Windows 10 special



Augustus 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



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, Peppermunt.net, PrivacyNieuws, HackInfo, HardwareInfo, Bright, Computerworld

Uw tablet beveiligen

Phishing-springplank verstopt in PDF-documenten

Ontwikkelaar encryptiesoftware doelwit van cyberspionage

Minister wil dat FIOD prepaid-telefoons kan aftappen

Bende haalde simkaarten op voor fraude met internetbankieren

Controleer de bevoegdheden van USB-sticks

Hackers stelen je auto wanneer je hem ontgrendelt

Hoe oud is “Sexy Annabel”

Problemen in Bitcoin-land: Wat is er aan de hand?

Windows 10

De verschillen: 10 versus 7 & 8.1

Windows 10: verbeter je privacy

Windows 10: Het menu Start aanpassen

Tien belangrijke sneltoetsen voor Windows 10

Schatkist

Snapshots

Cops in Cyberspace

Handig

Wetsartikelen

Net als een laptop of smartphone is een tablet een apparaat waar veel van uw persoonlijke gegevens op staan. U doet er dan ook verstandig aan om deze data af te schermen voor de buitenwereld. In dit artikel diverse tips om uw tablet te beveiligen.



UW TABLET BEVEILIGEN

Uw iPad beveiligen

U kunt er op diverse manieren voor zorgen dat anderen niet zomaar toegang tot de gegevens op uw iPad hebben.

Codeslot

Alle iPad modellen kennen de mogelijkheid om een pincode of codeslot in te stellen. Als iemand dan uw iPad wil gebruiken moet hij eerst een viercijferige code invoeren om de tablet te ontgrendelen. Een pincode instellen doet u onder Instellingen, Algemeen en Toegangscode.

Bij de instellingen van het codeslot vindt u tevens de optie 'Wis gegevens'. Als u deze inschakelt worden alle gegevens op de iPad gewist als iemand 10 keer een foute toegangscode invoert.

Touch ID

Als u een iPad Air 2 of iPad Mini 3 heeft beschikt uw tablet over een vingerafdrukscanner, ook wel beter bekend als Touch ID. De sensor, die uw vingerafdruk scant, is verwerkt in de Thuisknop. U hoeft dan alleen uw vinger hier op te leggen om uw iPad te ontgrendelen.

Om een vingerafdruk in te stellen gaat u naar Instellingen, Touch ID en toegangscode. Daar geeft u eerst een viercijferige pincode op, voor het geval de vingerafdruk niet herkend wordt. Vervolgens legt u uw vinger op de Thuisknop, totdat deze begint te trillen. Dit proces herhaalt u enkele malen, totdat uw iPad uw vingerafdruk heeft vastgelegd.

Automatisch slot

Tenslotte kennen iPads de optie 'Automatisch slot'. Hier stelt u in na hoeveel minuten uw iPad in de sluimerstand schiet. Eenmaal in de sluimerstand moet u opnieuw uw toegangscode opgeven om uw iPad te ontgrendelen. Tenminste, als u deze heeft opgegeven. U heeft de keuze uit 2 minuten, 5 minuten, 10 minuten, 15 minuten of nooit. Het automatische slot vindt u onder Instellingen, Algemeen en Automatisch slot.

Uw Android tablet beveiligen

Net als de iPad kennen de nieuwere Android tablets meerdere mogelijkheden om deze te beveiligen. De onderstaande beveiligingsopties vindt u onderInstellingen en Beveiliging.

Schermbeveiliging

De optie 'Schermbeveiliging' is wellicht de bekendste. In tegenstelling tot de iPad is een viercijferige pincode niet de enige beveiligingsoptie. U kunt er ook voor kiezen om een patroon te tekenen of een wachtwoord in te voeren met cijfers, letters en/of speciale tekens.

Automatisch slot

Hier geeft u aan na hoeveel seconden of minuten uw Android tablet op het automatische slot springt als hij in de sluimerstand overgaat. Ook kunt u aangeven dat de aan/uitknop uw tablet automatisch vergrendelt.

Smart Lock

Android 5.1 (Lollipop) kent een nieuwe beveiligingsoptie: Smart Lock. Met dit 'slimme slot' hoeft u geen pincode of wachtwoord in te voeren zolang uw smartphone in de buurt is, u zich op een 'vertrouwde plaats' begeeft (aan de hand van uw GPS locatie en tot 80 meter nauwkeurig), of uw gezicht of stem herkend wordt. Let wel: de laatste twee opties zijn minder accuraat dan de overige optie, zo waarschuwt Google.

Vingerafdrukscanner

Het aantal Android tablets met vingerafdrukscanner is op dit moment beperkt tot de eerste en tweede generatie Samsung Galaxy Tab S. Het instellen van een vingerafdruk en ontgrendelen van uw tablet werkt op dezelfde manier als bij de iPad.

Uw Windows tablet beveiligen

Als u alle stappen doorloopt tijdens het opstart- en installatieproces, dan heeft uw tablet een wachtwoord met cijfers, letters en of speciale tekens. Windows tablets kennen echter nog een aantal andere beveiligingsopties. Daarvoor opent u de charms bar door van rechts naar links te vegen op uw scherm. Vervolgens drukt u op Instellingen, PC instellingen wijzigen, Accounts en Aanmeldingsopties.

Afbeeldingswachtwoord

Hierbij kiest u een schermafbeelding en tekent u een patroon dat bestaat uit rechte lijnen, cirkels of tikken. De grootte, positie en richting van uw patroon zijn bepalend voor het inloggen.

Pincode

Met een viercijferige pincode ontgrendelt u snel een eenvoudig uw Windows tablet.

Wachtwoordbeleid

Deze beveiligingsoptie is te vergelijken met het automatische slot. U geeft hiermee aan na hoeveel minuten u uw wachtwoord opnieuw moet invoeren als uw Windows tablet in de sluimerstand verkeert.

Overige beveiligingstips

Tot slot nog een aantal algemene beveiligingstips voor uw tablet.

Gebruik een sterk wachtwoord

Gebruik geen bestaande woorden of zwakke wachtwoorden als 'password1234' of 'iloveyou'. Gebruik kleine letters, hoofdletters, cijfers en speciale tekens om het raden van uw wachtwoord zo moeilijk mogelijk te maken.

Gebruik een pincode of wachtwoord in plaats van een patroonIn het bedrijfsleven is dit de normaalste zaak van de wereld. Het nadeel van patronen is dat u strepen achterlaat met uw vingers op het scherm, die mogelijk uw geheime tekenpatroon verklappen.

Noteer uw wachtwoord

Schrijf het op een papiertje of bewaar het in uw cloud (niet overduidelijk onder wachtwoord uiteraard). Mocht u het dan een keer vergeten of kwijtraken, dan heeft u hem zo weer teruggevonden.

Vergrendel uw tablet op afstand

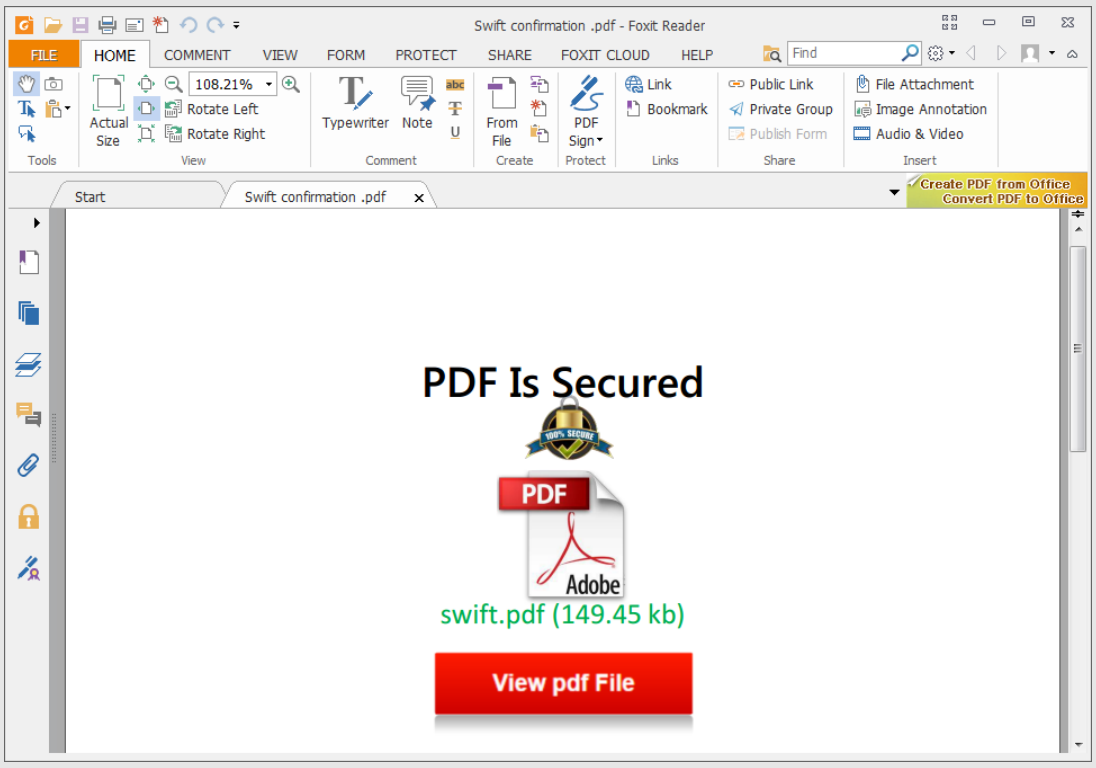
Bent u uw tablet kwijt of is deze gestolen, dan kunt u deze op afstand vergrendelen of uw gegevens wissen. Daarvoor gaat u naar Android Apparaatbeheer (Android tablets), de Verloren-modus (iPad) ofMicrosoft Account (Windows tablets).

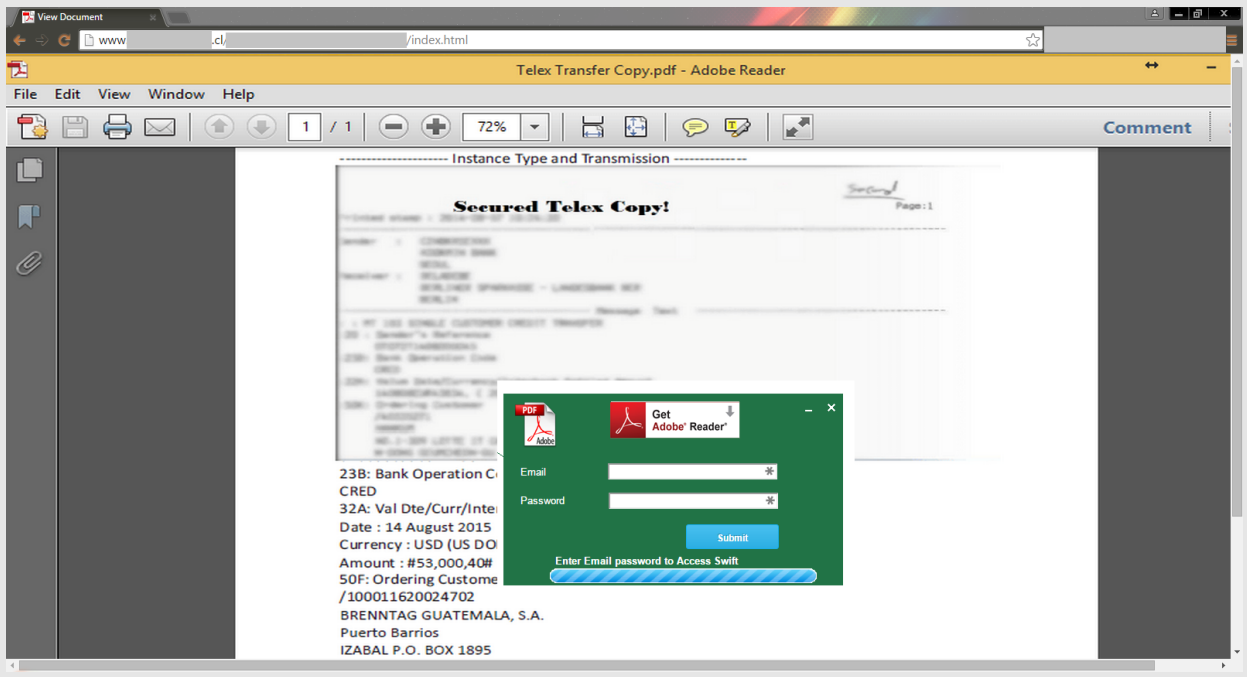
PDF-documenten worden regelmatig gebruikt om computers met malware te infecteren, maar cybercriminelen gebruiken het bestandsformaat nu ook om slachtoffers naar phishingsites te lokken. Onderzoekers van Kaspersky Lab ontdekten een PDF-document dat via een e-mailscam wordt verspreid

Phishing-springplank verstopt in PDF-documenten

Volgens de e-mail heeft de ontvanger van het bericht 53.000 dollar op zijn rekening ontvangen. Wel moet de ontvanger de transactie bevestigen, wat via het meegestuurde PDF-document kan. Het PDF-document bevat alleen een afbeelding die stelt dat het document beveiligd is en biedt de gebruiker een knop om de inhoud te bekijken. De knop wijst echter naar een phishingsite die er als een PDF-document met transactiegegevens uitziet.

Om de gegevens te bekijken moet de gebruiker vervolgens zijn e-mailadres en wachtwoord invullen. Deze gegevens worden naar de criminelen gestuurd. Volgens analist Dmitry Bestuzhev is dit een interessante techniek die sommige phishingfilters kan misleiden.





Bron: Security.nl

Index

De directeur van een Russisch bedrijf dat encryptiesoftware ontwikkelt is aangevallen door een groep die zich eerder bezighield met het aanvallen van NAVO, het Witte Huis en het Duitse parlement. Dat claimt het Japanse anti-virusbedrijf Trend Micro. Het zou om een groep Russische spionnen gaan.

