Secure Computing

Januari 2016 JAARGANG 5

Veel lees(r)plezier

(NB: met Ctrl+ scrolwieltje kunt u de pagina vergroten en

W.Bosgra Taakaccenthouder Digitale Criminaliteit Basisteam Enschede

Secure Computing

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 oa:

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. Tweede Kamer

Dit nieuwe jaar beginnen wij met een special betreffende gratis software. Onmisbare software om uw PC schoon en veilig te houden, alsmede een gratis alternatief voor Microsoft Office. De vermelde software is gratis te gebruiken.

Het is natuurlijk aan u of u het wilt gebruiken.

Daar waar mogelijk is gezorgd voor een handleiding.

Daarnaast natuurlijk weer het gebruikelijke nieuws.

Het kabinet heeft het voorstel voor de nieuwe wet computercriminaliteit naar de Tweede Kamer gestuurd.

Nieuwe wet computercriminaliteit naar Tweede Kamer

Het voorstel geeft politie de bevoegdheid om op de systemen van verdachten in te breken. Ook kunnen verdachten via een gevangenisstraf worden gedwongen om hun encryptiesleutel of wachtwoord af te staan en wordt het wederrechtelijk overnemen en 'helen' van gegevens strafbaar.

Volgens het kabinet zijn er nu onvoldoende mogelijkheden om bijvoorbeeld wachtwoorden te achterhalen, versleuteling van gegevens ongedaan te maken en illegale acties van terroristische organisaties op het internet tegen te gaan. Indien het wetsvoorstel wordt aangenomen kunnen het Openbaar Ministerie en politie straks op afstand 'heimelijk onderzoek' doen in computers van criminelen of terroristen en gegevens vastleggen of ontoegankelijk maken, zo laat het kabinet weten. Het betreft het zogeheten 'onderzoek in een geautomatiseerd werk' dat opsporingsambtenaren ruimte geeft om bepaalde onderzoekshandelingen toe te passen. Daarbij gaat het niet alleen om het ontoegankelijk maken of het vastleggen van gegevens maar ook om observatie en het aftappen van communicatie.

Concreet geeft het wetsvoorstel de autoriteiten de bevoegdheid om in te breken op de computer van een verdachte en daar bijvoorbeeld spyware te plaatsen die het gebruik van de computer in de gaten kan houden, zoals keyloggers om toetsaanslagen af te vangen of het aanzetten van de microfoon om een gesprek af te luisteren, zo liet Anke Verhoeven van advocatenbureau SOLV eerder al weten. Op deze manier kan er veel gerichter worden getapt. Ook voorziet het wetsvoorstel in de mogelijkheid dat de overheid heimelijk toegang kan verkrijgen tot gegevens die in de cloud zijn opgeslagen, zonder dat de verdachte of dienstverlener daarbij betrokken is.

Eerder dit jaar vroeg een coalitie van organisaties, bedrijven en individuen minister Van der Steur nog om een visie te ontwikkelen over de privacybescherming van burgers in de informatiemaatschappij, daarna een publiek debat erover te faciliteren en tot die tijd de behandeling op te schorten van wetten die ertoe leiden dat burgers zonder een specifieke en concrete verdenking toch worden gevolgd. De coalitie noemde onder andere het wetsvoorstel computercriminaliteit III. De visie waarom werd gevraagd wilde de minister echter niet geven.

In Groot-Brittannië is al een decryptieplicht van kracht. Begin deze maand werd bekend dat er steeds meer Britten achter de tralies belanden omdat ze hun wachtwoord niet willen geven. Burgerrechtenbeweging Bits of Freedom hekelt het moment waarop het kabinet de plannen bekendmaakt. "En wat gaat er vrijdagmiddag onder mom van antiterrorismewetgeving naar Tweede Kamer? Precies, het hackvoorstel", zo laat de organisatie via Twitter weten.

Bron: Security.nl

Index

VPN, waarschijnlijk heb je er weleens over gehoord en zo niet, dan moet je sowieso verder lezen. Want VPN is ook voor jou belangrijk, zelfs als je nooit downloadt of streamt. Wat VPN is, en waarom je het zou moeten gebruiken?

Virtual Private Network

1 - Wat is VPN?

VPN staat voor Virtual Private Network en kun je zien als een privénetwerk binnen een groter netwerk. Meestal gaat het om een versleutelde verbinding tussen twee andere netwerken via openbare netwerken (internet). Denk aan je thuisnetwerk en het bedrijfsnetwerk van je werkgever. VPN helpt je om een soort privétunnel of -pijplijn tussen die twee netwerken te maken.

2 - Waarom VPN?

Groot voordeel van VPN: geen pottenkijkers. Doordat de verbinding is versleuteld, kan iemand die ook toegang heeft tot datzelfde netwerk jouw VPN-verbinding toch niet afluisteren. Denk aan een hotel, trein, restaurant of een andere plek met open wifi. Dankzij VPN zien sniffers (afluisteraars) geen zinnige informatie voorbijkomen. Wel zo prettig als je je bankzaken of andere privédingen regelt.

3 - Wanneer VPN?

Van oudsher wordt VPN gebruikt in zakelijke omgevingen om werknemers overal ter wereld toch toegang tot het bedrijfsnetwerk te geven. De laatste maanden/jaren wordt VPN ook interessant voor particulieren. Zeker waar de overheid en andere diensten steeds meer meegluren met wat je op internet aan het doen bent. Daarnaast kunnen bepaalde diensten je niet zo makkelijk blokkeren als je uit een bepaald (voor hen ongewenst) land komt, omdat je met een VPN-dienst het kan laten lijken dat je uit een ander (wel gewenst) land komt.

4 - Ben ik echt anoniem met VPN?

Nee, echt anoniem op internet ben je nooit. Je internetprovider weet met wie je contact maakt, bijvoorbeeld je VPN-dienst. Je VPN-dienst weet wel wat je doet, maar houdt daar normaal gesproken geen logs van bij. Toch hoeft er maar iemand een tap te plaatsen en je bent gezien. Gelukkig kan dat niet zomaar, dat is zelfs voor een overheid, geheime dienst of andere kwaadwillige geen koud kunstje.

5 - Welke VPN-protocol kan ik het beste gebruiken?

De meest gebruikte protocollen zijn PPTP, L2TP/IPsec en OpenVPN. De meeste VPN-diensten en VPN-software ondersteunen deze drie protocollen. PPTP is de minst veilige en is relatief eenvoudig te kraken. Niet gebruiken dus! Het beste en snelste is OpenVPN, maar niet elk apparaat ondersteunt dat. Mocht je OpenVPN niet aan de praat krijgen, kies dan voor L2TP/IPsec.

6 - Thuis of extern?

Wil je vooral voorkomen dat niemand je internetgebruik kan zien als je onderweg bent? Dan kun je prima een VPN-verbinding met je thuisnetwerk opzetten. Dit kan via je router of NAS, of via een computer thuis die je altijd aan laat staan. Hiermee loopt al het internetverkeer op je smartphone via je internetverbinding thuis en kun je veilig op openbare wifi-netwerken je gang gaan. Zorg wel dat je een snelle internetverbinding thuis hebt, liefst via de kabel of glasvezel. Wil je ook thuis voorkomen dat men weet wat je online doet, maak dan gebruik van een VPN-dienst.

7 - Betaald of gratis?

Gratis VPN-diensten hebben beperkingen op snelheid, hoeveelheid data, aantal verbindingen of een combinatie hiervan. Wil je alleen veilig je mail op je smartphone of tablet checken als je niet thuis bent, dan biedt bijvoorbeeld VyprVPN een gratis abonnement aan waarmee je 500 megabyte per maand kunt verbruiken. Wil je meer, dan moet je gaan betalen.

Voor meer info over diverse VPN-diensten kun je kijken op www.bestvpn.com.

8 - Hoe zit het met mijn snelheid?

Gebruik je VPN, dan gaat dat altijd ten koste van je snelheid. Je aanvraag voor een bepaalde webpagina of andere internetinfo gaat niet meer direct naar die webserver, maar eerst naar de server van je VPN-dienst, dan naar die webserver, weer terug naar je VPN-dienst en dan weer naar jou. En dat gaat continu zo door. Heb je een snelle kabel- of glasvezelverbinding, dan hoef je er amper wat van te merken. Daarnaast heb je de extra rekenkracht die de versleuteling vraagt. Voor een dikke pc geen probleem, maar op sommige mobiele apparaten merk je er wel wat van. Ben je gamer, dan is een lage ping heel belangrijk en daar zijn de extra tussenstappen van een VPN-dienst niet bevorderlijk voor. In alle gevallen: test eerst of de VPN-dienst snel genoeg voor je is. Veel diensten bieden proefpakketten.

9 - Wat zijn alternatieven voor VPN?

Veelgenoemde alternatieven voor VPN zijn Tor en een anonieme proxy. Die laatste wordt gebruikt om regiogebonden content van bijvoorbeeld Netflix, Hulu, BBC iPlayer en Uitzending Gemist toch op een andere plek te kunnen bekijken. Veel anonieme proxy's doen alleen niets voor jouw privacy, sterker nog, ze delen deze gegevens met anderen. Bij Tor, een netwerk waarop je anoniem kunt surfen, is je privacy in principe wel goed geregeld, maar ook hier zijn er weleens 'infiltranten' en is de snelheid vaak een zwak punt.

Voor meer info over diverse VPN-diensten kun je kijken op www.bestvpn.com.

VPN installeren? Kijk hier.

