Secure Computing

W.Bosgra taakaccenthouder digitale criminaliteit

November 2013

Dit digitale magazine wordt verzorgd door Secure Computing.

Doel is bewustwording van wat u doet met de computer , kennis opdoen gericht op de opsporing van strafbare feiten (cybercrime) en veilig computergebruik.

U kunt deze nieuwsbrief opslaan op uw eigen "Home"-omgeving en als naslagwerk blijven gebruiken.

Indien u dit magazine tevens in uw eigen thuisomgeving bewaart, kunt u gebruik maken van de ingebouwde hyperlinks.

E-mail? klik hier !

Documenten beveiligen

Het schermtoetsenbord

Facebook gehackt?

EPIC browser

Bitcoin

De Wet Computercriminaliteit: Smaad, laster en belediging op internet

In dit digitakle tijdperk zien wij steeds vaker dat de sociale media ge(mis-)bruikt wordt om anderen te bedreigen en te beledigen. Steeds vaker wordt er dan ook aangifte gedaan.

Wanneer iemands eer of goede naam wordt aangetast, kan sprake zijn van belediging, smaad of laster. Ook als de bewering feitelijk juist is. Er moet een redelijk belang zijn bij de bewering. Ook iemand belachelijk maken in een parodie mag vaak wel.

Een belediging is een algemene negatieve uitlating over een persoon. Smaad is een specifieke uitlating die iemands goede naam probeert aan te tasten. Is de uitlating niet waar, dan heet het laster.

Smaad, belediging en laster zijn allemaal strafbare feiten. De grens tussen belediging, smaad en laster is alleen vaak lastig te trekken. Een belediging is een algemene negatieve uitlating over een persoon. Wie zegt, "Jansen is een dief", beledigt Jansen. Bij smaad wordt de uitlating specifiek en is het doel de eer of goede naam van die persoon aan te tasten. In het vorige voorbeeld zou de belediging smaad worden als er specifiek werd gezegd: "Koop niet op Marktplaats.nl bij Jansen, want hij incasseert wel je geld maar stuurt de spullen niet op". Je beschuldigt hem dan van oplichting.

Als de verteller weet dat het niet waar is wat hij vertelt, dan heet het laster. De waarheid vertellen kan dus nooit laster zijn, maar soms wel smaad.

Ook de waarheid vertellen kan smaad zijn. Pas wanneer de bewering in het algemeen belang is, is het toegestaan.

Veel mensen denken dat zolang je maar geen leugens vertelt, je uitlatingen geen smaad kunnen zijn. Dat is onjuist.
Wat wel een geldig excuus is, is dat het in het algemeen belang is om de bewering te doen. Als Jansen bijvoorbeeld zich er op laat voor staan tegen drankmisbruik te zijn, is het gerechtvaardigd om te melden dat hij zelf regelmatig veel drinkt. Hetzelfde geldt als Jansen door zijn drankmisbruik problemen veroorzaakt.

Meer algemeen hanteert de rechter de maatstaf of er sprake is van voldoende basis in de feiten. Dat wil zeggen dat een uiting onderbouwd moet zijn op basis van de feiten, en dat feiten en meningen duidelijk van elkaar gescheiden moeten zijn.

Het opzettelijk aantasten van iemands eer of goede naam door verspreiding van een bepaald feit is een misdrijf: smaad.
Als dat schriftelijk gebeurt, en publicatie op een website is "schriftelijk", maakt de dader zich schuldig aan smaadschrift.
Een verwant misdrijf is laster: het opzettelijk verspreiden van iets waarvan de dader weet dat het een leugen is.

De grens tussen feiten en meningen is lastig te trekken. Een puur feitelijke mededeling kan geen smaad zijn.

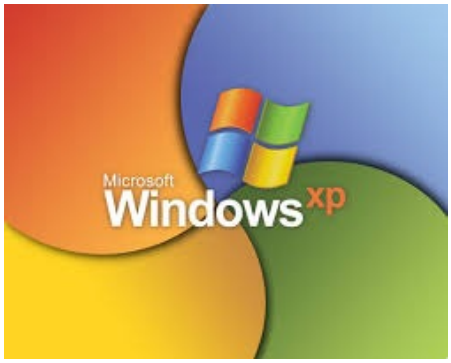
Het staat iedereen vrij zijn mening te geven over een bepaald onderwerp, dus ook over bijvoorbeeld de service bij een winkel of het gebruik van goedkope arbeiders in derdewereldlanden door een bedrijf. Actiegroepen doen dit al jaren, en of het nu via een poster, een folder of een website gebeurt maakt niet uit.

Die mening moet, voorzover het gaat over feitelijke zaken, natuurlijk wel kloppen. Als een bedrijf gebruik maakt van kinderarbeid, mag dat best gemeld worden. Echter, als iemand dat beweert terwijl het niet waar is, is het imago van dat bedrijf onterecht geschaad. En wie een ander schade toebrengt, moet deze vergoeden.

Het zal echter vaak niet meevallen om aan te geven waar een feit ophoudt en een mening begint. Vaak gaat het om de interpretatie van dat feit, bijvoorbeeld bij de vraag of er sprake is van kinderarbeid, of bij de vraag of de omstandigheden waarin varkens worden vetgemest acceptabel zijn of niet. De houder van die varkens zal van mening zijn dat dat het geval is, de actievoerders beweren het tegenovergestelde.