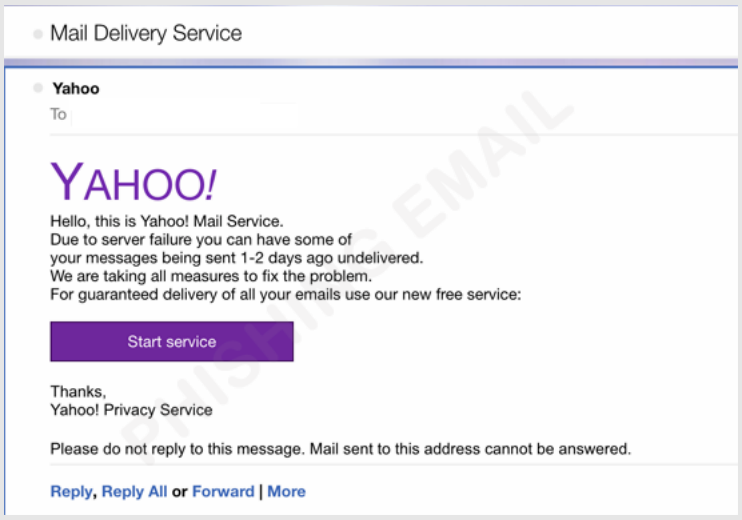
Ontwikkelaar encryptiesoftware doelwit van cyberspionage

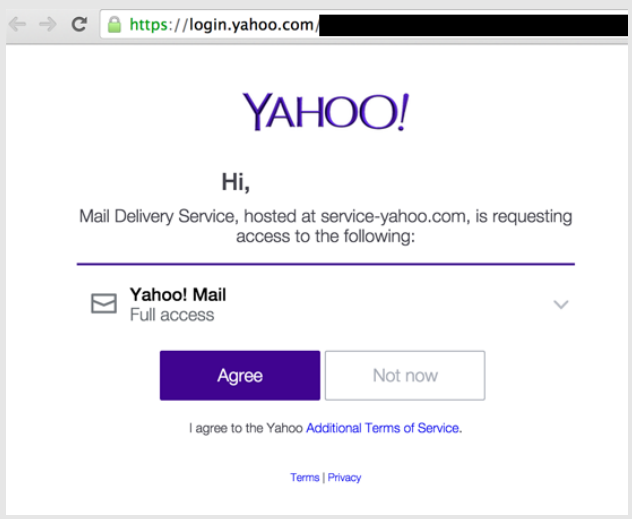
Hoewel verschillende organisaties in het buitenland het doelwit van de groep waren, worden er ook aanvallen binnen Rusland uitgevoerd. Het gaat dan om phishingaanvallen waarbij er op geraffineerde wijze wordt geprobeerd om inloggegevens van e-mailaccounts te stelen. Volgens Trend Micro zijn leden van de rockband Pussy Riot, politici, journalisten en softwareontwikkelaars het doelwit geweest. Naast de directeur van het bedrijf dat encryptiesoftware ontwikkelt werd ook een ontwikkelaar van de webmaildienst Mail.ru aangevallen.

Phishing

De aanvallen op de Russische personen waren onderdeel van een grotere campagne waarbij tienduizenden mensen met phishingmails werden bestookt. Het gaat dan om gebruikers van bekende webmailproviders zoals Gmail, Yahoo, Hushmail, Outlook en andere providers in de Oekraïne, Iran, Noorwegen en China. De manier waarop de aanvallen plaatsvinden verschilt. Sommige campagnes maken gebruik van malware en beveiligingslekken. De groep aanvallers heeft in het verleden tenminste zes zero day-lekken toegepast.

Daarnaast worden ook gerichte phishingaanvallen ingezet om inloggegevens te bemachtigen. De phishingmails beweren bijvoorbeeld dat er een nieuwe dienst is om e-mails gegarandeerd af te leveren. Vervolgens wordt geprobeerd om via OAuth, een open authenticatieprotocol dat bijvoorbeeld Yahoo aan app-ontwikkelaars aanbiedt, om toegang tot de mailbox van de gebruiker te krijgen. De links in het phishingmail wijzen daarbij naar een legitieme website van Yahoo voor OAuth. Daardoor kunnen gebruikers denken dat het om een onschuldige link gaat. Wat het doel is van de aanvallers weet Trend Micro niet, maar proberen ze mogelijk om potentiële dreigingen voor Rusland in de gaten te houden.

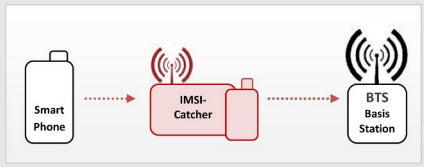




Bron: Security.nl

Index

Minister Kamp van Economische Zaken wil dat de Fiscale Inlichtingen en Opsporingsdienst FIOD zelf prepaid-telefoons en andere toestellen kan aftappen. Dat blijkt uit een conceptregeling die de minister ter consultatie online heeft gezet. De regeling geeft de FIOD de bevoegdheid om IMSI-catchers in te zetten.



Minister wil dat FIOD prepaid-telefoons kan aftappen

Daarmee is te achterhalen wie een bepaalde telefoon gebruikt. Bij veel onderzoeken van de FIOD zouden criminelen prepaid-telefoons gebruiken. Voorheen was de FIOD afhankelijk van de Nationale Politie om dit soort apparatuur te gebruiken. Volgens de minister blijkt dat de beschikbaarheid van zowel de apparatuur als van de bevoegde ambtenaren niet altijd aansloot bij de behoefte van de FIOD.

Impact

Kamp stelt dat de verwachte gevolgen voor burgers, bedrijven en milieu "nihil" zijn, aangezien de wijziging slechts tot een beperkte uitbreiding zal leiden van het aantal mensen dat dit soort apparatuur mag gebruiken. "Deze wijziging heeft geen gevolgen voor de regeldruk. De bevoegdheden van de FIOD worden uitgebreid", zo laat de minister weten. Dat houdt in dat de FIOD zelf de apparatuur mag aanschaffen en in de buurt van een verdachte mag gebruiken.

Een IMSI-catcher doet zich voor als een gsm-mast en misleidt op die manier de telefoons die in de buurt zijn. Als het toestel zich aanmeldt kan de IMSI-catcher een speciale code achterhalen die aan het telefoonnummer is gekoppeld. Daarmee kan de FIOD vervolgens de telefoon volgen en afluisteren. Kamp hoopt dat de maatregel helpt bij de bestrijding van fiscale, financieel-economische en goederenfraude. Tot 18 september kan erop het voorstel worden gereageerd. Het kabinet kan de maatregel zonder goedkeuring van de Eerste of Tweede Kamer invoeren.



Bron: Security.nl

Index

Een groep criminelen die zich bezighield met fraude met internetbankieren heeft bij slachtoffers thuis de simkaarten van hun mobiele telefoon opgehaald. De verdachten hadden die nodig om via mobiel internetbankieren de spaarrekeningen van vooral oudere slachtoffers te plunderen, zo meldt het OM.

Bende haalde simkaarten op voor fraude met internetbankieren

De slachtoffers ontvingen nagemaakte brieven die van hun provider afkomstig leken. De simkaart werd vervolgens opgehaald door iemand die zich in het tenue van een koeriersdienst had gekleed. Voordat de operatie met de simkaart plaatsvond hadden de criminelen al een phishingmail en nepbrief van de bank verstuurd en waren de slachtoffers opgebeld door iemand die zich voordeed als bankmedewerker.

Hoewel phishingmails normaal worden gebruikt om inloggegevens te stelen, stelt het OM dat met de phishingmails de computer van slachtoffers werd gehackt. Via de nepbrief van de bank werd geprobeerd de bankpassen van de slachtoffers in handen te krijgen en soms probeerden de verdachten ook nog om de simkaart uit de mobiele telefoon van slachtoffers te bemachtigen.

Volgens de officier van justitie zijn vooral oudere mensen het slachtoffer van de criminelen geworden, omdat ze vaak goedgeloviger zijn en meer geld op hun spaarrekening hebben staan. Inmiddels zijn zeker zes zaken uit diverse plaatsen in het land getraceerd, waarbij het om tienduizenden euro's schade gaat. De aangehouden verdachten zijn drie mannen van 20, 25 en 26 jaar oud uit Veenendaal en Rotterdam, en een vrouw van 25 uit Rotterdam. Ze werden begin juni aangehouden. Twee van hen zitten nog vast.



Bron: Security.nl

Index

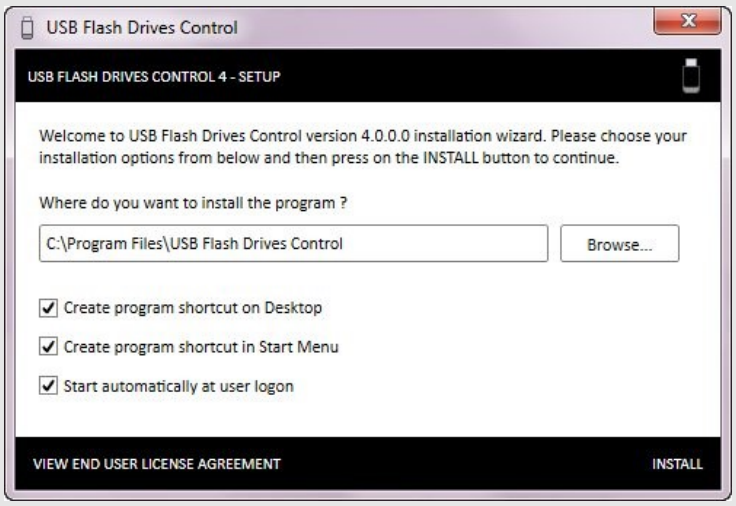
Slechts één op tien medewerkers in bedrijven controleert een usb-stick die door anderen is gebruikt op virussen. Het actua programma NOVA liet 80 usb-sticks zo gezegd 'per ongeluk' achter bij bekende organisaties.

Controleer de bevoegdheden van USB-sticks

Iedere geheugenstick was vooraf geprepareerd met een tool die stiekem informatie zou versturen over de computer waar hij werd in gestopt. Binnen de kortste keren werden twintig van deze sticks in bedrijfscomputers geplugd en maakte de programma's op deze sticks verbinding met het internet om aan hun spionagewerk te beginnen. Mobiele gegevensdragers vormen een risico als je niet zeker weet wat er op staat. USB Flash Drives Control doet precies wat de naam laat vermoeden, het legt de bevoegdheden van dit usb-flashgeheugen aan banden.

STAP 1 / Installatie

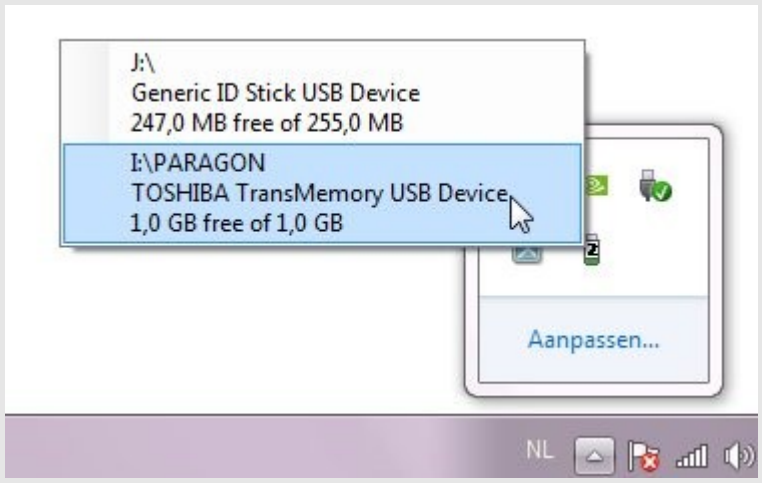
Haal het programma van www.binisoft.org/usbc.php en open de installer. Tijdens de installatie verschijnt er een venstertje met drie opties. Mag er een snelkoppeling op het bureaublad komen? Mag er een snelkoppeling in het Start Menu? En mag het programma



automatisch opstarten wanneer je de computer aan zet? Die laatste optie is een aanrader omdat de meeste gebruikers anders toch vergeten het programma te activeren. Daarna nestelt USB Flash Drives Control zich in het systeemvak vanwaar je deze tool aanspreekt met de linker- en rechtermuisknop.

STAP 2 / Linkermuisknop

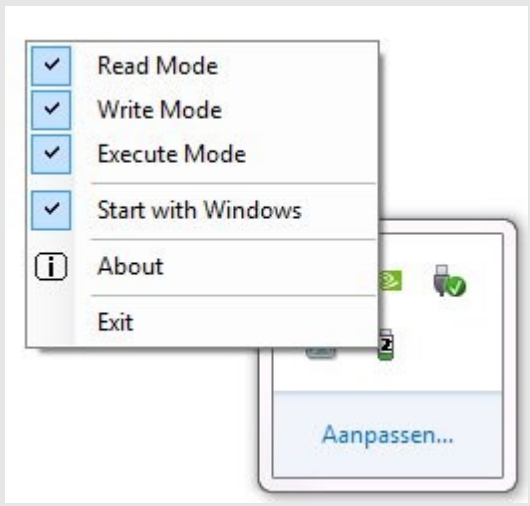
Wanneer je in het systeemvak met de linkermuisknop op het icoon van deze tool klikt, lees je hoeveel usb-sticks in de computer zitten. Je krijgt telkens de schijfletter te zien van het usb-station, je leest de naam van de stick en je ziet hoeveel vrije schrijfruimte er is. Wanneer je



dan nog een keer op de naam van flash drive klikt, opent Windows Verkenner de inhoud van deze gegevensdrager in een nieuw venster en heb je toegang tot de bestanden op de stick.

STAP 3 / Beheerder

Om de bevoegdheden van het usb-flashgeheugen in te perken, gebruik je de rechtermuisknop en klik je op hetzelfde icoon. Deze bevoegdheden slaan op Read Mode, Write Mode en Execute Mode. De opties die je hier zo dadelijk zal instellen gelden niet alleen voor jou, maar ook voor alle gebruikersaccounts op deze computer. Wanneer je als beheerder je account beschermt met een degelijk wachtwoord, kunnen andere gebruikers de instellingen van deze bescherming niet wijzigen. Bovendien gelden de instellingen voor alle usb-



flash drives die een gebruiker in de computer zal planten, je kan dus niet aangeven dat je stick A meer vertrouwt dan stick B.

STAP 4 / Lezen - schrijven

Wanneer je de optie Read Mode uitvinkt, zullen de verwisselbare gegevensdragers die je via de usb-poort inplugt niet langer tevoorschijn komen op de pc. Geen enkele gebruiker zal bijgevolg gegevens kunnen lezen van zo'n flash drive. Schakel je alleen de Write Mode uit, dan zullen deze usb-gegevensdragers uitsluitend in alleen-lezen modus verschijnen. Niemand zal dus gegevens kunnen wegschrijven of bestanden kunnen kopiëren naar zo'n geheugenstaafje. Al deze instellingen zijn van toepassing op de usb-sticks die je vanaf nu inplugt. Ze gelden dus niet voor de usb-flash drives die op dit moment al in de pc zitten.

STAP 5 / Uitvoeren

We hebben het al vaak gehad over zogenaamde 'portable apps', meestal kleine toepassingen die je rechtstreeks vanaf een usb-stick laat werken. Zo'n usb-staafje met reparatiesoftware is reuzehandig wanneer je de eigen of andermans computer moet herstellen. Toch zijn er ook goede redenen om net te vermijden dat toepassingen hun ding beginnen doen vanop zo'n stick, vooral als je niet precies weet wat er op deze gegevensdrager staat. Schakel je de Execute Mode uit, dan zal het systeem alle toegang weigeren aan processen die uitgevoerd worden vanaf de usb-gegevensdrager. Hiermee voorkom je het automatisch opstarten van schadelijke software die op een usb-stick is terechtgekomen.

