan naar het menu 'Nooduitzendingen'. Je ziet hier een aantal opties, waaronder ook Amber Alerts.

Er staan hier twee opties die erg veel op elkaar lijken: 'Extreme dreigingen weergeven' en 'Ernstige dreigingen weergeven'. Zet die allebei aan, en je kunt NL-Alerts ontvangen.

Instellen op iOS

NL-Alert werkt op de iPhone alleen met iOS 7 of iOS 8. Bovendien kun je de alerts alleen ontvangen op de iPhone 4s of hoger.

Je doet dat door naar 'Instellingen' te gaan, dan naar 'Berichtgeving' te gaan, en daar naar onderen te scrollen. Je ziet daar'Noodmeldingen' staan. Zet dat aan, en je iPhone is ingesteld om NL-Alerts te ontvangen!



Index

Bron: NU.nl

Facebook heeft van de rechtbank Amsterdam het deksel op de neus gekregen vanwege zijn gezwalk in de wraakpornozaak. Nu zit het klem.

Rechter straft Facebook voor laksheid met illegale content

Voorop gesteld, deze zaak is redelijk uniek. Geen paniek dus bij hosters dat ze alles wat gebruikers doen moeten bewaren. Wie hier wordt aangepakt is alleen Facebook zelf, en dan vooral de loze beloften om evident onrechtmatige content te bestrijden.

Want ondanks dit 'speerpunt' heeft het sociale netwerk zitten slapen, en zo meegeholpen aan het anoniem houden van de uploader van de wraakporno. De les is duidelijk: als je content offline haalt omdat het evident onrechtmatig is, doe je er verstandig aan om de account- en loggegevens van de uploader juist te bewaren. Dat is een rechtsplicht van Facebook en daarin heeft ze ten ene male gefaald, oordeelt de rechter.

Aan het lijntje gehouden

Facebook kan zich niet verschuilen achter het feit dat het geen formeel bevriezingsverzoek heeft gekregen, ten minste niet ten tijde dat de uploader zijn account verwijderde, eind januari. Op dat moment was er al minstens 5 keer geklaagd over het filmpje, onder meer door slachtoffer (en eiseres in deze zaak) Chantal. Facebook had het seksfilmpje ook al offline gehaald. Het concern wist dus dat het onrechtmatig was, maar ging desondanks over tot het wissen van het account van de uploader.

Vervolgens werd Chantal aan het lijntje gehouden, en meldde het sociaal netwerk pas vlak voor het kort geding plotseling dat alle accountdata was gewist. "Facebook heeft, door op de valreep te volstaan met de mededeling dat zij niet meer over de gevraagde gegevens beschikt bij het naleven van haar - in dit geval in beginsel aanwezige - rechtsplicht jegens eiseres tot het verstrekken van NAW-gegevens met betrekking tot degene die onrechtmatig jegens eiseres heeft gehandeld, onvoldoende zorgvuldigheid in acht heeft genomen. Daarmee heeft Facebook op haar beurt naar het oordeel van de voorzieningenrechter onrechtmatig gehandeld jegens eiseres", aldus de rechter.

Facebook zelf aansprakelijk?

Een terecht vonnis, vindt Fulco Blokhuis, advocaat bij Boekx. Hij ziet bovendien kansen voor Chantal om door te pakken, door Facebook zelf aansprakelijk te stellen voor de door haar geleden en te lijden schade. Facebook ontneemt Chantal de mogelijkheid om de uploader aan te spreken. Er is geklaagd over het filmpje. Maar Facebook verwijdert toch alle gegevens. De rechter oordeelt dat Facebook haar rechtsplicht verzaakt om er voor te zorgen dat slachtoffers gebruikers van Facebook aansprakelijk kunnen stellen. Daardoor wordt het nu zelf aansprakelijk, stelt Blokhuis. "Dat is tot nog toe niet aan de orde gekomen in deze zaak, maar daar liggen zeker kansen. Zeker gezien het recente Delfi-arrest."

Ondertussen heeft Facebook een catch 22 over zichzelf afgeroepen. Zijn er inderdaad helemaal geen NAW-gegevens van de uploader meer te vinden, dan blijft de conclusie dat het heeft verzaakt in zijn rechtsplicht en is het wellicht zelf aansprakelijk. Mocht er toch nog wel een back-up of andere identificerende logfiles zijn, dan kan waakhond CBP in actie komen, want daardoor overtreedt het concern mogelijk de privacywet.





Index

Bron: NU.nl

Door een slordigheidje in de software staan meer dan 600 miljoen Samsung Galaxy smartphones bloot aan hackeraanvallen.

Foutje in toetsenbord:

600 miljoen Samsung-smartphones onveilig

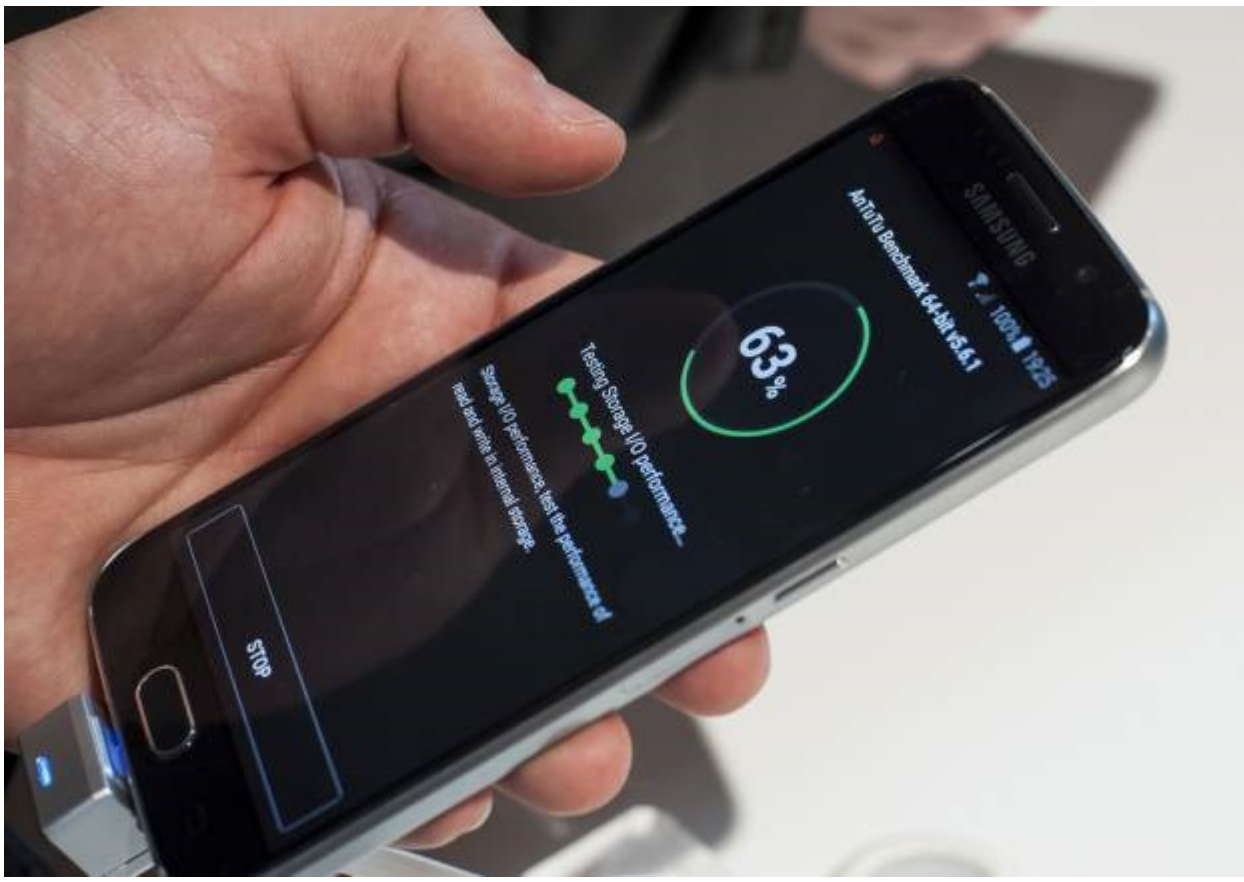
Door een zwakheid in het geïnstalleerde toetsenbord op verschillende versies van de Samsung Galaxy smartphone kunnen hackers potentieel binnendringen in het toestel. Specifiek gaat het over de taalpakketten van het toetsenbord die geregeld nagaan of er een update beschikbaar is. Dit gebeurt via een onversleutelde verbinding, een ernstig veiligheidsoverzicht.

Zo'n 600 miljoen smartphones zouden getroffen zijn. Heeft u een Samsung Galaxy gekocht in de afgelopen twee jaar? Dan is de kans groot dat uw gsm deze kwetsbaarheid bezit.

Met een nep proxy server kan een persoon met slechte bedoelingen relatief gemakkelijk controle nemen over apparaatsensoren en apps. Daarna hebben hackers vrij spel om data en persoonlijke informatie te stelen, kwaadaardige software te installeren, of frustratie te kweken door het toestel te saboteren.