Overheid en Microsoft: stop met gebruik Windows XP

In 2001 heeft Microsoft het besturingssysteem Windows XP op de markt gebracht. Op 8 april 2014 krijgt dit besturingssysteem na 13 jaar de status End of Life. Microsoft zal dan niet langer updates uitbrengen voor Windows XP. Als beveiligingslekken in Windows XP worden gevonden, zullen deze niet worden gedicht. Computers met Windows XP zullen dan kwetsbaar blijven. Het NCSC adviseert daarom computers met Windows XP voor april 2014 te vervangen of te voorzien van een besturingssysteem dat nog wel wordt onder- steund met (beveiligings)updates.



Het Nationaal Cyber Security Center (NCSC), het Team High Tech Crime, het Ministerie van Defensie en Microsoft waarschuwen internetgebruikers dat ze moeten stoppen met het gebruik van Windows XP. Vanaf 8 april 2014 stopt Microsoft met het uitbrengen van updates voor Windows XP.

Daardoor worden lekken in het OS niet langer gedicht. Het team High Tech Crime van de politie zou inmiddels signalen hebben dat er op grote schaal aanvallen op Windows XP-computers worden voorbereid. De verwachting is dat kwaadwillenden deze zullen uitvoeren als de ondersteuning van Windows XP stopt, zo laat de overheid via een bericht op de campagnewebsite van Alert Online weten.

Besturingssysteem

Het NCSC adviseert daarom met klem om computers die draaien op Windows XP, voor april 2014 te vervangen of te voorzien van een besturingssysteem waarvoor wel beveiligingsupdates beschikbaar worden gemaakt. Volgens het NCSC zijn Windows 7 en 8 geschikte besturingssystemen, of besturingssystemen gebaseerd op Linux, zoals Ubuntu en Red Hat.
"Ook Mac OS X van Apple is een geschikt besturingssysteem. Dit besturingssysteem werkt alleen niet op computers die eerder draaiden op Windows XP. Bij de keuze voor Mac OS X moet daarom een nieuwe computer worden aangeschaft", aldus het advies van de overheidsinstantie.

Afscheid

"Na meer dan een decennium van trouwe dienst is de tijd gekomen om afscheid te nemen van Windows XP. Er zijn gelukkig meerdere goede alternatieven van verschillende leveranciers beschikbaar, maar de overgang zal moeite kosten, zowel voor zakelijk als thuisgebruik", aldus een speciale factsheet die het NCSC over het einde van XP maakte.

Wat kan er gebeuren?

Een computer die na april 2014 nog Windows XP gebruikt als besturingssysteem, zal kwetsbaar zijn en blijven voor aanvallen van buitenaf.

Zo lang Windows XP nog veel gebruikt wordt,valt te verwachten dat kwaadwillenden software zullen blijven ontwikkelen waarmee op grote schaal aanvallen kunnen worden uitgevoerd op computers met Windows XP.

Het Team High Tech Crime van de politie signaleert dat dergelijke aanvallen momenteel worden voorbereid. De verwachting is dat kwaadwillenden deze willen uitvoeren nadat Windows XP de status End of Life heeft bereikt.

Als Windows gebruiker is vooral de Linux distributie Ubuntu 12.04 LTS aan te raden. Gebruikersvriendelijk en support tot april 2017.

Politie waarschuwt winkeliers voor ransomware

De politie waarschuwt winkeliers om niet zomaar Ukash en Paysafecard vouchers aan slachtoffers van ransomware te verkopen. Uit onderzoek van de politie blijkt dat in oktober honderden Nederlandse computers met ransomware geïnfecteerd waren.
De ransomware vergrendelt de computer en stelt dat het slachtoffer een misdrijf heeft begaan. Om weer toegang tot zijn computer te krijgen moet het slachtoffer een "boete" betalen, die via een voucher van bijvoorbeeld Ukash en Paysafecard kan worden voldaan.

Voorlichting

De politie stelt in een nieuwe factsheet over ransomware voor winkeliers dat winkeliers kunnen helpen door het eigen personeel goed voor te lichten, zodat niet zomaar vouchers worden verkocht aan slachtoffers van ransomware. De politie heeft tevens een adviesposter ontwikkeld om op te hangen.
Om slachtoffers die in winkels een voucher kopen te waarschuwen wordt in Groot-Brittannië veel succes geboekt met een andere manier. Daar wordt op de kassabon waar de vouchercode op staat ook een waarschuwing geprint. De politie hoopt dat de winkeliers in Nederland dit voorbeeld willen volgen.

Omvang

In een onderzoek van deze maand ontdekte de politie honderden Nederlandse besmettingen van één variant. Er zijn echter tientallen varianten van ransomware in omloop en hun aantal is groeiende, zo laat de politie weten. Uit cijfers van anti-virusbedrijven blijkt dat Nederland één van de meest getroffen landen in Europa is.
"Dat heeft waarschijnlijk te maken met de internetdichtheid, maar mogelijk ook met de betalingsbereidheid", zo meldt de factsheet. Naar schatting betaalde in 2012 zo'n tien procent van de Nederlandse slachtoffers. Dit percentage daalt inmiddels. Een betaling bedraagt doorgaans 50 of 100 euro.

Voorkomen

Voor zover bekend zijn alle infecties door ransomware te voorkomen, aangezien de infecties plaatsvinden via softwarelekken die gebruikers niet hebben gepatcht of doordat internetgebruikers ongevraagde e-mailbijlagen openen. De politie adviseert het besturingssysteem en programma's altijd up-to-date te houden, niet te surfen op internet zonder virusscanner, geen onbekende bijlagen van e-mails te openen en door alert te zijn bij het downloaden van software en media.

Ondanks deze adviesmaatregelen lopen internetgebruikers nog steeds risico stelt de politie in de factsheet. "Besmetting is nooit volledig te voorkomen. Soms raken computers besmet via een reguliere website die door de criminelen is gehackt. Een besmetting met ransomware zegt dus niets over het (surf)gedrag van de computergebruiker."