Bron: Webwereld

Index

Wie dacht dat zijn auto ontgrendelen veilig was, heeft het mis. Met een simpel en goedkoop toestelletje kunnen hackers je auto stelen.

Hackers stelen je auto wanneer je hem ontgrendelt

Wie zijn auto ontgrendelt, denkt dat alle gevaar geweken is. Het voertuig staat er immers nog, dus je beveiliging heeft zijn werk gedaan. Alweer een goeie dag, zonder incidenten. Je klikt op je sleutel om je wagen te ontgrendelen en je vertrekt naar huis, je werk, je pedicure. Het moment dat je je auto ontgrendelt, begint het gevaar echter.

Samy Kamkar, een bekende hacker die beveiligingsproblemen wil aantonen met zijn vernuft, bedacht namelijk een klein apparaatje dat je zelf in elkaar kan vijzelen met slechts 30 euro aan materiaal. De Rolljam, zoals hij het noemt, stelt hem in staat om je auto-ontgrendeling over te nemen, en het werkt zelfs met garagepoorten. Hij stelde zijn uitvinding voor op Defcon 2015.



Vaste code

Het gaat heel eenvoudig in zijn werk: je komt aan je auto, je drukt op ontgrendelen en je merkt dat het niet werkt. Je probeert nogmaals en je deur gaat alsnog open. Geen probleem denk je dan, maar het kwaad is geschied: de hacker heeft je beveiligingscode en kan volgende keer zijn slag slaan.

Normaal gezien zou het niet mogen werken omdat autobouwers een stevige veiligheid hebben ingebakken in hun systemen. Vroeger kwam dit soort praktijken vaak voor dankzij de vaste code die de sleutels verzonden. Reeds enkele jaren is die vaste code echter ingewisseld voor een wisselende code. Je sleutel verstuurt met andere woorden nooit twee keer dezelfde code.

Rollende code

Telkens je op ontgrendelen drukt, of je nu in de buurt van je auto bent of niet, wordt een code verstuurt vanaf je sleutel. Daarna wordt overgegaan naar de volgende code. Dat je per ongeluk op ontgrendelen drukt wanneer je niet in de buurt bent, en je auto later toch nog opengaat, komt doordat de ontvanger (je auto) een honderdtal codes klaar heeft staan die het kan ontvangen. Druk je dus honderd keer 'per ongeluk' op ontgrendelen, zonder ontvanger in de buurt, dan krijg je waarschijnlijk je auto niet meer open en moet je de garage bellen.

Kamkars toestelletje weet deze wisselende code toch te omzeilen. Door twee goedgeplaatste radio's wordt je signaal geblokkeerd en opgevangen door een derde. Wanneer je een tweede keer drukt, gebeurt hetzelfde, maar stuurt het toestelletje de eerste code toch naar je wagen. Zo is jouw wagen ontgrendelt, en beschikt de hacker over de volgende code.

Als dit apparaat niet ontdekt wordt, kan de hacker zo codes vergaren, zodat hij altijd beschikt over één werkende code. Volgens Kamkar zijn onder andere wagens van Nissan, Ford, Toyota en Volkswagen in gevaar. Met garagepoorten werkt het net zo goed. Autofabrikanten zijn al enkele tijd op de hoogte van het probleem, maar lijken zich vooralsnog niet te haasten om het euvel te verhelpen. Wel zijn er naar verluidt al enkele fabrikanten die overschakelen op een nieuw systeem.



Bron: Security.nl

Index

Achter het raam of in een privéclub tref je vrijwel geen minderjarige prostituees (meer) aan, zeggen deskundigen. Maar op internet?

Hoe oud is “Sexy Annabel”

Daar staan contactsites als Kinky en Sexjobs nog barstensvol advertenties à la ‘young sexy blond girls with nice boobs’ en ‘superknap sletje, net 18, 50 euro all-in’. De advertenties melden expliciet wat de mogelijkheden zijn: pzc, groepsseks, plasseks. En hoewel de exploitanten graag meewerken met politie en OM, is het aanbod te groot om er grip op te houden. Sexjobs zegt dertigduizend nieuwe advertenties per maand te hebben, en elke dag zestigduizend bezoekers.

Bij Kinky gaat het om achtduizend advertenties per maand en 130 duizend bezoekers per dag. Het is al enkele jaren duidelijk dat prostitutie voor een groot deel naar internet verschoven is en dat daarmee ‘de gedwongen prostitutie verder weggezakt is in de schemer van de illegaliteit’.

De genoemde sites staan onder druk na enkele geruchtmakende zaken (Valkenburg, Kerkrade, Amsterdam) waarin pooiersboys voor minderjarige meisjes accounts maakten, foto’s plaatsten, afspraken regelden en (vooral) grof geld verdienden. Volgens vrouwenhandel-officier Warner ten Kate is het gebruik van zulke advertentiesites ‘betrekkelijk nieuw’ en is het ingewikkeld om advertenties te herleiden naar personen.

De sites zijn daarom genoodzaakt zelf ‘hun verantwoordelijkheid te nemen’. Vooral vanwege hun imago en het risico voor sluiting. ‘We zijn in gesprek. Wij hebben hen ook nodig’, aldus Ten Kate van het OM.

Kinky heeft daarom een ‘deurbeleid’: adverteerders moeten 21 zijn en dat met een id-bewijs aantonen. Ook de exploitanten van de sites, van het bedrijf Midhold, zien het terugdringen van illegale internetprostitutie als een gezamenlijk belang.

Beide sites hebben protocollen, die ‘niet waterdicht’ zijn maar wel bewustwording creëren bij adverteerders en prostituees. ‘Dat is al heel wat’. Dit jaar gaven de twee websites al tien zaken aan de politie door. En ‘zeker twee keer per week’ krijgen ze een vordering voor gebruikersgegevens.

Mede-aandeelhouder Wang Ko van Sexjobs zegt gewoon een advertentieplatform te zijn. ‘Wij balen er ook van dat ons platform wordt misbruikt door criminelen’. Voor het OM was het ook even wennen, om met deze exploitanten te praten. ‘Om alleen al te gaan kijken op die sites moet je een brug over, maar we moeten afdalen uit onze ivoren toren, want beleid op papier maken is één ding, de uitvoering is wel wat anders. Dit gaat allemaal over de voorkant van de zaak, wij zien normaal gesproken alleen de achterkant’, zegt Ten Kate.

Bron: Cops in Cyberspace

Index

Het gaat niet goed met de Bitcoin. Niet met de koers, maar ook het protocol erachter zit in de problemen. De digitale munt dreigt op te splitsen in twee 'forks', waardoor het decentrale karakter van de valuta dreigt te verdwijnen.

Problemen in Bitcoin-land: Wat is er aan de hand?

Het is al weken hommeles in Bitcoin-land. Dat zucht namelijk onder zijn eigen populariteit, want door het grote aantal gebruikers en transacties is het huidige werkmodel niet meer houdbaar.

Het probleem

Een essentieel onderdeel van de Bitcoin is de blockchain, een 'ketting' waarin alle transacties van de digitale munt worden opgenomen. De blockchain moet constant worden geüpdate, zodat iedere gebruiker altijd de meest actuele informatie heeft over welke Bitcoins waar zijn uitgegeven.



Je kunt je voorstellen dat die blockchain steeds groter wordt naarmate er meer transacties worden gedaan. Dat is nu een probleem aan het worden, want de blocks zijn inmiddels te groot. Een block kan maximaal 1 MB zijn. Dat was bij de oprichting van de Bitcoin nog niet zo'n probleem, maar dat was voordat de munt zo populair werd.

Er wordt nu ongeveer iedere 10 minuten een nieuwe block aan de blockchain toegevoegd. Dat betekent dat er steeds meer bandbreedte nodig is om Bitcoins te mijnen of zelfs te houden - niet erg realistisch.

Het dilemma

Er moet daarom iets gebeuren bij de Bitcoin, dat is zeker. Maar wát er moet gebeuren, daarover zijn de meningen verdeeld. In ieder geval moeten de blocks in de blockchain groter worden gemaakt, maar het is vooral de manier waarop dat gebeurt, en de frequentie, die zorgen baren. In september staat er een congres gepland van de Bitcoin Foundation (de oprichters van de munt), waarin de ontwikkelaars praten over de mogelijk stappen.

Om de grotere vraag aan te kunnen, is het volgens veel Bitcoin-adepten nodig om in te grijpen. Dat kan bijvoorbeeld in de vorm van hogere transactiekosten bij het kopen van Bitcoins, of het opzetten van betaalhubs. Daarmee wordt Bitcoin echter steeds meer als een bank, waarbij één of een aantal autoriteiten de valuta aansturen. Dat gaat volgens een deel van de oprichters in tegen het decentrale karakter van de munt.

Dat is niet alleen een praktisch probleem, maar ook een probleem in hoe Bitcoin nu wordt gerund. Dat gebeurt namelijk door een grote groep (semi-)vrijwillige ontwikkelaars, die geen baas hebben, geen verdienmodel, geen winstoogmerk en geen enkele motivatie behalve een idealistische.

Die gemeenschap is in twee kampen verdeeld. Dat wordt goed beschreven door Mike Hearn, één van de oprichters van de nieuwe Bitcoin-fork. Hij legt in een blogpost uit wat de verschillen tussen de beide kampen zijn.

Een kleine groep ontwikkelaars trekt nu aan de bel, want zij vinden dat de munt niet verder kan steggelen zoals dat nu gaat. Gavin Andresen en Mike Hearn, twee van de belangrijkste originele ontwikkelaars van de munt, willen zich daarom afsplitsen van de Bitcoin-beweging.

Hearn en Andresen zijn daarom aan de slag gegaan met een tweede protocol, genaamd Bitcoin XT. Dat is gebaseerd op de open sourcecode van de originele Bitcoin, die voor iedereen in te zien is. Op het eerste gezicht is de nieuwe fork exact hetzelfde als de originele Bitcoin, maar er ontstaan daardoor wel twee verschillende blockchains.

Het grote verschil is dat de grootte van de blocks is veranderd. Die worden (bij Bitcoin XT) vanaf 11 januari 2016 8 MB groot, maar de grootte verdubbelt iedere 2 jaar tot de blocks een limiet van 8,912 MB hebben bereikt.

Volgens Hearn en Andresen is een dynamische verandering in de grootte (die dus iedere 2 jaar verandert) de enige manier om de Bitcoin succesvol te maken. Met de Wet van Moore in het achterhoofd is het namelijk een kwestie van tijd voor ook de nieuwe grootte van 8 MB bereikt is.

Bovendien, zeggen de oprichters van Bitcoin XT, kan de munt ineens sterk in populariteit stijgen zoals dat in 2013 en 2014 gebeurde. Door toenemende media-aandacht werd de munt ineens veel meer waard, en gingen meer mensen Bitcoins gebruiken. Ook tijdens de Griekse crisis was goed te zien hoe de munt even in waarde steeg.

De complicaties

Het nieuwe systeem heeft echter geen ondersteuning van het ecosysteem dat Bitcoin wel heeft. Door de jaren heen zijn er tientallen Bitcoin-handelsplaatsen ontstaan (waarmee het niet altijd even goed ging), en die werken allemaal onderling samen op één protocol.

Bitcoin TX is echter zo anders, dat oude mijn-computers niet meer kunnen samenwerken met het protocol. In dat geval zal de gebruiker van zo'n mijn-computer moeten kiezen: Blijft hij 'gewone' Bitcoins mijnen, of toch de nieuwe?

Bron: PCM web

Index

Wilt u upgraden naar Windows 10, dan zijn er een aantal zaken die u kunt doen ter voorbereiding. Met een slimme voorbereiding stapt u straks probleemloos over op Windows 10.

Windows 10

1. Controleer of uw computer geschikt is

Om er zeker van te zijn dat u computer geschikt is voor een upgrade naar Windows 10 raden we u aan dit te controleren. Als u uw computer of tablet wilt upgraden naar Windows 10, heeft u het volgende nodig:

- **Nieuwste besturingssysteem:** Zorg dat deze laatste versies zijn geïnstalleerd: Windows 7 SP1 of Windows 8.1 Update.
- Weet je niet welke versie is geïnstalleerd, kijk dan hier.

Moet je de nieuwste versie downloaden? Klik hier voor Windows 7 SP1 of Windows 8.1 Update.

- **Processor:** 1 gigahertz (GHz) of sneller of SoC
- **RAM:** 1 gigabyte (GB) voor 32-bits of 2 GB voor 64-bits
- **Schijfruimte:** 16 GB voor 32-bits OS of 20 GB voor 64-bits OS
- **Grafische kaart:** DirectX 9 of nieuwer met WDDM 1.0-stuurprogramma
- **Beeldscherm:** 1024 x 600

De mogelijkheid om een apparaat te upgraden is niet alleen afhankelijk van de systeemspecificaties. Kijk hier voor alle vereisten.

Als ik nu een nieuwe computer koop, kan deze dan worden bijgewerkt naar Windows 10?
Ja, nieuwe, in aanmerking komende computers, zijn geschikt voor Windows 10. Windows 10 is ontworpen op compatibiliteit met elke laptop, tablet of desktop met Windows 8.1, die nu verkrijgbaar is. Fabrikanten beslissen uiteindelijk over de configuratie van hun apparaten. Bepaalde functies van Windows 10 zijn daardoor mogelijk niet op bepaalde apparaten beschikbaar. Vraag dit na bij de winkel of fabrikant.

2. Controleer of u een back-up van uw bestanden heeft

Windows 10 neemt bij de upgrade automatisch alle bestanden en documenten mee. Een back-up blijft natuurlijk altijd nodig. Bestanden als uw documenten, foto's en video's staan normaal gesproken in standaardmappen (zoals Documenten), maar misschien heeft u ze wel op een andere plek opgeslagen. Zorg dat u alle bestanden kopieert naar een back-uplocatie, bijvoorbeeld een externe schijf, USB stick of de OneDrive cloud. Bij OneDrive heeft u 15GB opslagruimte, waarvan u gratis gebruik kunt maken. Tip: vergeet niet ook de bestanden van andere gebruikers veilig te stellen.

Heeft u Windows 7, dan kunt u de ingebouwde back-upfunctie gebruiken. In Windows 7 opent u 'Back-up maken en terugzetten' via 'Start', 'Configuratiescherm', 'Systeem en onderhoud' en 'Back-up maken en terugzetten'. Klik op 'Back-up instellen' en volg de stappen in de Wizard.

