Top Tips van Tuts

Interessante informatie, gratis software en websites die je veel nuttige toepassingen bezorgen!

Deel XX

Top tips van Pctuts deel 1 had het over: ***Abby Finereader 9; Adobe Starter free; CCFinder; Cookienater; CrystalDiskInfo; Format Factory; Free OCR; First PDF; Gladinet; Irfanview; Lastpass; Ninite Pro; Paragon Backup & Recovery free; Recuva; Secunia PSI; Software Informer; Spacesniffer; Speccy; Speckie; Tweaknow Winsecret en TN Powerpack; Vista Sortcut Manager; What's my Computer Doing;***
Windows 7 Logon background changer; WOT for IE en YoWindow.
Top Tips van Pctuts deel 2 had het over: ***Groovedown; Music Downloadcenter; Spybot Search & Destroy; MBAM; SuperAntispyware; Agics Systemscan; IE Passview; Online beter leren typen; Internet radio; Toolbar Cleaner; Betrouwbaarheid van je systeem nazien; perfmon /report; BitMeter OS; Spotflux; Lockhunter en FileASSASIN; Hotspot vinden voor Laptop gebruikers; Systeemherstel; Sneller opstarten; Sysinternals Autoruns; Windirstat; Spellingscontrole in Windows Live Mail;***
Media Player Classic; Microsoft Security Essentials; Menu Uninstaller; Windows Installer Cleanup; Sfc /scannow; Process Explorer; Tubulator en QR–Code.
Top Tips van Pctuts deel 3 had het over: ***Gebruik van het Uitvoeren venster (Winkey+R); SIW = Mega-Systeem Informatie voor Windows; AM Deadlink; MJM Data Recovery; SUMo; Process Library (online); ScanCircle; Vertalen in Word; Multiboot CD, DVD of USB Startup en Help; Puran Utilities; SugarSync Bèta V.2.00; CyberGhost; Microsoft Safety Scanner;***
Met VLC Media Player Audio of Video inkorten; Open Hardware Monitor en Geluid opnemen.
Top Tips van Pctuts deel 4 had het over: ***GsmartControl; Frostwire; Keepvid; Imgburn; Free Video Flip and Rotate; Songbird; Muziek naar je Audiosysteem; Post-it's; Avast! Free Antivirus; Online Armor Free; Right Click Enhancer(1); Right Click Extender (2); Hexonic ScanToPdf; Onnodige Herstelpunten deactiveren; Ultimate Windows Tweaker; PhotoScape; Msconfig; Freemake Video downloader; Diagram Designer en iLivid Media Downloader.***
Top Tips van Pctuts deel 5 had het over: ***Keyfinder; CleanAfterMe; Geek Uninstaller; Stoffi mediaspeler; Ghostery; Do Not Track Me; PatchMyPC; Wifi Protector; iCopy & Photocopier; VarieDrop; Bios tips; Probleemoplosser Windows; Prioriteiten instellen; Wisselbestand optimaliseren; Open Hardware Monitor(3); Temp File Cleaner en***
FlipPDF to Word.
Top Tips van Pctuts deel 6 had het over: ***Licencecrawler; Universal Viewer; OSForensics; ChangeIcon; SharkEmailExtractor; EnhanceMySe7en; Google Music; Specefieke Afbeeldingen zoeken met Google; DNLA; .Zip, .Rar en meer; IZArc; ZipGenius; EasyBrake; Media Hint; Blokkades in YouTube opheffen en MP3Gain.***
Top Tips van Pctuts deel 7 had het over: ***Google Images; Deezer; AdwCleaner; Steganografie; WM Recorder; Fotor; Weatherbug; Slimware Utilities; Duckduckgo; Startpage; Perspectiveimg; Planet Mars; Synei System Utilities; Opswat Security Score; XnSketch en Sketsch Drawer; Fequal; Testmy.net; Chromecast en Geluid Opstarten Windows uitschakelen.***
Top Tips van Pctuts deel 8 had het over: ***oCam; 8GadgetPack; Adblock Plus; Cookienator; CrystalDiskInfo 6 Shizuku; Everything; Glary Utilities; VarieDrop; Wunderlist; Probleemstappen; Systernals Suite; Free Music Downloader; Astra32 System Info; Bootracer; Nieuwe Malwarebytes; PicBackMan; Ribbon Disabler; AutoHDR en Foxit Reader.***
Top Tips van Pctuts Deel 9 had het over: ***PUP's en andere Malware vermijden;***
Quick Restore Point maker; Genie Timeline Backup; Microsoft Office Gratis en legaal!; Prachtige Visitekaartjes maken!; ESET-Sysinspector; Administator paswoord omzeilen; Testmynet; Easy Context menu (aanmaken); Windows Repair All-in-One; CapslockGoodbye; Aeroglass terug in W8.1; Google Scholar en Sophos Anti-Virus Removal tool.
Top Tips van PCTuts Deel 10 had het over: ***Windows De Luxe, Mini-workshop met: Opstartsnelheid; BIOS; Slaapstand; Help en ondersteuning; Services; Auslogics Disk Defrag; Prestaties; Malware; Energiebeheer; GodMode; CCleaner; Tweakers; Bestandssysteem; Prioriteit voor toepassingen;***

Wisselbestand; Update Checker; Lege mappen weg; Memory Cleaner; Autoruns; Temperatuur processors; Should I Remove It?; PrivaZer; Schijfcontrole; Nuttige gebruiks-informatie vinden;
More Freeware: ***TuneIn; BlueStacks App Player; FastStone Image viewer; GrooveWalrus; Mooo WindowMenuPlus; VLC Video player; Don't Sleep; WhoCrashed; Free OCR; Simply Good Pictures; Revo Uninstaller; Folder Colorizer; Wise Folder Hider; Do It Again en Bits & Bytes.***
Top Tips van PCTuts Deel 11 **had het over:** ***Het einde van de Desktop Pc?; Pc's van de toekomst; Startmenu downloads; Nazicht v.d. Pc gezondheid; HWINFO; EHBO-kit combined Cleaners; FIXWIN 1 & 2; Arcsoft Perfect 365; Drie Driver programma's: Driver Booster, SlimDrivers*** *en* ***Drivers Update Monitor*** *(#3);* ***Image Resizer 3 with right-click; Fotobewerken; ScanCircle (updated); Free Pdf to Word; Process monitor; Resource Monitor; Norton Power eraser; Verdubbel Netflix; Windows Firewall; Bureaublad Roulerend en Windows 8 Sneltoetsen.***
Top Tips van PCTuts Deel 12 **had het over:** ***Cyberoorlog, Cybercrime, Gehackt worden, Virussen en andere Malware; 360 Total Security; Fotor; PrintFriendly; Cute PDF; MasterSeaker; TreeSize; Process Explorer; Services herstellen; Resource Monitor; Snelheid SSD testen; Quick Clean; Portable Apps en Faststone.***
Top Tips van Pcuts deel 13 **had het over:** ***Malware in 2014; Wegwijs in de kabelspagetti; Fresh Diagnose; TweakNow Powerpack; Mp3 Rocket; xVideoService Thief; Favorieten van IE naar Chrome; HDGraph; Nexus Radio; Win-UFO; PdfImage11; SuperAntiSpyware; HerdProtect; Paragon Backup & Recovery; iCopy en Patch my Pc.***
Top Tips van Pctuts deel 14 **had het over:** ***Chryptolocker; EHBO voor langzaam geworden Pc's; Net Guard; Easeus Data Recovery; Aomei OneKey Recovery; RecImg Manager; Unchecky; Bitvo; Jeta Logo Designer; Ultimate Windows Tweaker 3; CPID HWmonitor; Geek Uninstaller; Simply Good Pictures; Delete Doctor en Popcorn Time.***
Top Tips van Pctuts deel 15 ***had het over:*** ***Cyberoorlog; Chinese spionage; Back-up strategieën; |*** *Macrium Reflect free;* *Nieuwe* ***Ninite; Nieuwe Free Studio; Easy Service Optimizer; SpeedOf.me; WhoCrashed; HDR fotografie; Ghostery; SecureAPlus; Bright Explorer; InstantPhotoSketch; Convert.files; PhotoCat; Starter 5.6.2.9; EULAlyser 2.2; Tray Radio 10.0.1.0; Junkware Removal tool.***
Top Tips van Pctuts Deel 16 ***had het over:*** ***Intel CPU's; Hi-Res Audio; Veilig on-line shoppen |***
Privacy in Windows 10; CleanMem; Ultimate Windows Tweaker 5.2; Jscreenfix; recALL; Romeolight photo resizer; Belarc Advisor; Emsisoft emergency kit; Paragon Rescue kit; Nirsoft Utilities panel; Je SSD ontlasten; Eigen handschrift als font; Yippie add-on;
HD Tune 2.55; IrfanView; PrimoPDF.
Top tips van Pctuts Deel 17 ***had het over:*** ***TV en beeldscherm technologieën; Audio Streaming; Aomei OneKey Recovery; Windows System control Center; HoldKey; Driver Booster 3; Kerish Doctor; Quick Startup; Heimdal; PCFerret; GlassWire; SpywareBlaster; Zar X; GSmartControl; USBLogView; FileExile en Win10 Spy Disable.***
Top tips van Pctuts Deel 18 ***had het over:*** ***Groot beeld zonder beeldscherm; Vintage Audio; Hoe je Wi-Fi verbeteren; Ant-Ransomware; WhySoSlow; Start-Up Manager; Super F4; SecurAble; 10AppsManager; FileExile; Plagiarisma; PicBackMan; Kaspersky Cleaner; Imagine.***
Top Tips van PCtuts Deel 19 ***had het over:*** ***Technologie in een stroomversnelling; Sophos antivirus; Easy Context Menu; Spywareblaster; Bestandsconverter; Picosmos Tools; Xinorbis; Nasa's Eyes; Thunderbird; MEmu Android; Emsisoft Anti-Malware; OpenFreely; New Secunia.***