Gebruik het schermtoetsenbord

In een eerdere uitgave bent u reeds gewezen op het gevaar van de zogenaamde keyloggers.

Computers in openbare ruimtes - zoals internetcafé's, hotels en buurthuizen - zijn vaak onveilig. Er kan een keylogger zijn geïnstalleerd: software die de aanslagen op het toetsenbord registreert. Hiermee kunnen persoonlijke gegevens worden onderschept, zoals wachtwoorden en creditcardnummers.

Ook in Nederland kun je er niet van uitgaan dat publieke computers veilig zijn. Als je zo'n computer móet gebruiken is het verstandig om gebruik te maken van het Online Screen Keyboard (OSK).

Wanneer is het aan te raden om het schermtoetsenbord te gebruiken?
Bij het invoeren van wachtwoorden en persoonlijke gegevens op publieke computers.

Hoe veilig is het schermtoetsenbord?
Als je gebruik maakt van het schermtoetsenbord wordt de computer aangestuurd via muisklikken. Een gewone keylogger kan dan geen toetsaanslagen vastleggen. Alleen zeer gespecialiseerde software - waarbij ook screenshots worden gemaakt - is in staat om te traceren wat er op een schermtoetsenbord gebeurd.

Het schermtoetsenbord gebruiken

In Windows 8:

Ga naar naar het blokjesscherm typ in: osk.
Klik op Schermtoetsenbord.
Het toetsenbord verschijnt.

In Windows 7 en Vista:

Ga naar Start en typ in het zoekveld osk.
Enter.
Het toetsenbord verschijnt.

In Windows XP:

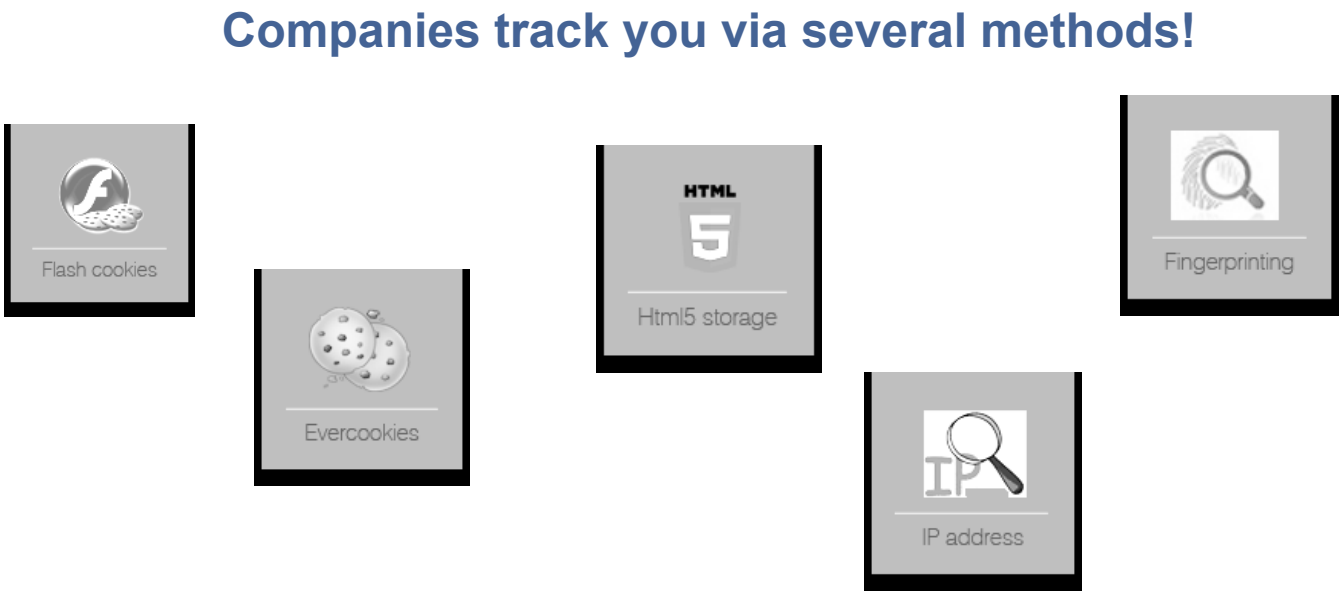
Ga naar Start - Uitvoeren.
Typ in: osk.
OK.
Het toetsenbord verschijnt.

Nieuwe browser beschermt privacy en blokkeert tracking

Na een jaar van ontwikkeling is er een nieuwe browser verschenen die de privacy van internetgebruikers centraal stelt.

Epic, zoals de browser heet, is op Chromium gebaseerd. Dit is de open source browser die ook de basis van Google Chrome vormt.

Er zijn echter verschillende aanpassingen aan de broncode doorgevoerd om tracking te voorkomen en extra privacy te bieden. Zo geeft de adresbalk geen suggesties meer, is er geen URL-controle, is het automatisch vertalen van websites verwijderd en is er geen URL-tracker. Verder zijn de installatie-ID, RLZ-trackingnummer, de standaard updater en installatie time stamp verwijderd.



Zoekmachine
Ook worden er geen alternatieve foutmeldingspagina's getoond en fouten naar de ontwikkelaars doorgestuurd. Na het sluiten van de browser worden alle opgeslagen gegevens verwijderd. Verder beschikt de browser over uitgebreide mogelijkheden om advertenties en webtrackers te blokkeren.
Een ander groot 'privacylek' is het zoeken op internet. Zodra gebruikers van Epic een zoekopdracht versturen, gaat dit via een proxy, om te voorkomen dat zoekmachines de zoekopdracht aan een IP-adres kunnen koppelen. Ook wordt de referral header niet meegestuurd als de gebruiker op een zoekresultaat klikt.