3. Pak de gegevens van uw Microsoft account erbij

Windows 10 maakt gebruik van een Microsoft account. U kunt een Microsoft account vaak herkennen aan @hotmail.com of @outlook.com. U heeft straks uw e-mailadres en wachtwoord nodig. Het wachtwoord heeft u nodig om u na de upgrade weer aan te melden bij Windows en apps in de Windows Store te vinden. Heeft u nog geen Microsoft account? Maak er dan gratis eentje aan via www.outlook.com.

4. Controleer of u de installatiebestanden van uw programma's heeft

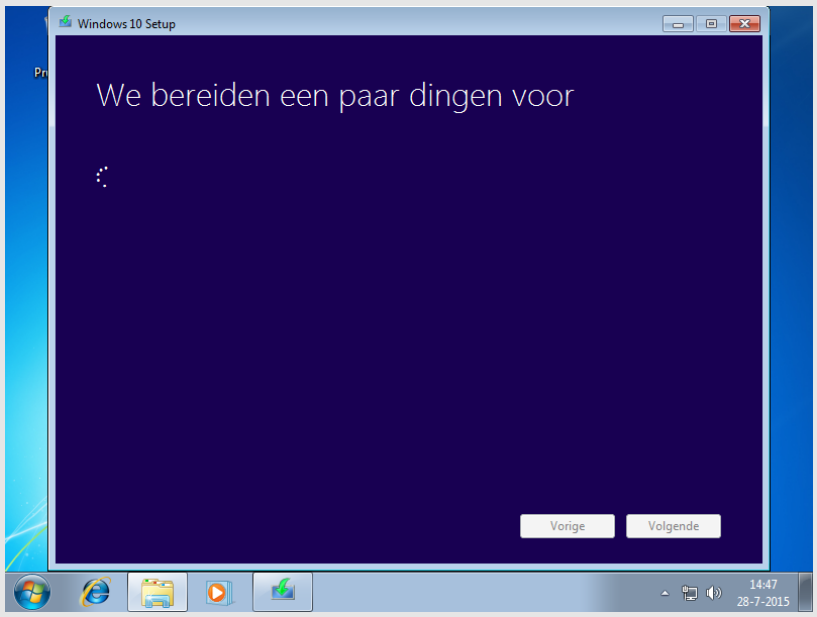


Eerlijk is eerlijk; sommige programma's moet u na de upgrade even opnieuw installeren. De installatiebestanden van uw programma's kunt u vaak downloaden via de website van de maker. Zo kunt u deze programma's straks na de upgrade naar Windows 10 gemakkelijk weer installeren.

5. Verwijder (tijdelijk) bestaande antivirusprogramma's

Veiligheid voor alles! Antivirusprogramma's beschermen uw apparaat en gegevens. Stapt u over naar Windows 10, verwijder dan eventuele bestaande antivirusprogramma's. Zo voorkomt u dat uw antivirusprogramma de installatie van Windows 10 'tegenhoudt'. Na de upgrade naar Windows 10 installeert u het antivirusprogramma opnieuw. Zorg dat u een eventuele licentiecode bij de hand heeft, zodat u de software snel kunt installeren. Ook goed om te weten: Windows 10 heeft een goede virusscanner ingebouwd!

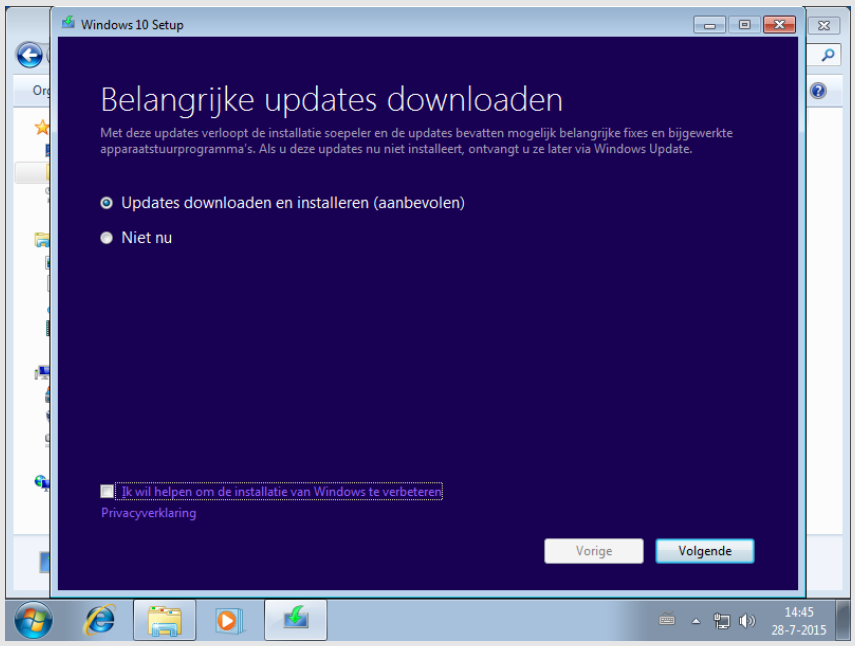
STAP VOOR STAP UPGRADEN NAAR WINDOWS 10

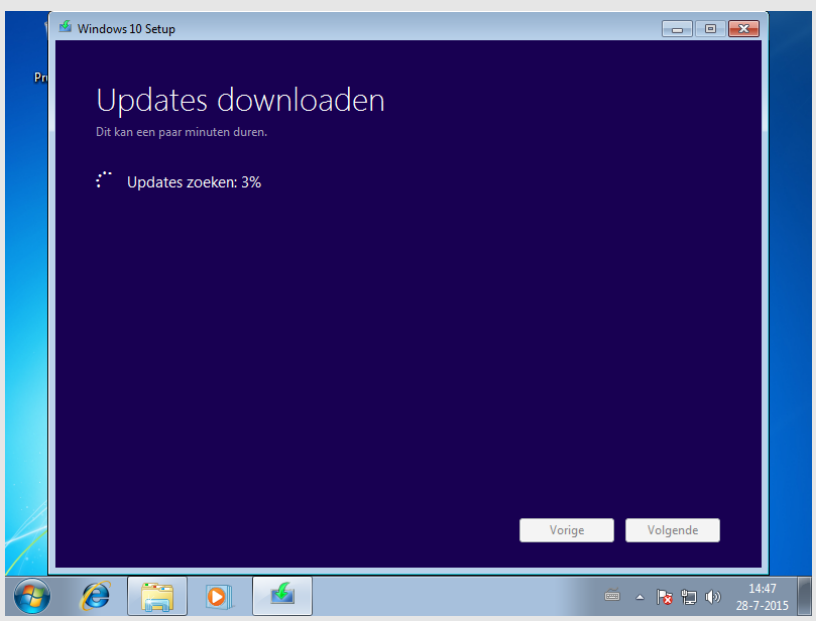


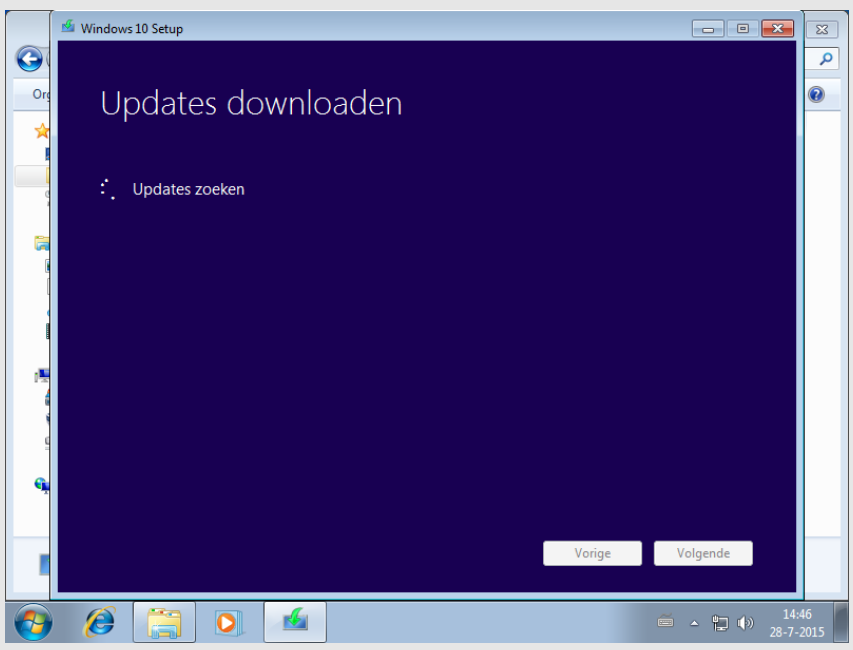
En dan is het zover, het daadwerkelijke upgraden. We laten hierna stap voor stap zien welke schermen u moet doorlopen bij het upgraden.

Allereerst worden er een aantal belangrijk updates gedownload, zodat u kunt upgraden naar Windows 10. Kies voor 'Updates downloaden en installeren' en klik op 'Volgende'.



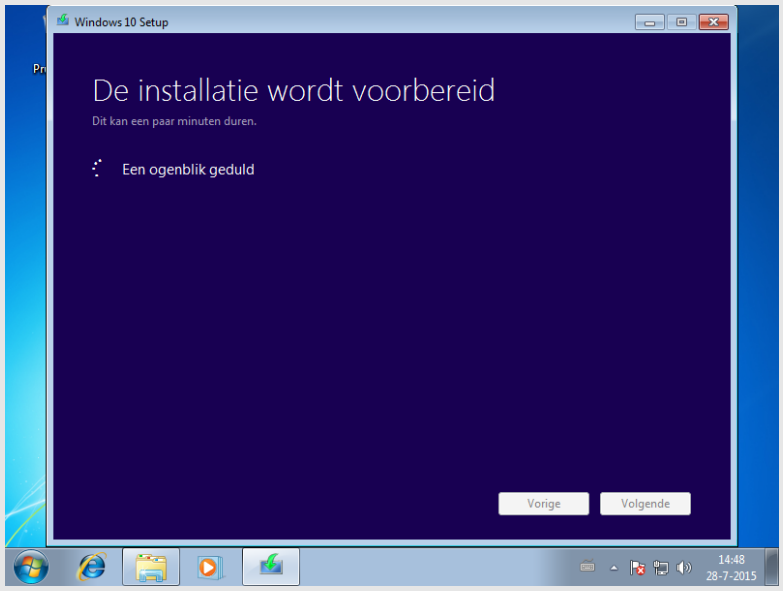






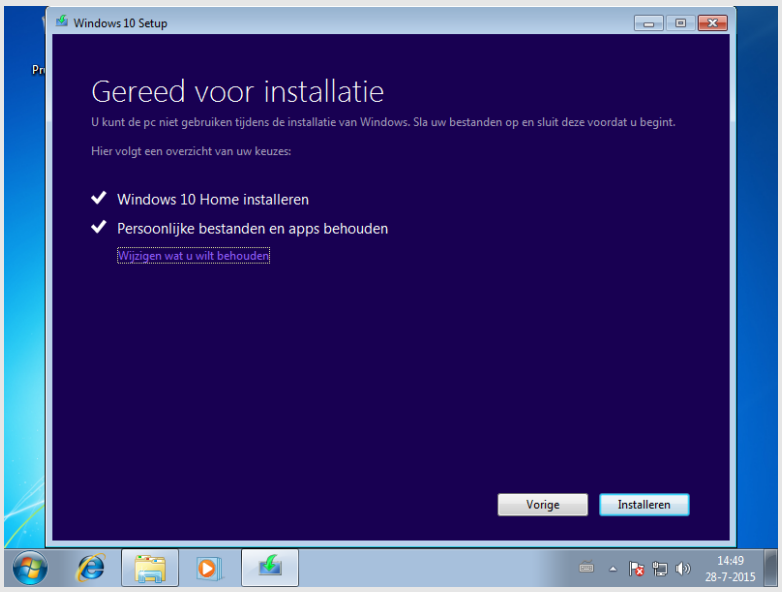
Bron: Paradigit

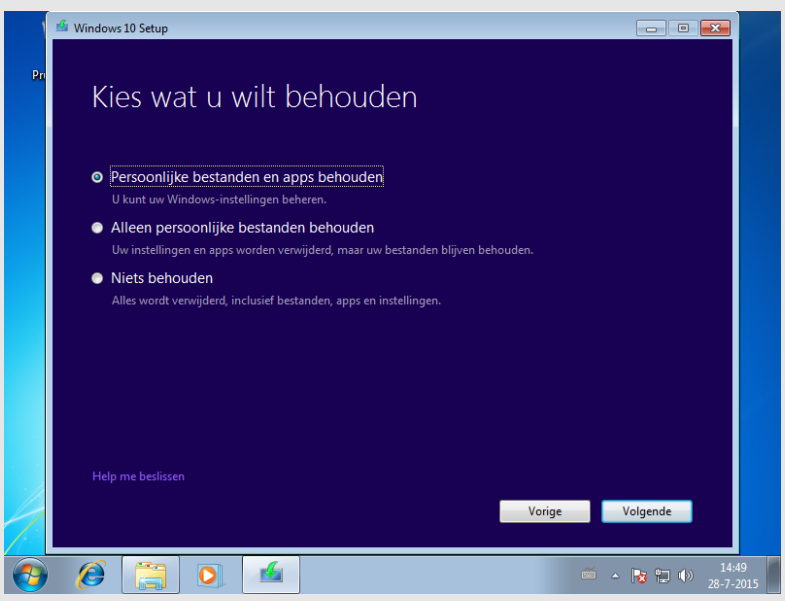
Index



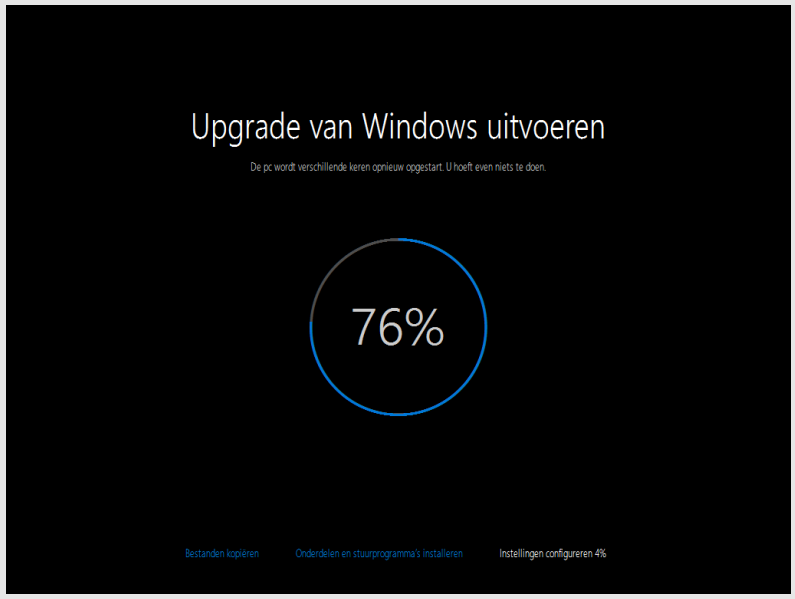


Uw computer is nu klaar voor installatie. Tijdens dit proces kunt u de computer niet gebruiken. Zorg dat u uw bestanden heeft opgeslagen en afgesloten. Klik op 'Wijzigen wat u wilt behouden' en selecteer wat u wilt behouden. Klik daarna op 'Volgende' en 'Installeren'.