Dit is de TopTips Deel 20

►► Klik op de blauw onderlijnde titels en je hebt een directe link naar vroegere edities en achteraan vind je directe links naar alle uitgaven in deze serie.
Je vindt er 300+ programma's, websites en praktische tips die je nergens anders samen vindt zoals hier!
Met de directe links op p. 1 en 2 kan je ook de gewenste oude nummers downloaden..!

Ofwel nog *directe links* via ons Forum:
Bovenaan de homepagina >> Downloads >> Top Tips Tuts

Zoals altijd komen er ook in deze uitgave nogal wat blauwe onderlijnde 'Hyperlinks' voor.

Hierop moet je klikken om verder te lezen of om een video te bekijken.

We beginnen de TopTips tegenwoordig met interessante technologische informatie die iedereen aanbelangt en nuttig vindt, waarna we enkele zeer nuttige programma's voorstellen.
We hebben het deze keer over technische informatie i.v.m.:
Gecomputeriseerd autorijden, omgaan met Ransomware en Phishing

Gecomputeriseerd autorijden - toch niet voor morgen?

In ons artikel van de vorige TopTips hadden we het o.m. over de invloed van autonoom rijdend transport op ons leven tussen nu en het jaar 2030. Hierover hebben enkele lezers nogal wat vragen gesteld. Daarom nu nog wat ter verduidelijking:

Er wordt her en der veel over zelfrijdende auto geschreven en autofabrikanten over de hele wereld haasten zich om ze in productie te krijgen. De overtuiging heerst dat zelfrijdende auto's het aantal auto-ongevallen drastisch zal verminderen. Een ander voordeel is een grote toename van het systeem van autodelen en dat laat eigenaren van auto's toe om inkomsten te genereren door het verhuren van hun auto's aan anderen als ze door henzelf niet worden gebruikt.

Er is veel verwarring over wat een autonome auto eigenlijk betekent. In Duitsland, maar ook in de V.S., zijn er nieuwe regels die Tesla en andere bedrijven zou verbieden de termen *Auto Pilot* of *Self Driving* te gebruiken zolang de wagen niet in staat is om *Niveau 5* van de autonomie te bereiken. Het probleem is, dat de meeste mensen geen idee hebben dat er verschillende niveaus van autonomie zijn en hierdoor nogal wat verwarring ontstaat. Dus, laten we beginnen met de definities van de verschillende niveaus te bespreken om te zien of we die misverstanden kunnen wegnemen:

▪ **Niveau 0**: het systeem heeft geen controle over het voertuig, maar kan wel waarschuwingen geven;

▪ **Niveau 1:** het systeem heeft een beperkte controle over het voertuig en de bestuurder moet altijd klaar zijn om op elk moment de controle over te nemen.
Dit geautomatiseerd systeem kan o.m. automatische besturing-functies toepassen zoals Adaptive Cruise Control (ACC), Parking Assistance (PA) en Lane Keeping Assistance (LKA). Dit is op nieuwe voertuigen vanaf de middenklasse nu al het geval.

▪ **Niveau 2:** De bestuurder is verplicht om op voorwerpen en gebeurtenissen te reageren als het automatische systeem niet goed werkt. Het automatische systeem accelereert, remt en stuurt. Het schakelt onmiddellijk uit zohaast de bestuurder overneemt;

▪ **Niveau 3:** Het systeem werkt alleen in bepaalde omgevingen (zoals snelwegen of files). De bestuurder hoeft alléén in die omstandigheden zijn aandacht niet bij de weg te houden;

▪ **Niveau 4:** Het automatische systeem kan het voertuig onder controle houden in nagenoeg alle omstandigheden, met enkele uitzonderingen zoals extreme weersomstandigheden. De bestuurder kan het automatische systeem inschakelen wanneer het veilig is om dat te doen en dan is de aandacht van de bestuurder op de weg niet meer nodig;

▪ **Niveau 5:** Behalve voor het instellen van de bestemming en het systeem op te starten, is geen verdere menselijke tussenkomst nodig. De automaat kan rijden van- en naar een locatie waar het over de ganse weg wettelijk is toegelaten.

Wanneer zal het hoogste niveau beschikbaar komen?

Op de Parijse autoshow, verklaarde Akio Toyoda, CEO van Toyota dat volledig autonoom rijden een langdurig validatieproces is dat miljarden mijlen van testen en kalibreren vereist. Tesla's CEO, Elon Musk heeft onlangs getweet dat Tesla's **nu** al meer dan 220 miljoen mijl gereden hebben op de automatische piloot. Dat is een opmerkelijke prestatie, maar Toyoda zegt dat tenminste 10 keer zo veel gegevens nodig zullen zijn voordat een echt zelfrijdende auto realiteit wordt. Kortom, er werden verschillende verklaringen gedaan, gaande van drie- tot tien jaar.

De belemmeringen voor het perfectioneren en in massaproductie brengen van volledig geautomatiseerde voertuigen die veilig een passagier van deur-tot-deur kunnen vervoeren zonder menselijke tussenkomst zijn zeer talrijk. Camera's en LIDAR-systemen* moeten veel efficiënter worden en drastisch in prijs dalen voordat dat gebeurd.
De software voor autonome systemen moet in staat zijn om te anticiperen op bijna elk scenario die een voertuig kan tegenkomen: slecht weer, een verkeerslicht, handsignalen van een politieman tot een voetganger kunnen spotten die onverwacht in het verkeer komt, enz. Ook zullen er verbeteringen aan de infrastructuur moeten komen. Dat geldt o.m. voor betere wegmarkeringen en verkeersborden, alsook voertuig-tot-voertuig en voertuig-tot-infrastructuur communicatiesystemen. Het moet te allen tijde weten waar het is en wat er gaande is in de wereld om zich heen.

[*]=**LIDAR** (***LI****ght* ***D****etection* ***A****nd* ***R****anging* of ***L****aser* ***I****maging* ***D****etection* ***A****nd* ***R****anging*) is een technologie die de afstand tot een object of oppervlak bepaalt door middel van het gebruik van laserpulsen. De techniek is vergelijkbaar met radar, dat echter radiogolven gebruikt in plaats van licht. De afstand tot het object of oppervlak wordt bepaald door de tijd te meten die verstrijkt tussen het uitzenden van een puls en het opvangen van een reflectie van die puls. (Bron: Wikipedia)

De indruk, die veel chauffeurs hebben, is dat deze hard- en software hen zal beschermen tegen alle onverwachte gebeurtenissen, waardoor ze zich concentreren op andere dingen zoals het controleren van hun e-mail, het Sms'en of het plaatsen van Selfies van zichzelf terwijl ze zonder handen aan het stuur rijden en hun foto op Facebook plaatsen.