IP-adres
Voor internetgebruikers die hun IP-adres willen afschermen is er de mogelijkheid om via één muisklik een proxy in te stellen. Deze proxydienst wordt door Spotflux aangeboden. De browser is volledig open source en ontwikkeld door Hidden Reflex, een Amerikaans bedrijf met Indiase ontwikkelaars.

Facebook gehackt? Problemen oplossen

Lijkt je Facebook account niet meer veilig? Zo check je of er iemand vanaf een andere plek in je profiel is geweest, en kun je je account herstellen als je geen toegang meer hebt.

Controleren waar is ingelogd op je Facebook

- Klik in Facebook op het **wiel-icoon** en ga naar **Accountinstellingen**.
- Klik in het menu links op **Beveiliging**.
- Klik bij **Actieve sessies** op **Bewerken**.
- Je ziet nu de plaatsen waarop is ingelogd op je Facebook.
- Klik op **Sluiten** om verdachte sessies - of locaties die per ongeluk openstaan - af te sluiten.

Als je het vermoeden hebt dat iemand je Facebook wachtwoord kent, wijzig dit dan meteen.

Facebook wachtwoord wijzigen

- Klik in Facebook op het **wiel-icoon** en ga naar **Accountinstellingen**.
- Klik bij **Wachtwoord** op **Bewerken**.
- Er wordt nu gevraagd om het oude wachtwoord, en een nieuwe wachtwoord.
- Wachtwoord vergeten? Kijk op: **Facebook wachtwoord vergeten**

Gehackt Facebook account terugvragen

Als je Facebook account is gehackt, en je wachtwoord niet meer werkt, probeer dan **zo snel mogelijk** je account terug te vragen.

- Ga naar **Gekraakt account rapporteren**
- Klik op **Mijn account is gekraakt**. Je krijgt vragen over je account, bijvoorbeeld de namen van vrienden of IP-adressen van computers waarop je het account hebt gebruikt. Geef zorgvuldig antwoord op de gestelde vragen. Vraag zonodig anderen om hulp om de gevraagde gegevens op te zoeken. Geef alleen de gegevens door die je zeker weet.
- Als Facebook op deze manier je identiteit kan controleren wordt je wachtwoord opnieuw ingesteld.

Zoeken op Facebook

Mensen zoeken op Facebook? Zo kun je personen vinden met een Facebook profiel.

Mensen zoeken op Facebook - voor niet-Facebook gebruikers

Let op: om deze zoekfuncties te gebruiken moet je **niet** ingelogd zijn op Facebook. Je krijgt alleen mensen te zien die hun profiel op "openbaar" hebben staan. Het wil dus niet zeggen dat iemand niet op Facebook zit als hij of zij niet bovenkomt.

Zoeken op naam

Vul in de bovenste zoekbox een (voor)naam in. Na het doorklikken krijg je een lijst met profielen te zien. Na het doorklikken krijg je ook enkele vrienden te zien.

Zoeken in een alfabetische lijst

Hier kun je bladeren door een alfabetische lijst. Na het doorklikken krijg je ook een aantal vrienden van een persoon te zien.

Mensen zoeken op Facebook - voor Facebook gebruikers

Mensen zoeken met de Friend Finder

Let op: voor deze zoekfuncties moet je ingelogd zijn op Facebook. Je krijgt niet alleen openbare profielen te zien, maar ook de namen van mensen die hun profiel hebben afgeschermd.

Op naam zoeken

- Open je Facebook profiel.
- Typ de (voor)naam in het zoekvak bovenaan de pagina.
- Klik op het **vergrootglas** om te zoeken.
- Er opent een lijst met profielen.
- Klik in de linkerkolom op **mensen**.
- Geef bij **Locatie** zonodig een plaats, opleiding of werkplek op.
- Klik onderaan op "meer resultaten weergeven".

- Open je Facebook profiel.
- Klik rechtsboven op **Vrienden zoeken**.
- Facebook toont nu een aantal mensen waarmee je gemeenschappelijke vrienden hebt.
- Aan de linkerkant kun je meer gericht naar mensen zoeken door het invullen van een plaats, school of werkgever.

Documenten beveiligen

Document beveiligen

Documenten kunnen snel worden beveiligd met een wachtwoord, bijvoorbeeld via een tekstverwerker of PDF programma. Ook zijn er speciale tools voor de encryptie van vertrouwelijke gegevens.

OpenOffice en Word bestand beveiligen

Office en OpenOffice.org kunnen een document beveiligen: bij het openen wordt dan een wachtwoord gevraagd. Het is ook mogelijk om alleen het wijzigen te beveiligen: het document kan dan wel worden gelezen, maar niet worden veranderd. Dit soort wachtwoorden biedt bescherming tegen gewone gebruikers, als er een sterk wachtwoord wordt gekozen. Professionals kunnen de wachtwoorden wel kraken.

Het instellen van een wachtwoord gaat via:
Extra - Opties - Beveiliging/Veiligheid.

PDF's beveiligen

De meeste programma's die **PDF's maken** kunnen deze ook beveiligen met een wachtwoord. Het hangt van de encryptie af hoe krachtig de beveiliging is. Voor huis-tuin-en-keuken gebruik is het bruikbaar: gebruik wel een sterk wachtwoord.

Ingepakte bestanden beveiligen
Programma's die bestanden comprimeren - bijvoorbeeld naar ZIP, RAR of TAR.GZ - kunnen deze ook beveiligen met een wachtwoord. De gebruikte encryptie is zeer krachtig. Als zo'n bestand wordt verstuurd moet degene die het bestand ontvangt hetzelfde programma gebruiken.