Bron: ZDnet

Index

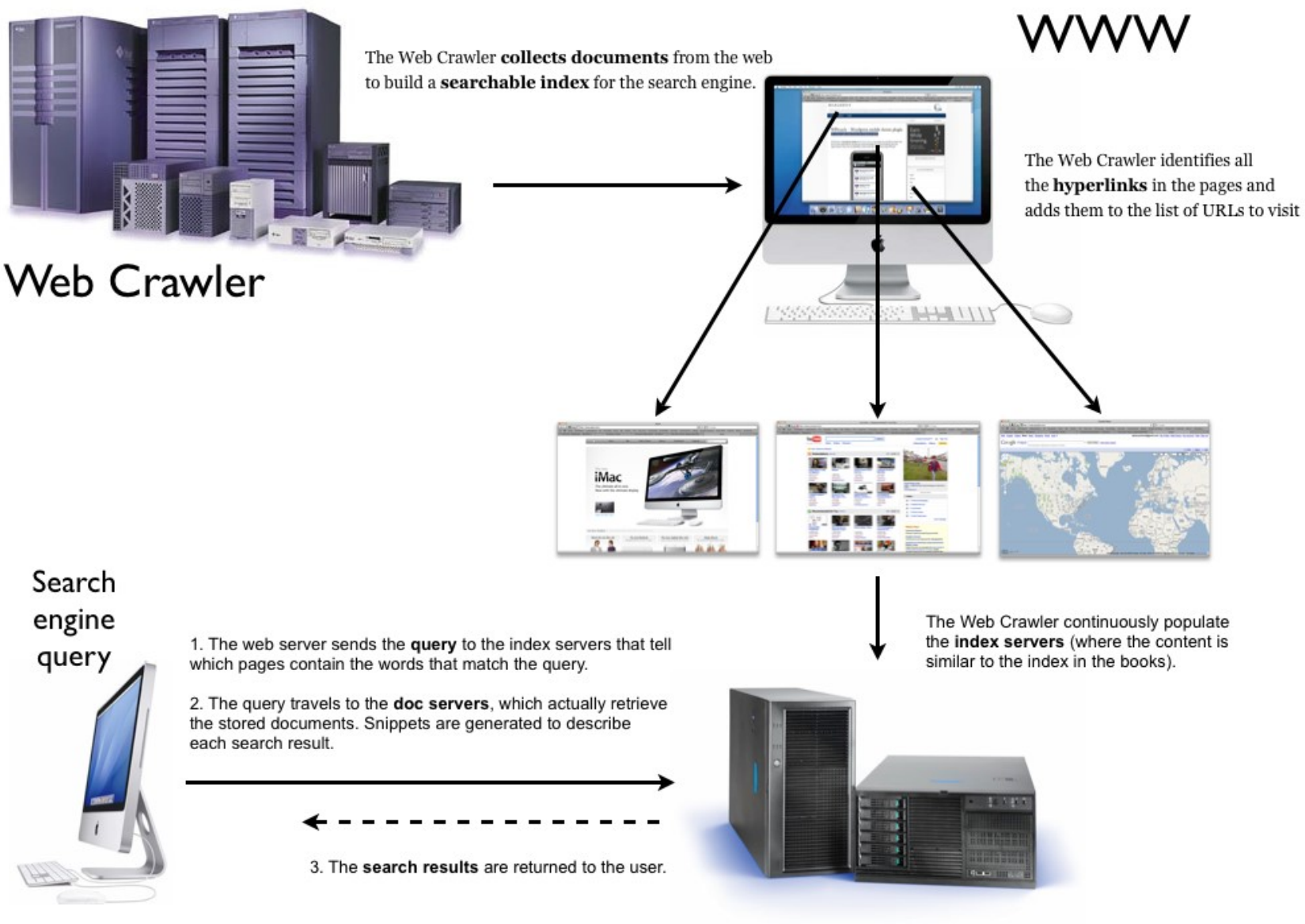
De politie heeft een webcrawler ontwikkeld om advertenties van loverboys op internet te vinden.

Webcrawler politie speurt naar advertenties loverboys

Dat blijkt uit een brief (pdf) van minister Van der Steur van Veiligheid en Justitie aan de Tweede Kamer. Volgens Van der Steur laten verschillende recente zaken zien dat de Loverboyproblematiek nog altijd actueel is.

Het gaat hier om mensenhandelaren die met verleidingstactieken, manipulaties, chantage en geweld meisjes inpalmen om hen later voor zich te laten werken in de prostitutie of illegale sectoren, aldus de minister. Om de problematiek aan te pakken zijn er verschillende initiatieven gestart. Zo heeft de politie een webcrawler (ook wel Sipeder genoemd) ontwikkeld waarmee verdachte advertenties op internet op basis van zoektermen automatisch kunnen worden doorzocht. Hierbij is het mogelijk om na te gaan wie die advertenties heeft geplaatst en welke personen erop de advertentie hebben gereageerd.

Dit stelt de politie in staat gerichter te zoeken naar minderjarige slachtoffers van mensenhandel, de loverboys die hen aanbieden, en de klanten die hen bezoeken. De webcrawler wordt ingezet voor controleacties in de prostitutiebranche. Momenteel wordt de webcrawler verder ontwikkeld om de van het internet gehaalde resultaten nog effectiever te kunnen benutten voor de handhaving en opsporing, aldus Van der Steur. Hij stelt dat de webcrawler een belangrijk instrument vormt om mensenhandelaren - inclusief loverboys - op te sporen, ook wanneer er nog geen aangifte is gedaan.



Bron: Min. Veiligheid en Justitie

Index

Europese bedrijven mogen de persoonlijke chat- en e-mailberichten van werknemers die onder werktijd en vanaf werkcomputers worden verstuurd monitoren, zo heeft het Europees Hof voor de Rechten van de Mens bepaald .

Europees hof: bedrijven mogen privémail monitoren

De zaak was door een Roemeense man aangespannen, nadat hij was ontslagen door zijn Roemeense werkgever omdat hij zijn zakelijke Yahoo-account voor persoonlijke communicatie had gebruikt.

Volgens de man had de werkgever zijn recht op respect voor privé- en gezinsleven en correspondentie geschonden. De man werkte van 2004 tot en met 2007 als sales engineer voor het Roemeense bedrijf. Voor zijn werk moest hij een Yahoo Messenger-account aanmaken, om vragen van klanten te beantwoorden. In juli 2007 liet zijn werkgever weten dat zijn berichten gedurende meerdere dagen waren gemonitord. Daaruit bleek dat hij het bedrijfsbeleid had geschonden door de dienst ook voor privécommunicatie te gebruiken.

Volgens de rechter in Straatsburg is het niet onredelijk voor een werkgever om te controleren dat werknemers hun werk tijdens werkuren uitvoeren. In het geval van de Roemeense man was de monitoring daarnaast beperkt in omvang en proportioneel. Ook had de Roemeen niet goed uitgelegd waarom hij het zakelijke Yahoo-account voor privézaken had gebruikt.

Bron: Europees Hof

Index

De afgelopen jaren zijn duizenden Franse bedrijven het slachtoffer van de 'ceo-fraude' geworden, ook bekend als Business Email Compromise, en voor miljoenen euro's opgelicht.

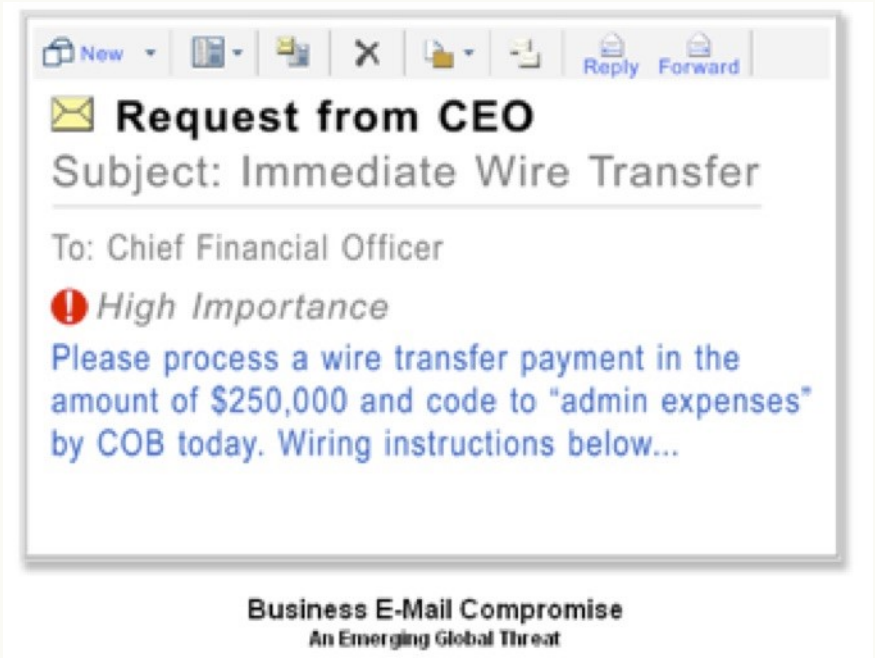
CEO fraude

Onder de getroffen bedrijven bevinden zich grote namen, zoals Michelin, KPMG en Nestle.

Oplichters sturen financiële personen binnen de organisatie een e-mail die zogenaamd van de directeur afkomstig is, waarin staat dat er met spoed een bedrag moet worden overgemaakt. De rekening waar het geld naar toe moet worden overgemaakt is in handen van de criminelen. De afgelopen vijf jaar zijn op deze manier naar schatting 15.000 Franse bedrijven opgelicht, met een schadebedrag van 465 miljoen euro. Eén bedrijf zag hoe de oplichters 32 miljoen euro buitmaakten, aldus de Franse politie.

Naast het sturen van e-mails worden de bedrijven ook telefonisch benaderd. Eén van die bedrijven is Etna Industrie. De accountant van het bedrijf werd door iemand gebeld die vertelde dat de directeur een e-mail zou sturen met instructies voor een vertrouwelijke transactie en alle instructies moesten worden uitgevoerd. De accountant kreeg vervolgens een e-mail die zogenaamd van de directeur afkomstig was. Vervolgens volgden er nog verschillende e-mails en telefoontjes.

Uiteindelijk maakte de accountant 500.000 euro over naar de oplichters. De bank wist verschillende transacties te stoppen, maar één transactie van 100.000 euro was succesvol voor de oplichters. Het bedrijf kreeg dit bedrag na een rechtszaak vergoed, hoewel de bank tegen het vonnis van de rechtbank in beroep is gegaan. Volgens Aaron Higbee van beveiligingsbedrijf PhishMe zijn de aanvallen zo succesvol omdat personeel opdrachten van managers minder snel in twijfel trekken en er ook een gevoel van urgentie meespeelt.



Bron: BBC

Index

Wie twittert of post dat hij tégen de komst van een azc is, moet er tegenwoordig rekening mee houden dat de politie even langs komt.

Politie aan de deur: “U twittert wel heel veel”

In uniform en liefst in een herkenbare auto, zodat de rest van de straat het ook ziet. In onder meer Leeuwarden, Enschede en Kaatsheuvel kregen al tientallen mensen huisbezoek.

De politie probeert met die bezoekjes de burger duidelijk te maken ‘welk effect een post of tweet kan hebben’, aldus een woordvoerder. De agenten vertellen dat de tweets opruiend kunnen overkomen, dan wel ‘te ver gaan’ maar vragen soms ook gewoon of voor de geplande demonstratie wel een vergunning verkregen is.

Er is veel kritiek op zulke huisbezoeken. Logischerwijs van de protesterende burgers. Die roepen over een politiestaat, vrijheid van meningsuiting en dat ze de mond gesnoerd wordt. Terwijl de bedreigingen die sommigen uiten, niet mals zijn. ‘Laat ze oprotten die teringleiers, we gaan met z’n allen naar het gemeentehuis’. Of de vraag of ‘we er hier ook een Geldermalsen van gaan maken’. Tja. Is dat nou vrijheid van meningsuiting, is het haatzaaien dan wel een oproep tot geweld? Volgens een woordvoerder van de nationale politie is het onderscheid soms moeilijk en wordt per geval een nieuwe inschatting gemaakt.

Het tv-programmaEenVandaag sprak met journalist Huub Bellemakers die via twitter ‘een grappig verband’ wilde leggen tussen een verloren voetbalwedstrijd en reacties op asielzoekers. ‘Morgen protesteren in Zeist. Bivakmuts op. Wij burgers pikken dit niet meer #kominverzet’, twitterde hij. Waarop de politie aan de deur kwam. Er was immers geen link te bedenken tussen voetbal en azielzoekers.

Er is ook kritiek van politiedeskundigen. Zo spreekt hoogleraar strafrecht Nico Kwakman (RU Groningen) van een subtiele grens die gemakkelijk overschreden wordt. Hij denkt echter dat in bepaalde gevallen ‘fout ingeschat wordt wat [een huisbezoek] voor de desbetreffende persoon betekent’. Kwakman denkt dat het handiger is dit door een ambtenaar zónder uniform te laten doen. ‘Als er een politieman komt vertellen dat wat je doet niet in de haak is, voel je je gekleineerd en gecriminaliseerd’.