Elon Musk van Tesla zegt dat ze hun gebruikers er dikwijls genoeg aan herinneren dat hun Autopiloot vereist om nog steeds veel aandacht te besteden aan de weg en ze te allen tijde klaar moeten zijn om de controle over de auto over te nemen. Een klant had ooit gezegd dat de verkoper die hem zijn model S verkocht vertelde dat de auto zelfstandig kon rijden en maakte er zelfs een punt van om met zijn handen los van het stuur tijdens een demonstratie te rijden. Deze dingen gebeuren nu eenmaal, maar ondertussen is er toch ook niemand die zijn GPS 100% vertrouwd om de weg naar een bestemming te vinden. Met software voor autonoom rijden is dat tot nader order niet anders! Tesla zegt gereed te zijn met 360° radar en sensoren, nodig voor alle informatie die tijdens het rijden ongevallen zal vermijden en een vlotte doorstroming verzekeren.

Video met demo autonoom rijden: HIER

Omgaan met Ransomware en Phishing

In onze TopTips zijn we gewoonlijk zeer positief over de omgang met de PC omdat het een plezierige activiteit moet blijven. Ondanks alles moeten we het nu toch eens over de ongemakken die twee bepaalde soorten van Malware kunnen hebben (Malware is het verzamelwoord voor alles wat je ongewenst op je computer krijgt). De laatste tijd wordt het namelijk wel zéér erg met twee bepaalde soorten van Malware:
Ransomware (= Gijselsoftware) **en Phishing.** 2016 is heel zeker het jaar van Ransomware en nu, zover in 2017 houdt het nog niet op! Met meer apparaten aangesloten op het internet dan ooit tevoren en iedereen die in toenemende mate afhankelijk is van een constante toegang tot dergelijke verbonden systemen, is het geen wonder dat misbruik er van dit jaar zo is toegenomen.

Ransomware

Ransomware is een strafbaar kwaadaardig programma dat je persoonlijke gegevens of de gehele PC versleutelt. Je wordt dan gevraagd om een anonieme dienst te betalen om je computer - of de gegevens ervan – opnieuw vrij te geven. Ransomware is uitgegroeid tot een van de grootste bedreigingen, omdat het wel degelijk heeft bewezen een goede bron van inkomsten voor de aanvallers te zijn. Andere vormen van Malware komen de ontwikkelaars slechts indirect ten goede (bijvoorbeeld door het gebruik of de verkoop van speciale computer programma's). Echter, deze bedreiging eist geld direct bij het slachtoffer (jij?), zodat het je de toegang tot je gegevens of je computer terug geeft. Deze eis wordt meestal gedaan door middel van een Lock-scherm met een countdown teller en de link naar de pagina waarop het losgeld voor de sleutel om de computer of bestanden te ontgrendelen dient te worden betaald.

Zoals in elke winstgevende business, is er ook m.b.t. Ransomware een constante strijd om het bestaan op de markt. De verkoop van een sleutel om de geblokkeerde en gecodeerde gegevens terug vrij te geven is een zeer lucratieve illegale vorm van zakendoen voor Ransomware-ontwikkelaars. De strategie is zo succesvol dat sommigen van hen zelfs zijn begonnen met de Ransomware van andere programmeurs te saboteren om hun eigen aandeel veilig te stellen.

Betalen lijkt de snelste weg naar het 'bevrijden' van je bestanden. Maar garanties dat het probleem daarmee (volledig) verholpen is, heb je niet. En bovendien moedig je criminelen aan om door te gaan. **Een recente back up van (gevoelige) bestanden is goud waard in deze situatie!** Want na het scannen van je computer met antivirussoftware, het terugzetten van de fabrieksinstellingen en het terugplaatsen van je back-up, kun je snel weer aan de slag!

F-secure meldde onlangs dat gebleken is dat sabotage van grote ondernemingen als een belangrijke inkomsten-generator op dit gebied is. Een Ransomware groep beweert dat ze rijkelijk betaald werden door een Fortune 500 bedrijf om een concurrerend bedrijf te hacken en te infecteren. Door het blokkeren van de dossiers van de concurrent, waren ze in staat om de productie van de concurrerende onderneming te stoppen en een soortgelijk product het eerst vrij te geven. Deze Ransomware ontwikkelaar werd dus tweemaal betaald, eerst door het overtredende bedrijf en ten tweede door het besmette bedrijf via de Ransomware lock-out-instructies.

Hoe kun je jezelf beschermen tegen Ransomware?

1. Zorg ervoor dat al je software up-to-date is - vooral het besturingssysteem, de webbrowser en alle browser plug-ins zoals Adobe Flash Player of Oracle's Java Platform. Gebruik hiervoor Ninite (Uitleg in TopTips #15), Secunia (#19), PatchMyPc (#5) Glary (#8) of SUmo (#3).

2. Wees voorzichtig. Stel jezelf vragen voordat je klikt. Lees meer over hoe bedreigingen (en oplichting) werken om te voorkomen dat je een slachtoffer wordt. Krijg je een onduidelijke mail met bv. een bijlage over een pakje dat je toegestuurd werd, terwijl je niets in bestelling hebt? Bedwing je nieuwsgierigheid en open de bijlage niet!

3. Maak regelmatig een Back-up van al uw persoonlijke bestanden en documenten. Als op een of andere manier je computer is geïnfecteerd met Ransomware, kan je je systeem opnieuw installeren en/of je bestanden herstellen. Back-up's maken is een van die dingen die we wel weten dat we dat moeten doen, maar we doen het soms te zelden tot dat het te laat is, ook al dienen ze niet alleen om je te beschermen tegen Ransomware maar ook tegen meer alledaagse bedreigingen zoals harde schijf-defecten of computerdiefstal.
Een externe schijf, die na kopie wordt losgekoppeld van je computer of een soort van Cloud-gebaseerde opslag is een goed idee. Het maakt niet uit welke optie je ook kiest, zorg ervoor dat je ze regelmatig maakt, bij voorkeur dagelijks en zorg er ook voor dat je het restauratieproces regelmatig ook test.

4. Zorg er ook voor dat je een goede antimalware software met realtime bescherming gebruikt. Ofwel een betalende-, ofwel een goede gratis virusscanner, zoals Sophos, die we in onze vorige TopTips besproken hebben.

5. Voer af en toe een scan met een second-opinion-scanner, zoals Emsisoft Emergency Kit, Malwarebytes Anti-Malware of Hitman Pro om te controleren of je Pc ransomware-vrij blijft.

(deels vrij vertaald uit de oktober nieuwsbrief van Emsisoft – met toelating)

Je kunt op enkele websites zoals nomoreransom.org, decrypter.emsisoft.com en ID-ransomware ontsleutelings-software downloaden, maar, dit soort software is voor een beperkt aantal varianten van Ransomware beschikbaar. De kans dat het lukt je bestanden te bevrijden, is klein. Je moet het natuurlijk wel eerst proberen! Op veiliginternetten.nl vind je een stappenplan voor wat je kunt doen als je Ransomware op je computer hebt staan. En op de site van de politie (NL) en van fraudehelpdesk is nog veel informatie te vinden over Ransomware.

Wat je zeker moet toepassen is de Anti-Ransomware van Malwarebytes. HIER kan je het gratis downloaden. Dit zou een goede realtime anti-Ransomware scanner zijn en kan samen met de gewone Virusscanner werken, want het houdt alléén Ransomware tegen. We wensen je succes met al deze pogingen om deze verschrikking buiten je PC te houden. Twee geslaagde methodes om Ransomware te omzeilen en/of te ont-crypten zijn hier getoond (EN):
https://youtu.be/kbTTL2Cz5Vg en https://youtu.be/8mCtBQqHZQA

Phishing

Phishing (afgeleid van *phreaking* en *fishing*: "vissen", "hengelen") is een andere vorm van internetfraude. Het bestaat uit het oplichten van mensen door ze te lokken naar een valse (bank)website, die een kopie is van de echte website, om ze daar – nietsvermoedend – te laten inloggen met hun inlognaam en wachtwoord of hun creditcardnummer.
Hierdoor krijgt de fraudeur de beschikking over deze gegevens met alle gevolgen van dien. De fraudeur doet zich hierbij voor als een vertrouwde instantie, zoals een bank.