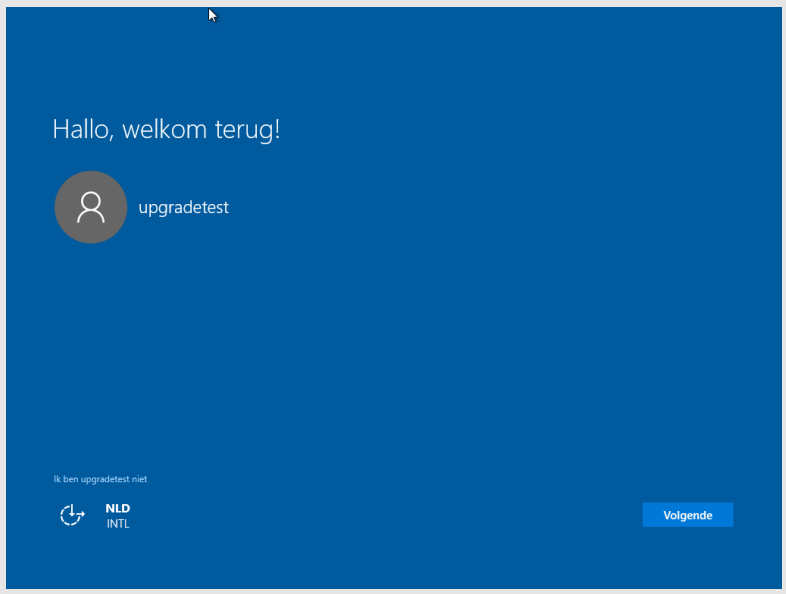




Windows 10 wordt nu geïnstalleerd. Dit kan even duren en uw computer wordt verschillende keren opnieuw opgestart. De upgrade zelf duurt gemiddeld één uur. Bij nieuwere apparaten kan dit 20 minuten zijn, bij oudere meer dan een uur. U kunt ondertussen gerust even iets anders gaan doen.



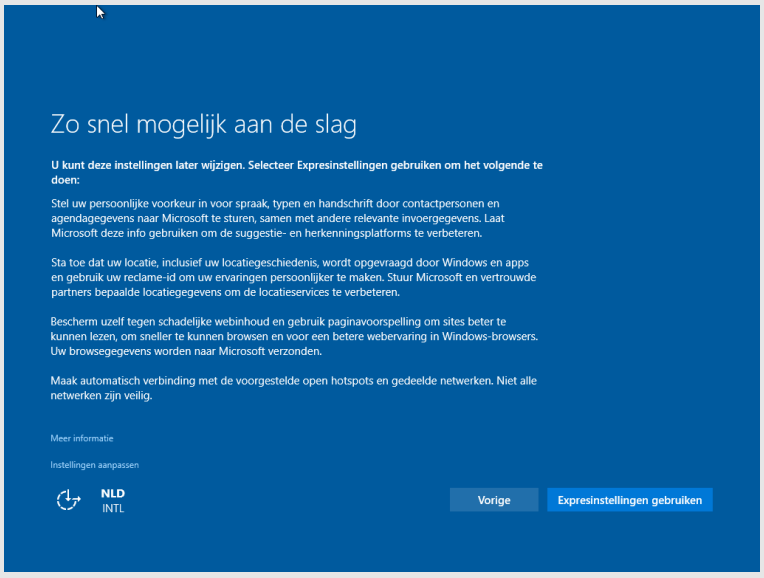
De installatie is voltooid. Check of uw gebruikersnaam klopt, pas deze aan indien nodig en klik op 'Volgende'.



Bron: Paradigit

Index

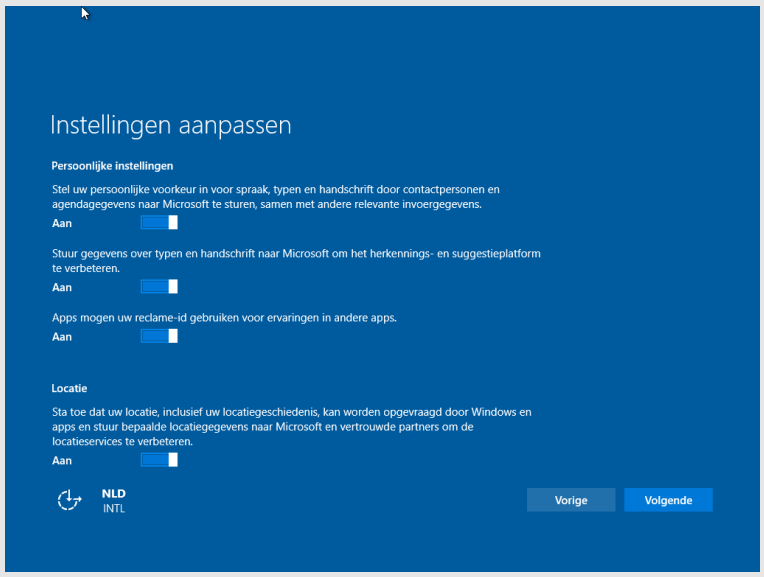
U kunt nu de instellingen aanpassen of voorlopig kiezen voor de Express instellingen.



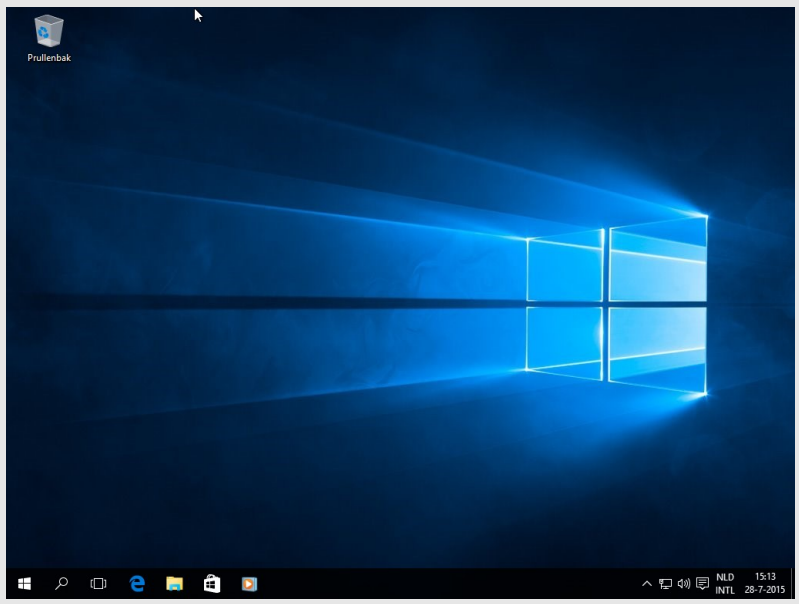
Uw apps worden nu geïnstalleerd.



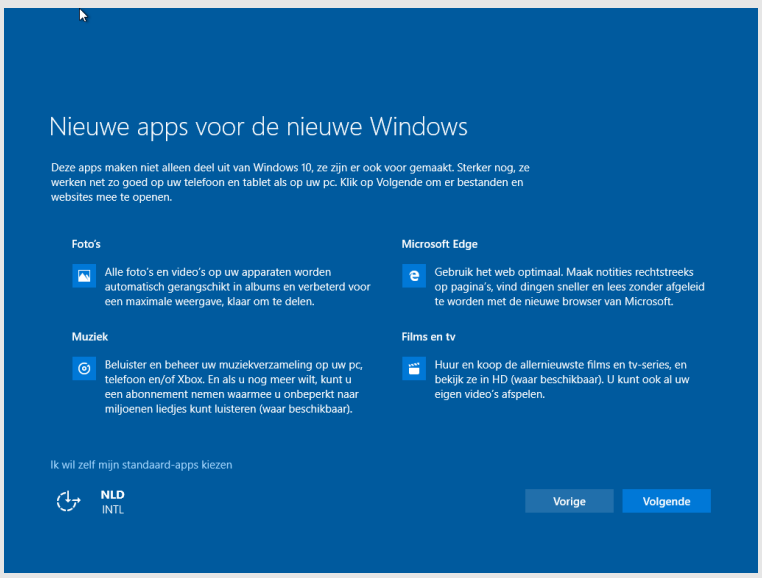
Kiest u voor het aanpassen van de instellingen, dan krijgt u het volgende scherm. Pas aan waar nodig en klik op 'Volgende'.

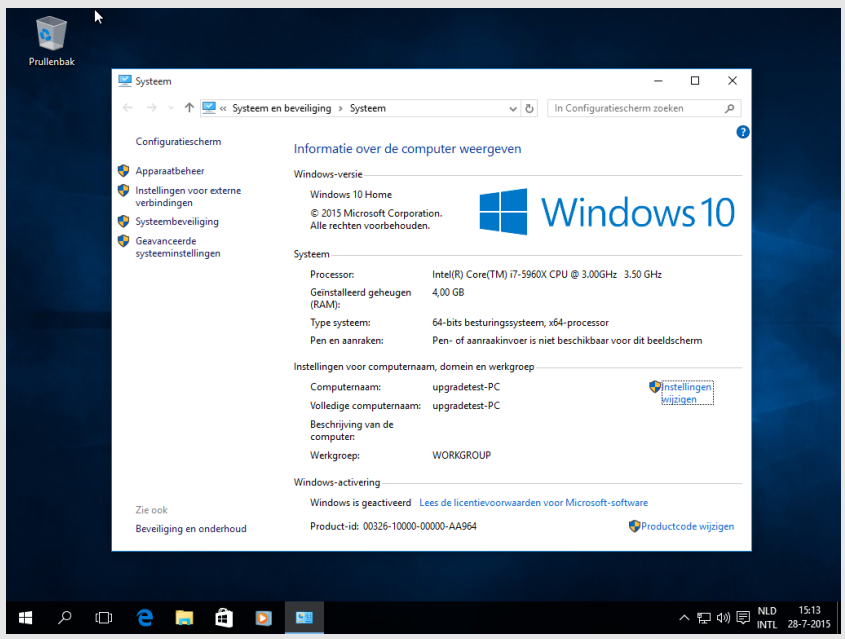


Klaar! U kunt nu op uw gemak Windows 10 gaan verkennen.



Kies indien gewenst uw eigen standaard apps of gebruik degene die Microsoft voor u geselecteerd heeft. Klik daarna op 'Volgende'.





Bron: Paradigit

Index

Windows 10 is uit. Overstappen is niet verplicht, maar Microsoft maakt de keuze een stuk gemakkelijker doordat het upgraden het eerste jaar gratis is. Dit geldt zowel voor gebruikers van Windows 7 als van Windows 8.1. Maar welke voordelen brengt die overstap met zich mee? Windows 10 niet of juist wél installeren.



DE VERSCHILLEN: 10 versus 7 & 8.1

Verbeteringen van Windows 10 ten opzichte van Windows 7

Voor wie Windows 7 gewend is, is de overstap naar Windows 10 niet zo'n 'schok' als de overstap naar Windows 8.1.

Windows 10 start razendsnel op. Het energiemanagement is ook stukken efficiënter, wat betekent dat laptopaccu's langer kunnen draaien. De exclusieve toegang tot DirectX 12 is voor gamers interessant.

- Het **nieuwe Startmenu** ziet er anders uit dan in Windows 7. Het bevat de 'tegels' die u misschien al heeft gezien in Windows 8.1. Als u het niet prettig vindt om daarmee te werken, kunt u ze met een druk op de rechtermuisknop verwijderen. U vindt onder de Start knop gewoon de programma's die u heeft geïnstalleerd en de opties om de computer in de slaapstand of uit te zetten.

- Windows 10 bevat de zogeheten **Universal Apps**. Dat zijn programma's die op al uw Windows apparaten draaien en synchroniseren: uw laptop, desktop, smartphone, tablet en Xbox. Via de Windows Store kunt u meer apps downloaden.

Internet Explorer gaat ophouden te bestaan. De **standaard browser** in Windows 10 heet **Edge**. Deze browser kan beter met de nieuwe standaarden overweg en biedt meer functies dan Internet Explorer, waaronder de mogelijkheid om (aan) tekeningen op webpagina's te maken en een 'sobere' versie van artikelen te bewaren om later zonder afleidingen te kunnen lezen.

- Om settings te veranderen is er nu de gebruiksvriendelijke **Settings app**. Toch kunt u er niet alles in configureren. Daarom bestaat het vertrouwde Controlepaneel nog steeds, waarmee u bijvoorbeeld oudere instellingen kunt wijzigen.

Op de **taakbalk** staan standaard een zoekveld en een icoon voor de taakweergave. Het **zoekveld** is zowel voor offline als voor online zoekopdrachten geschikt. De **digitale assistent Cortana** springt bij wanneer u een vraag intypt of via de microfoon stelt.

- Gebruikt u een desktop, dan zult u het prettig vinden dat **meerdere monitors** nu nóg beter ondersteund zijn. Indien gewenst kunt u elke monitor een eigen achtergrond, slideshow en taakbalk geven.

Het besturingssysteem Windows 10 neemt **minder geheugen en schijfruimte** in gebruik dan Windows 7. Dat maakt het ook voor gebruikers met een oudere computer interessant om de overstap te maken.

Verbeteringen van Windows 10 ten opzichte van Windows 8.1

Voor het oog is de omschakeling van Windows 8.1 naar Windows 10 even wennen. Microsoft heeft goed naar de feedback van toetsenbord en muisgebruikers geluisterd en deze meegenomen in een nieuwe versie, die vriendelijker is voor apparaten zónder touchscreen.

- Windows 10 gebruikt de 'tegel interface' nog wel, maar heeft deze nu achter de **teruggekeerde Startknop** verstopt. Als u de Tablet Mode activeert, bedekken de tegels weer het gehele scherm.

- In Windows 8.1 waren de apps uit de Windows Store fullscreen, wat overbodig was op pc's. In Windows 10 zijn de **vensters** er weer en bepaalt u zelf de grootte van openstaande programma's.