Politiekenner Jaap Timmer (VU) ziet de politie gewoon met haar tijd meegaan. ‘Als iemand vroeger in een café zei dat hij ging demonstreren en dat de ruiten eruit zouden gaan, zou diegene ook een huisbezoekje krijgen. De politie heeft kennelijk ontdekt dat het publieke domein zich ook op sociale media afspeelt’.

Dat beaamt districtschef Arjan Mengerink (eenheid Oost) die tegen EenVandaag zei dat de politie op twitter en facebook ingrijpt ‘net zoals we dat op straat ook doen’. Volgens Mengerink overschrijdt je een grens als je iets schrijft ‘waardoor een ander strafbare feiten kan gaan plegen’. Hij geeft ook toe dat het allemaal nieuw is en ‘dat we onze weg nog een beetje moeten vinden’.

Er is meer kritiek. Lees hier.

Bron: Cops in Cyberspace

Index

De Nederlandse banken zijn een nieuwe televisiecampagne gestart waarbij ze consumenten voor bankpas-phishing waarschuwen, aangezien criminelen hier gebruik van maken.

Banken starten tv-campagne tegen bankpas-phishing

Slachtoffers ontvangen een e-mail waarin staat dat de bankpas wordt vervangen en er een nieuwe moet worden aangevraagd.

De link in de e-mail wijst naar een phishingiste die om de pincode vraagt. Tevens wordt er gevraagd om de pinpas naar een inleverpunt te sturen. Op deze manier hebben criminelen al bijna 2 miljoen euro weten te stelen, zo maakte de politie gisteren bekend. Om consumenten voor deze vorm van phishing te waarschuwen laat Betaalvereniging Nederland, waar onder andere de banken lid van zijn, een nieuwe televisiereclame zien. In de commercial verschijnt 'Marc', die in zijn bestelbus door Nederland op phishingpatrouille gaat.

"Zodra hij een onveilige situatie vermoedt, grijpt onze knullige held daadkrachtig in. De manier waarop hij ingrijpt en zijn leuzen "Hang op! Klik weg! Bel uw bank!" benadrukken op een luchtige manier hoe u uzelf kunt verdedigen tegen internetcriminelen. Een boodschap die we inmiddels goed kennen, maar dan in een nieuw jasje", aldus Betaalvereniging Nederland. Volgens de organisatie zijn de fraudecijfers de afgelopen jaren flink afgenomen en gaan criminelen daarom op zoek naar nieuwe vormen van fraude.

Op verzoek van de gezamenlijke banken besteedt de Betaalvereniging in haar nieuwe campagne aandacht aan één van deze vormen van fraude. "Op dit moment vragen criminelen of u uw betaalpas op wilt sturen. Uw pincode hebben zij vaak al op een ander moment van u afgekeken, of u heeft hem zonder dat u het doorhad online ingevuld. Soms vragen zij u de pincode met uw betaalpas mee te sturen", zo stelt de organisatie. De commercial laat consumenten echter weten dat ze nooit hun pas moeten opsturen.

Bron: Security.nl

Index

Vaak bedenk je twee seconden nadat je een bericht hebt verstuurd dat je iets bent vergeten. Was de bijlage wel toegevoegd? Heb ik de spelling goed gecontroleerd? Met een snelle internetverbinding ben je na één seconde al te laat.

Voorkom dat e-mails direct worden verstuurd

Gmail

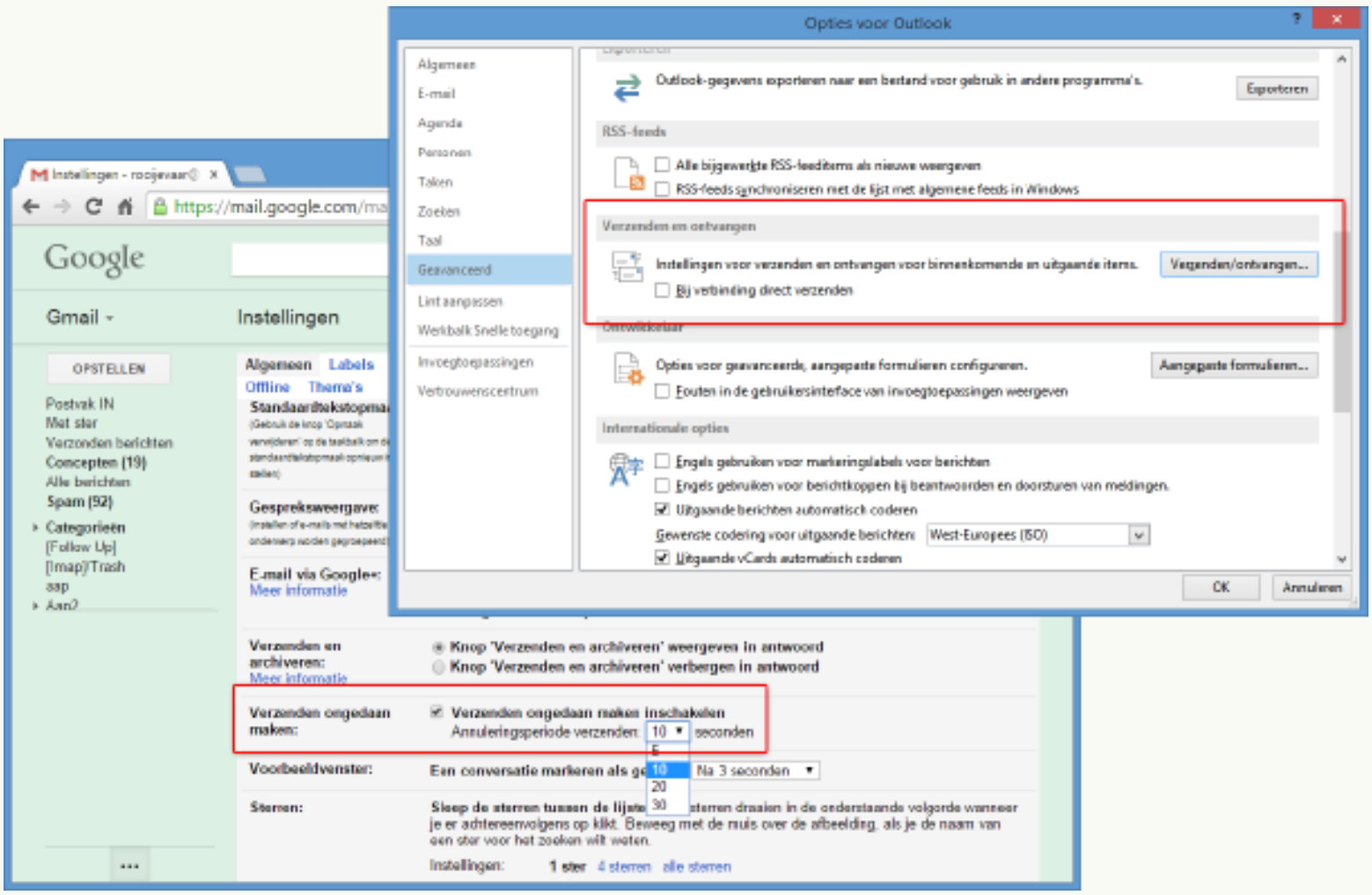
Excuses maken omdat je een bijlage bent vergeten staat niet al te snugger en dat geldt helemaal voor slordige spelfouten. Dit alles is eenvoudig te voorkomen door extra 'bedenktijd' in te bouwen en berichten niet direct te versturen. In Gmail klik je op het icoontje met het tandwieltje.
Kies Instellingen en zoek in het tabblad Algemeen naar Verzenden ongedaan maken. Activeer deze optie en geef in het keuzemenu aan hoe lang je de tijd wilt hebben om een mail 'in te trekken', bijvoorbeeld 30 seconden. Zodra je nu een bericht verstuurt, krijg je de melding Bericht is verzonden met hiernaast de optie Ongedaan maken.

Outlook

Het is in Outlook 2013 eenvoudig om te voorkomen dat je mail direct wordt verstuurd zodra je op de verzendknop klikt. Ga naar Bestand > Opties > Geavanceerd en kijk bij Verzenden en ontvangen. Verwijder het vinkje Bij verbinding direct verzenden. Klik hierachter ook op de knop Verzenden/ontvangen om te voorkomen dat Outlook na een x-aantal minuten berichten automatisch alsnog verzendt en ontvangt.
Vanaf nu belandt een bericht dat je verstuurt via de knop Verzenden eerst in het Postvak UIT. Pas als je op Alle mappen verzenden/ontvangen (of op F9) klikt wordt het bericht daadwerkelijk verstuurd.

Thunderbird

In Thunderbird zijn er meerdere manieren om berichten niet direct te versturen. De eenvoudigste manier is via de uitbreiding Send later. Zoals de naam al doet vermoeden, worden berichten niet direct verstuurd, maar op een later tijdstip. Wanneer dit gedaan wordt, bepaal je zelf. Een andere manier vereist discipline. Zoals veel mensen weten werkt de Ctrl + Enter in bijna elk mailprogramma om een bericht direct te versturen. Als je in Thunderbird Ctrl + Shift + Enter gebruikt, wordt het bericht niet verstuurd maar belandt het in je Postvak UIT. Pas als je de opdracht geeft om berichten te versturen, gaat je mail de deur uit.



Bron: ZDnet

Index

Deze gratis virusscanner van Chinese makelij maakt gebruik van verschillende engines om bestanden op kwaadaardige code te scannen. Zo is er onder meer een cloud-egine, Qihoo's eigen QVMII en het benut technologie van Avira en Bitdefender.