De meeste vormen van phishing gebeuren via e-mail. De slachtoffers worden hierbij met een e-mail naar deze valse website gelokt. De mail bevat een link naar de (valse) website met het verzoek om zogenaamd "de inloggegevens te controleren". Een variante vorm van phishing is *spearfishing*, waarbij de persoonlijke gegevens (naam, e-mailadres, telefoonnummer) van het slachtoffer worden gebruikt om hem een gevoel van vertrouwen te geven.

De ontvanger van het bericht wordt aangespoord om naar een bepaalde website te surfen om zijn persoonlijke gegevens te bevestigen of te corrigeren. In veel gevallen gaat het om financiële informatie, zoals bankgegevens of kredietkaartnummer, maar ook gebruikersnamen en wachtwoorden van shopping-sites of internetabonnementen zijn gewild.

De excuses die aangehaald worden om naar je persoonlijke gegevens te vragen, zijn bijna altijd dezelfde: je moet een bestelling bevestigen, je account dreigt te verlopen, door een crash van de bedrijfscomputer, waardoor een deel van uw gegevens verloren is gegaan (maar vreemd genoeg niet uw e-mailadres), u kunt een flinke korting krijgen als trouwe klant… Alle foefjes zijn goed om u naar de website te lokken.

Het beste is dit eens te illustreren met een echt gebeurd verhaal, want hiervan kan je leren waar je zoal voor moet opletten:

Een werknemer van een ziekenhuis werd het slachtoffer van een Phishing-aanval die ook te laat werd ontdekt. Niemand had wat ondervonden en men wist niet dat het gebeurd was tot twee weken na de eerste inbraak.

De aanvallers hadden eerst gezocht naar gegevens van hun beoogde slachtoffer op *LinkedIn* (een sociale website voor professionelen) en via deze site waren ze in staat om o.m. te zien waar ze naar school was geweest. Met deze gegevens waren de aanvallers in staat om te kijken op de website van deze school. Het slachtoffer werd als aanvoerder van het rugbyteam geïdentificeerd. Met behulp van deze extra informatie deden ze nog wat aanvullend onderzoek en vonden ze de precieze naam van een ander medelid van deze sport club. Vervolgens gebruikten ze dit om een overtuigende zoek-mail op te bouwen op basis van een echt uitziend mailadres van een oude teamgenoot, compleet met foto.

Wanneer het slachtoffer enthousiast klikte op de bevestiging, ontstond een mooi dialoogvenster en klikte ze op 'OK'. Daarmee kreeg de aanvaller de controle over de PC via het gebruik van Trojaans spyware. Vervolgens ging het bespieden onopgemerkt verder gedurende twee weken en werd een ton delicate gegevens verzameld.

Het klinkt misschien als een nogal geavanceerde aanval-methode, maar het feit is dat Phishing-aanvallen van deze soort relatief eenvoudig zijn uit te voeren door iedereen met wat tijd - en de wens om een slachtoffer te maken. Dat was geen door de staat gesteunde hacking van Chinezen of Russen, dat was gewoon iemand die heel slim in staat was om delicate gegevens van deze persoon te bemachtigen, waarmee ze achteraf werd onder druk gezet.

Informatie is een belangrijke eis in de strijd tegen dit soort aanvallen zodanig dat de dreiging kan worden verminderd. Werknemers als deze moesten veel voorzichtiger met hun online gegevens omgaan. Ze moesten altijd op hun hoede blijven voor vreemde of onverwachte e-mails. [Wij dus ook!].

15 procent van de ziekenhuizen in Engeland draaiden toen nog steeds op Windows XP, die allang niet meer ondersteund werd en ze daardoor een enorm gat in de beveiliging binnen dit bepaald netwerk hadden. Veel van deze software was speciaal geschreven om patiënten te behandelen en men ziet er tegen op om de software te herschrijven en te migreren naar een jonger O.S.

Echter, er is een nog groter probleem: veel van de gebruikte hardware kon geen ondersteuning voor Windows 10 of zelfs Windows 7 krijgen. Dit was het geval voor 83 procent van de ziekenhuizen in het V.K.! Bezuinigingen en druk op de financiën betekende dat deze ziekenhuizen zich niet konden veroorloven om deze apparaten te vervangen omdat ze ook nog steeds vitale diensten verrichtten. Toch was de voorgestelde oplossing om alles direct van het netwerk los te koppelen.

Algemene Anti-virus informatie vind je HIER (< klik op de link) = enkele grafieken van AV-Test, hèt onafhankelijk testlabo voor antivirusscanners. Je kunt elk O.S. aanklikken om eens de testresultaten voor ieder gebruikt O.S. te zien. Echt interessant!

Het aantal virussen zelf is de afgelopen jaren trouwens afgenomen omdat Cybercriminelen zich toeleggen op Ransomware en Phishing. Virussen verspreiden zichzelf als zelfstandige programma's door bestanden te infecteren, maar malwareontwikkelaars gebruiken minder vaak deze technologie. Ze doen beroep op z.g. Trojaanse paarden. Een Trojaans paard zit meestal in andere software verscholen of bereikt je via een e-mailbijlage.

Het blijkt dat Bitdefender - en per definitie ook Emsisoft die op Bitdefender en Avira is gebaseerd - een zelflerend mechanisme gebruiken om kwaadaardige patronen te herkennen. Hierdoor zou het lukken het om schone en geïnfecteerde bestanden van elkaar te scheiden. Gegevens van nieuwe Malware worden aangeboden aan het zogeheten 'Global Protective Network'. Dit is een Cloud-toepassing waarop al hun klanten automatisch zijn op aangesloten. Op deze wijze blijft een systeem automatisch up-to-date met de recentste malwaredefinities. Nieuwe bedreigingen zouden dus dankzij deze slimme technologie geen tijd krijgen om zich op het systeem te nestelen. Laten we het hopen. Voor de volledigheid hierna een korte samenvatting van de - op dit ogenblik - meest voorkomende Malware-gevaren. Deze samenvatting komt van de site van Smartbiz.be die professionelen via seminaries en hun tijdschrift over IT informeert.

1. Phishing: Phishing is nog steeds een van de meest bekende bedreigingen. Hedendaagse phishing mails zijn nu bedrieglijker dan ooit: geen spelfouten of ongeloofwaardige beloften meer. Er zijn nog te veel mensen er in trappen en het dus rendabel maken voor de criminelen.

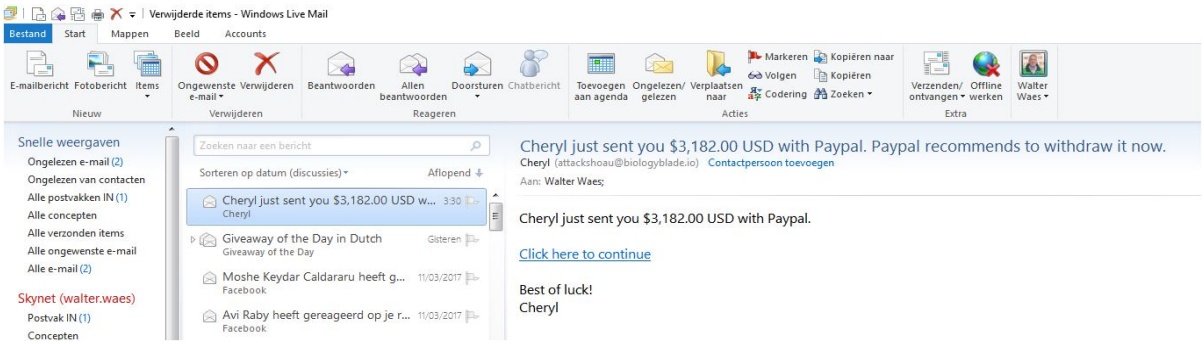
2 Exploit-kits: Exploit-kits zijn stukjes software die op een webserver draaien. De kit controleert elk systeem die in contact komt met de server en gaat op zoek naar mogelijke kwetsbaarheden. Bij een lek kan de kit het kwetsbare systeem Malware bezorgen, zoals ransomware of een Trojaans paard.