Encryptie software

EncryptOnClick

Klein, simpel programma dat alle soorten documenten en mappen beveiligt met zware encryptie. Handig voor het verzenden van vertrouwelijke documenten, maar niet voor documenten waar je vaak in werkt: er moet steeds opnieuw een wachtwoord op worden gezet. Het werkt snel: naar een document bladeren, wachtwoord opgeven, klaar. Je ziet nu een 'slot' op het document zitten. Als het beveiligde bestand wordt verstuurd moet degene die het ontvangt het wachtwoord kennen, en EncryptOnClick hebben of een recente versie van WinZip.
Platform: Windows (alle versies).
Nederlands: Nee.
Gratis: Ja.

Programma beveiligen met een wachtwoord

Empathy

Dit programma kan een wachtwoord zetten op software: een programma is dan niet meer te openen zonder wachtwoord. Ook als het wordt gekopieerd naar een andere computer. Het wachtwoord is niet terug te vinden in bestanden op de computer. De standaardversie heeft geen sterk wachtwoord. De volledige versie is te verkrijgen door de maker een ansichtkaart te sturen.
Platform: Windows.
Nederlands: Nee.
Gratis: Gratis basisversie.

Bitcoin

Onlangs werd er in Enschede aangifte gedaan van diefstal van BITCOIN,s
Wat is nu een Bitcoin?

Bitcoin is een vorm van elektronisch geld, en tevens de naam van de opensourcesoftware die is ontworpen om dit te gebruiken. Bitcoins, afgekort BTC, kunnen worden opgeslagen op een personal computer in de vorm van het wallet bestand of worden beheerd door een derde partij, een portemonneedienst. In beide gevallen kan het geld naar een ander persoon worden verzonden via het internet door iedereen met een Bitcoinadres.

Dit elektronische geld maakt gebruik van een database verspreid over knooppunten van een peer-to-peer-netwerk om transacties te journaliseren, en maakt gebruik van cryptografie om te voorzien in de nodige beveiliging, zoals dat Bitcoins alleen kunnen worden uitgegeven door de persoon die er eigenaar van is, en nooit meer dan één keer uitgegeven kan worden door die eigenaar.

De peer-to-peertopologie van Bitcoin en het ontbreken van centrale administratie maakt het praktisch onmogelijk voor een overheid, of ieder ander, om de waarde van Bitcoins te manipuleren of meer inflatie te induceren dan er van tevoren is vastgelegd. Het ontwerp zorgt voor anoniem eigendom en overdracht van waarde.

De Bitcoin dient virtueel "gedolven" te worden. Elke dag wordt er een bepaalde hoeveelheid vrijgegeven aan mensen die de Bitcoin delven ('mining'). Dit wordt gedaan door het inzetten van de rekenkracht van computers. Er zijn inmiddels diverse groepen actief op internet waar mensen samen kunnen zoeken naar het elektronische geld, door alle gezamenlijke rekenkracht van de computers in te zetten tijdens het delven, de zogeheten 'mining pools'.

Dit zijn de standaardeigenschappen die elk Bitcoin-achtig netwerk vertoont:

Elk aangesloten systeem kan Bitcoins overmaken naar elk ander systeem in het netwerk.
Transacties zijn onomkeerbaar.
Dubbele uitgaven worden voorkomen door het gebruik van een blokketen.
Transacties worden binnen enkele seconden door het netwerk heen uigezonden en binnen 10 tot 60 minuten gecontroleerd.
Verwerking van transacties en uitgifte van geld gebeurt collectief door middel van delven.
Transacties kunnen worden ontvangen of uw computer aanstaat of niet.

Aan minister Dijsselbloem werden onlangs enkele kamervragen gesteld betreffende de Bitcoin.

Wordt er toezicht gehouden en/of opsporing verricht op het mogelijke gebruik van
Bitcoins als instrument voor het witwassen van crimineel geld of het oppotten van zwart geld?

Is het private partijen onder Europees of nationaal recht toegestaan een alternatieve
(digitale) betaaleenheid te ontwikkelen en commercieel (op grote schaal) te gebruiken?

Antwoorden:

Het staat een ieder vrij om alternatieve (digitale) producten te ontwikkelen en/of te gebruiken, zolang dat geen strijd oplevert met de Nederlandse wetgeving, zoals bijvoorbeeld de Wet op de kansspelen.

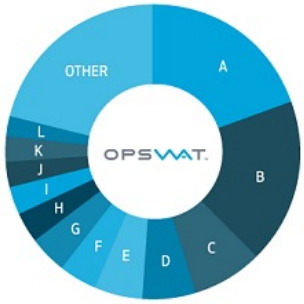
Naar huidig inzicht is Bitcoin geen elektronisch geld in de zin van de Wet op het financieel toezicht, onder meer omdat Bitcoins niet zijn uitgegeven in ruil voor ontvangen geld en geen vordering op de uitgever vertegenwoordigen. Daarmee voldoet de Bitcoin in ieder geval niet aan twee van de vier in de wet gestelde vereisten. Bitcoin is ook anderszins geen financieel product in de zin van de wet. Ook de (bemiddeling bij de) aan- of verkoop van Bitcoins is geen financiÃ«le dienst, zodat de Wet op het financieel toezicht niet van toepassing is.

Voor wat betreft de opsporing heeft de FIOD vanuit zijn opsporingstaak aandacht voor het mogelijk gebruik van Bitcoins in witwaspraktijken. Uit onderzoek zal moeten blijken in hoeverre Bitcoins voor criminele doeleinden gebruikt worden en op welke wijze de FIOD daar in de toekomst op gaat inspelen. Hierbij wordt nauw samengewerkt met het High Tech Crime Unit van de Politie.