Het was het Amerikaanse bedrijf Nowsecure dat de fout opspoorde en deze al in december 2014 aan Samsung rapporteerde. De Zuid-Koreaanse firma heeft in maart een patch uitgebracht voor Android 4.2 en hoger, die het probleem zou moeten aanpakken. Nowsecure voerde echter recent testen uit met een Galaxy S6 en vond nog altijd dezelfde maas in het net.

Nowsecure heeft een drietal aanbevelingen voor getroffen eigenaars: vermijd onveilige wifinetwerken, gebruik gewoon een ander mobiel toestel en contacteer je provider voor informatie over veiligheidspatches.



Index

Bron: Security.nl

Naast Facebook is Twitter één van de grootste sociale netwerken. Je kan tegenwoordig geen televisieprogramma meer opzetten zonder dat je wordt gevraagd mee te tweeten onder een bepaalde hashtag. Twitter is echter vooral om plek om bij te houden wat je vrienden zoal uitspoken.

Hoe werkt Twitter : basishandleiding

Twitter heeft twee belangrijke verschillen ten opzichte van Facebook. Berichten kunnen maar uit 140 tekens bestaan, zodat je wordt gedwongen de kern van je boodschap zo kort en bondig mogelijk over te brengen.

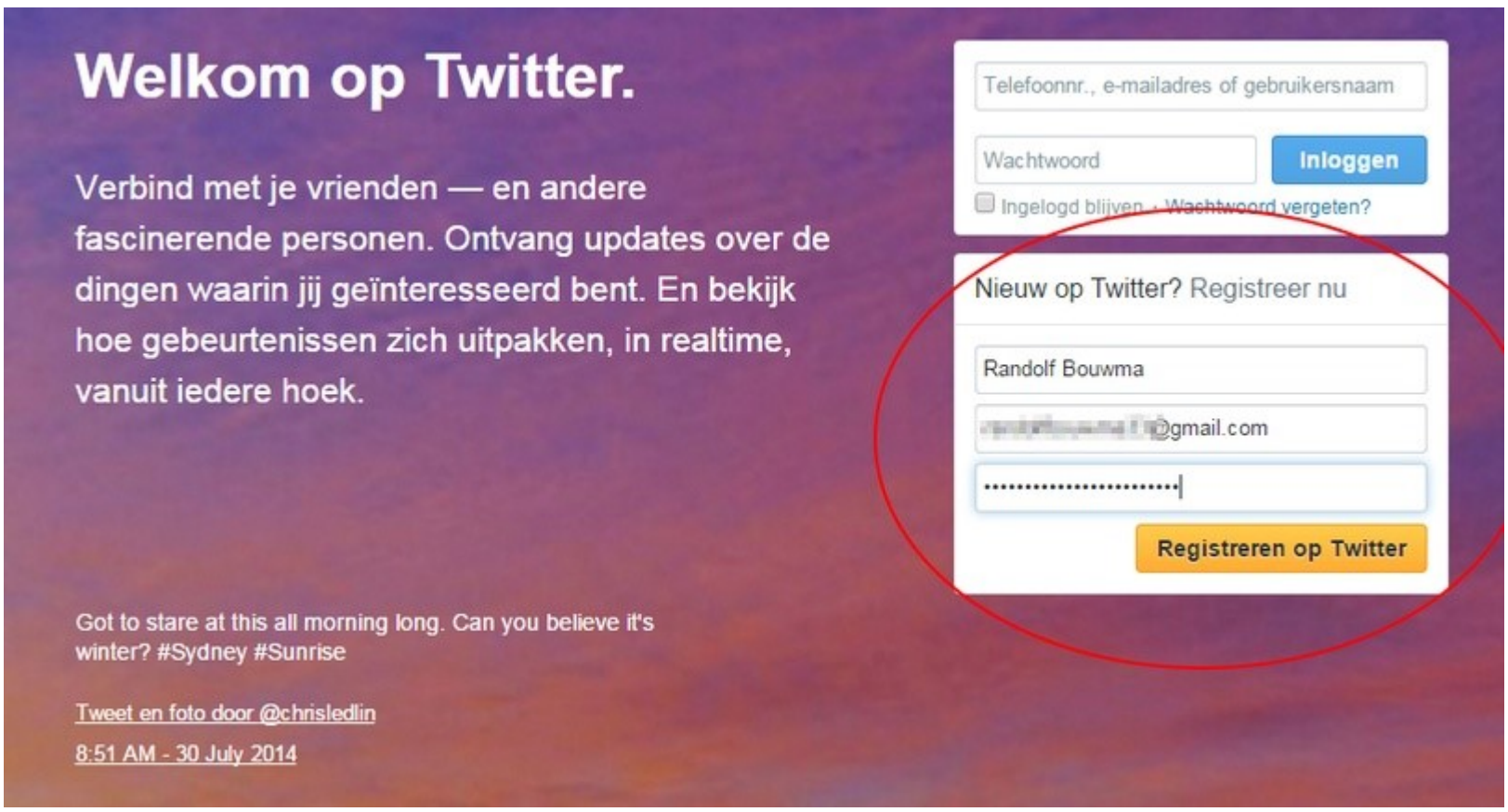
Daarnaast zie je berichten van de mensen die je volgt in chronologische volgorde. Dit in tegenstelling tot Facebook, die je posts toont waarvan het algoritme denkt dat je die het liefste wilt zien.

Apps downloaden

Twitter is via je browser te gebruiken via www.Twitter.com. Daarnaast zijn er apps voor vrijwel elk denkbaar mobiel platform.

Een account aanmaken

Om Twitter te gebruiken, heb je eerst een account nodig. Registeren doe je op de homepage van Twitter, maar dat kan ook in de apps. Vul je volledige naam en e-mailadres in en kies in het laatste vak een wachtwoord. Klik dan op 'Registreren op Twitter'.



Index

Bron: ComputerIdee

In het volgende scherm hoef je nu alleen nog maar een gebruikersnaam te kiezen. Twitter geeft alvast wat suggesties, op basis van je naam. Wanneer je er eentje hebt verzonnen, klik je op ’Registeren’.



Telefoonbeveiliging

Daarna vraagt Twitter je om je telefoonnummer voor tweestapsverificatie. Dat is een manier om je account beter te beveiligen door je telefoonnummer bovenop je wachtwoord te gebruiken. Dit kun je overslaan, maar tweestapsverificatie is wel een manier om je account beter te beveiligen. Weeg dus goed af of je dit wilt - wij raden aan het in te stellen!



Twitter stuurt je nu een verificatiecode via sms naar je telefoon. Die hoor je vrijwel direct binnen te hebben: duurt het een aantal minuten, schroom dan niet om op 'Sms opnieuw versturen’ te klikken. Grote kans dat je de code binnen een paar seconden alsnog toegestuurd krijgt. Voer hem in en kies voor ’Verifiëren’.

Index

Bron: ComputerIdee



Suggesties

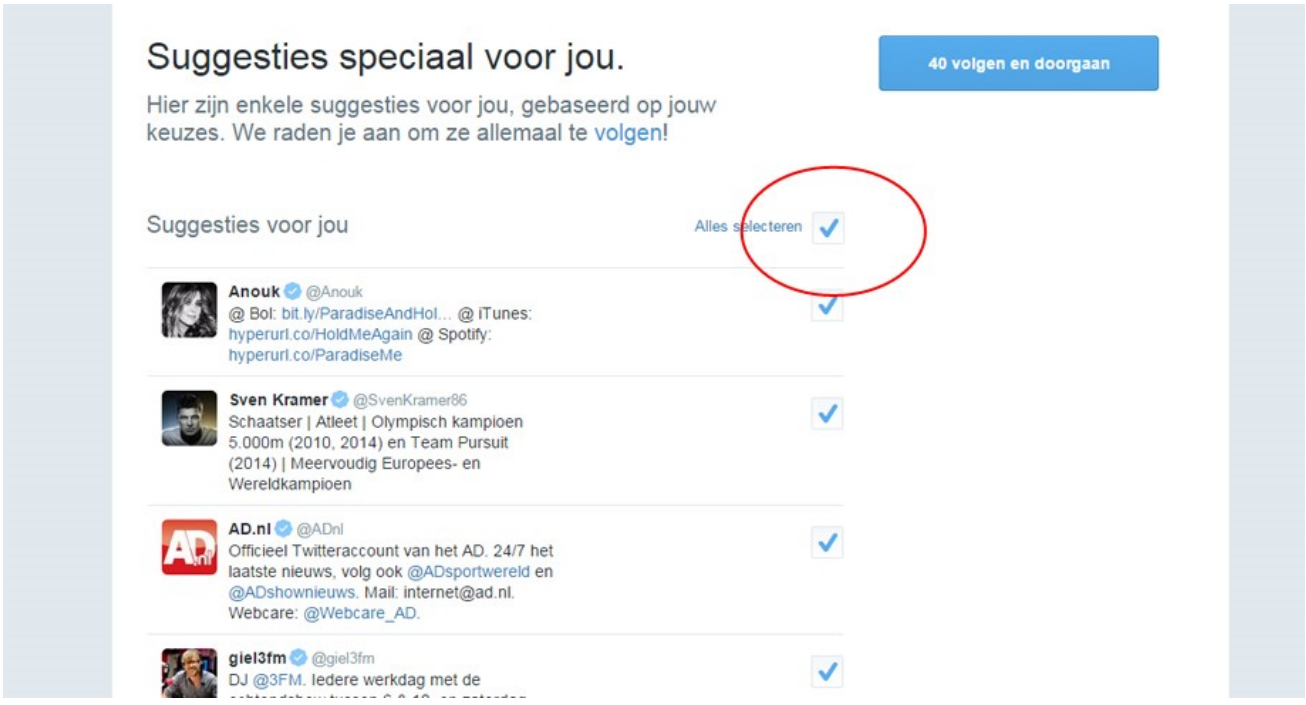
Druk in het volgende scherm op 'Laten we beginnen!' Nu vraagt Twitter je in welke onderwerpen je geïnteresseerd bent, waarna je suggesties krijgt voor te volgen Twitter-accounts. In het daaropvolgende scherm kun je die accounts aanvinken. Wil je nog niet direct iemand volgen of zit er niets voor je tussen, haal dan het vinkje weg achter 'Alles selecteren'. Hoe dan ook, om verder te gaan druk je rechtsboven op de grote blauwe knop.