3. Mirai: Op 21 oktober werden grote delen van het internet verlamd. Wat nu al de grootste DDoS-aanval aller tijden wordt genoemd, werd mogelijk gemaakt door de Mirai-malware. De malware was verantwoordelijk voor de infectie van talloze geconnecteerde toestellen. Velen wijzen met de vinger naar de beveiliging van het Internet of Things.

4. Macro-malware: Al jaren wordt er gewaarschuwd voor de gevaren van macro-malware. Het gevaar schuilt meestal in een Microsoft Word- of Exel-document dat als bijlage per mail wordt verstuurd. Tegenwoordig zijn macro's in die documenten automatisch uitgeschakeld, maar in het document zal gevraagd worden om dat om te keren. Wanneer de gebruiker de bewerkingsmodus activeert, en dus de macro's inschakelt, krijgt de malware die tevens verpakt werd in het document vrij spel.

5. Ransomware: Bij Ransomware worden gegevens gegijzeld tot de gebruiker betaalt. De gebruiker wordt na een infectie geconfronteerd met een scherm met instructies, en kan niet meer aan de gegevens tot hij het nodige losgeld overmaakt. Bovendien evolueert deze vorm van Malware snel.

6. De gebruikers zelf…: Het gedrag van de gebruiker speelt een grote rol bij cyberbedreigingen. Vaak moet malware een handje geholpen worden. De gebruiker moet op een link klikken, rechten toekennen of zich gewoon op het foute moment op de foute plaats bevinden. Zo'n 20 procent gaat nog altijd op die foute links blijven klikken.



Mails zoals hierboven krijgt ondergetekende meer dan me lief is. "Cheryl just sent you $ 3.182 (USD) via Paypal" Click here to continue in order to be able to withdraw the money. Dat doe ik dan wijselijk niet, want je kan er van op aan dat ik met een Ransomware opgeschept zou zijn..! Waren die stortingen maar waar, dan was ik al goed rijk geworden. Er bestaat trouwens een PayPal-site die als twee druppels water op de echte lijkt. Ze doen je er naartoe gaan en dan gaan de poppen aan het dansen..!

foto: Paul Langrock (D)

Ook hernieuwbare energie komt niet vanzelf. De schoepen van windmolens vragen ook een wasbeurt en dat is geen klusje voor iedereen.

Zonne-energie is wat gemakkelijker, maar ze moeten er beiden zijn om een constante energievoorziening te blijven garanderen.

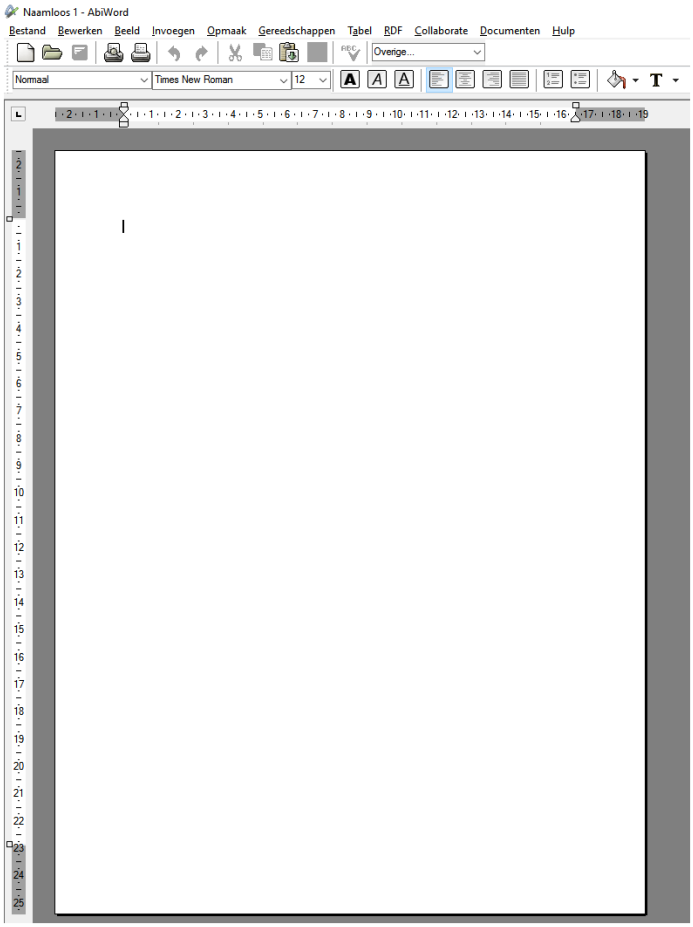
Zie ook onze TopTips #19, het artikel over *Clean Disruption*..!

En nu enkele gratis programma's:

Abiword

http://www.abisource.com/download/

Abiword is een zeer gebruikersvriendelijke en snelle tekstverwerker met een Nederlandstalige gebruikersinterface en het heeft ook Nederlandstalige spellingcontrole (die je wel apart moet downloaden of tijdens de installatie aanvinken). Het is compatibel met Microsoft Word. Het is wel minder uitgebreid dan Microsoft Word, maar dat is juist het mooie er van. Hoe dikwijls wordt niet een complete Office-versie gedownload met een presentatie- en rekenprogramma om alleen maar simpele brieven te kunnen schrijven? Abiword is een perfecte keuze voor wie geen behoefte aan een compleet kantoorpakket heeft!



De linten en menubalken lijken zeer goed op Microsoft Word en dat is wat direct opvalt door iemand die gewoon is met Word te werken. Perfect om op een Pc van een beginnende gebruiker te installeren! De bestanden worden opgeslagen als *.abg of desgewenst als *.docx of *.doc. Al deze extensies zijn met elkaar compatibel.

Doro Pdf writer

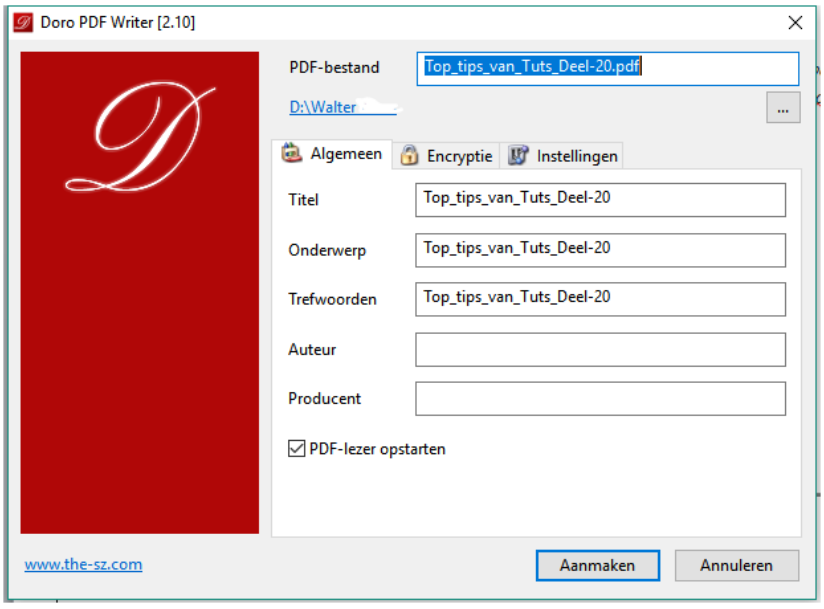
http://www.the-sz.com/products/doro/

Vanuit een recente Office-applicatie is het geen enkel probleem om documenten als pdf op te slaan of naar pdf te exporteren. Om dat op te lossen kun je Doro PDF Writer installeren, dat zich als een virtuele printer bij je printers (en apparaten) installeert: 'Doro PDF Writer' Dit is het geval als je bv. Abiword i.p.v. een office-programma gebruikt.

Doro PDF Writer

Via de link bovenaan is het eenvoudig om dit te installeren. Je klikt op «Doro setup.zip« , na het 'unzippen' krijg je de *.exe file en je bent vertrokken.

Zodra je de "afdruk" bevestigt, opent een venster van Doro PDF Writer waarin je desgewenst nog allerlei metadata voor je aan te maken PDF-document kwijt kunt, zoals auteur, titel, onderwerp, producent en sleutelwoorden.