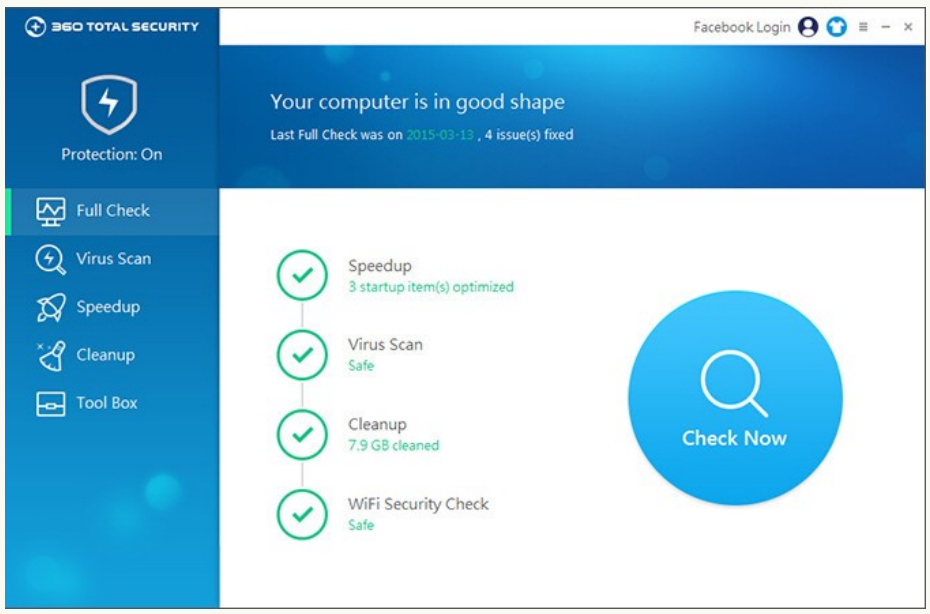
360 Total Security

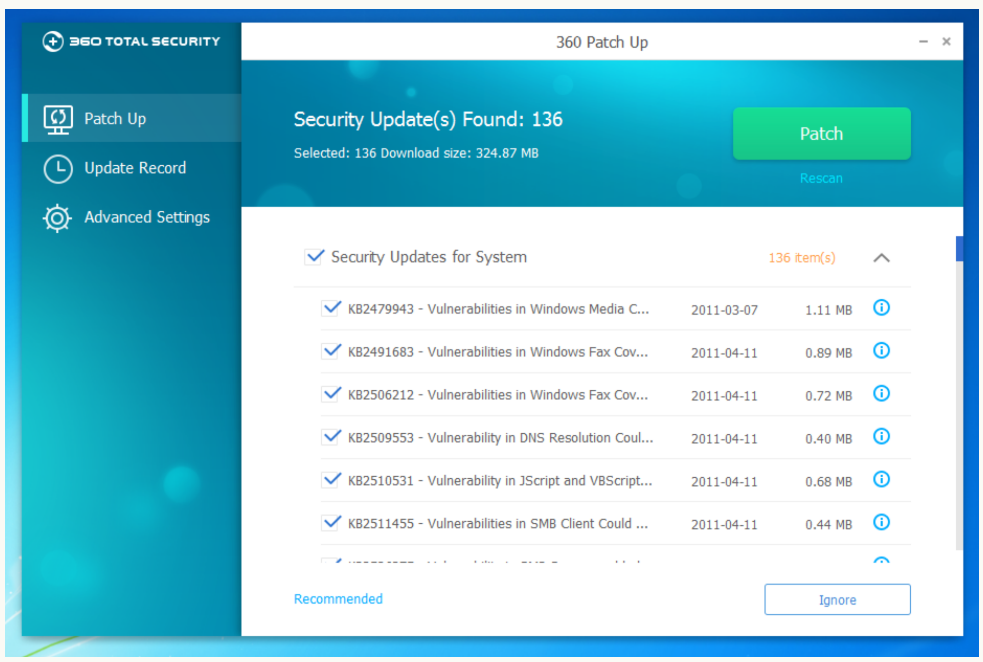
360 Total Security. De naam zegt het al. Dit programma is een totaal oplossing voor veilig computergebruik. Het is een virusscanner en optimalisatie programma in 1. Het maakt gebruik van 4 virusengines, waaronder die van Bitdefender en Avira.

Het is eenvoudig in gebruik en scoort als een van de beste gratis anti-virus programma's in de laatste testen.

Verder zorgt het voor browserprotectie, speed up, patch up en clean up.

De aanwezige toolbox geeft u nog meer optimalisatie mogelijkheden.





Bron: 360 Total Security

Index

CCleaner (voorheen Crap Cleaner) is een freeware-programma gemaakt door Piriform om computers te onderhouden die werken onder Windows en OS X. Het programma probeert het systeem "schoon" te maken door het opsporen en verwijderen van overbodige, ongebruikte of ongeldige bestanden.

Piriform CCleaner

Windows opschonen[bewerken]

Het programma kan Windows opschonen door middel van deze selectie:

Tijdelijke internetbestanden

Cookies

Geschiedenis

AutoAanvullen-geschiedenis

Recent getypte URL's

Prullenbak

Klembord

Logbestanden

Rechtermuismenu van Windows Verkenner

Register opschonen[bewerken]

Ook kan het register worden opgeschoond.

Hierbij kan door de gebruiker een selectie worden gemaakt uit volgende mogelijkheden:

Ontbrekende gedeelde DLL-bestanden

Niet gebruikte bestandsextensies

Problemen met ActiveX en bestandsklasse

Type bibliotheken

Applicaties

Lettertypes

Applicatiepaden

Helpbestanden

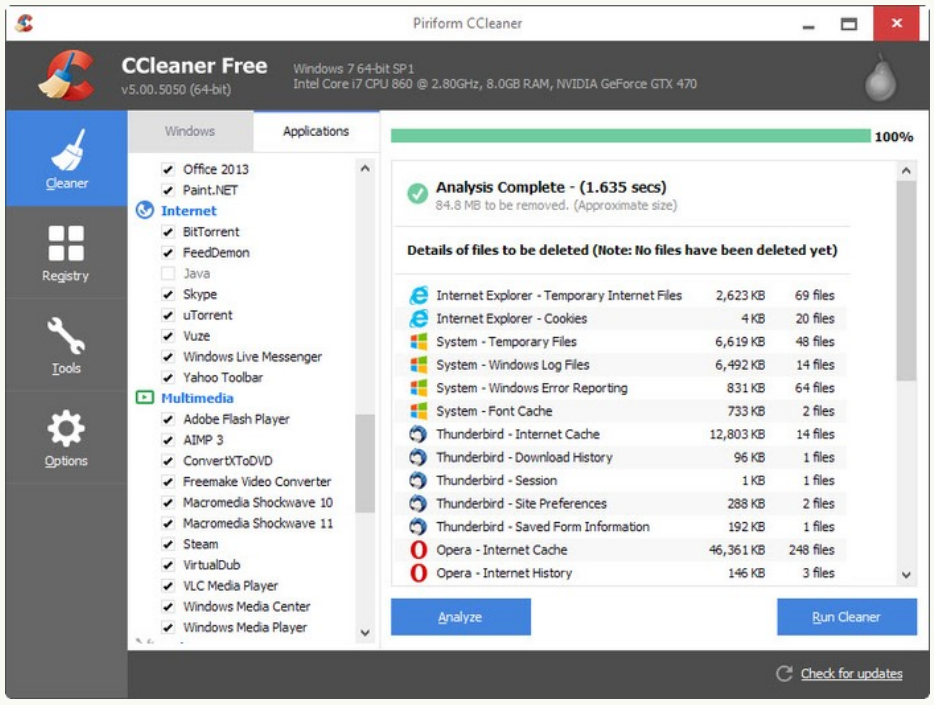
Installatieprogramma

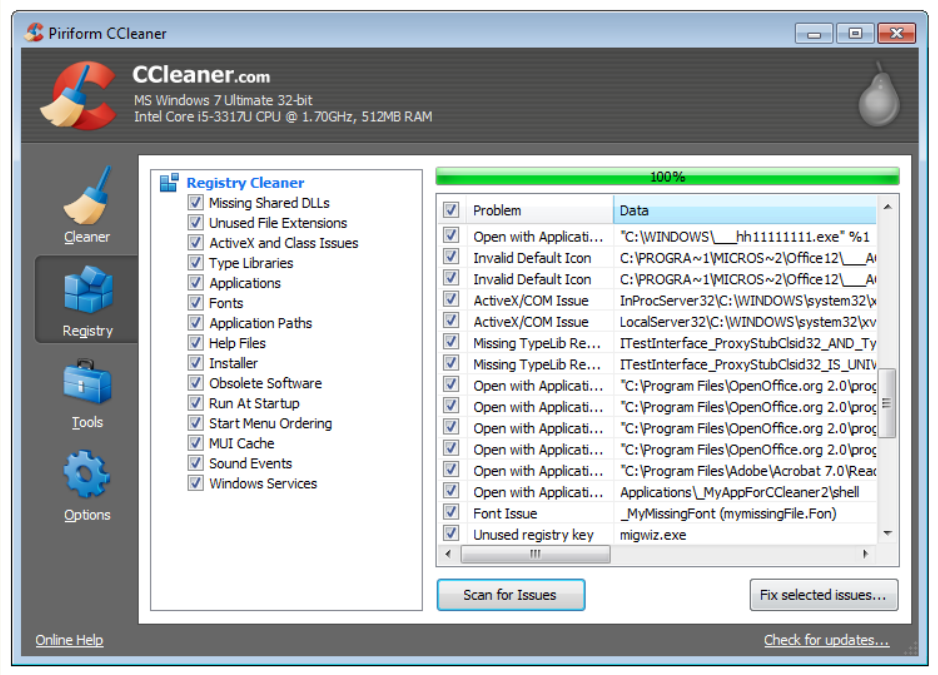
Verouderde software

Uitvoeren tijdens opstarten

Volgorde iconen Startmenu

MUI-cache





Bron: Piriform

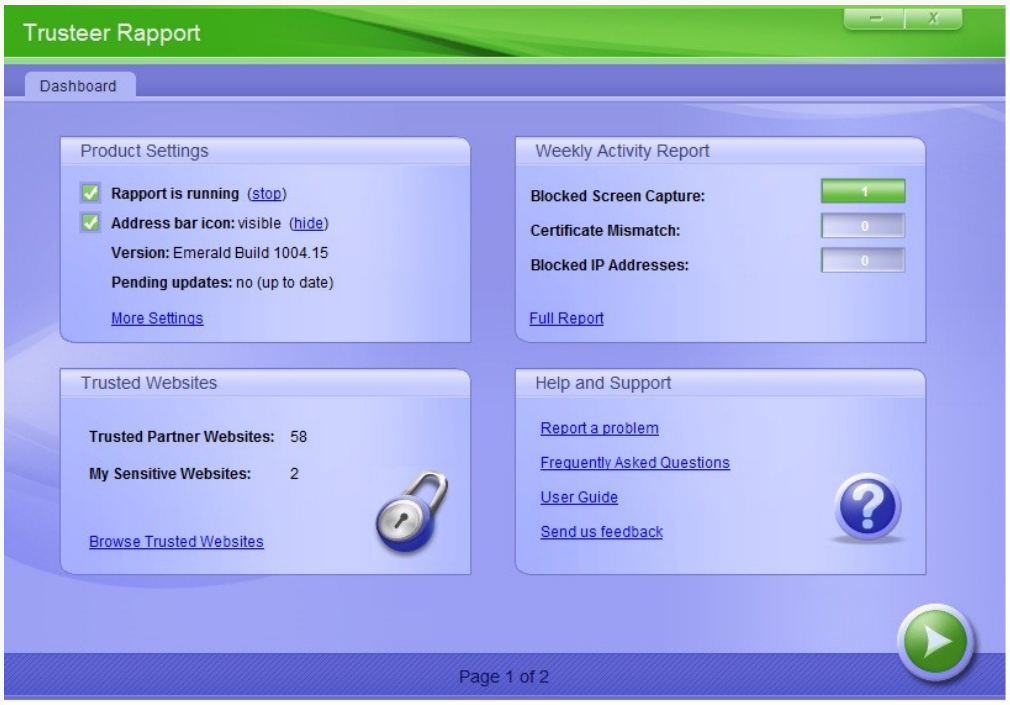
Index

Naast uw virusscanner, firewall en anti-spyware, beschermt IBM Security Trusteer Rapport uw computer of laptop tegen kwaadaardige software.