Je komt uit op een pagina die je een profielfoto laat instellen. Bij de optie 'Foto maken' kan dat via je webcam. Je kunt ook een bestaande foto instellen. Kies dan voor 'Foto uploaden'.

Index

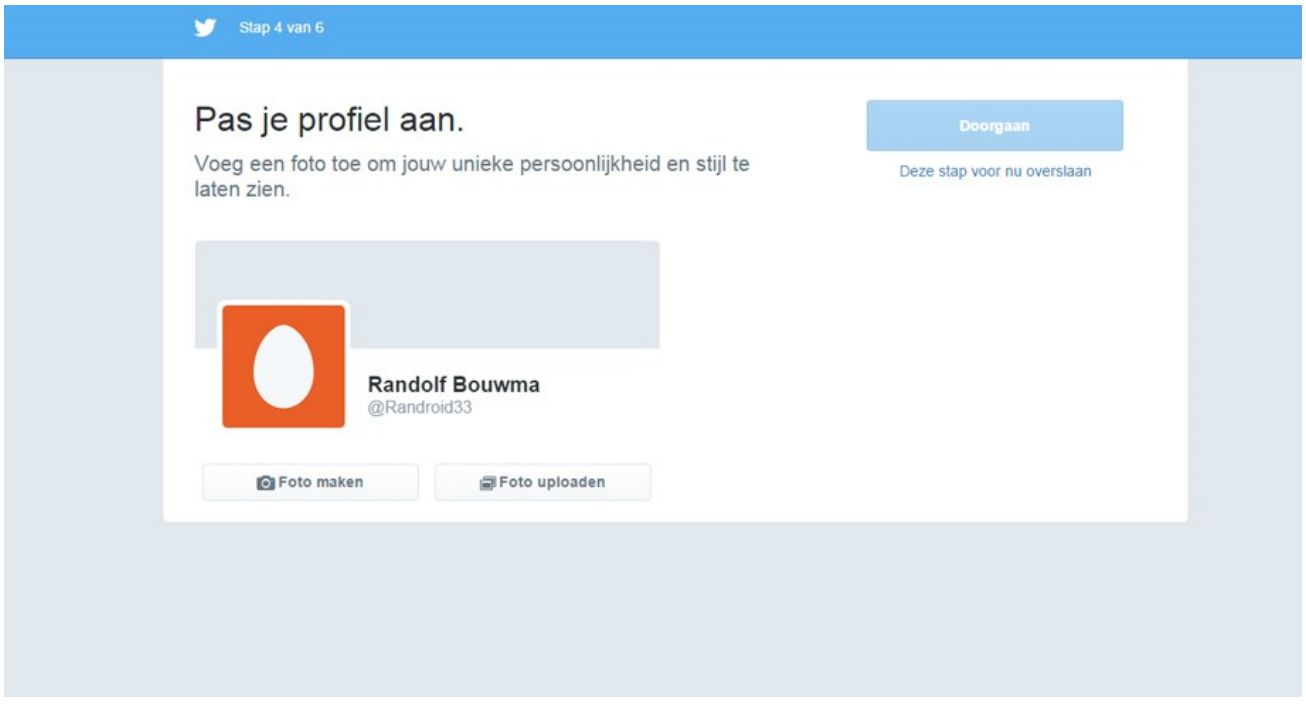
Bron: ComputerIdee



Accounts vinden

Stap 5 van 6 laat je opnieuw personen zoeken om te volgen. Dat kan onder meer door te kiezen voor 'Gmail-contacten uploaden', en de stappen te doorlopen die het pop-upvenster je voorschotelen. je kan ook een andere e-maildienst hiervoor gebruiken: AOL, Outlook of Yahoo. Twitter kijkt daarbij welke van je vrienden een Twitter-account hebben gekoppeld aan hun mailadres. Je kunt deze stap ook overslaan.

In de laatste stap volg je de personen die je in het vorige scherm hebt opgezocht, als je wilt. Bevestig dan nog even je e-mailadres door de instructies in de gele balk op te volgen. Daarna ben je klaar met de introductie en kun je beginnen met posten!





Index

Bron: ComputerIdee

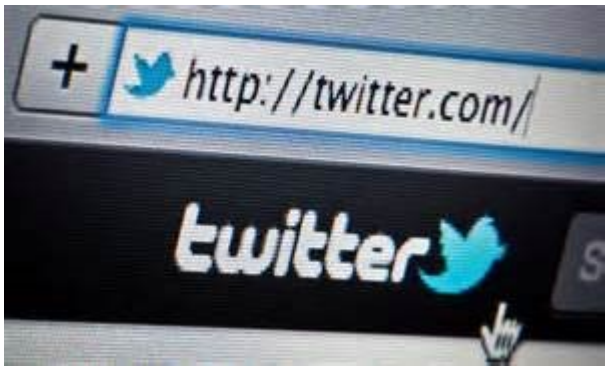
Een profielfoto instellen
Om een nieuwe profielfoto in te stellen, klik je **rechtsboven** op je huidige foto. In het drop-down menu kies je vervolgens **'Profiel weergeven'**. Klik daarna aan de rechterkant op de knop **'Profiel bewerken'**.





Je komt uit in een omgeving met verschillende opties. Kies hier **'Je profielfoto wijzigen'**, als je een nieuwe wilt.





Index

Bron: ComputerIdee

Op dezelfde manier kun je hier een omslag toevoegen. De standaard blauwe balk bovenaan je tijdlijn is zo ook te voorzien van een persoonlijke afbeelding.

Zodra je een plaatje hebt uitgekozen vanaf je harde schijf, krijg je nog de kans om deze passend te maken. Dat kan door de afbeelding te verslepen of door de schuifbalk voor **'Omslag positioneren en bepalen'** te gebruiken. Als je klaar bent, druk je op **'Toepassen'**.



Een profieltekst instellen

Met een profieltekst kun je mensen die je Twitter-tijdlijn bezoeken, snel iets meer over jezelf vertellen. Vul daaronder bij **'Bio'**een tekstje in, waarin je iets over jezelf vertelt. Als je wilt, kun je ook een **locatie toevoegen**. En als je een eigen site hebt, dan kun je die hier ook aangeven. Bij **'Themakleur'** bepaal je de kleuren van de knoppen en dergelijke.