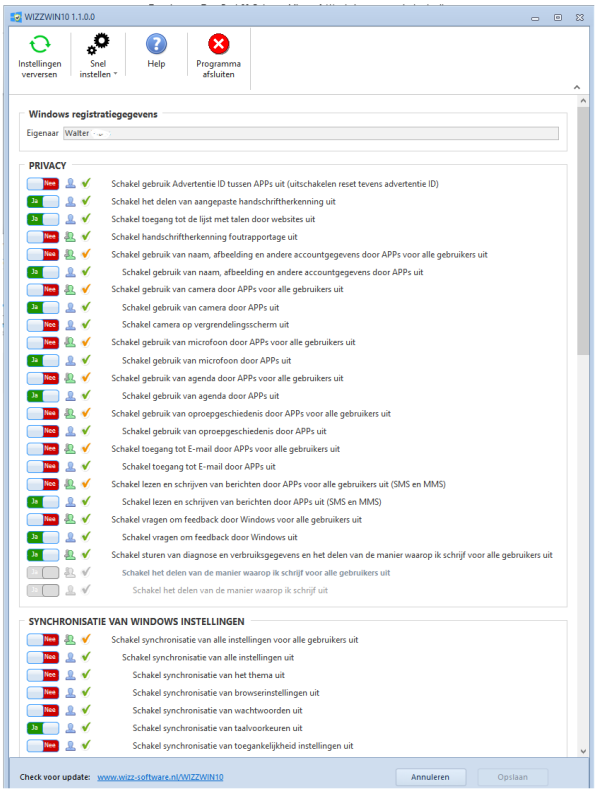


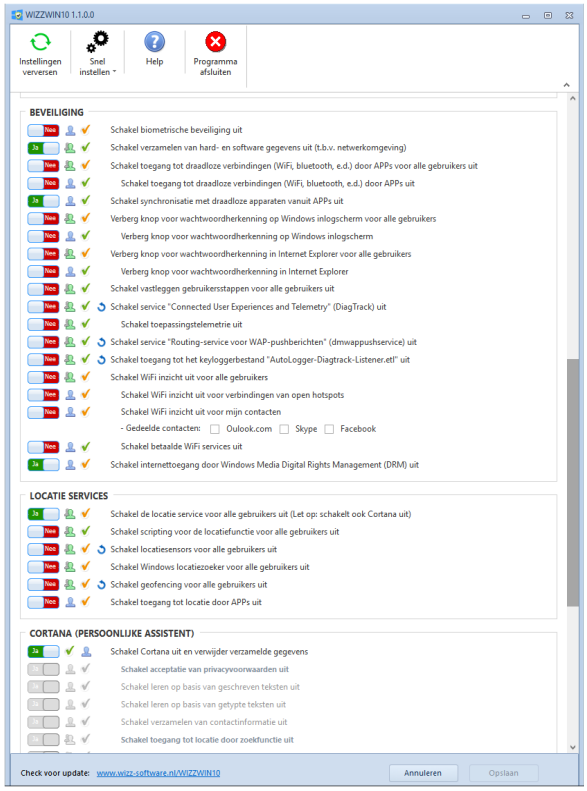
Laat je hier het vinkje staan bij Start PDF Viewer, dan zal automatisch je standaard pdf-lezer (zoals Adobe Reader) opstarten zodra het pdf-document met de knop Aanmaken is gecreëerd.

WizzWin10

https://www.wizz-software.nl/windows-10-privacy

Dat is nu eens een nuttig - en bovendien Nederlandstalig - programma om duidelijkheid te scheppen in alle privacy-instellingen van Windows 10. Je kunt hiermee ook alle ongewenste 'inbreuken' op een simpele manier in- of uitschakelen.





Deze instellingen zijn in Windows 10 zeer verspreid en kan het gebeuren dat ze na een upgrade weer op de originele instellingen komen te staan.

Met **WizzWin10** krijg je in een oogopslag een overzicht hoe het met je privacy instellingen staat. Ze zijn netjes verdeeld in categoriën zoals Beveiliging, Syncronisatie, enz. Elke individuele instelling kan je met een simpele klik aanpassen, maar je kunt ook alles ineens op de aanbevolen waarde zetten.

De gewijzigde instellingen worden in vet gedrukt, waardoor het zeer duidelijk wordt wat er is gebeurd.

Voordat de wijzigingen van kracht worden, maakt **WizzWin10** een Herstelpunt.

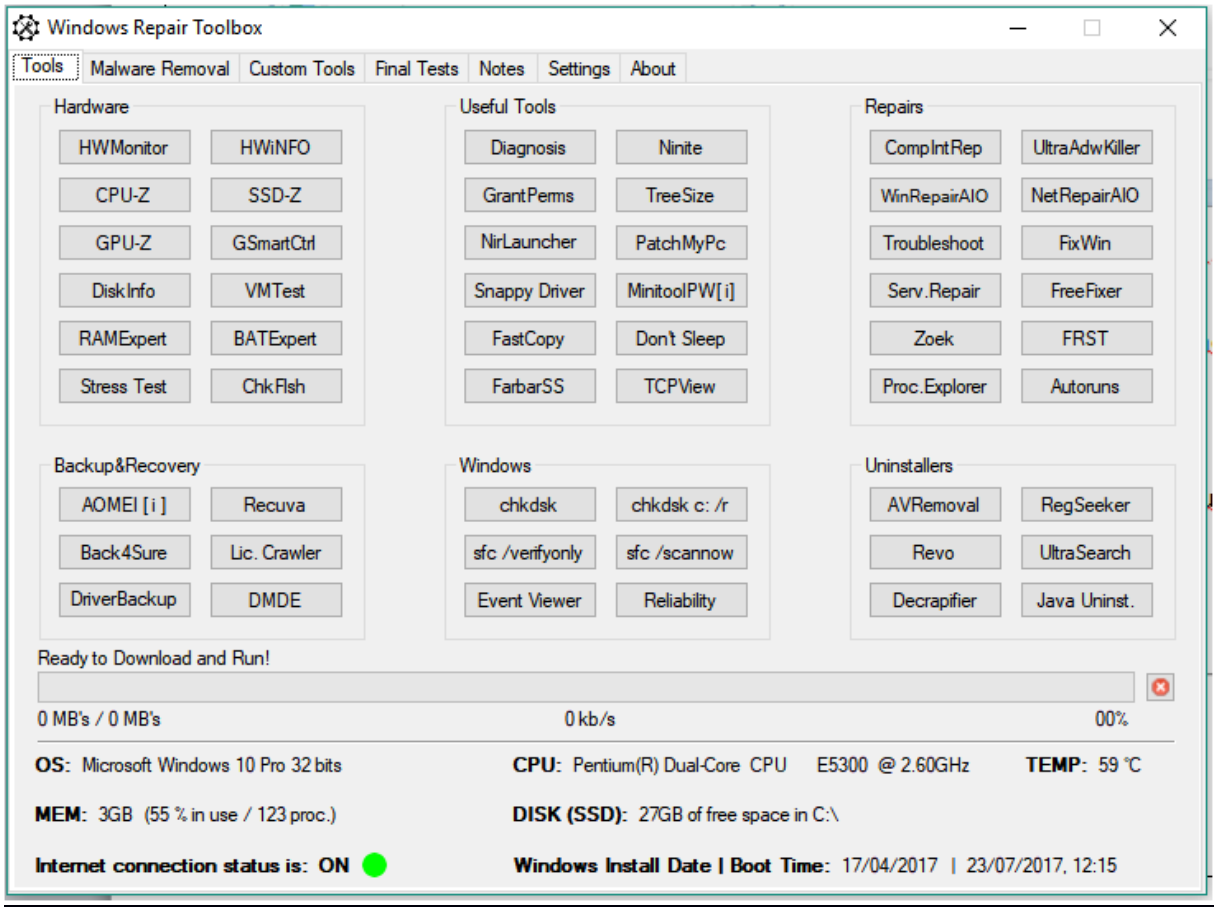
Windows Repair Toolbox

https://windows-repair-toolbox.com/

Dit is dan wel een tooltje waar je een beetje Engels moet voor begrijpen, maar het is zo nuttig dat we het er toch over willen hebben.