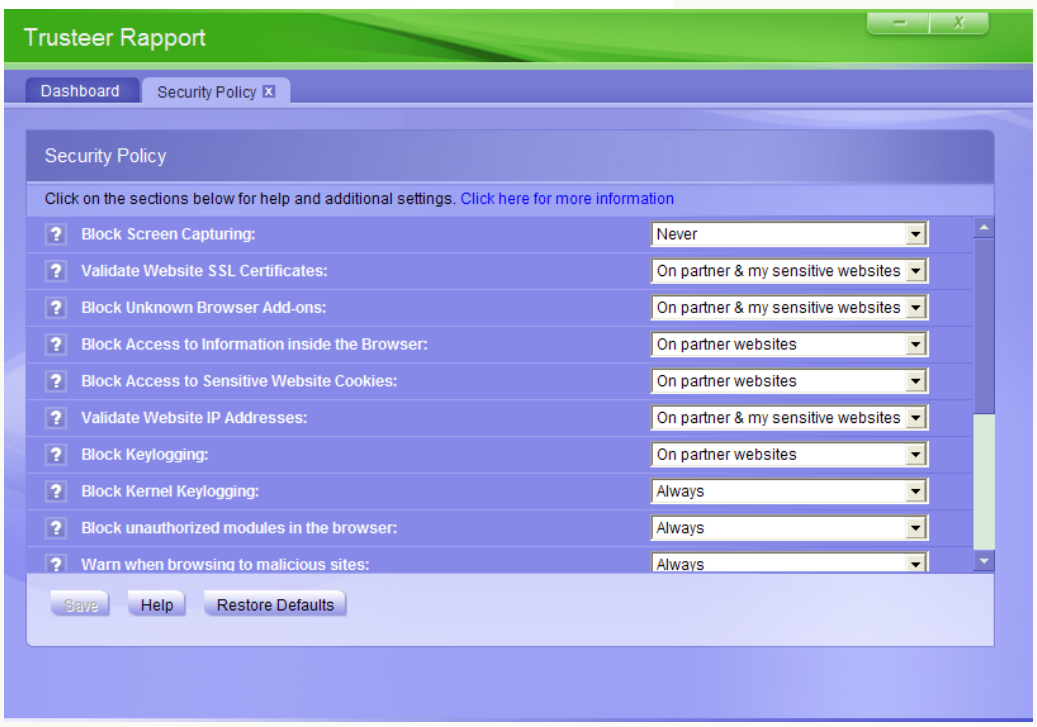
IBM Security Trusteer Rapport

Wat doet IBM Security Trusteer Rapport

Trusteer is een programma dat wereldwijd door banken gebruikt wordt. Naast uw virusscanner, firewall en anti-spyware beschermt het uw computer of laptop specifiek tegen kwaadaardige software (malware) gericht op internetbankieren. Met name de echtheid van de website waarop u uw inloggegevens invoert, wordt nauwlettend gecontroleerd.



Powered by Trusteer



Bron: ING

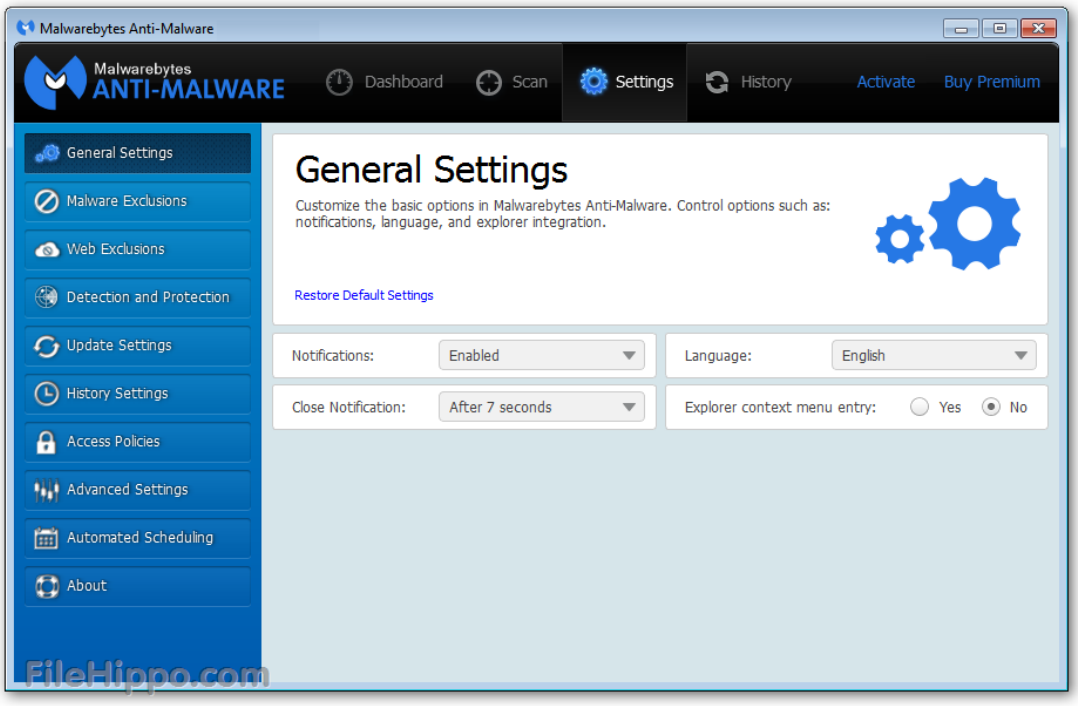
Index

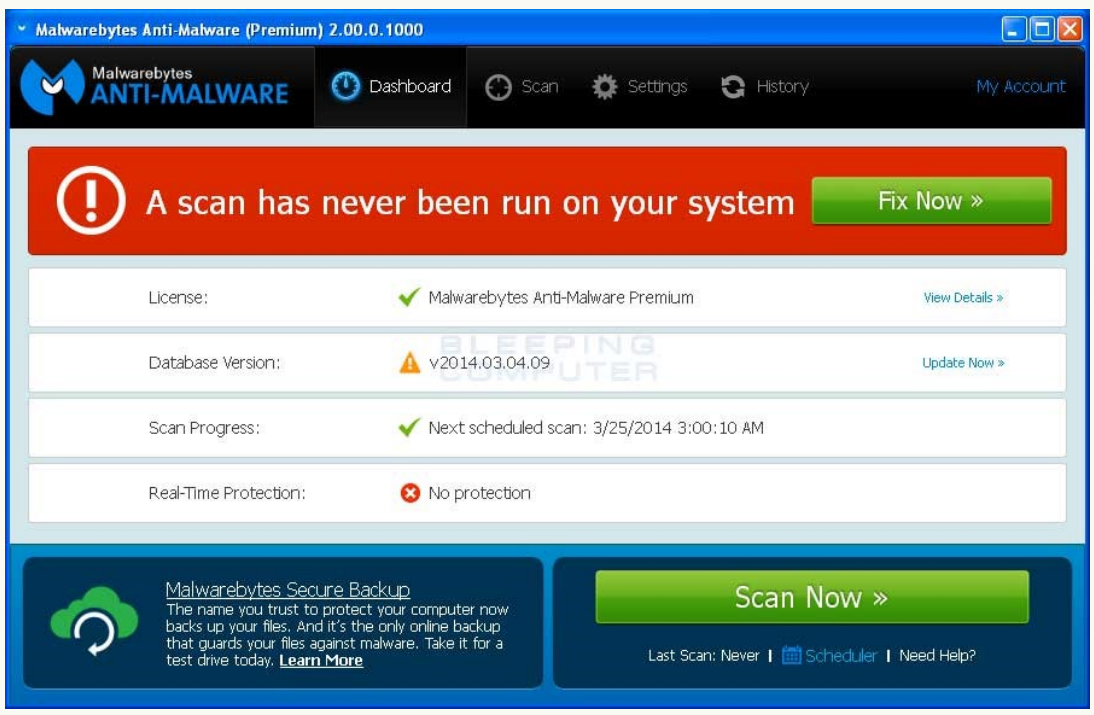
Malwarebytes Anti-Malware scant, detecteert en verwijderd kwaadaardige software zoals malware, spyware, trojans, rootkits, rogues, spyware, en andere gevaarlijke programma's op je PC.

Malwarebytes Anti-Malware

Het programma is erg belangrijk voor de beveiliging van al je computers. Daarnaast is het programma erg klein en de scan functie werkt erg snel waardoor je je computer binnen enkele minuten kunt scannen en kwaadaardige bestanden kunt laten verwijderen. Doordat de makers van het programma dagelijks bezig zijn met het updaten van het programma is het belangrijk om het programma regelmatig te updaten om ook beschermt te zijn tegen de nieuwste infecties.

Malwarebytes is gratis te downloaden en te gebruiken.





Bron: Mallwarebytes

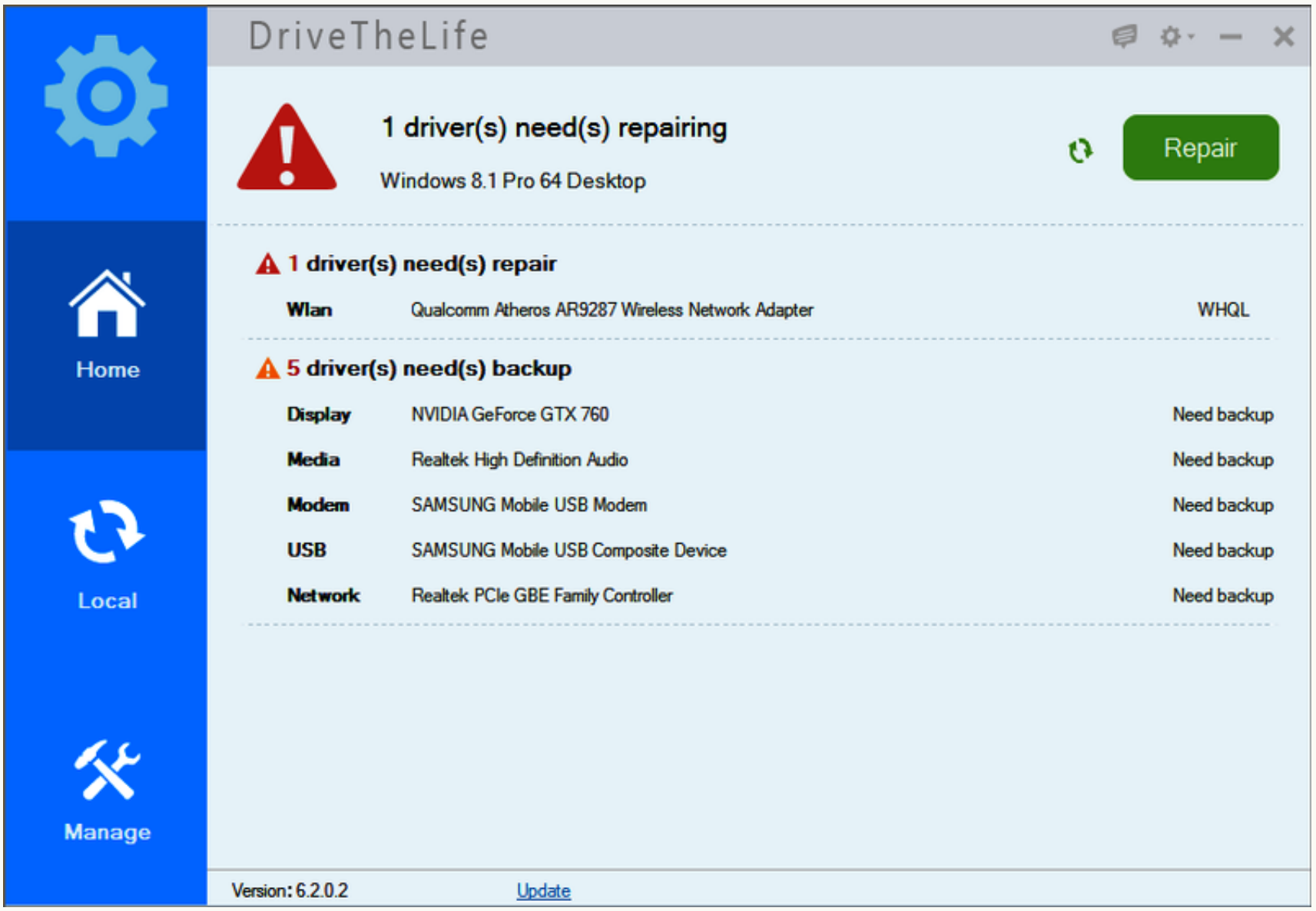
Index

DriveTheLife scant je pc en let daarbij vooral op hoofdzaken (audio, video, enzovoort). Het programma ziet stuurprogramma's die niet goed werken of die verouderd zijn en stelt je dan in staat deze te vervangen. Ook kun je bestaande drivers opslaan en usb-apparaten beheren.