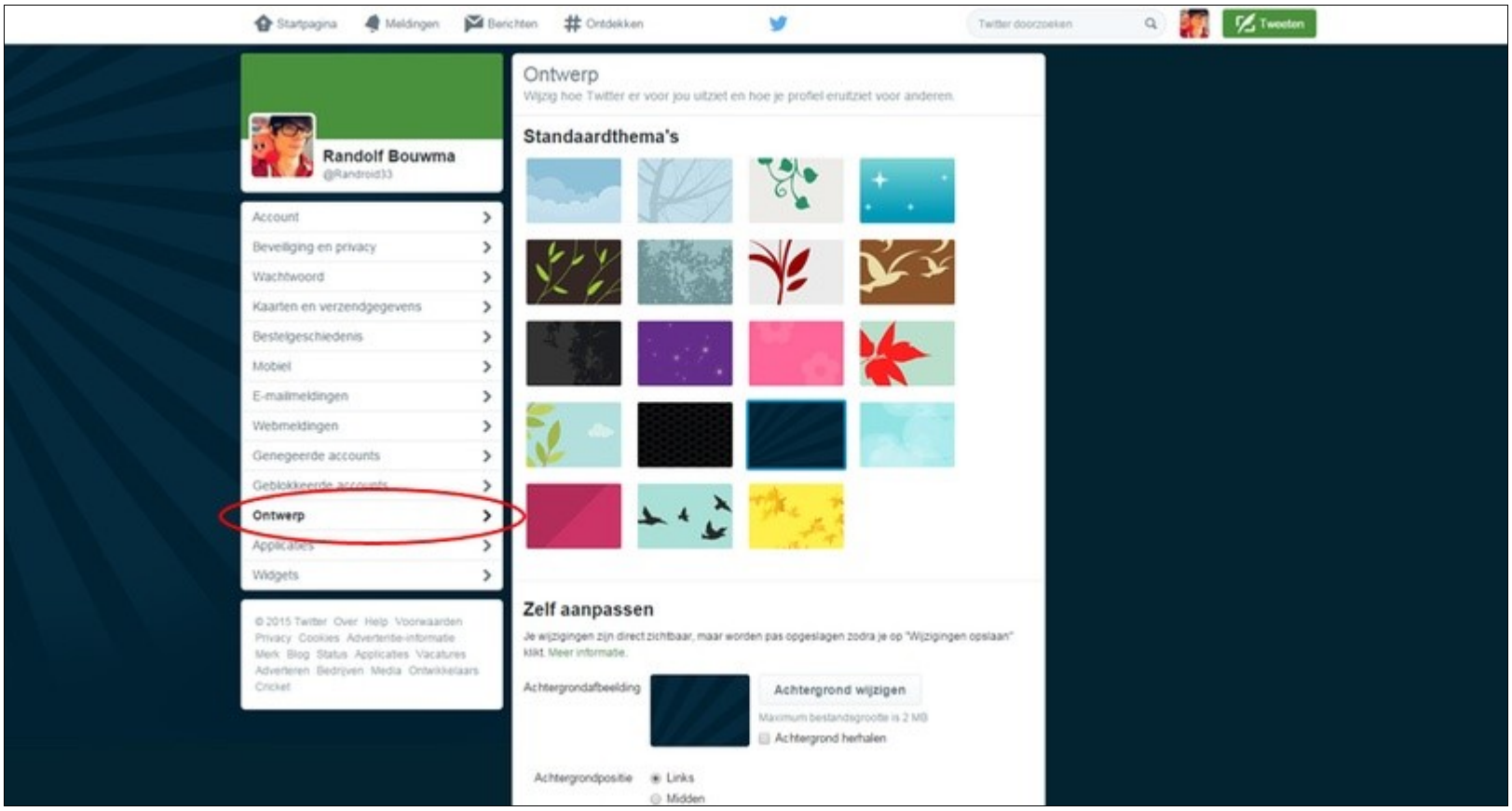
Wanneer alles naar wens is, kies je tot slot aan de rechterzijde voor **Wijzigingen opslaan'**.

Index

Bron: ComputerIdee

Een thema voor je profiel instellen
Er zitten nog wat extra personalisatie-opties verstopt in Twitter. Je vindt deze onder **'Instellingen'** (in het drop-down menu onder je profielfoto). Een van de onderste opties aan de linkerkant is **'Ontwerp'**.

Bij **'Standaardthema's'** kun je nu een achtergrond kiezen voor je héle Twitter-profiel. Je kan ook zelf een afbeelding uploaden, of kiezen hoe je het plaatje uitgelijnd wil hebben. Speel gerust met de opties, want ze worden pas opgeslagen zodra je onderaan de pagina kiest voor **'Wijzigingen opslaan.'**



Achtergrondthema's zie je overigens alleen zelf op je tijdlijn. Wanneer anderen je profiel bezoeken, zien ze de standaard lichtblauwe achtergrond. Een thema kies je dus alleen om Twitter voor jezelf wat op te vrolijken.

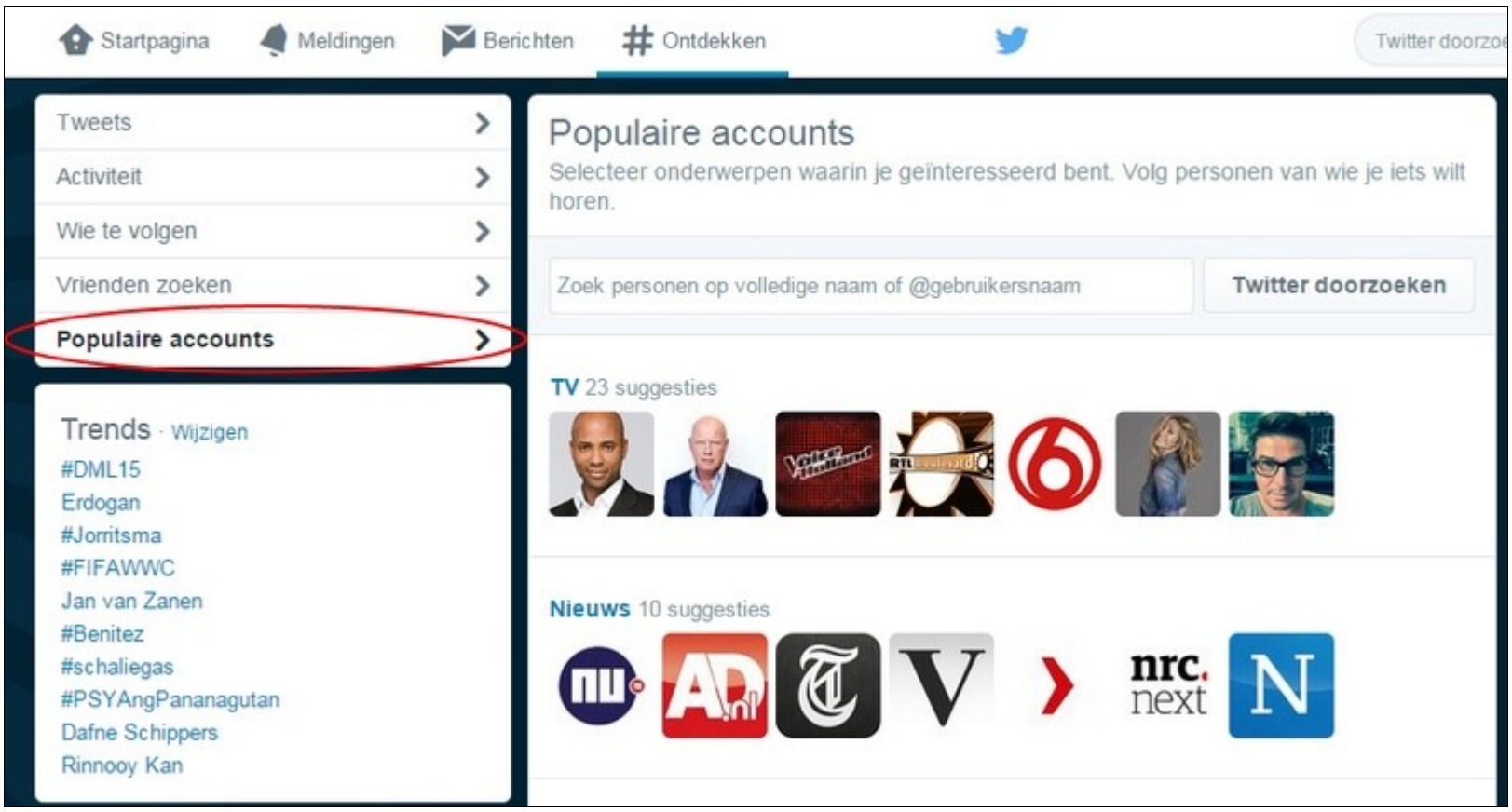
Een van de simpelste manieren om Twitter-accounts te vinden om te volgen, is de zoekbalk rechts bovenin. Je merkt daar bijvoorbeeld al snel dat de meeste organisaties tegenwoordig een Twitter-account hebben, als ook veel celebrities, programma's, artiesten en politici. Eens je een account hebt gevonden die je aanspreekt, druk je op de **'Volgen'**-knop. Zo simpel is dat.