De **digitale assistent Cortana**, die voorheen alleen op smartphones beschikbaar was, komt dankzij Windows 10 ook naar de computers. Op de taakbalk staat een handige zoekbalk waarmee u snel in uw computer en online zoekt.

Windows 10 is stukken interessanter voor gamers. De Xbox app geeft u niet alleen toegang tot allerlei gamestatistieken, maar laat u ook games van de Xbox One naar de desktop streamen. Ook wordt **DirectX 12** ondersteund en kunt u de laatste dertig seconden van elke game die u speelt (oud of nieuw) opnieuw afspelen.

In Windows 10 ziet u niet langer Internet Explorer als standaard browser geïnstalleerd. In plaats daarvan is er de **nieuwe browser Edge**. Hierin kunt u aantekeningen op webpagina's maken, artikelen voor later bewaren en deze zonder afleidingen laten weergeven. Uiteraard kunt u naar keuze een andere browser, zoals Chrome of Firefox, gebruiken.

Samengevat heeft Microsoft alles wat het met Windows 8.1 fout deed weer **rechtgezet**. Wel is het zo dat u in snelheid niet veel verbetering zult merken, Windows 10 is namelijk op het fundament van Windows 8.1 gebouwd.

Bron: Paradigit

Index

Wie Windows 10 installeert met de aanbevolen standaardinstellingen, doet concessies aan zijn privacy. Gelukkig kun je eenvoudig betere instellingen kiezen.

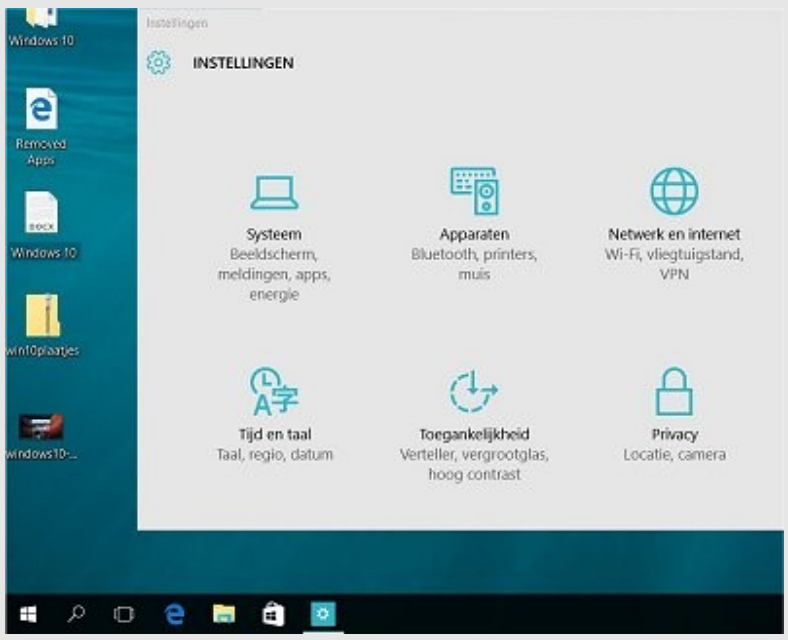
Windows 10: verbeter je privacy

De privacyopties aanpassen (na de installatie)

Uitschakelen van het nieuwsgierige gesnuffel kan gelukkig ook ná de installatie van Windows 10. Windows 10 beschikt namelijk over een nieuw Privacymenu waarin alle opties keurig op een rij staan (en waarin ook de privacyvoorwaarden aanklikbaar zijn).

Je vindt het Privacymenu via: Start > Instellingen > Privacy.

Afbeelding 1: Instellingen



Afbeelding 2: Privacyopties wijzigen



Doorloop alle submenu's van het privacymenu (klik op de links, zie afbeelding 2) en schakel alle privacyopties in een minder nieuwsgierige stand of uit.

Wifi-wachtwoorden delen (uitschakelen)

De wifi-wachtwoorden die je op de pc invoert en laat onthouden kun je standaard eenvoudig delen met al je 'vrienden' op sociale netwerken. Zo hoeven zij (en jij) minder vaak wachtwoorden in te voeren, want dat doet Windows 10 al voor je.

Het is een nieuwe functie in Windows 10 die in bepaalde situaties vast handig is maar ook wel een die een veiligheidsrisico met zich meebrengt. Het vergroot namelijk de kans dat je je wifi-netwerk deelt met mensen die je eigenlijk helemaal geen toegang wil geven. Als je iemand in goed vertrouwen toegang geeft tot je persoonlijk wifi-netwerk geef je feitelijk ook al zijn vrienden toegang.

De 'sociale wifi-toegang' maakt geen onderdeel uit van het Privacymenu maar is wel uit te schakelen, via:

Start > Instellingen > Netwerk en internet > Wifi-instellingen beheren > Wifi-inzicht.

Kijk bij 'Netwerken die ik selecteer, wil ik delen met mijn' … En haal de vinkjes weg bij: Outlook.com contacts, Skype contacts, Facebook friends en alle andere diensten die je daar ziet.



Bron: Consumentenbond

Index

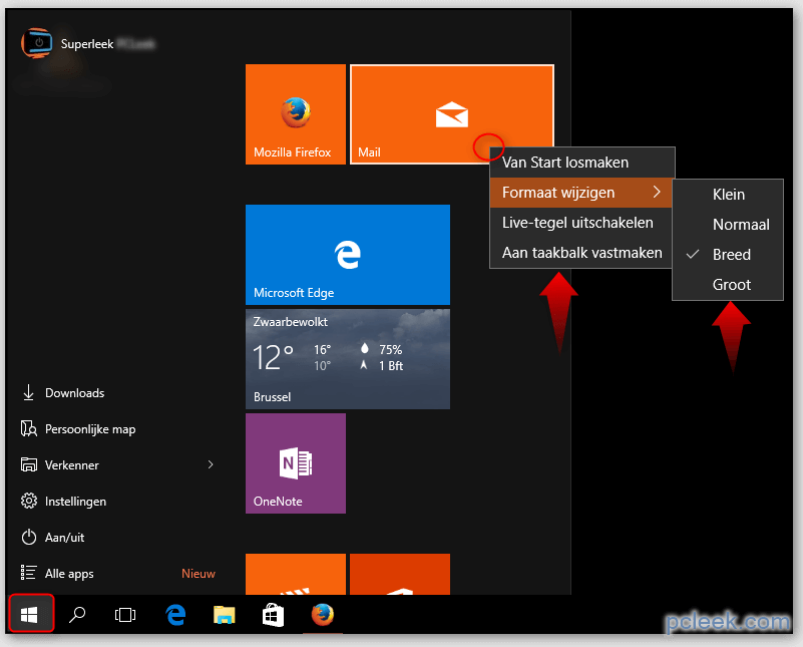
Het menu Start is terug van weggeweest in Windows 10. Lees in deze tip hoe u het menu Start kan aanpassen en/of personaliseren.

Windows 10: Het menu Start aanpassen

Windows 8 kreeg tonnen kritiek te verwerken toen bleek dat men het menu Start gesloopt had. Of dat terecht is of niet laten we in het midden, feit is wel dat Microsoft het menu Start opnieuw introduceerde in Windows 10. Meer nog, Microsoft opteerde voor een combinatie van het klassieke menu Start in combinatie met de verguisde metro-interface. Het menu Start in Windows 10 bestaat dus uit 2 onderdelen die elk afzonderlijk kan aanpassen of personaliseren.

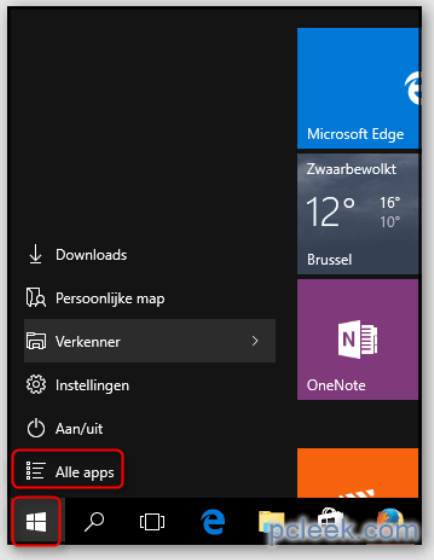
We beginnen met het aanpassen van menu Start het metro-gedeelte (rechts).

- Het menu Start opent u door op de Startknop (Windows-logo) te klikken (linkermuisknop) in de linker benedenhoek.
- Zoals u ziet in onderstaande schermafdruk, bestaat het menu Start uit 2 delen. Links lijkt meer op een klassiek menu Start, terwijl het rechtse gedeelte erg doet denken aan het metro-startscherm uit Windows 8 (althans de mini-versie er van). Dit deel van het menu Start kan u aanpassen, zo kan u onder andere:
- Tegels verwijderen uit het menu Start (Van Start losmaken).
- Het formaat wijzigen (klein, normaal, breed of groot)
- De live tegel uitschakelen (de tegel blijft aanwezig maar wordt niet langer geüpdatet met live informatie).
- Of u kan een tegel vastmaken aan de taakbalk (Aan taakbalk vastmaken).



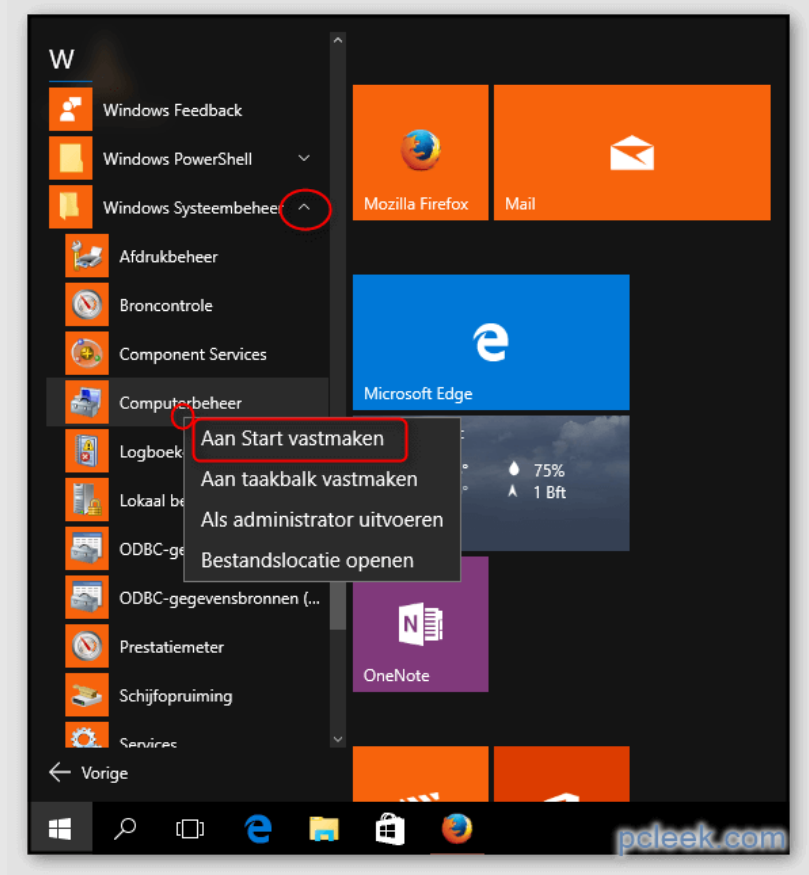
Nadat u de overbodige tegel(s) verwijdert hebt uit het menu Start, wilt u er natuurlijk toevoegen die wel belangrijk zijn voor u.

- Open het menu Start en klik vervolgens op: *Alle apps*.



Navigeer naar de app/onderdeel/item dat u wenst toe te voegen aan het menu Start. Klik er op met rechts en kies voor: *Aan Start vastmaken*.

Opgelet! Als u onderdelen ziet met een pijltje naast, wil dat betekenen dat er nog onderliggende items/onderdelen beschikbaar zijn.



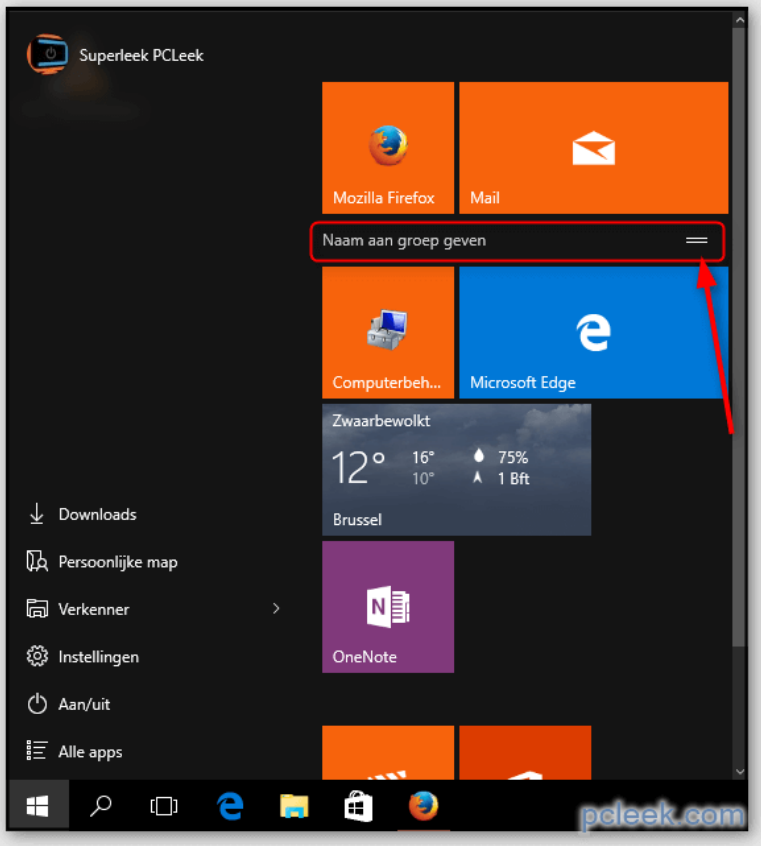
Bron: PCleek

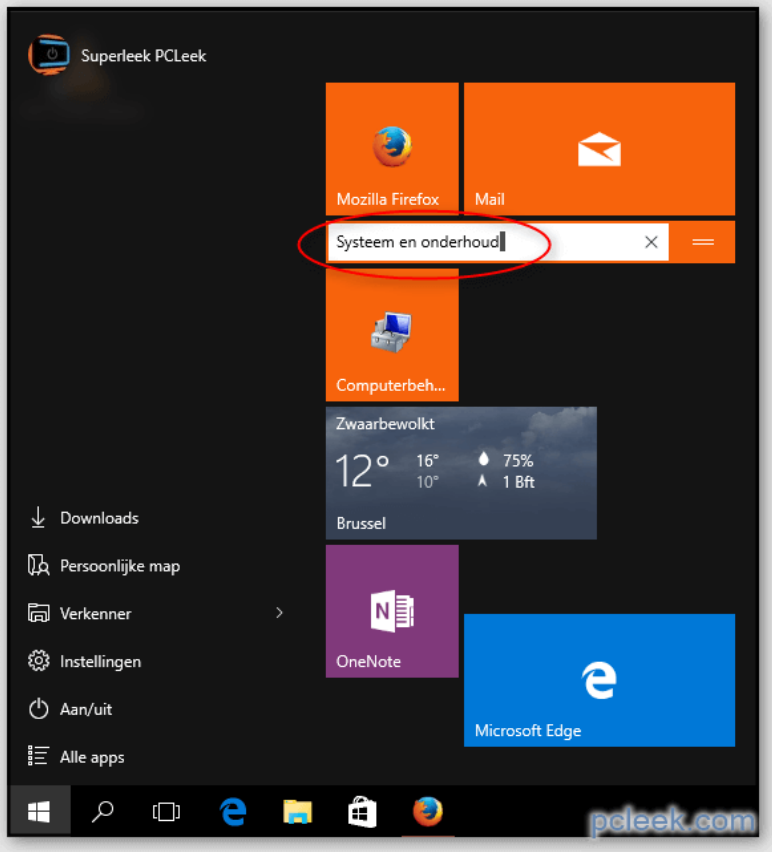
Index

Zodra u al de gewenste apps/items hebt toegevoegd aan het menu Start, kunt u ze ordenen en groeperen.