Af en toe blijven er Windows-problemen op te lossen en is **Windows Repair tool** uiterst nuttig. Vanaf dit programma kan je een groot aantal gratis programma's opstarten. Je kunt ook systeemonderdelen nazien die je kunnen helpen om een probleem te localiseren. Hardware diagnose is ook mogelijk.

De hulpprogramma's worden gecategoriseerd op basis van hun functie en het programma downloadt automatisch de juiste versie voor de Windows-editie waarin je werkt. Je vindt er relevante informatie weer over je computer: CPU temperatuur en % van gebruik; hoeveelheid RAM en % van het gebruik; schijfmodel, capaciteit, rotatiesnelheid, SATA-versie, hoeveelheid vrije ruimte in de systeempartitie; windows editie, installatiedatum en systeem-opstarttijd.



SNAILDRIVER

http://snailsuite.com/download-snaildriver

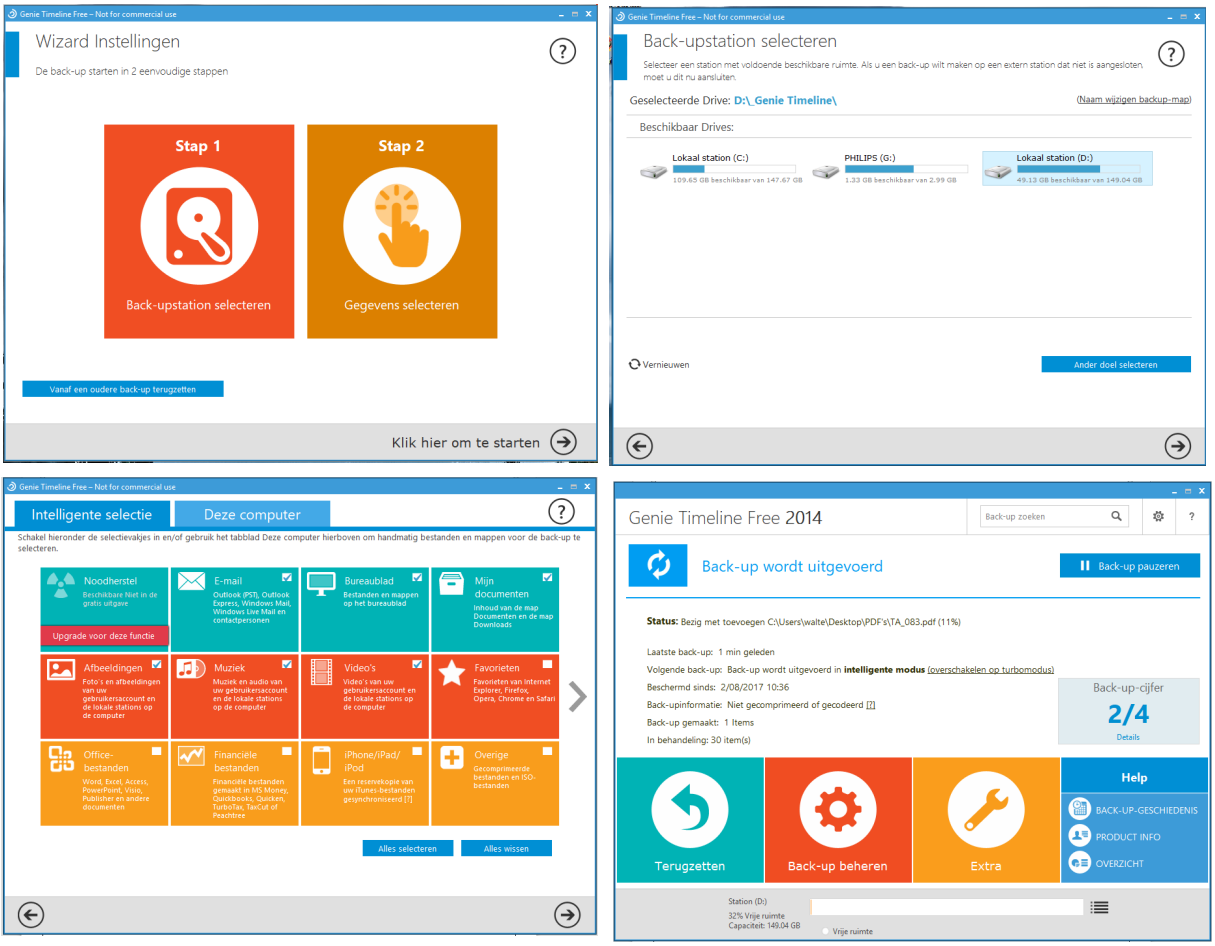
Windows moet goed communiceren met allerlei losse onderdelen die in je pc zitten of erop aangesloten zijn. Dat gebeurt door middel van stuurprogramma's en die zijn soms niet meer actueel. Hoewel stuurprogramma's het best vanaf de site van de fabrikant gedownload worden is het niet altijd evident de juiste plaats te vinden.
SnailDriver maakt dat eenvoudiger en levert keurig werk. Het programma is zeer overzichtelijk en doet zijn taak goed en snel. Binnen een minuut zie je welke onderdelen aan vervanging toe zijn en kunt je die klus vervolgens met een enkele muisklikken klaren.

Het werkingsprincipe van SnailDriver is zeer eenvoudig. Je laat je systeem scannen, na enkele seconden heeft de tool de geïnstalleerde drivers geanalyseerd en aan een online database van meer dan 300.000 drivers getoetst. Het resultaat is een lijst van stuurprogramma's die volgens het programma niet helemaal up-to-date zijn. Je verneemt om welke drivers het gaat, wat de reeds geïnstalleerde en tevens de up-to-date driver-versies zijn. Met een druk op de knop 'Update' haalt SnailDriver alle driver-updates op en begint die meteen ook te installeren.

Het programma is wel zo slim om automatisch eerst een Herstelpunt te maken zodat je nog altijd op je stappen kan terugkeren mocht er onverhoopt iets fout lopen. Het is ook wel mogelijk zelf aan te duiden welke van de drivers je niet mee wil updaten. Veel gemakkelijker dan dit kan niet. Je hoeft echter ook nauwelijks instellingsopties te verwachten.

GENIE Timeline Free

http://www.genie9.com/Free_products/download.aspx



Dat back-up's maken een meer dan noodzakelijk kwaad is, heeft Ransomware nog maar eens duidelijk gemaakt. We stellen in onze TopTips bij voorkeur gemakkelijk te gebruiken programma's voor en dit is voor Back-up programma's niet anders. Samen met AOMEI die we vroeger voorstelden is **Genie Timeline Free** net zo gemakkelijk en heeft toch wat meer mogelijkheden.

Je krijgt voor elke instelling een mooie, uitgebreide Wizard, zodat je duidelijk ziet wat er allemaal gebeurd. Je wordt vooral goed geholpen bij je keuzes voor opslaglocatie en welke mappen er belangrijk zijn. Terwijl de back-up loopt kan je ongestoord aan iets anders verder werken.

Een ideaal back-up programma om eenmalig op je PC te installeren en er verder (bijna) nooit meer naar om te kijken. Alle instructies ook in keurig Nederlands.

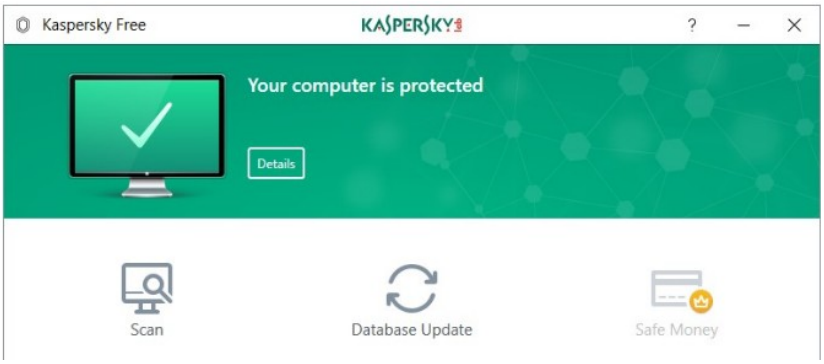
Kaspersky Antivirus Free

https://www.kaspersky.com/free-antivirus

Kaspersky heeft vanaf Juli 2017 een gratis variant van zijn virusscanner geïntroduceerd. In tests van onafhankelijke organisaties als AV-Test en AV-Comparatives scoort Kaspersky altijd zeer hoog. Nu krijg je gratis hun excellente bescherming, zonder al teveel vervelende onnodige extraatjes. Een aanrader.