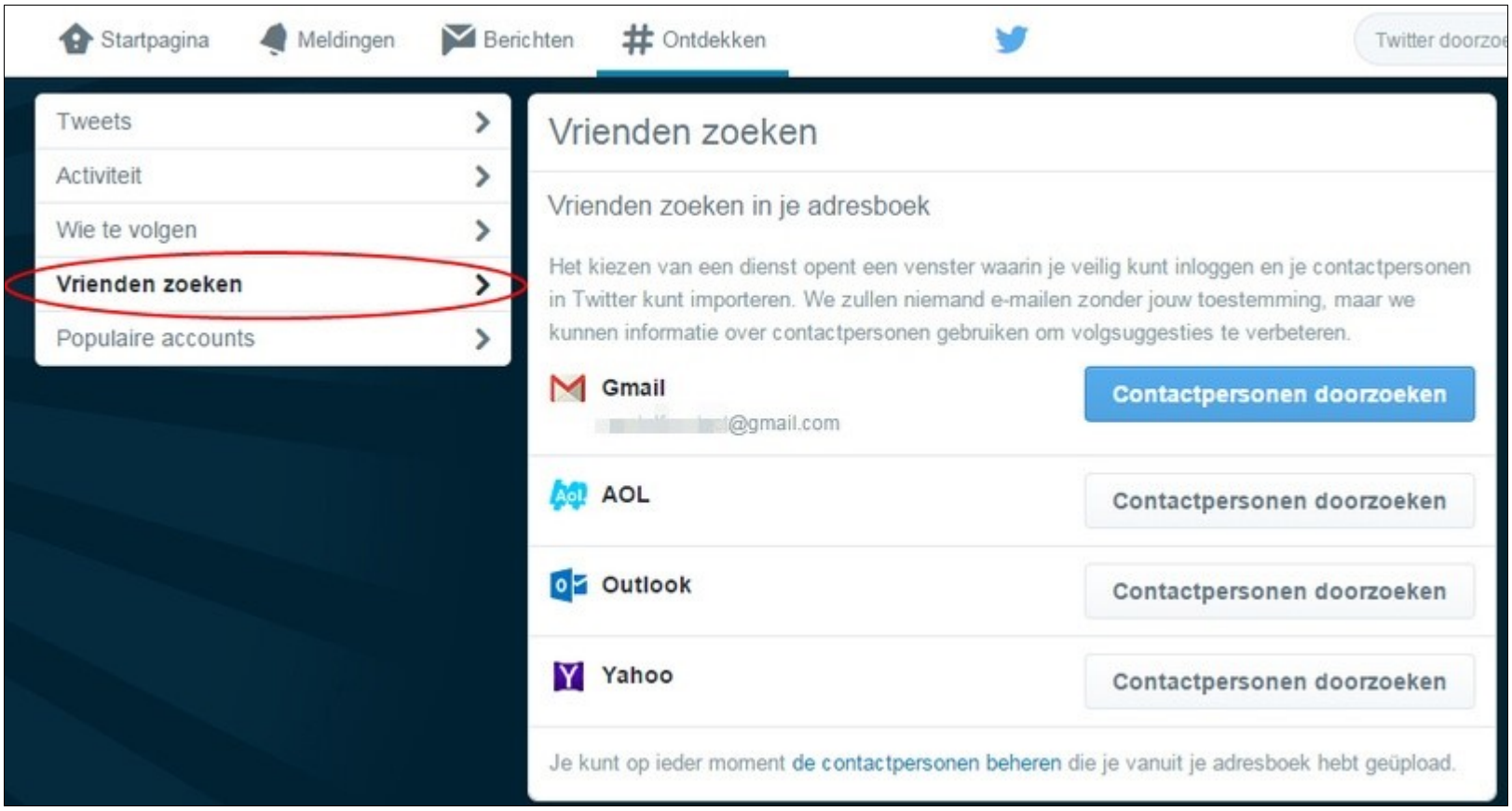
Index

Bron: ComputerIdee

Op je hoofdpagina krijg je tevens suggesties bovenaan je tijdlijn, mocht de inspiratie je even ontbreken. Door te kiezen voor **'Vernieuwen'** krijg je drie nieuwe suggesties. Druk op **'Meer'** om een letterlijk eindeloze lijst met interessante accounts voorgeschoteld te krijgen.



Meer geavanceerde opties vind je onder de knop **'Ontdekken'**, het vierde menu van links aan de bovenkant. Daar zie je niet alleen waar zoal over getweet wordt op dat moment, maar kun je bijvoorbeeld ook vrienden zoeken op basis van je emailcontacten. Kies dan rechts voor **'Vrienden zoeken'**, waar je vervolgens contactpersonen kan vinden op basis van een Gmail, AOL, Outlook of Yahoo-adres.



Tot slot kun je nog eens kijken onder **'Populaire accounts'**. Handig hierbij is dat deze accounts zijn verdeeld in categorieën zoals politiek, muziek of televisie. Wel zo overzichtelijk. Tip: Sommige mensen doen zich op Twitter graag voor als bekende personen, terwijl ze dat niet zijn. Of een account nep is of juist geverifieerd (dus echt), zie je aan het blauwe icoontje met het witte vinkje.

Follow us on Twitter

Index

Bron: ComputerIdee

Is het verboden om valse gegevens te verstrekken als een website of bedrijf deze wil hebben maar eigenlijk niet nodig heeft? Denk aan een telefoonnummer of geboortedatum bij gewoon een online bestelling.



Mag je valse gegevens op een site invullen?

Er is geen algemeen verbod in de wet om valse gegevens op te geven. Natuurlijk is er het strafbare feit 'valsheid in geschrifte', art. 225 Strafrecht. Het moet dan echter gaan om geschriften die opgemaakt worden om als bewijs ergens van te dienen. Dat houdt in dat de informatie van wezenlijk belang moet zijn. Bij overbodige informatie is daar per definitie geen sprake van.

Een winkel kan wel in haar voorwaarden eisen dat alle informatie naar waarheid moet worden verstrekt, en dan op die grond een overeenkomst annuleren. Je zou wel gek zijn als winkel om te annuleren bij een onjuiste geboortedatum, maar dat terzijde.

Echter, op grond van de privacywetgeving mag een bedrijf niet meer gegevens eisen dan nodig voor de overeenkomst. Je huisadres moet je dus geven (want daar moet de bestelling heen) en je naam ook (in verband met betaling) maar je geboortedatum of geslacht is niet echt relevant. Daar mogen ze dus niet naar vragen, en doen ze dat toch dan is het toegestaan hier valse gegevens in te vullen.



Index

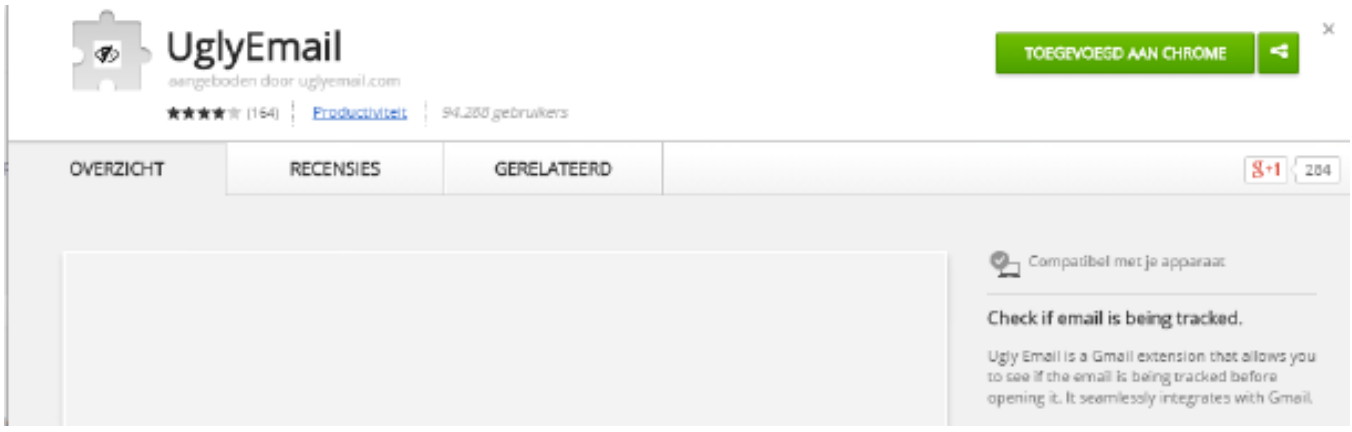
Bron: Arnoud Engelfriet ICT jurist

We leven in een tijd waarin privacy steeds schaarser wordt. Maar hoe weet je nu of, bijvoorbeeld, je mail gemonitord wordt? UglyE-mail helpt je, en zo werkt het ……



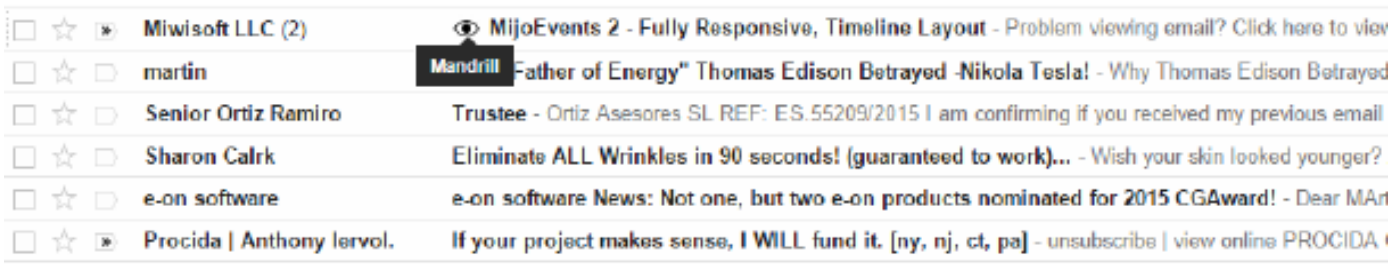
Wordt mijn e-mail gemonitord?