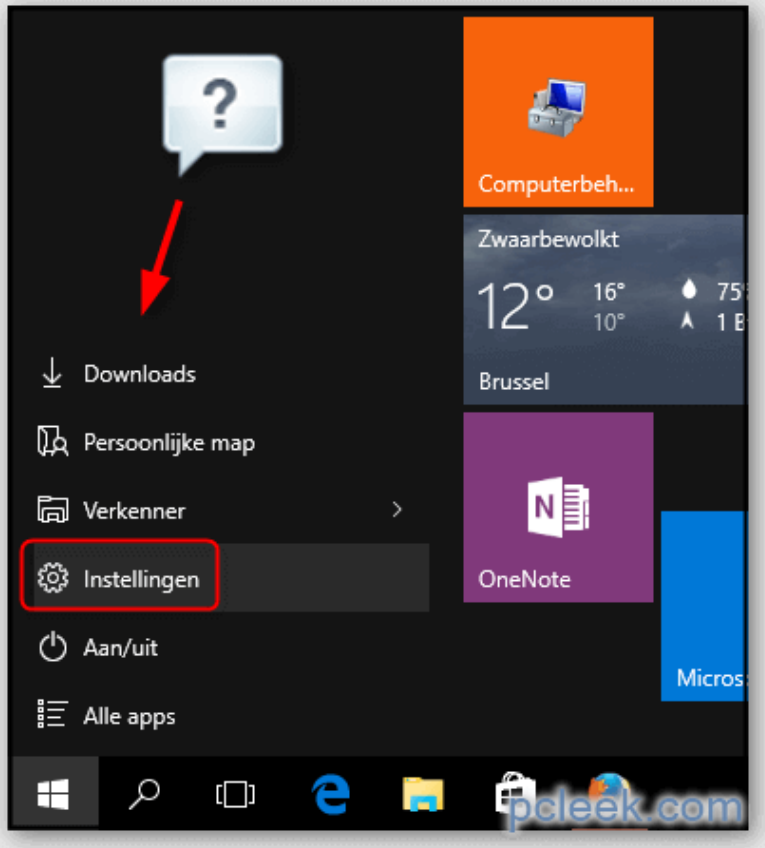
Hou de linkermuisknop ingedrukt en sleep ze naar de gewenste positie.

Bent u klaar met de items te ordenen, kan u elke groep een toepasselijke naam geven (zie schermafdruk).

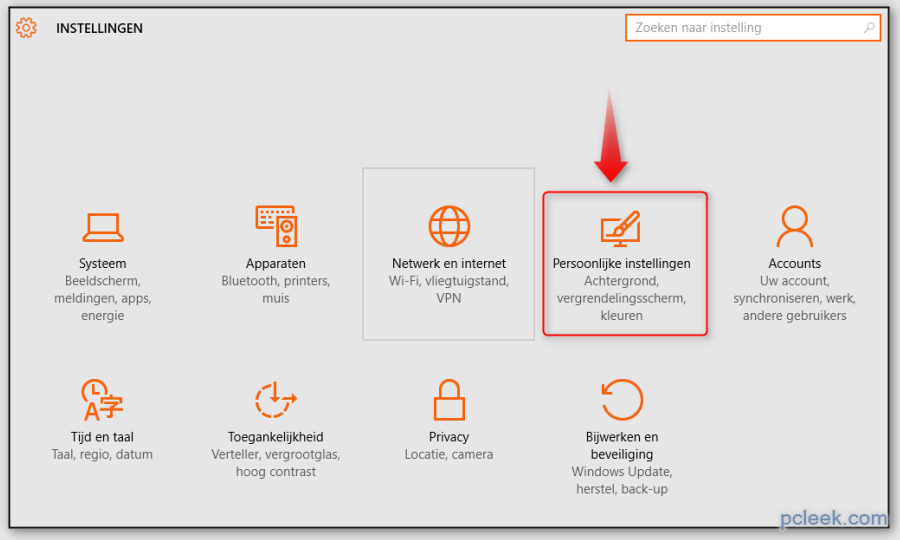




Open het menu Start > instellingen.



In het dialoogvenster dat volgt, kiest u voor: Persoonlijke instellingen, Achtergrond, vergrendelingsscherm, kleuren.



Bent u klaar met het aanpassen van het metro-gedeelte van het menu Start, kan u beginnen het klassieke gedeelte van het menu Start.

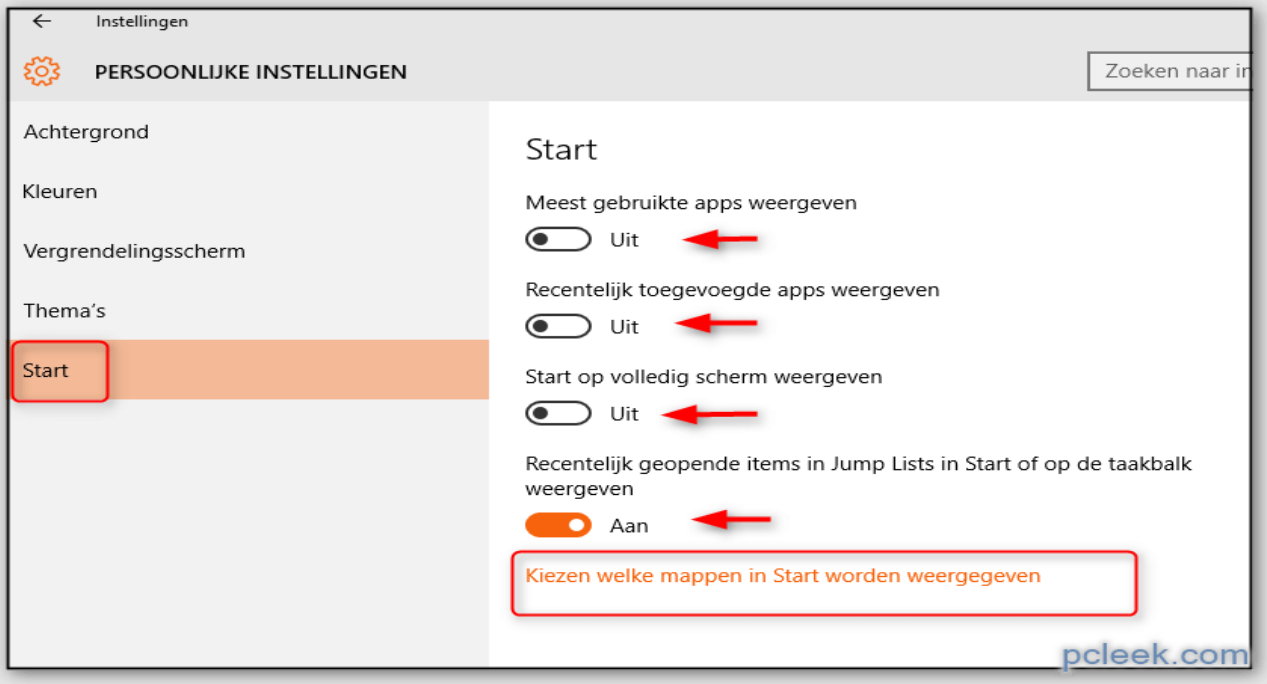
Bron: PCleek

Index

Selecteer Start in de linker kolom.

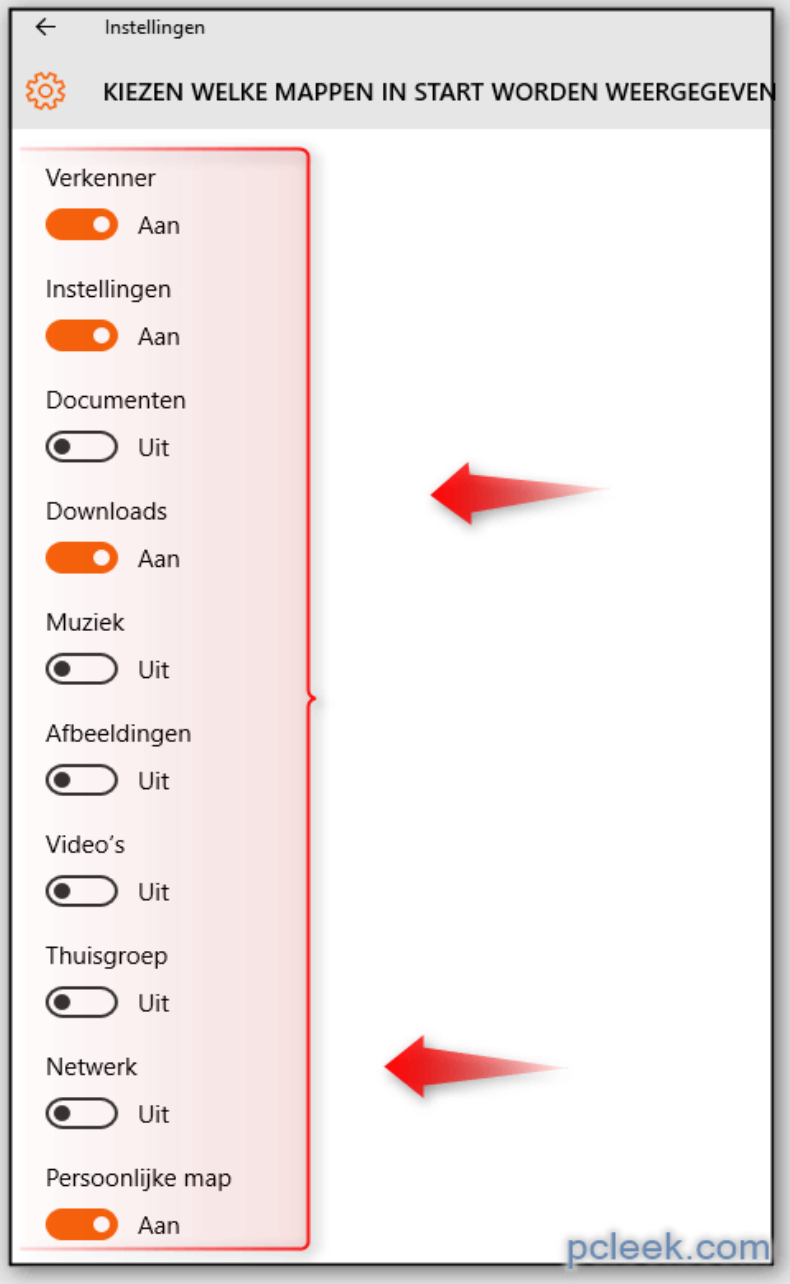
In het rechtergedeelte kan u met behulp van schuifregelaars aangeven welke items/locaties u wenst toe te voegen aan het menu Start van Windows 10.

Het menu Start op een volledig scherm weergeven is eveneens mogelijk.



Indien u een veelgebruikte map/item wil toevoegen aan het menu Start, klikt, of drukt u op: Kiezen welke mappen in Start worden weergegeven.

Door het verplaatsen van de schuifregelaars, kan u dan aangeven welke mappen/items u wil zien in het linker gedeelte van het menu Start.



U hoeft trouwens nergens te bevestigen met een klik op OK. Alle wijzigingen worden meteen doorgevoerd.

Succes!

Bron: PCleek

Index

Windows 10 komt met enkele nieuwe en verbeterde features, zoals de Snap Assist en het virtuele bureaublad. Om het ons nog makkelijker te maken komt het nieuwe besturingssyteem met tien nieuwe sneltoetscombinaties om deze features aan te spreken.

Tien belangrijke sneltoetsen voor Windows 10

Verplaats je vensters
Om je Windows-vensters aan jouw voorkeuren te laten voldoen, levert Microsoft niet minder dan vijf shortcuts bij Windows 10. In een handomdraai maximaliseer je je scherm, laat je het snappen naar een schermrand en minimaliseer je het terug.

- Venster snappen naar linkerkant scherm: Windows-toets + links
- Venster snappen naar rechterkant scherm: Windows-toets + rechts
- Venster snappen naar een kwadrant: Windows-toets + boven of onder
- Venster maximaliseren: Windows-toets + boven
- Venster minimaliseren: Windows-toets + onder

Om een venster in een kwadrant te snappen, moet het eerst naar de linker- of rechterkant van je scherm zijn gesnapt. Indien dit niet het geval is, zal je venster maximaliseren of minimaliseren.

Virtueel bureaublad
Om je beter wegwijs te maken tussen al je applicaties bevat Windows 10 de mogelijkheid om oneindig veel virtuele bureaubladen te maken. Hierdoor kan je je applicaties mooi sorteren per bureaublad en hier gemakkelijk tussen wisselen. Uiteraard komt Windows 10 ook met sneltoetsen voor deze nieuwe feature.

- Bekijk alle virtuele bureaubladen: Windows-toets + Tab
- Creëer een nieuw virtueel bureaublad: Windows-toets + Ctrl + D
- Sluit het huidige virtueel bureaublad: Windows-toets + Ctrl + F4
- Ga naar het volgende virtueel bureaublad: Windows-toets + Ctrl + rechts
- Ga naar het vorige virtueel bureaublad: Windows-toets + Ctrl + links



Bron: Clicks

Index



Software schatkist

De kist is gevuld met fraaie software en naslag.

Nieuwsgierig?

Open de kist middels de sleutel en ontdek…….