Kaspersky Free biedt dezelfde beschermingsgraad als de betaalde versie, Alleen heeft u niet de beschikking over enkele extra componenten zoals Ouderlijk Toezicht, Privacy bescherming, VPN, Anti-spam, Firewall, Veilig internet bankieren en winkelen.

Kaspersky Free biedt natuurlijk wel zeer goede realtime basisbescherming van bestanden, e-mail, instant messaging (chat) en als u websites bezoekt. Verder heeft de virusscanner zelfbescherming (om te voorkomen dat malware Kaspersky uitschakelt) en kan je schadelijke bestanden in quarantaine stoppen.



Aanvankelijk moest je je **gratis registreren** met je mailadres. Nu schijnt het niet meer nodig te zijn. Tijdens de registratie kon je het vinkje weglaten bij "*I agree … to receive information…*".

SoftKey Revealer

https://sites.google.com/site/cakirbey/SoftKeyRevealer.zip?attredirects=0

SoftKey Revealer is er voor je, mocht je je licentiecode van eender welk programma kwijt zijn en je het bv. nodig hebt om het te herinstalleren.

SoftKey Revealer achterhaalt alle licenties van op je computer geïnstalleerde programma's. Heel nuttig wanneer bijvoorbeeld uw Windows-licentie sticker niet meer te lezen is of je deze verloren bent.

Je moet het programma niet installeren.
Het volstaat dat je de **SoftKeyrevaeler.exe** file op je bureaublad zet.

Je klikt op Scan en je krijgt een lijst van je codes. Meer moet dat niet zijn!

Clean Space

https://www.cyrobo.com/software/en/pages/welcome.php

Clean Space is het krachtigste programma die we ooit gebruikt hebben om je computer achterblijvers op te ruimen en je online privacy te beschermen. Echte achterblijvers zijn o.a. cache-files van diverse programma's en Windows, tijdelijke internetbestanden, logboeken, index.dat-bestanden, registeroverschotten, enz. Die objecten zitten overal verspreid op je computer, meestal in verborgen systeemmappen, waardoor je soms gigabytes aan schijfruimte kunt verspillen zonder het te beseffen.

Clean Space beschermt je online privacy door het opruimen van gebieden die verband houden met je internet browsegeschiedenis, bijvoorbeeld internetcoekies en dergelijke. Goed gewist kan niemand erachter komen wat je op het web hebt gedaan. Elke computeranalist kan gemakkelijk ontrafelen wanneer en wat je deed door het analyseren van computerlogboeken, cache en andere items. Deze mensen kunnen zelfs verwijderde items herstellen om een heldere inzicht van je activiteiten te krijgen.
Clean Space verwijdert alles die informatie over je recente activiteit bevat.

Toffe Websites…

…die je zeker moet bezoeken:

https://blogs.office.com/en-us/2013/03/19/free-office-webinars-every-tuesday-watch-videos-anytime/
Oké, je moet Engels redelijk begrijpen, maar hier kan je 50+ video's zien van Microsoft vroegere Webinars die max. 15 minuten duren. Je leert er zeker van!

http://www.copypastecharacter.com/
Hier vind je zeker een speciaal teken of icoontje die je nodig hebt. Copy+Paste het om t e kopiëren.

http://www.accountkiller.com/en/
Hier kan je definitief en grondig van een account af geraken.

https://www.printfriendly.com/
De URL in het vakje kopiëren en je bekomt een print-vriendelijke kopie.

http://www.donothingfor2minutes.com/
Uitgeput? Hier krijg je twee minuten gecontroleerde rust.

https://wetransfer.com/
Te groot voor e-mail (max. 15 MB)? Via WeTransfer kan je Gigabytes versturen!

https://www.homestyler.com/
Plannetjes maken om je nieuwe woning in te richten.

https://www.google.com/culturalinstitute/beta/?hl=nl
Fenomenale dingen van over de ganse wereld.

http://attackofthecute.com/popular.php
Grote verzameling van toffe foto's.

http://www.snesfun.com/
Toch nog gek van spelletjes?

http://drinkify.org/
Een gepast drankje bij je favoriete muziek.

Hier kan je de vorige versies van de uitgaven *in deze serie* downloaden.

Beeldscherm van TV of PC op een gemakkelijke manier beter afstellen

Het is bedroevend vast te stellen dat bij veel Tv-kijkers en zelfs Pc-gebruikers de kleurregeling van hun beeldscherm veel te wensen overlaat. Dit is jammer, want het kan op een eenvoudige manier zelf optimaal afgeregeld worden.

Beeldscherm van TV of PC op een gemakkelijke manier beter afstellen

Digitale Televisie handleiding – Hierna eens alles op een rijtje gezet om *Digitale Internet Televisie* uiteindelijk goed te integreren met je PC. Als je het stap-voor-stap doet zoals in dit document beschreven zal je je veel ergernis besparen. De gegeven informatie gold voor de datum van deze uitgave**.** **eBookDigitale_Televisie_V1.13.pdf**

De TopTips:

Top tips van PCTuts Deel 1

Top Tips van PCTuts Deel 2

Top Tips van PCTuts Deel 3

Top Tips van PCTuts Deel 4

Top Tips van PCTuts Deel 5

Top Tips van PCTuts Deel 6

Top Tips van PCTuts Deel 7

Top Tips van PCTuts Deel 8

Top Tips van PCTuts Deel 9

Top Tips van PCTuts Deel 10

Top Tips van PCTuts Deel 11

Top Tips van PCTuts Deel 12

Top Tips van PCTuts Deel 13

Top Tips van PCTuts Deel 14

Top Tips van PCTuts Deel 15

Top Tips van PCTuts Deel 16

Top Tips van PCTuts Deel 17

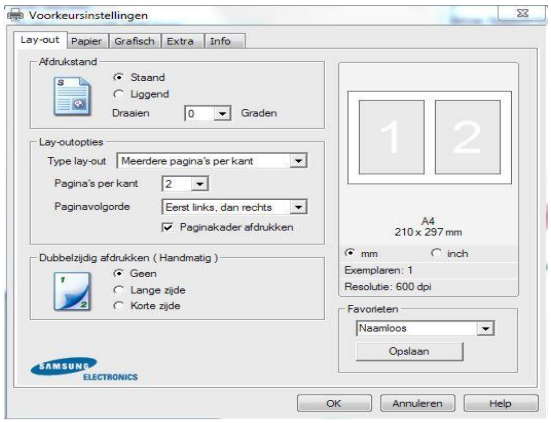
Top Tips van PCTuts Deel 18

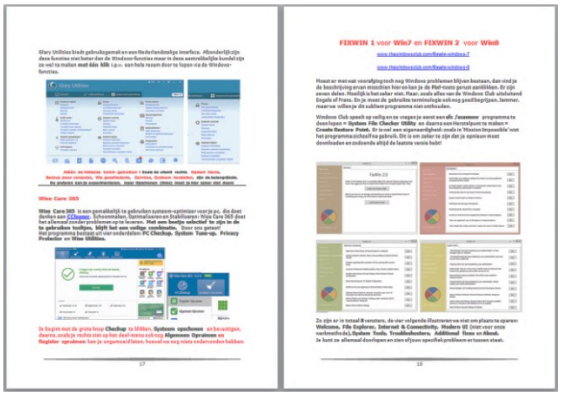
Top Tips van PCTuts Deel 19

De meeste programma's in onze TopTips zijn uitgebreid en langdurig getest door de schrijver. Deze die niet zijn getest, werden gekozen omdat ze worden aanbevolen door zeer betrouwbare bronnen. Niettemin kunnen wij (PCTuts) niet aansprakelijk gesteld worden als er iets misgaat. Het aantal variabelen in computerland is hiervoor echt te uitgebreid.
Dit geldt ook voor de vermelde websites.

Opgemaakt door **WaWa** van **PCTuts.be** = www.pctuts.be **Gratis Computerhulp**

De Lay-out is aangepast om uit te printen met 2 p./A4,





2 pagina's per **A4**

► ***Tot volgende keer met Deel XXI.*** *WaWa van PCTuts* ◄