Laten we voorop stellen dat het natuurlijk nooit mogelijk zal zijn om een situatie te creëren waarin niemand in staat is om je 'af te luisteren' of je activiteiten te volgen. Dat gezegd hebbende is het wel degelijk mogelijk om iets proactiever om te springen met je privacy, door in ieder geval moeite te doen om te ontdekken wanneer iemand je volgt. Je kunt bijvoorbeeld een browser gebruiken als Tor om ervoor te zorgen dat je surfverkeer anoniem blijft. Maar hoe zit dat dan met e-mail? Als je Gmail gebruikt, is daar een superhandige extensie voor, genaamd UglyEmail.



Zien welke mail je in de gaten houdt

UglyEmail is een extensie die je gratis kunt downloaden via de Chrome Webstore. Klik op Toevoegen aan Chrome en vervolgens nogmaals op Toevoegen om de extensie te installeren, je hoeft daarvoor niet je browser opnieuw te starten. Vervolgens surf je (uiteraard ook in Chrome) naar Gmail. Wanneer er nu een e-mail in je account staat waar één of andere vorm van monitoring op wordt toegepast, bijvoorbeeld door te kijken of je de mail hebt geopend, hoe lang enzovoort, dan wordt er voor het onderwerp van het mailbericht een pictogram van een klein oog geplaatst. Zo weet je voordat je het mailtje opent al welke mailgegevens van jou worden verzameld.



Tracking is niet per definitie slecht

Overigens betekent een oogje niet meteen dat je met een mail te maken hebt die afkomstig is van kwaadwillenden, want maildiensten als Mailchimp verzamelen ook statistieken om zenders te helpen bij het optimaliseren van hun mail (bijvoorbeeld door ervoor te zorgen dat mensen die geen mail willen, geen mail meer krijgen). Kortom, een oogje is niet direct alarm, maar het is wel goed dat je in ieder geval wéét welke mails wat extra aandacht vereisen.

Index

Bron: ComputerTotaal



Software schatkist

De kist is gevuld met fraaie software. Nieuwsgierig?

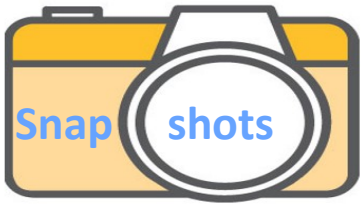
Open de kist middels de sleutel en ontdek…….



(Enkelen onder jullie weten dat ik regelmatig lange remixen maak van trance– en dancemuziek onder de naam DoubleYouAB.

Omdat de vakantietijd is aangebroken kunnen jullie via de schatkist mijn nieuwe Summermix 2015 downloaden. Lekker voor in de auto af aan het strand….!!. Try it out!)

Index



Een Nederlands meisje van 13 is op internet uitgegroeid tot ‘een wereldwijd lustobject voor pedofielen’. Haar foto’s worden digitaal wereldwijd gedeeld, en duiken op in politieonderzoeken in Nederland, Duitsland, Engeland, Australië, Mexico en de VS. Mannen noemen zich ‘volgeling’ en er blijkt zelfs een pornografisch computerspelletje in omloop met het meisje in de hoofdrol. Het meisje, dat ook thuis belaagd wordt, gaat onder begeleiding naar school, speelt nauwelijks nog buiten en is gestopt met hockey. En met alle sociale media. Haar verhaal wordt vertelddoor haar vader, tijdens een rechtszaak tegen een oud-leraar van een basisschool in Vessem, Brabant. Die man staat terecht omdat hij foto’s van het meisje digitaal had bewerkt tot pornografische afbeeldingen. De slachtofferverklaring van de vader heeft veel impact. ‘Mannen uiten de meest smerige fantasieën. En iedere pedofiel op internet kent haar’, stelt hij. Foto’s van het meisje komen al in 2005 online, op fotosite Flickr. De vader vertelt hoe hij van lieverlee steeds meer reacties kreeg van mannen die blootfoto’s wilden of ranzige comments onder de foto’s schreven. Hij negeerde dat aanvankelijk, maar toen de aandacht steeds vervelender werd, zette hij de foto’s achter een slotje. ‘We dachten dat de rust was weergekeerd’. Eind 2014 bleek die hoop ijdel. De vader kreeg via twitter een tip. ‘Of ik daar eens wilde kijken. Onze dochter liep gevaar’. Hij schrok toen hij zag dat op bepaalde websites ‘hele discussies’ aan het meisje waren gewijd. Het meisje zelf had overigens op Instagram en facebook tientallen onbekenden als vriend geaccepteerd, allemaal (zogenaamde) fans van One Direction. Alle foto’s die het meisje zelf op die sites geplaatst had, bleken gebruikt en gephotoshopt. Mannen vroegen of ze haar mochten ontmaagden, mannen gingen naar haar school en maakten stiekem foto’s van haar, fietsten achter haar aan en wisten zelfs in welke klas ze zat omdat de school de nieuwe indelingen op internet had gezet. ‘Haar naam googelen en je wist haar lesschema’. De vader deed uiteindelijk aangifte maar de politie kon weinig: de foto’s zelf waren niet pornografisch en bovendien door het meisje zelf online gezet. Pas toen agenten de sites bezochten die de vader doorgaf, werden ze zich bewust van het gevaar. De schoolleiding werd ingelicht, de politie surveilleerde rond het schoolplein en alle sociale media werden geschrapt. De man beschrijft ook de reacties die hij kreeg van de pedo’s: ‘deze mannen hebben een heel verkeerd beeld van de werkelijkheid. Zij zijn goed en de rest van de wereld is gek. Ze vinden dat ik de vrijheid van meningsuiting belemmer en een grondrecht schend’.

———————————————————-

Een uitspraak van het Europees Hof voor de Rechten van de Mens heeft de discussie over de verantwoordelijkheid van websitebeheerders nieuw leven ingeblazen. In de zaak, over een nieuwssite in Estland, bepaalde het Hof dat een eigenaar van een website niet alleen verantwoordelijk is voor nieuwsartikelen maar ook voor de commentaren daarop. De zaak is uit 2006; op nieuwssite Delfi verscheen een artikel over een scheepvaartbedrijf dat bepaalde ‘ijswegen’ zou heben vernield. Op dat bericht verschenen, anoniem, enkele negatieve reacties. Delfi beriep zich op de vrijheid van meningsuiting maar dat argument werd al in 2013 verworpen: het waren bedreigingen en Delfi had de technische middelen al in huis om zulke reacties te verwijderen. Later moest Delfi een schadevergoeding betalen omdat het bedrijf financieel voordeel had bij het exploiteren van de site en de commentaren. Het Hof heeft nu definitief geoordeeld: websites kunnen verantwoordelijk gehouden worden voor de reacties van anderen.

———————————————————————

Zou het dan toch? Hebben sociale media dan toch die … Zouden we de kracht van facebook onderschat hebben? Uit onderzoek van het Britse CBS blijkt dat jongeren tegenwoordig minder drinken. De reden? Jongeren zeggen dat ze niet willen dat er beschamende foto’s van hen op facebook verschijnen. In Engeland steeg van 2013 op 2015 het aantal 16-24 jarigen dat níet drinkt, met een kwart. Jongeren willen naar eigen zeggen niet langer dat vrienden hen op sociale media in allerlei compromitterende poses zien. Ze drinken minder, roken minder, blowen minder en hebben zelfs minder seks. Uit cyberschaamte? Zou facebook dan wel lukken wat menig ouder niet lukt? Volgens onderzoekster Kelly O’Sullivan lijkt het daar wel op. ‘Jonge mensen vinden het leuk om dronken foto’s van hun vrienden te bekijken, maar hun eigen foto’s zien ze liever niet opduiken’.

———————————————————————

Sexting tussen tieners is zo standaard dat het opvalt als je er nog géén last van gehad hebt. Dat stelt het Britse National Crime Agency, dat een campagne is begonnen om kinderen bewuster te maken van de gevaren. Vrijwel dagelijks komen er meldingen over sexting bij het Child Exploitation and Online Protection Centre (CEOP) van de NCA. Onvoorstelbaar veel tieners sturen en ontvangen (bijna-) naaktselfies, of plaatsen die op sociale-mediasites. Een van de gevolgen is dat veel tieners met die foto’s worden gechanteerd of afgeperst. De campagne is gericht op ouders die moeten leren hoe ze met zulke foto’s (en zulke kinderen) moeten omgaan. Voor de campagne zijn tientallen jongeren ondervraagd over hun onlinegedrag. Ze kunnen vooral niet omgaan met de druk die ze wordt opgelegd om zo’n foto tóch maar te maken en te sturen. Opvallend is dat de jongeren zelf nauwelijks over sexting praten maar gewoon over selfies praten. Ze zien sexting niet per se als gevaarlijk en risicovol. ‘It can start off as a bit of fun but the issues start when that image gets into the wrong hands’.