57% internetters gebruikt gratis virusscanner

Het gebruik van gratis virusscanners is het afgelopen jaar sterk gestegen, waarbij 57% van de internetgebruikers een gratis anti-virusprogramma heeft geïnstalleerd, zo blijkt uit cijfers van softwarebedrijf OPSWAT. Het bedrijf verzamelt gegevens over softwaregebruik.

In de Top 12 van meest gebruikte anti-virusprogramma's worden de eerste vijf plekken door gratis virusscanners in beslag genomen, te weten: Avast Free Antivirus (19,5%), Microsoft Security Essentials (18,3%), Windows Defender (7,7%), AVG Anti-Virus Free Edition (6,1%) en Avira Free Antivirus (5,5%). Bij elkaar opgeteld hebben deze gratis oplossingen een marktaandeel van 57%. Een jaar eerder hadden de gratis programma's, zonder dat Windows Defender werd meegeteld, een aandeel van 37%.



	Antivirus Product	Market Share
A	avast! Free Antivirus	19.5%
B	Microsoft Security Essentials	18.3%
C	Windows Defender	7.7%
D	AVG Anti-Virus Free Edition	6.1%
E	Avira Free Antivirus	5.5%
F	Norton Internet Security	4.1%
G	ESET Smart Security	4.1%
H	Kaspersky Internet Security	3.2%
I	AVG Internet SEcurity	3.1%
J	avast! Internet Security	2.8%
K	ESET NOD32 Antivirus	2.5%
L	McAfee VirusScan	2.4%
	Other	20.9%

Het werkelijke aandeel van gratis virusscanners kan nog veel hoger liggen, aangezien anti-virusprogramma's die vanwege hun kleine marktaandeel niet in de Top 12 verschenen onder één noemer werden ondergebracht. Het gaat hier echter om producten die bij elkaar een aandeel van 21% hebben.
Windows Defender

OPSWAT keek ook naar het gebruik van Windows Defender, dat standaard met Windows 8 wordt meegeleverd, en het gratis Microsoft Security Essentials. Dan blijkt dat een groot percentage van de Windows 8-gebruikers Windows Defender heeft uitgeschakeld en door een ander anti-virusprogramma heeft vervangen.

Van de Windows 8-gebruikers die Windows Defender gebruiken, blijkt dat 65% nog een aanvullend anti-virusprogramma met real-time bescherming gebruikt. Bij Security Essentials is dit juist omgekeerd, waarbij 86% alleen Security Essentials gebruikt, terwijl 14% het combineert met een virusscanner waar real-time bescherming is ingeschakeld.

Security Essentials verslaat McAfee in anti-virustest

Het gratis Microsoft Security Essentials heeft de betaalde Internet Security Suites van Trend Micro en McAfee in een realistische anti-virustest van Dennis Technology Labs verslagen. Security Essentials kwam de afgelopen maanden vanwege slechte scores bij andere tests regelmatig negatief in het nieuws.

Volgens Microsoft werden deze testresultaten veroorzaakt doordat de virusscanner zich vooral richt op echte dreigingen waar gebruikers mee te maken hebben, in plaats van dat er naar de einduitslag van een anti-virustest wordt gekeken. In een nieuwe test van Dennis Technology Labs weet Security Essentials, dat in principe alleen een virusscanner is, de Security Suites van Trend Micro en McAfee achter zich te houden.

Product	Protected	Legitimate accuracy	Total accuracy
Kaspersky Internet Security 2013	100	740	1040
ESET Smart Security 6	97	716.5	990.5
Norton Internet Security 2013	98	704	986
Avast! Free Antivirus 8	94	746	962
AVG Anti-Virus Free 2013	93	738	959
BitDefender Internet Security 2013	97	626	882
Microsoft Security Essentials	82	748	872
Trend Micro Internet Security 2013	96	593.5	842.5
McAfee Internet Security 2013	81	583	719

Test

De test heeft betrekking op de periode van juli tot en met september en werd op een realistische manier uitgevoerd waarbij er echt gehackte websites werden bezocht die bezoekers via lekken in veel gebruikte programma's probeerden te infecteren. De testcomputer draaide Windows 7 en was opzettelijk van onveilige versies van Adobe Flash Player, Adobe Reader en Java voorzien.

Dennis Technology Labs laat weten dat het de lijst met besmette websites zelf heeft opgesteld en dat de gebruikte websites niet van een anti-virusbedrijf afkomstig zijn, wat de testresultaten zou kunnen beïnvloeden.

Naast het bezoeken van geïnfecteerde websites werd ook gekeken hoe de beveiligingspakketten met legitieme software omgaan. Het komt nog altijd voor dat beveiligingssoftware ten onrechte een legitiem programma blokkeert omdat het denkt dat het met malware is besmet, ook wel een 'false positive' genoemd.
Einduitslag

Aan de hand van de malwaredetectie en omgang met legitieme software werd een einduitslag berekent. Dan blijkt dat Kaspersky bovenaan eindigt. Het beveiligingspakket wist alle malware te stoppen. Security Essentials scoort 82% en presteert daarmee net iets beter dan McAfee Internet Security 2013, dat op 81% uitkomt.

Trend Micro stopt 96% van de malware, maar gaat vaker met legitieme software de fout in. Aangezien Security Essentials hier de hoogste score neerzet, eindigt het uiteindelijk ook boven Trend Micro. Hieronder de einduitslag.