DriveTheLife / Driver Talent

Sommige software-onderdelen moet je voor je eigen veiligheid altijd up-to-date houden maar dat geldt doorgaans niet voor stuurprogramma's. Daarvoor geldt meestal: als het goed werkt, lekker laten werken. Een nieuw stuurprogramma kan echter wel de prestaties van je pc verbeteren, iets dat zeker bij grafische kaarten vaak het geval is.

Om niet voor onaangename verrassingen te komen staan is het voor het updaten wel handig om stuurprogramma's eerst te back-uppen. Een handige totaaloplossing voor beide handelingen is DriveTheLife. Inmiddels is de naam aangepast en heet het nu Driver Talent.



Bron: DriveTheLife

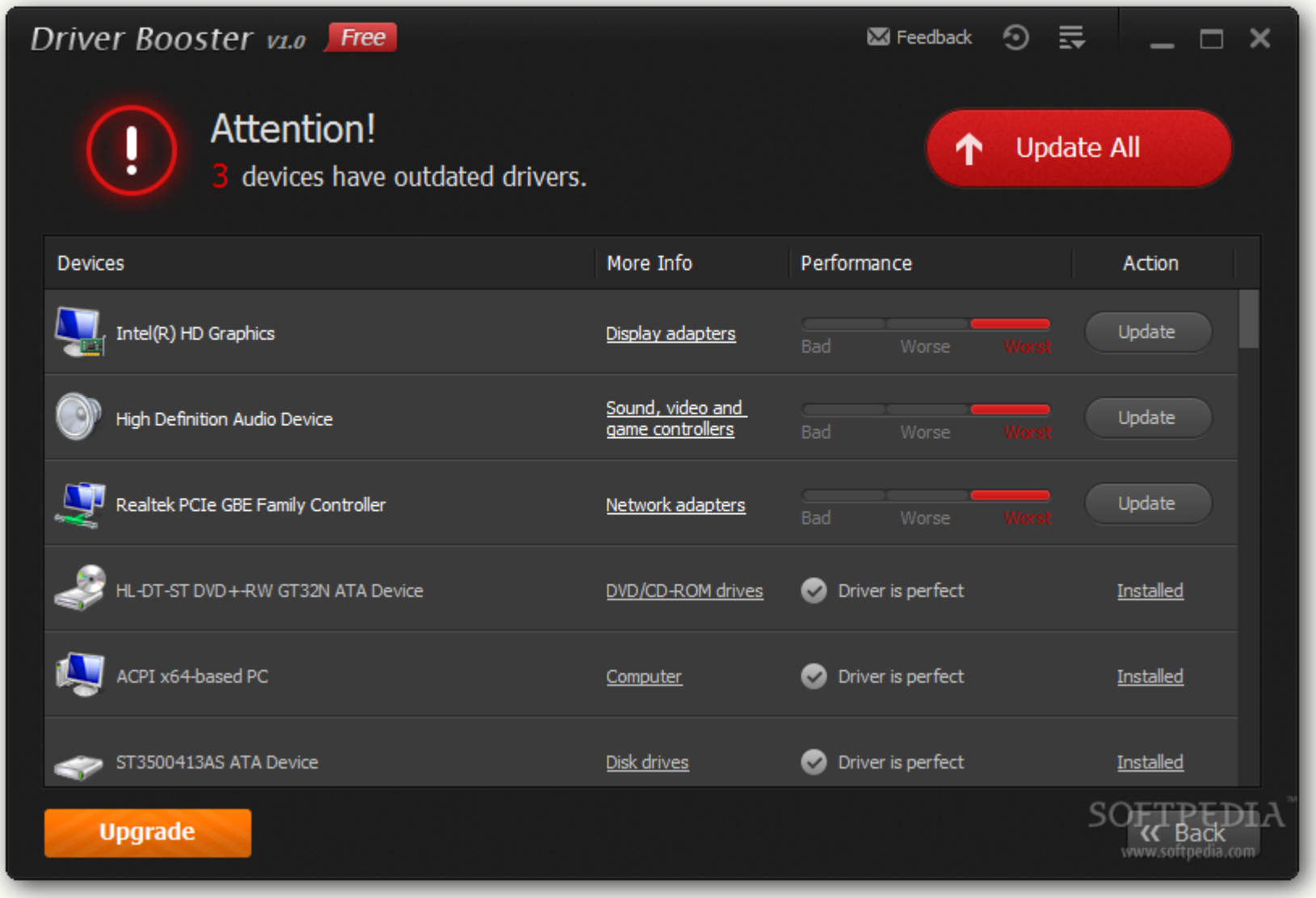
Index

Repareert & Update meer dan 200,000 Drivers Snel & Veilig
Verbetert Game Ervaring & PC Prestaties met Up-to-date Drivers!

Driver Booster

Met een enorme driver database helpt Driver Booster 3 met het vinden van zeldzame en recent uitgegeven audio drivers, network drivers, graphics drivers, chipset drivers en nog veel meer van meer dan 3000 driver fabrieksmerken. De online database functie is ontworpen voor het up-to-date houden van uw drivers zodat problemen en conflicten met uw printer, scanner, muis, toetsenbord, scherm, speakers etc. voorkomen kunnen worden. Driver Booster 3 update niet alleen verouderde drivers maar scant automatisch en download ook missende drivers, met name na het upgraden van uw besturingssysteem of het gebruik van uw PC na een lange tijd. Driver Booster 3 helpt snel met het vinden en installeren van correcte drivers met 1-klik voor het voorkomen van langzame pc's, het crashen van uw pc of apparaten die niet meer functioneren. Voor het significant verbeteren van uw game ervaring, streaming of media bewerkings ervaring, houdt Driver Booster 3 audio & graphics drivers up-to-update. Daarnaast kan Driver Booster 3 automatisch game componenten detecteren in de database inclusief PhysX, DirectX, OpenAL, VC Runtime, Adobe Flash, UnityWeb en met 1-klik installeren zodat uw game ervaring verbetert kan worden. Om de beveiliging van de drivers te waarborgen, zijn alle drivers van Driver Booster 3 getoetst door WHQL. In het geval iets onverwachts gebeurt zal Driver Booster 3 automatisch een backup maken en een systeem herstel punt creëren voordat drivers geïnstalleerd worden. De Uninstall & Rollback functie zal de pc beschermen zodra iets onverwachts gebeurt.

Let bij het installeren wel even op de vinkjes. Kijk goed wat u wel en niet wilt installeren!



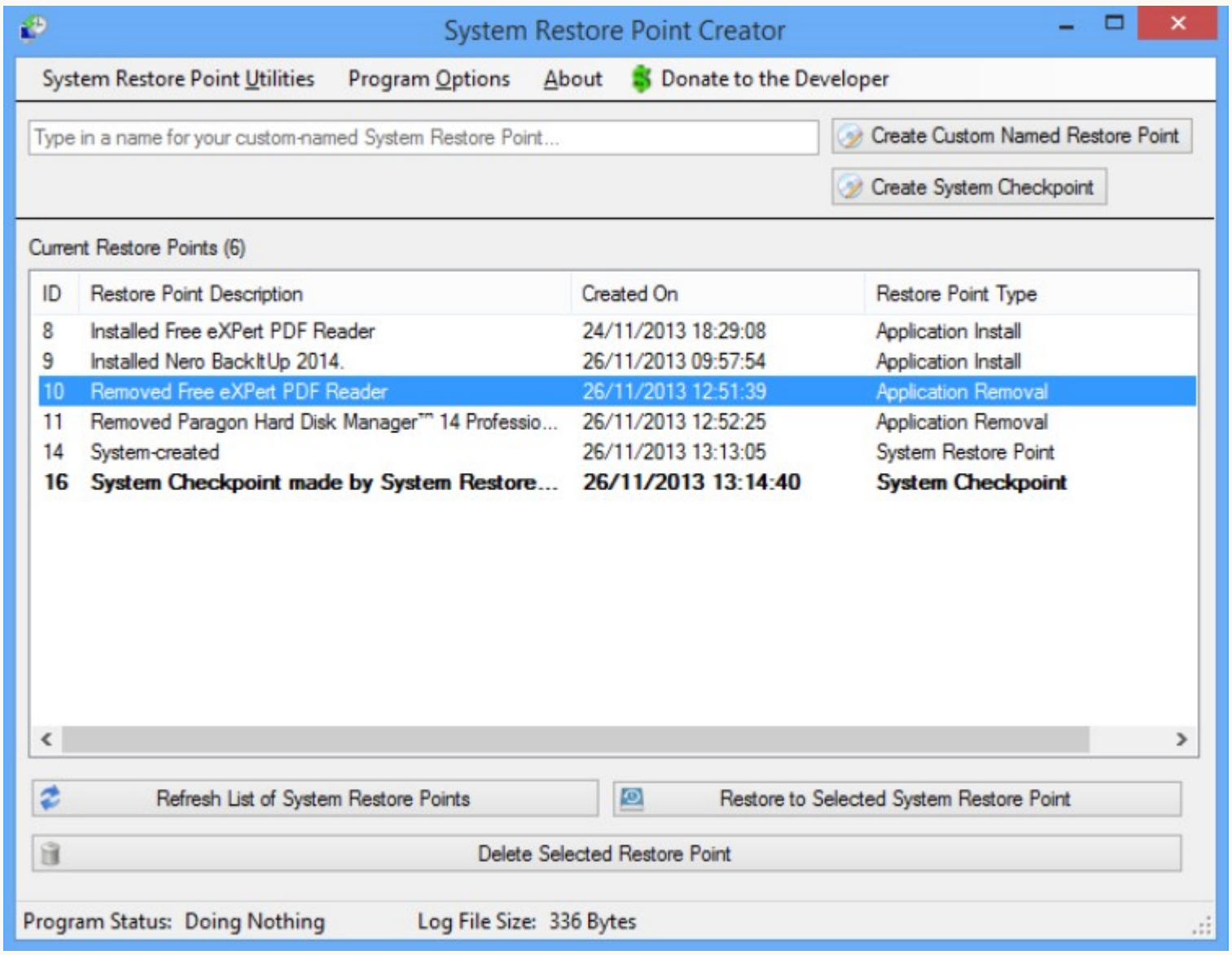
Bron: iObit

Index

Er kan natuurlijk altijd iets mis gaan. Handig is het dan om naar een eerder aangemaakt herstelpunt terug te kunnen gaan.