———————————————————————-

Je ooit afgevraagd wie er nu allemaal ingeschreven staan op datingsites? Een aardige bijkomstigheid van de diefstal van de database van de erotische datingsite Adult FriendFinder is dat er nu inzicht is in de leden. De database kwam online, beveiliger John McAfee analyseerde deze en vond onder de 3,9 miljoen leden onder meer zestien leden van het Amerikaanse Congres, twee senatoren en maar liefst 1420 directeuren van Fortune-500-bedrijven. McAfee zag, op basis van ip-adressen, verder dat maar liefst 120 duizend Amerikaanse ambtenaren ingeschreven stonden ‘die onder werktijd de website gebruikten, foto’s bekeken, tekstberichten en e-mails verstuurden en seksuele fantasieën met tal van mensen uitwisselden – via overheids- of kantoorcomputers’. De database is daarmee ‘goud waard’ voor bendes/landen die de leden willen afpersen. ‘Bijna alle functionarissen zijn getrouwd en hebben kinderen’. Onder de 3,9 miljoen leden zaten volgens McAfee overigens ruim 35 duizend Nederlanders.

———————————————————————

Justitieminister Ard van der Steur wil dat er in het strafrecht meer mogelijkheden komen om de ongewenste verspreiding van vertrouwelijke gegevens te bestraffen. Van der Steur refereert onder meer aan wraakporno – seksfoto’s of -filmpjes die online komen uit wraak op een ex. Dat blijkt niet altijd even goed strafrechtelijk dan wel civielrechtelijk aan te pakken en daarom komen er ‘nieuwe strafbaarstellingen’, aldus de minister .

In-



Een nieuw opsporingsteam binnen Europol gaat proberen te achterhalen wie er achter de vijftigduizend twitter-accounts zitten die aan IS zijn gelieerd. Vanaf die accounts worden dagelijks zo'n honderdduizend tweets verstuurd, ter propaganda en recrutering. Het team gaat IS-accounts blokkeren, elke gevonden account moet binnen twee uur weg zijn, aldus het plan. Volgens Europol-directeur Rob Wainwright gaat het team niet alleen kijken naar de beheerders van de accounts maar ook naar de volgers en gevolgden. Uiteraard is de hulp van internetbedrijven nodig, maar Wainwright wilde niet zeggen om welke bedrijven het gaat en hoe zij gaan helpen in de strijd.
Wel erkende Wainwright dat het moeilijk de vele duizenden IS-accounts te blokkeren. 'Het zijn er simpelweg te veel'. Het plan is deels gebaseerd op het werk van de Counter Terrorism Internet Referral Unit van Scotland Yard, die sinds 2010 al meer dan negentigduizend 'terroristische uitingen' van internet verwijderd heeft. BZ-minister John Hayes zegt 'zero tolerance' na te streven als het gaat om internet. Hij hoopt dat providers hun verantwoordelijkheid pakken. 'We will encourage companies to produce industry standards for the identification, removal and referral of terrorist activity and will consider further action as necessary'.

———————————————————

Wat kochten mensen nou precies op Silk Road? Uit alle onlangs gepubliceerde rechtbankdocumenten rond de levenslange celstraf voor oprichter Ross Ulbricht is mooi te herleiden wat er nu allemaal verkocht werd. Eigenlijk maar één ding: drugs. Onder de twintig meest populaire producten zaten zestien verschillende drugs, waaronder wiet, cocaine, pillen, lsd, mdma, heroine, dmt en opiaten. De omzet op Silk Road bedroeg tussen 2011 en 2013 ruim 214 miljoen dollar. Hoewel Silk Road opgerold werd en de oprichter levenslang heeft, gaat de 'amazonificatie' van de drugshandel gewoon
door, schrijft drugsonderzoeker Russell Webster. 'Wie zoekt op een alternatief, vindt bij Google 3,9 miljoen hits'.

———————————————————

Nederland Schoon, het project waarbij de politie hostingproviders aanspreekt, is niet bedoeld om content offline te krijgen maar om het bewustzijn over cybercrime te vergroten. Staatssecretaris Dijkhoff (VenJ) verduidelijkt zo het project, dat veel kritiek kreeg. De politie gaat providers aanspreken op hun faciliterende rol bij cybercrime? Huh? Volgens Dijkhoff is de soep niet zo heet. Hijdenkt dat 'bepaalde hostingbedrijven' zich mogelijk niet bewust zijn van het feit dat zij cybercrime faciliteren. Daarom zal, binnen het project Nederland Schoon, een gesprek met hen plaatsvinden, om ze meer inzicht te geven in de wijze waarop cybercriminelen gebruik maken van de Nederlandse hostinginfrastructuur en om ze op hun erantwoordelijkheid te wijzen. 'De verwachting is dat vanuit deze bewustwording hostingproviders zelfstandig maatregelen nemen om crimineel misbruik van hun dienstverlening tegen te gaan', schrijft Dijkhoff die benadrukt dat providers natuurlijk wel gevorderd kunnen worden om bepaalde content te verwijderen, via OvJ en rechter-commissaris.

———————————————————

Het Meldpunt Kinderporno op internet heeft in 2014 bijna 29 duizend meldingen behandeld, 5700 (24%) meer dan in 2013. En bij de jongerenhulpsite Helpwanted.nl steeg in 2013 het aantal meldingen zelfs met 77%. Volgens het meldpunt is de stijging onder meer te verklaren door de goede it-infrastructuur die Nederland heeft. In Nederland wordt veel meer kinderporno gehost dan in andere landen. Niet alle meldingen werden door het meldpunt afgehandeld. Een deel ging naar de politie, maar een ander deel kon door capaciteitsgebrek niet worden onderzocht.

———————————————————-

Europol heeft een internationale bende cybercriminelenopgerold. In totaal werden 49 mensen, vooral afkomstig uit Nigeria, Kameroen en Spanje, opgepakt. Ze worden verdacht van het gebruik van malware en social engineering om in te breken op websites van bedrijven. Daarbij maakte ze 'in zeer korte tijd' zes miljoen euro buit. De bende was actief in België, Groot-Brittannië, Italië, Spanje, Polen en Georgië. Bendeleden die toegang hadden tot de bankgegevens, konden meekijken met de betalingen. Klanten van de gehackte bedrijven moesten het geld overmaken naar een rekeningnummer in handen van de hackers, waarna het geld binnen no time buiten de EU werd getransporteerd. Bij zoekingen in 58 woningen van bendeleden werden laptops, harde schijven, telefoons, tablets, simkaarten, usb-sticks, vervalste documenten, credit cards en contact geld in beslag genomen.

———————————————————-

Een agent (42) van de politie Rotterdam is aangehouden omdat hij politiesystemen misbruikte én omdat hij kinderporno in bezit had. De man zocht in de systemen naar nabestaanden van dodelijke ongelukken, naar vrouwen van wie de partner net was overleden en naar andere 'kwetsbare vrouwen'. Via facebook of e-mail benaderde hij die vrouwen voor een afspraak.

Index

Phishing- / valse e-mails melden

ABN AMRO Bank: valse-email@nl.abnamro.com
ING Bank: valse-email@ing.nl

Rabobank: valse-email@rabobank.nl

SNS Bank: valse-email@sns.nl

ICS- / ABN AMRO creditcards: valse-email@icscards.nl

opgelet op internet.nl

Voor vragen over veilig internetbankieren bij uw eigen bank, kunt u op een van de onderstaande websites terecht.

Websites banken	
ABN AMRO	LeasePlan Bank
Argenta	Rabobank
Credit Europe Bank	SNS Bank
DeltaLloyd Bank	Staal Bankiers
DHB Bank	Triodos Bank
Friesland Bank	Van Lanschot Bank
ING Bank	ASN Bank

MARKTPLAATS: "Wat moet ik doen als ik denk dat ik ben opgelicht?"

Antwoord

1. Wanneer u vooraf betaalt, maar de verkoper het product vervolgens niet levert, adviseren wij het volgende:

Neem eerst nogmaals contact op met de verkoper. Mogelijk is er sprake van een misverstand of wordt het product alsnog geleverd. Breng in geval van oplichting altijd de Politie op de hoogte (dit kunnen wij niet voor u doen). Zij hebben immers de kennis, expertise en opsporingsbevoegdheden om onderzoek te doen naar strafbare feiten. Wij adviseren u om aangifte te doen bij het Meldpunt Internetoplichting van de Politie via www.mijnpolitie.nl (formulier Melding Internetoplichting).
Wij adviseren u om het formulier zo accuraat en volledig mogelijk in te vullen.
Zorg dat u, wanneer u aangifte gaat doen, alle relevante gegevens bij de hand heeft zoals:

- Uw eigen (contact)gegevens, inclusief uw Burgerservicenummer (BSN).
- De (contact)gegevens van de partij met wie u heeft gehandeld (zoals naam en bankrekeningnummer).
- De gegevens van de transactie, zoals het advertentienummer en de onderlinge communicatie.

Meld oplichting ook altijd aan Marktplaats. Wij nemen dergelijke meldingen zeer serieus en nemen waar mogelijk gerichte maatregelen. Indien u aangifte doet via het formulier Melding Internetoplichting op www.mijnpolitie.nl wordt direct



Index

Cybercrime wetsartikelen

Wetsartikelen voor computercriminaliteit in enge zin

(ruime zin: algehele benamingen / enge zin: specifieke verschijningsvormen)

Voor cybercrime in enge zin zijn de volgende wetsartikelen beschikbaar:

. Artikel 138a WvSr: het binnendringen in een geautomatiseerd werk.