Panda Cloud Free, Emsisoft en TrendMicro beste in real-world protection test

Vorige maand gebruikte AV Comparatives voor de test 326 schadelijke sites (inclusief enkele mailbijlagen) die malware aanboden via drive-by downloads. De computers die getest werden waren bijgewerkt met de laatste updates voor Windows en software van derde partijen (zoals Flash en Java). Virussen, Trojaanse paarden en dergelijke die via gaten in verouderde software pc's proberen te besmetten werden dus niet meegeteld. Gekeken werd hoeveel van deze 326 dreigingen geblokkeerd werden door de virusscanners.

Panda Cloud Free Antivirus, TrendMicro en Emsisoft waren deze maand foutloos bij het onderscheppen van de malware. Ze werden op de voet gevolgd door BitDefender (dat op deze test ook heel vaak 100% scoort), F-Secure, McAfee en Kaspersky die één schadelijk exemplaar doorlieten (rood) of de gebruiker vroegen of deze mogelijke bedreiging geblokkeerd moest worden of niet (geel). De betaalde Avira liet één virus door, avast! Free Antivirus twee en de betaalde AVG vier.

Rusland wil geheime dienst cybercrime laten bestrijden

De Russische overheid heeft een wetsvoorstel ingediend waardoor de geheime dienst FSB de bevoegdheid krijgt om cybercrime te onderzoeken en bestrijden. Als het voorstel wordt goedgekeurd kan de FSB speciale operaties uitvoeren om naar informatie over gebeurtenissen of acties te zoeken die een dreiging voor de Russische informatiebeveiliging vormt.

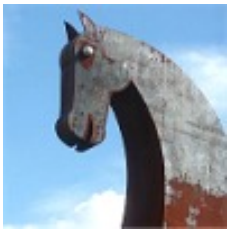
Naast de staats, militaire, economische en ecologische veiligheid wordt de FSB daardoor ook verantwoordelijk voor informatiebeveiliging. De opstellers van het voorstel beweren dat de informatieoorlogsvoering tussen landen aan het intensiveren is en dat malware als informatiewapen kan worden ingezet. Het wetsvoorstel laat niet in detail weten hoe de FSB zich straks met het identificeren en bestrijden van cybercriminelen gaat bezighouden.

Straffen

Volgens het Russische persbureau RIA Novosti is cybercrime een groot probleem in Rusland, mede veroorzaakt doordat de overheid nauwelijks ingrijpt, lichte straffen en het feit dat cybercriminelen zelden worden vervolgd. Op dit moment staat er op het veroorzaken van grootschalige schade van meer dan 23.000 euro of het stelen van computergegevens voor financieel gewin een gevangenisstraf van 6 maanden. In augustus werd er nog voorgesteld om dit naar 4 jaar te verhogen.

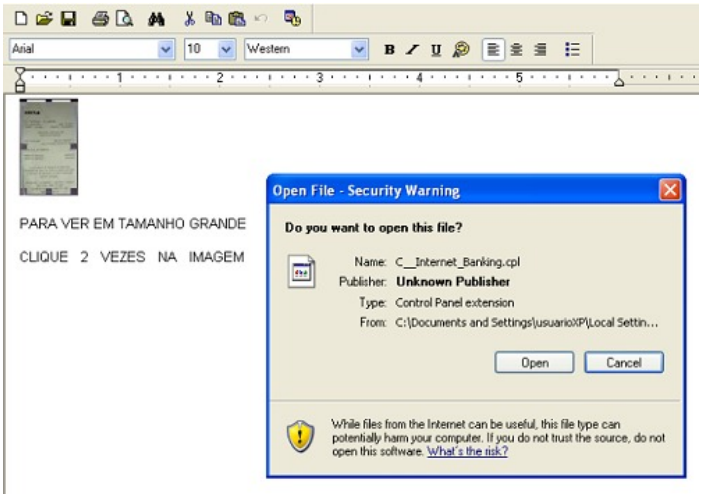
Trojaans paard verstopt zich in RTF-document

Braziliaanse cybercriminelen gebruiken een nieuwe truc om internetgebruikers met malware te infecteren, namelijk RTF-documenten waarin een Trojaans paard is ingebed. Slachtoffers ontvangen eerst een e-mail die zogenaamd een afschrift van internetbankieren zou zijn, zo meldt Kaspersky Lab.



De meegestuurd bijlage is een RTF-document dat een kleine afbeelding van een bankafschrift bevat, met daaronder de tekst dat de gebruiker er op moet klikken. De ingebedde afbeelding is in werkelijkheid een CPL-bestand. CPL-bestanden worden normaliter voor het Configuratiescherm gebruikt.

In dit geval gaat het echter om een bekende Braziliaanse banking Trojan die gegevens voor internetbankieren steelt, waardoor de criminelen achter de malware geld van de rekening kunnen halen. De infectie treedt op zodra de gebruiker het CPL-bestand opent.



Gratis Nederlandse tool beschermt tegen CryptoLocker

Een gratis tool van het Nederlandse beveiligingsbedrijf SurfRight voorkomt dat de CryptoLocker-ransomware bestanden op computers kan versleutelen. CryptoLocker is sinds september actief en verspreidt zich via e-mailbijlages, ongepatchte softwarelekken en al op het systeem aanwezige malware.

Eenmaal actief vergrendelt CryptoLocker foto's, documenten en andere bestanden op de computer. Om weer toegang tot de bestanden te krijgen moeten slachtoffers binnen 72 uur 300 euro betalen. Daarna wordt er bijna 1600 euro gevraagd. Door geen ongevraagde e-mailbijlages te openen en softwarelekken te patchen kunnen internetgebruikers infectie voorkomen

Tool

Voor gebruikers die een extra beveiligingslaag willen is er nu een bètaversie van de gratis tool HitmanPro.Alert 2.5 verschenen. Het beveiligingsprogramma is eigenlijk bedoeld om malware in de browser te detecteren, zoals banking Trojans die gegevens voor internetbankieren onderscheppen en naar criminelen doorsturen.