Restore Point Creator

Normaliter kun je Windows zo instellen dat automatisch herstelpunten worden aangemaakt. Dat is niet altijd makkelijk te vinden. Restore Point Creator neem dit werk uit handen. Met aan paar klikken is een herstelpunt aangemaakt en net zo makkelijk weer terug gezet. U hoeft zich nu niet meer door meerdere menu's heen te werken om bij de herstelpunten te komen.



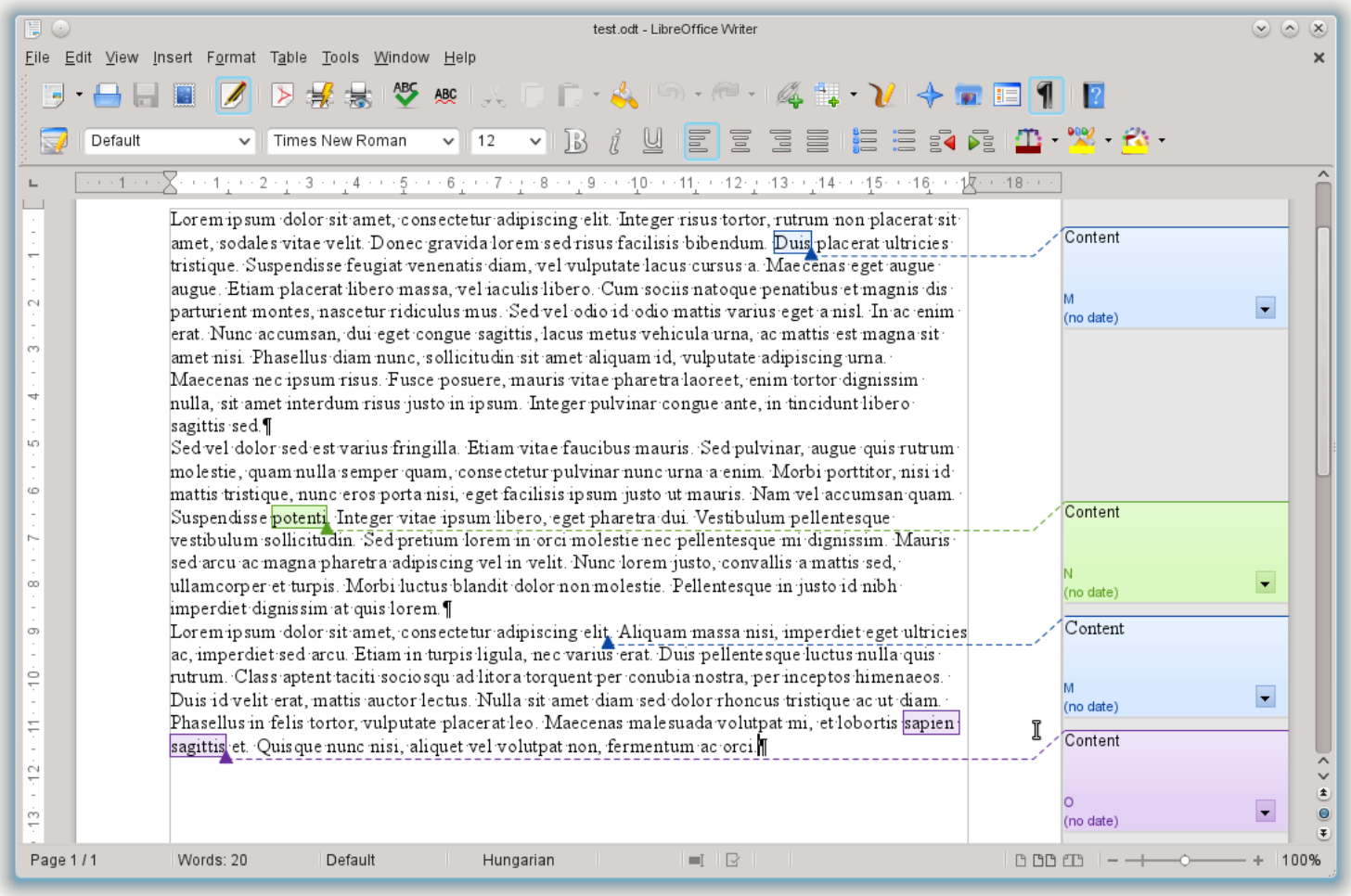
Bron: Major Geeks

Index

LibreOffice is het moderne, gratis programma voor persoonlijke office-productiviteit voor uw Windows-, Mac- of Linuxcomputer. Het programma bevat zes modules: Writer, Calc, Impress, Draw, Math en Base.

Libre Office

Waarschijnlijk werkt u zakelijk met Microsoft Office. Dat is nu eenmaal de leidende software in een kantooromgeving. Privé heeft u waarschijnlijk alle functies van Microsft Office niet nodig. Daarbij komt dat het niet gratis is. LibreOffice is dat wel. De 6 programmaonderdelen zijn volledig compatibel met Microsoft Office. Het programma bevat zes modules: Writer, Calc, Impress, Draw, Math en Base. U kunt de bestanden dan ook opslaan met Microsoft extensies.



Bron: Libre Office

Index

De tijd dat You Tube alleen bestemd was voor het bekijken van videoclips en zelfgemaakte filmpjes ligt inmiddels achter ons.

YouTube is onderdeel geworden van het nieuwe leren.

(Voor u gevonden op YouTube……..en Tek Tok.

TEK TOK

Tek Tok Late Night:

1. Privacy
2. Internetvrijheid
3. Digitale veiligheid
4. High Tech Crime
5. Data in onderwijs
6. Cybersurveillance
7. Techtrends in onderwijs
8. Veilig internetten
9. MKB cyber secure
10. Cyberellende bij Tek Tok
11. Standaarden en keurmerken
12. Operation Hijg Tech Crime
13. Kraak van de Maand

YouTube
Teach
~~Broadcast~~ Yourself™

Mobiele Eenheid achter de schermen

Verleiding van de misdaad

Kun jij beslissen wat de hoogste prioriteit heeft

Draadloos netwerk

Doe jij het veilig online

Malware

WiFi ontvangst verbeteren

Inbraakbeveiliging

Hoe gaat de inbreker te werk

Internetfraude via de telefoonDocumentaire: Veiligheid en privacy

Herken een nep-hotspot

Gebruik wachtzinnen

Drive-by-downloads voorkomen

Hoe herken je een phishing mail

Beveiligd internetbankieren

Privacy—ik heb toch niets te verbergen

Veilig politiewerk

Gezag op straat .. Als het moeilijk wordt

Bron: YouTube

Index

Schatkist

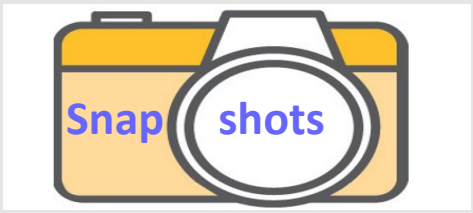
Naslag:

- Handleiding Twitter
- Gebruik tweetraps authenticatie
- Windows 10 installatie
- Online verdwijnen
- Centraal cloudbeheer
- Online kopen
- Cybersecurity 2015
- Stickware
- Netwerk in de knoop

Software:

- 360 Total Security
- AS SSD benchmark
- Cdex
- Cleanmaster
- CPU-Z
- Emsisift Emergency Kit
- KillDiskSuite
- Mp3Gain
- MultiCommander
- SyneiSystemUtilities

Index



Om verslaving en matchfixing zo veel mogelijk tegen te gaan, wil een kamermeerderheid dat er op internet niet gegokt mag wordenop sportelementen die ‘makkelijk te beïnvloeden zijn’. Gokken op een rode kaart, een dubbele fout, een eigen doelpunt etcetera moet verboden blijven omdat manipulatie hier op de loer ligt. Gokken op de uitslag mag nog wel, aldus VVD en PvdA. Het kabinet worstelt al jaren met internetgokken. In 2014 werd besloten dat online gokken vanaf 2015 legaal zou zijn maar dat wordt niet gehaald. De verwachting is dat in 2016 een definitief besluit genomen wordt.

———————————————————

Nederlandse drugsdealers waren op de illegale marktplaats Silk Road 2 goed voor tien procent van alle verkopen. In totaalverdienden ze zo in drie jaar tijd ruim 32 miljoen euro. Het OM meldde deze cijfers op een internationale opsporingscongres over marktplaatsen op het dark web. Op deze sites, zoals Silk Road, Agora en Evolution, werden/worden voornamelijk drugs aangeboden. Op het congres, in Noordwijk, praten 25 EU-landen, de VS en Australië over de gezamenlijke aanpak van zulke sites in het zogeheten ITOM project (Illegal Trading on Online Marketplaces) dat twee jaar geleden door de Nederlandse politie opgezet is. In 2014 zijn in dit project 17 illegale online marktplaatsen opgerold, waaronder Silk Road 2.

———————————————————

Via open bronnen, sociale media en andere plekken op internet is zo veel informatie te vinden over politiemensen, hulpverleners, militairen en andere ambtenaren, dat het Internet Crime Complaint Center (IC3) van de FBI waarschuwt voorzichtig te zijn met wat je zelf online zet. Het IC3 verwijst naar een recente zaak waarin een oplichter, ‘vermomd’ als overheidsmedewerker, bij een provider een e-mailadres weet te verkrijgen en daarmee ook allerlei privéinformatie. IC3 spreekt van doxing: het ongevraagd verzamelen van gegevens over iemand, op basis van openbare bronnen (facebook, twitter, google). ‘Zet de privacyinstellingen zo hoog mogelijk op uw social media-accounts. Plaats geen verwijzingen naar uw functie, werklocatie of lopende dossiers. Vraag aan familieleden om hetzelfde te doen’, is daarom het advies. Ook: ‘wees terughoudend met het plaatsen van opmerkingen op social media’.

———————————————————

Wel last maar geen pijn. Uit onderzoek van het ministerie van Binnenlandse Zaken naar agressie op sociale media tegen hulpverleners en mensen in andere publieke functies blijkt datvooral politiemensen en docenten er ‘last van hebben’. Toch onderneemt slechts een kwart van de medewerkers die uitgescholden worden, daadwerkelijk actie. Een op de drie scheldpartijen wordt bij de werkgever aangekaart, een op de tien stapt naar de politie – waar dergelijke meldingen serieus genomen worden, aldus het onderzoek. In driekwart van die gevallen wordt een onderzoek gestart. Binnen de politie heeft 21% van de agenten ‘wel eens’ te maken gehad met ‘wangedrag richting zijn of haar persoon via sociale kanalen’. Bij de docenten wordt vooral gescholden tegen docenten in het primair, voortgezet en middelbaar beroepsonderwijs. Volgens het onderzoek nemen werknemers en -gevers onacceptabel gedrag op internet ‘dus nauwelijks serieus’. Ook nazorg ‘is een vies woord’.