. Artikel 161 sexies WvSr: opzettelijk veroorzaken van stoornis in de gang of in de werking van een geautomatiseerd werk of werk voor de telecommunicatie.

. Artikel 161 septies WvSr: stoornis in de gang of in de werking in een geautomatiseerd werk of werk voor telecommunicatie door schuld.

. Artikel 350a WvSr: het opzettelijk onbruikbaar maken en veranderen van gegevens.

. Artikel 350b WvSr: het onbruikbaar maken en veranderen van gegevens door schuld,

. Artikel 139c WvSr: het aftappen en/of opnemen van gegevens en

Artikel 139d WvSr: het plaatsen van opname-, aftap- c.q. afluisterapparatuur.

Er zijn geen specifieke wetsartikelen om cybercrime in ruime zin aan te duiden. Voor de hoofddaad worden dezelfde wetsartikelen gebruikt als wanneer de criminele daad niet metICT zou worden gepleegd.

———————————————————

Haatzaaien.

'Het zaaien van haat of het (opzettelijk) beledigen of discrimineren van een groep mensenwegens hun ras, hun godsdienst of levensovertuiging, hun hetero- of homoseksuelegerichtheid of hun lichamelijke, psychische of verstandelijke handicap, zonder een bijdrage te leveren aan het publieke debat, waarbij ICT essentieel is voor de uitvoering' .

Haatzaaien staat niet als zodanig in het wetboek.

Aan de hand van de geformuleerde definitie kunnen echter de volgende wetsartikelen worden onderscheiden die delicten omschrijven welke vallen onder deze noemer:

- Artikel 147 WvSr: godslastering
- Artikel 90quater WvSr: discriminatie.
- Artikel 137d WvSr: aanzetting tot discriminatie van een bevolkingsgroep.
- . Artikel 137e WvSr: openbaarmaking discriminerende uitlatingen.
- . Artikel 137f WvSr: deelname of steunen van discriminatie.
- . Artikel 137g WvSr: discriminatie in ambt, beroep of bedrijf.
- . Artikel 131 WvSr: opruiing.

———————————————————

Cyberstalking.

'Cyberstalking' is de verzamelnaam voor het stelselmatig lastigvallen van een persoon doorprovocerende uitspraken te doen en/of berichten te plaatsen via online forums, bulletin boards en chatrooms, of de ander als het ware via spyware te bespioneren dan wel voortdurend ongevraagd e-mail en spam te sturen. Er is sprake van een verregaande inbreuk op de privacy van het slachtoffer' .

Relevante wetsartikelen zijn:

Artikel 285b WvSr: belaging.

Artikel 138a WvSr: computervredebreuk.

Artikel 266 WvSr: belediging.

———————————————————

Grooming.

Grooming wordt door het particuliere Meldpunt Kinderpornografie op Internet (MKI) opgevat als het zich op internet anders voordoen (door een volwassene) met het doel om seksueel getinte contacten te leggen met kinderen. Deze contacten kunnen zowel virtueel (seksuele handelingen voor de webcam) als fysiek (een ontmoeting waarbij het kind daadwerkelijk seksueel misbruikt wordt) zijn . Op dit moment is grooming niet strafbaar.

Grooming is echter wel opgenomen in het door Nederland ondertekende, maar nog niet door Nederland geratificeerde EU-verdrag van Lanzarote van 25 oktober 2007, artikel 23 ('Solicitation of children for sexual purposes'), waarin landen zich verplichten om grooming strafbaar te stellen. Grooming is dan het door een volwassene via ICT leggen van contacten-met een jongere met de intentie deze te ontmoeten voor het verrichten van seksuele handelingen, gevolgd door het feitelijk geven van uitvoering aan het tot stand brengen van die ontmoeting. Dat is een aanzienlijk engere uitleg dan het MKI geeft, vooral omdat volgens het verdrag begonnen moet zijn met het realiseren van de ontmoeting ('material acts leading to such a meeting').

———————————————————

Handel in mensen of foute goederen.

Verschijningsvormen:

drugs, geneesmiddelen, vuurwapens en explosieven, mensenhandel- en smokkel, heling.

Kenmerkend bij deze vormen van cybercrime is dat de handel plaatsvindt op of middels ICT

(bijvoorbeeld marktplaats) en dat de betrokken partijen weten dat het gaat om illegale handel.

Relevante artikelen zijn:

Artikel 273a WvSr mensenhandel.

Artikel 416 WvSr opzetheling.

Artikel 417 WvSr opzetheling (gewoonte).

Artikel 274 WvSr slavenhandel.

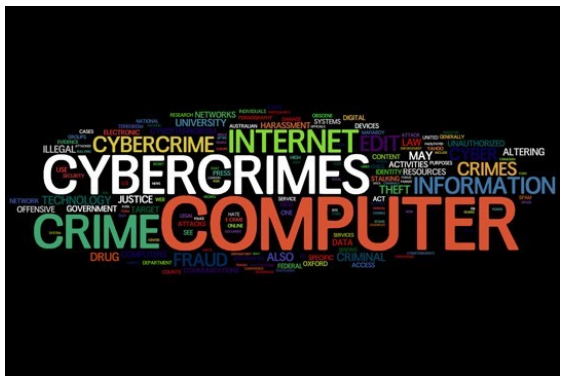
Artikel 2 Wwm: wet wapens en munitie

Artikel 31 Wwm: overdragen van wapens of munitie

Artikel 2 Ow: opiumwet

Artikel 3 Ow: opiumwet

Artikel 3b Ow: opiumwet



Index

Cybercrime wetsartikelen (2)

Bij piraterij gaat het feitelijk om illegale handel van allerhande 'cd's, dvd's, films, software en andere producten waarvoor auteursrechten gelden' . De nadruk ligt volgens het KLPD veelal bij eindgebruikers, internetpiraten en vervalsers, en in mindere mate bij gebruikers van licenties (bijvoorbeeld bedrijven) en computerverkopers. In alle gevallen is piraterij echter strafbaar en valt het onder meer onder het Wetboek van Strafrecht, de Auteurswet en de Merkenwet.

Relevante artikelen uit het wetboek van strafrecht zijn:

- Artikel 337 WvSr: handel goederen vervalste merken.
- Artikel 328 WvSr: oneerlijke mededinging.
- Artikel 441a WvSr: heling.
- Artikel 1 AW: auteurswet
- Artikel 31 AW: opzettelijk inbreuk op auteursrecht
- Artikel 31a AW: voorwerp met daarop een inbreuk op auteursrecht
- Artikel 31b AW: beroep maken van inbreuk op auteursrecht

———————————————————————————-

Kinderpornografie.

Kinderpornografie is in Nederland strafbaar gesteld in artikel 240b Wetboek van Strafrecht.

Kinderpornografie is volgens dit artikel iedere afbeelding - of gegevensdrager die een afbeelding bevat - van een seksuele gedraging waarbij iemand, die kennelijk de leeftijd van achttien jaar nog niet heeft bereikt, is betrokken of schijnbaar betrokken is'. Zowel het verspreiden, tentoonstellen, vervaardigen, invoeren, doorvoeren, uitvoeren als in bezit hebben ervan is in Nederland strafbaar. In Nederland is het enkel kijken naar kinderpornografie niet strafbaar.

———————————————————————————-

Illegale kansspelen.

'Volgens de Wet op de kansspelen (Wok) is er in Nederland een verbod op het aanbieden,

propageren en gebruikmaken van kansspelen waarvoor geen vergunning is verleend. Illegale

kansspelen en gokken op het internet (bijvoorbeeld het online casino) is één van de groeiindustrieën

op internet' .

Relevante wetsartikelen zijn:

Artikel 1 Wks: wet op de kansspelen

Artikel 1a Wks: piramidespelen

———————————————————————————--

E-fraude.

'De essentie van fraude is steeds dezelfde: mensen eigenen zich middels bedrog geld of vermogensbestanddelen toe waarop ze geen recht hebben en tasten daardoor de rechten van anderen aan. Er zijn verschillende begrippen in omloop om de cybervorm van fraude te beschrijven, zoals fraude in e-commerce en internetfraude . 'Bij deze vorm van fraude wordt het internet gebruikt om op oneigenlijke wijze gelden, goederen en diensten te verkrijgen zonder daarvoor te betalen of tegenprestaties te leveren' .

Bij internetfraude wordt er al snel gedacht aan oplichtingen via verkoopsites op internet zoals marktplaats en e-bay. Wij gebruiken de term 'e-fraude' als overkoepelende term. E-fraude is bedrog met als oogmerk het behalen van financieel gewin waarbij ICT essentieel is voor de uitvoering. Fraude staat niet als zodanig in de wet genoemd. Relevante wetsartikelen uit het wetboek van strafrecht zijn:

Artikel 326 WvSr: oplichting.

Artikel 225 WvSr: valsheid in geschrifte.

Artikel 231b WvSr: identiteitsfraude

Artikel 310 WvSr: diefstal.

Artikel 321 WvSr: verduistering.

Artikel 416 WvSr: heling.

———————————————————————————



Index