Index



Een 37-jarige medewerker van de supermarktketen Jumbo is veroordeeld tot een voorwaardelijke gevangenisstraf van drie weken, een taakstraf van 120 uur en het betalen van een schadevergoeding van 30.000 euro wegens het hacken van bijna honderd bedrijfslaptops.

De man zou vorig jaar naar eigen zeggen "uit verveling" op de computers hebben ingebroken. Zo wist hij inloggegevens van privé -mailadressen van andere werknemers te verkrijgen. De man was als bedrijfscontroleur bij de supermarktketen werkzaam en werd na te zijn betrapt op non-actief gezet, zo meldt Omroep Brabant. De rechter besloot de man niet naar de gevangenis te sturen omdat hij meteen zelf een psycholoog had ingeschakeld om te achterhalen waar zijn gedrag vandaan kwam. De Telegraaf meldt dat de man een keylogger gebruikte om de wachtwoorden van andere medewerkers te achterhalen. In totaal zou de keylogger op 96 laptops zijn geïnstalleerd. De verdachte activiteiten op het netwerk werden na twee maanden door de ICT -afdeling van Jumbo ontdekt. Uit onderzoek van een beveiligingsbedrijf bleek dat de bedrijfscontroleur de dader was.

———————————————————

Onderzoekers van Fox-IT, die samen met de FBI onderzoek deden naar een groep cybercriminelen, melden dat deze 'Business Club' de afgelopen jaren voor ten minste 100 miljoen dollar aan banktegoeden gestolen heeft. De bende gebruikte daarvoor vanaf 2009 de zogeheten GameOver Zeus-malware, en werkte vanuit meerdere landen. Er werd onder meer ingebroken op computers van ministeries en inlichtingendiensten in Georgië, Turkije en Oekraïne. De malware werd al in 2005 ontwikkeld door een Rus, op wiens hoofd de FBI inmiddels een beloning van drie miljoen dollar heeft gezet. Volgens de onderzoekers wordt deze Rus, Evgeniy Bogachev aka de Slavik, beschermd door de Russische overheid.

———————————————————

In Rusland zijn drie Tsjetsjeense vrouwen opgepakt die IS hadden opgelicht. De vrouwen schreven op sociale media dat ze wel naar Syrië wilden, maar geen geld hadden voor de reis. Meerdere Jihadisten hapten toe en maakten geld over. De vrouwen lieten – net als Westafrikaanse 419-fraudeurs – vervolgens niks meer van zich horen. De accounts werden verwijderd en met nieuwe accounts werd een volgende scam gestart. De politie kwam de dames op het spoor bij een onderzoek naar jihad-recrutering op internet. De buit was overigens niet groot: de drie vrouwen hebben naar schatting drie mille verdiend. Ze riskeren nu overigens zes jaar celstraf.

———————————————————

Verdacht internetverkeer erin, schoon er weer uit. Zo werkt simpel gezegd Nawas, oftewel de Nationale Wasstraat.
De Nationale Beheersorganisatie van Internetproviders (NBIP) heeft de handen ineen geslagen om de weerbaarheid van hun klanten tegen ddos-aanvallen te vergroten. Nawas is een geautomatiseerde dienst van de gezamenlijke Nederlandse internetindustrie die ddos-aanvallen onschadelijk
maakt, meldt het FD. Het systeem met speciale software past in twee serverkasten van twee bij één meter, opgesteld in een datacentrum op het Sciencepark in Amsterdam. Verdacht internetverkeer dat bij een provider via het netwerk binnenkomt wordt gedetecteerd en onmiddellijk 'omgeklapt' naar Nawas, die het verkeer reinigt en schoon weer terug stuurt. Onlangs bezweek het netwerk van Ziggo urenlang onder een ddos-aanval van buitenaf. De grote jongens als Google en KPN en Ziggo, en ook trouwens de Rijksoverheid, hebben echter hun eigen beveiliging.

———————————————————-

Kwaadwillende hackers richten zich steeds vaker op zorginstellingen, omdat die sneller geneigd zijn te betalen. Van alle hacks vindt zo'n 30 procent plaats bij een zorginstelling. Het gaat soms om honderdduizenden tot miljoenen euro's. Hackers kiezen die instellingen als doelwit omdat ze met gevoelige informatie werken, en dus makkelijk onder druk te zetten zijn. Zo dreigen ze bijvoorbeeld om patiëntgegevens naar buiten te brengen. Voor veel behandelingen zijn de zorginstellingen ook nog eens afhankelijk van ICT.

———————————————————

Nederlanders zijn in de eerste zeven maanden van dit jaar voor bijna 5,5 miljoen euro via internet opgelicht. Het gaat voornamelijk om verschillende vormen van voorschotfraude, zo laat de Fraudehelpdesk
tegenover Metro weten. Bij voorschotfraude claimen oplichters bijvoorbeeld dat iemand een loterij heeft gewonnen of een groot geldbedrag of erfenis kan krijgen.

Vervolgens vragen de oplichters geld van het slachtoffer om de zogenaamde miljoenen over te kunnen overmaken. Een andere bekende vorm van voorschotfraude is datingfraude, waarbij oplichters een relatie met iemand aangaan om vervolgens voor allerlei zaken geld te vragen. Van januari tot en met juli werden Nederlanders op deze manier voor een bedrag van in totaal 2,8 miljoen euro opgelicht. Daarmee is het totale schadebedrag van 2014 nu al geëvenaard.

Een categorie die in de eerste zeven maanden voor inmiddels meer schade heeft gezorgd is "cybercrime". Hieronder vallen zaken als phishing en "hacken". Vorig jaar kwam het totaalbedrag op 345.000 euro uit, terwijl de teller nu al op 655.000 euro staat. Ook de schade door identiteitsdiefstal is toegenomen. Het gaat dan om oplichters die andermans gegevens gebruiken om bestellingen te plaatsen. Op deze manier wisten oplichters dit jaar al 390.000 euro te stelen, tegenover 222.000 euro vorig jaar.

———————————————————-

Microsoft heeft gebruikers en beheerders die computers handmatig updaten gewaarschuwd voor een belangrijke beveiligingsupdate die opnieuw is uitgebracht en opnieuw moet worden geïnstalleerd. Op 11 augustus dichtte Microsoft verschillende lekken in Windows, .NET Framework, Office, Lync en Silverlight.

Via de kwetsbaarheden zou een aanvaller de computer volledig kunnen overnemen als de gebruiker een speciaal geprepareerd document opent of onbetrouwbare websites bezoekt met embedded TrueType- of OpenType-fonts. Als oplossing publiceerde Microsoft Security Bulletin MS15-080. Deze update wordt op de meeste Windowscomputers automatisch via Windows Update geinstalleerd. Het is echter ook mogelijk om de update via het Microsoft Download Center te downloaden.

De update voor Vista SP2, Windows Server 2008 (R2) SP2 en Windows 7 SP1 die via het Download Center wordt aangeboden werd op 18 augustus geüpdatet. Microsoft adviseert Windowsgebruikers die de update voor 18 augustus via het Download Center hebben gedownload om die opnieuw te downloaden en installeren, zodat ze volledig beschermd zijn tegen de kwetsbaarheden die in het bulletin worden genoemd. Dit geldt alleen voor mensen die de update via het Download Center hebben gedownload.

Index



Internetgebruikers van wie de computer met ransomware besmet raakt moeten altijd aangifte bij de politie doen. Dat laat het Team High Tech Crime (THTC) van de politie via Twitter weten. Aanleiding is een juridische vraag van Arnoud Engelfriet op Security.NL.

De vraagsteller wilde aangifte van ransomware doen toen een computer van zijn kennis besmet raakte, maar de agent op het politiebureau wilde de aangifte niet opnemen. Volgens het THTC moeten slachtoffers van ransomware bij het maken van een afspraak om aangifte te doen naar een digitaal expert vragen. "Voor de politie is cybercrime een relatief nieuw fenomeen. Er wordt hard aan gewerkt alle collega's er mee bekend te maken", aldus de politie.

Een aantal jaren geleden was er nog een aparte website van het Meldpunt Cybercrime waar internetgebruikers melding konden maken. De website ging uiteindelijk op in politie.nl. Het THTC laat echter weten dat er aan een beter alternatief wordt gewerkt. In april van dit jaar werd het doen van online aangifte in het geval van internetoplichting al vereenvoudigd.

———————————————————

YouTube heeft, na klachten, het kanaal Dutch Moving Asses verwijderd. Het kanaal, van een onbekende 'billenfilmer', toonde opnamen van vrouwenbillen. De man (?) filmde, op bilhoogte, de afgelopen maand in Eindhoven 'tientallen vrouwen en meiden'. YouTube verwijderde de beelden 'wegens een schending van het beleid van YouTube op het gebied van naaktheid of seksuele inhoud'. Naakt was er overigens niet te zien, alle gefilmde vrouwen waren volledig gekleed. De politie meldde daarom dat er niets strafbaars gebeurd was. Filmen in de openbare ruimte is gewoon toegestaan. 'En daarom kan de politie weinig doen als jouw achterwerk op deze manier op YouTube staat', aldus een woordvoerder. Strafbaar is het pas als het om upskirt-beelden gaat, of als bijvoorbeeld sterk wordt ingezoomd op het kruis. Om die reden werd in 2009 in Groningen een man opgepakt voor aanranding. Overigens zijn er ook geen aangiften of meldingen gedaan.

———————————————————

Het ministerie van Veiligheid en Justitie heeft 'per ongeluk' de plattegrond van een gevangenis op Bonaire online gezet. De blunder werd snel ontdekt maar de plattegrond is mogelijk wel verspreid. Opvallend is dat het gaat om plattegronden van een gevangenis die nog in aanbouw is en de oude gevangenis moet vervangen omdat daaruit regelmatig mensen ontsnapten. Plattegronden van gevangenissen zijn 'een goudmijn voor criminelen', schrijft het AD.

———————————————————

Politiechef Henk van Middelkoop (58) van de politie Brabant Zuid-Oost heeft op facebook veel steun gekregen nadat hij een emotionele persoonlijke brief online had gezet. In de brief, oorspronkelijk gericht aan politieminister Ard van der Steur, schrijft Van Middelkoop 'op zijn eigen manier' voor een betere politie-cao. Meedoen aan acties past hem niet, schrijft hij. maar hij wil wel meer aandacht voor de verslechterde arbeidsvoorwaarden van zijn kinderen die ook bij de politie werken. 'Mijn kinderen willen met net zo veel optimisme als ik de maatschappij dienen, maar deze maatschappij vraagt heel veel meer van hen dan van mij destijds. En daar hoort een passende beloning bij'. Van Middelkoop kreeg geen reactie van Van der Steur en zette de brief daarom online. 'Open jullie ogen en besef dat dit de mensen zijn die er voor jullie zijn'.

———————————————————

Agenten uit verschillende landen hebben een vijfdaagse cursus gevolgd over de verborgen services van Tor, illegale marktplaatsen en cryptogeld. De opleiding, georganiseerd door Interpol en TNO en gehouden in Singapore, was bedoeld om politiemensen meer te leren over het darknet en de illegale praktijken die daar plaatsvinden. De cursisten, waaronder ook Nederlandse, oefenden op een gesimuleerd darknet, met nep-cryptogeld en gesimuleerde marktplaatsen, en leerden onder meer hoe ze de marktplaats offline konden halen. November 2015 is de volgende cursus, in Brussel.

———————————————————

De politie in Griekenland heeft een 4-jarig meisje uit Winterswijk weten te redden uit een sekte. In de zaak speelde facebook een belangrijke rol: uit berichten op dat medium bleek dat het meisje Zarah op het eiland Patmos verbleef. Ze werd eind juli bij een 'contactmoment' ontvoerd door haar moeder Nienke en meegenomen naar Griekenland. De ouders van het meisje, beiden lid van de sekte River of Glory, werden eind 2014 uit de ouderlijke macht gezet. De sekte predikt hel en verdoemenis omdat 'Het Einde Der Tijden' aanstaande is en is bij toeristen bekend vanwege doopritуelen in zee. Zarah werd eind 2014 in een pleeggezin geplaatst. Een paar dagen na de ontvoering plaatste vader Barry – ook bekend als 'hogepriester Israël Immanuel' – foto's en filmpjes op facebook waarop hij, op Patmos, met zijn dochtertje poseerde. Bij een van de foto's schreef hij dat zijn dochter 'floreert' en tijdens de reis naar Patmos 'nagenoeg aanhoudend gezongen' heeft. Daarmee maakte hij het de Griekse én Nederlandse politie en Jeugdbescherming wel erg gemakkelijk. Deze instantie heeft aangifte gedaan, het OM moet nog beslissen over vervolging.

———————————————————

Met behulp van facebook heeft manage-eigenaar Arnoud van Daatselaar zijn gestolen tractor weer terug. De tractor, nieuwwaarde tachtig mille, werd op een nacht gestolen. Van Daatselaar zette foto's op facebook en al snel kwamen er tips van mensen die de tractor hadden gezien. Deze werd uiteindelijk gelocaliseerd en door de politie van een gps voorzien, in de hoop de dief te traceren. Dat lukte niet, Van Daatselaar had de tractor na enkele dagen weer nodig. Hij is blij met alle tips, zijn bericht werd drieduizend keer gedeeld. 'De dader heeft duidelijk niet gerekend op de kracht van dat medium'. Volgens politiewoordvoerder Hans Meuleman is de tractor mogelijk gestolen door iemand die 'een voertuig nodig had', mogelijk met het oog op een ramkraak.

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

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
Delta Lloyd 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

Computerwoordenboek

POLITIE Meldpunt internetoplichting
Controleer vooraf de (bank)gegevens van de verkoper op
www.mijnpolitie.nl/miocheck

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 met ICT zou worden gepleegd.

———————————————————

Haatzaaien.

'Het zaaien van haat of het (opzettelijk) beledigen of discrimineren van een groep mensen wegens hun ras, hun godsdienst of levensovertuiging, hun hetero- of homoseksuele gerichtheid 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 contactenmet 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.

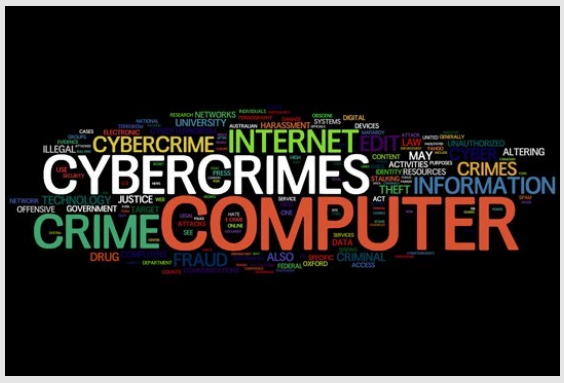
Artikel 2 Wwm: wet wapens en munitie

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 groei-industrieën

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