———————————————————-

Iemand afpersen met ransomware? Voor eenmalig vijftig dollar is bij de nieuwe CryptoLocker Service de daarvoor benodigde malware te koop. Bij de koop kan de afperser aangeven hoeveel slachtoffers moeten betalen om weer toegang tot hun bestanden te krijgen. Aanbevolen wordt een bedrag van 200 dollar. De dienst incasseert tien procent van de opbrengst, die in bitcoins uitbetaald zal worden aan de opdrachtgever, schrijft beveiliger Trend Micro. Trend Micro. Achter de nieuwe dienst zit ‘Fakben’, die ooit de illegale tor-marktplaats Evolution beheerde. Eerder voorspelde Trend Micro en andere beveiligers voor 2016 al een stijging van het aantal ransomware-aanvallen.

———————————————————

In Denemarken heeft een man aangifte gedaan tegen het bedrijf Facebook Inc omdat deze de handel in verdovende middelen zou faciliteren. Gert Fruelund, vader van vier tieners, ging naar de politie toen hij ontdekte hoe gemakkelijk het was om via facebook aan drugs te komen. ‘Als een voedselproducent weet dat er met een bepaald product iets mis is, moeten ze dat bij de autoriteiten bekend maken. Waarom moet Facebook dat niet?’ Facebook zegt dat alle verantwoordelijkheid bij de gebruikers ligt. De Deense tv toonde onlangs de documentaire Jagten: De Nye Pushere waarin de dood van enkele tieners gekoppeld werd aan de synthetische drugs die ze in een gesloten groep op facebook hadden gekocht. ‘Drugsdealers zijn geen verdachte mannen meer die in steegjes rondhangen’, zegt Fruelund.

———————————————————

Een drone heeft in Oklahoma, VS een man betrapt die seks had in zijn auto met een prostituee. De drone werd bestuurd door Brian Bates, een activist die prostituees en klanten te kijk zet op zijnwebsite. Bates filmde hoe de bejaarde Douglas Blansett (75!) in een suv van bil ging met Amanda Zolicoffer, een vrouw die hij al eerder betrapt had. Toen Zolicoffer op een avond bij Blansett in de auto stapte, reed Bates achter hen aan. Toen het stel op een afgelegen terrein parkeerde, stuurde Bates zijn drone de lucht in. Het filmpje stuurde hij ook naar de plaatselijke politie die Zolicoffer en Blansett arresteerde. Volgens agent Ben Lacaze zijn ze weer vrij na het betalen van vijfhonderd dollar borg.

———————————————————

Silk Road, das war einmal. Maar alle marktplaatsen die er sinds het oprollen van Silk Road – nu twee jaar geleden – zijn ontstaan, halen het niet bij het origineel. De nieuwe alternatieven zijn onbetrouwbaar, soms opeens verdwenen of ontoegankelijk en zitten vol met oplichters. Dat zeggen meerdere onderzoekers tegen de NOS. Zo stelt Danny Mekic dat ‘de alternatieven noch de naam noch de betrouwbaarheid hebben die Silk Road wel had’. En waar de ene beveiligingsonderzoeker zegt dat er ‘altijd een actieve markt’ zal zijn voor mensen die drugs of wapens zoeken, wijst een andere op het zelfregulerende systeem dat Silk Road had. ‘Mensen konden zien dat je een goede dealer bent’, zegt Rickey Gevers. ‘Dealers leverden vrijwel altijd goede kwaliteit’. Daarnaast zijn er ‘jongens die een marktplaats aanmaken’ en er met de buit vandoor gaan.

———————————————————

Index

Al van vipping gehoord? De politie Roosendaal doet sinds kort aan vipping, oftewel very irritating policing, om vier groepen probleemjongeren in de gaten te houden. Politiechef Rens van den Oever noemt vipping een logisch antwoord op de veranderingen in de probleemgroepen zelf. De groepen zijn meer fluïde dan voorheen, wisselen van samenstelling, communiceren via sociale media en 'zijn eerder op een groepschat te vinden dan in een winkelcentrum'. Door ze 'hinderlijk te volgen' op alle beschikbare openbare bronnen krijgt de politie beter zicht op ze, zegt Van den Oever.

———————————————————-

Voor de zoveelste keer is 'de grootste kinderpornowebsite ter wereld' opgerold. Dit keer betrof het een hierarchisch netwerk met 45 duizend leden en meer dan 360 duizend plaatjes en filmpjes. Het netwerk, waar kinderporno 'op bestelling' werd geproduceerd, werd opgerold door de polities van Nederland, de VS en Australië. Onder meer twee Nederlanders en een Australiër werden opgepakt, de Australische beheerder Shannon McCoole (33, uit Adelaide) zelfs al veroordeeld – tot 35 jaar celstraf. McCoole werd opgespoord omdat hij zichzelf 'verraadde': hij gebruikte opvallend veel het woord hiya in zijn berichten, waarna een internetspeurtocht uiteindelijk leidde naar een facebookpagina waar dat woord ook vaak gebruikt werd. Een foto van een VW op die pagina leverde een kenteken, dat weer naar McCoole verwees. Hij werd geïdentificeerd dankzij een moedervlek op een vinger, aangeklaagd en (begin augustus 2015) veroordeeld tot 35 jaar cel. McCoole, de hoofdbeheerder van het netwerk, werd op heterdaad aangehouden, zodat rechercheurs van de Australische politie de website konden overnemen. Een half jaar lang chatten agenten met de leden – om dat netwerk zo veel mogelijk op te rollen. Dat leverde ondermeer vijf Nederlandse verdachten op. Naar nu blijkt zijn die allemaal al veroordeeld. De vijf kregen straffen van twee jaar jeugddetentie tot vijf jaar celstraf.

———————————————————-

In Brussel lukte het aardig, die sociale-mediastilte tijdens de anti-terreuracties van de Belgische politie. Maar in Amsterdam zal zoiets niet snel gebeuren, zei de Amsterdamse hoofdcommissaris Pieter-Jaap Aalbersberg tegen AT5. Volgens Aalbersberg moet de politie 'gewoon beter worden in ons eigen werk dat we daar rekening mee houden'. Zo'n mediastilte is ook geen garantie, vindt hij. 'Op hele belangrijke momenten kan je dat vragen, want het heeft invloed op je operatie, maar ik geloof niet dat we dit moeten gaan afdwingen of grote dingen moeten gaan doen'. Sociale media zijn immers altijd en overal aanwezig. 'Het is nu eenmaal een gegeven. Of het nou een ernstig ongeluk of incident midden in onze binnenstad is, er zijn altijd camera's en telefoons bij. Daar moet je op voorbereid zijn.'

———————————————————

In Krabi, Thailand is acht jaar celstraf geëist tegen twee personen die op facebook kritiek uitten op de lokale politie. Een vrouw (23) maakte opmerkingen over een verkeersagent van wie ze haar auto ergens anders moest parkeren, ze plaatste een filmpje online waarin ze de agent ook beschuldige van corruptie. En een man (22) vond dat de politie te weinig deed met een melding over huiselijk geweld. Korpschef Sompong Thip-Aphakul noemt de eis 'a moral lesson to warn people who post stuff on social media'. Zijn medewerkers doen gewoon hun werk, zei de korpschef. 'Some people just don't understand our work'. De twee verdachten staan terecht voor laster, belediging van politiemensen en het overtreden van de Computer Crime Act. 'People should be careful with what they say'.

———————————————————-

In de Havenloods schrijft zsm-officier Maurice van Heemst over een man die 'van een vage vriend' een gloednieuw politieshirt kocht. Voor de spiegel nam de man een paar selfies die natuurlijk op facebook gedeeld werden. Tientallen likes en reacties als 'staat je goed' en 'gaaf' waren het gevolg. Maar ook een melding bij de politie. 'Gelukkig lezen op internet ook mensen met gezond verstand mee', aldus Van Heemst. De verdachte werd aangehouden en kreeg van de rechter zestig uur werkstraf.

———————————————————

Frits van Loosen uit Nijmegen zegt te worden bedreigd door Indiase criminelen. Die gebruiken sinds zes weken zijn telefoonnummer om mensen op te lichten – de bekende telefoonscam waarbij iemand telefonisch meldt dat er een lek in je beveiliging zit. Van Loosens nummer staat dan in het display, terwijl het telefoontje uit India komt. Van Loosen zegt niet meer te kunnen uitleggen dat hij niets met de scam te maken heeft. Hij zegt bedreigd te worden. 'Mensen roepen dat ze me weten te vinden als het niet stopt'. Volgens Van Loosen kunnen politie en providers hem niet helpen. De Fraudehelpdesk bestrijdt dat: 'KPN kan er best wat aan doen maar wil dat kennelijk niet omdat er te weinig slachtoffers zijn'.

———————————————————

Internetaangifte – lang niks over gehoord. Maar in een nieuw rapport daarover staat dat ruim een derde (37%) van alle aangiften bij de Nederlandse politie inmiddels via internet gaat. In het rapport, van onderzoeksbureau BSSO en de Radboud Universiteit, staat echter ook dat burgers uit 'bepaalde doelgroepen' (laagopgeleiden, allochtonen en ouderen worden genoemd) internetaangifte liever vermijden en dat burgers minder tevreden zijn met de behandeling én de informatievoorziening bij een internetaangifte. Politiechef Oscar Dros, portefeuillehouder Dienstverlening, zegt dat veel van de kritiek uit rapport inmiddels 'ondervangen' is. Zo is eind 2015 gestart met de ontwikkeling van Mijn Politie, waar mensen in een door DigiD beveiligde omgeving online aangifte kunnen doen maar ook de status daarvan kunnen bijhouden. De politie zet al jaren in op internetaangifte omdat dat efficiënter zou zijn. Volgens de onderzoekers is dat nog maar de vraag: bij internetaangiften moet vaak nog veel extra opsporingsinformatie worden vergaard waardoor de tijdswinst maar beperkt is.

———————————————————

Index

Actuele phishingmails:

klik hier

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

Computerwoordenboek

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

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 een deel van de informatie die u daar heeft verstrekt door het Meldpunt Internetoplichting aan Marktplaats doorgestuurd.

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.

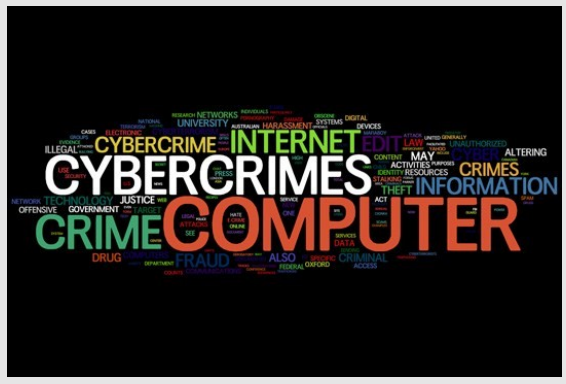
Artikel 2 Wwm: wet wapens en munitie

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