De ontwikkelaars hebben een nieuwe feature toegevoegd genaamd CryptoGuard, die het mogelijk maakt om CryptoLocker en andere malware te blokkeren die lokale bestanden probeert te versleutelen. CryptoGuard zou op bestandssysteemniveau werken en niet met encryptiesoftware zoals BitLocker en TrueCrypt conflicteren.

HitmanPro.Alert zal onmiddellijk meer dan 99 % van alle bekende en nieuwe banking trojans .
Het informeert gebruikers automatisch wanneer kritische systeemfuncties worden doorgeschakeld naar niet-vertrouwde programma's .

Het onthult effectief de aanwezigheid van een zogenaamde Man- in-the - Browser malware .

CryptoLocker verhoogt losgeld voor gegijzelde bestanden

De makers van de CryptoLocker-ransomware die allerlei bestanden op besmette computers versleutelt, hebben het losgeld voor de decryptiesleutel verhoogd naar 10 bitcoins. CryptoLocker versleutelt foto's, documenten en zakelijke bestanden en vraagt het slachtoffer vervolgens om losgeld.

De bestanden zijn met AES-encryptie versleuteld, wat inhoudt dat ze alleen door middel van een back-up zijn terug te halen, aangezien de gebruikte encryptie zeer lastig te kraken is. In eerste werd slachtoffers voor het ontsleutelen van de bestanden 300 dollar of 300 euro gevraagd, of hetzelfde bedrag in een andere valuta, zoals bitcoin.

Opstelten maakt weg vrij voor elektronisch strafdossier

Minister Opstelten van Veiligheid en Justitie wil een elektronisch strafdossier invoeren om zo de stukkenstroom in het strafproces te verbeteren en te versnellen. De minister heeft vandaag een wetsvoorstel voor advies naar verschillende instanties gestuurd, zoals de Raad voor de rechtspraak.

Digitalisering is een belangrijke voorwaarde om strafzaken beter af te wikkelen. Dossiers komen daardoor sneller beschikbaar, het vermindert de administratieve rompslomp en zaakstromen zijn beter te volgen. Dat zorgt voor meer kwaliteit in zaaksafhandeling, voor minder ongewenste uitstroom en past in het programma om de strafrechtsketen te verbeteren en versterken, een speerpunt in het beleid van de minister.

Het is de bedoeling dat het openbaar ministerie, de rechtspraak en de partners in de tenuitvoerlegging - zoals het CJIB - in 2016 processtukken elektronisch uitwisselen. In datzelfde jaar zullen naar verwachting ook de voorzieningen zijn gerealiseerd voor elektronische uitwisseling van processtukken door openbaar ministerie en rechtspraak met de burger en de advocatuur. Het wetsvoorstel maakt de stapsgewijze overgang van papieren naar elektronische processtukken mogelijk. Elektronische uitwisseling is in 2016 de norm, maar de burger kan desgewenst nog papieren stukken opsturen.

Een verdachte, zijn raadsman, een slachtoffer of een getuige, kunnen er baat bij hebben om via internet in contacten te leggen met het openbaar ministerie of het gerecht. Ze kunnen dan sneller en eenvoudiger communiceren, bijvoorbeeld om aangifte te doen, verzoeken in te dienen of in hoger beroep te gaan. Bij elektronische verzending moet vast te stellen zijn van wie het stuk afkomstig is en of het authentiek en betrouwbaar is. In het wetsvoorstel staan daarvoor regels. Het gebruik van een beveiligd webportaal is verplicht en, als er ondertekend moet worden, een elektronische handtekening die voldoende betrouwbaar is.

Opstelten wil ook naar aangifte via het internet, als startpunt van een opsporingsonderzoek. Nu is dat nog beperkt tot enkele delicten, maar straks kan dat bij alle strafbare feiten. De ondertekening van de aangifte gebeurt dan door elektronische identificatie met DigID-sms.

Politie adviseert TrueCrypt voor versleutelen laptop

Nederlanders die op reis gaan en hun laptop meenemen krijgen het advies om die met het gratis opensourceprogramma TrueCrypt te versleutelen. Ook wordt reizigers afgeraden om gevoelige zaken, zoals een kopie van het paspoort, in Dropbox of Evernote op te slaan.

Vanwege de Alert Online campagneweek heeft de politie een speciale factsheet met tips om veilig op reis te gaan gepubliceerd. Naast het installeren van trackingsoftware voor de smartphone of laptop, krijgen reizigers ook het advies om hun data te versleutelen.

"Op een Android telefoon of tablet kun je via instellingen ook de gegevens op je SD-kaart coderen." Wie zijn of haar laptop op reis meeneemt wordt aangeraden om het encryptieprogramma TrueCrypt te gebruiken. "TrueCrypt is een gratis programma om je schijf goed en gemakkelijk te kunnen versleutelen."

Verder wordt het inschakelen van twee-factor authenticatie aangeraden en het gebruik van Dropbox en Evernote voor de opslag van gevoelige gegevens afgeraden, omdat deze diensten de data onversleuteld opslaan. "Diensten die je data versleuteld opslaan (zoals Spideroak of Wuala) zijn dan beter", laat de factsheet weten.

Internetverbinding

Daarnaast worden er nog allerlei tips gegevens voor het gebruik van wifi in het buitenland en dat het beter is om de eigen internetverbinding te gebruiken. "Ben je met een groep dan kun je je internetverbinding delen op je smartphone of een "mifi" aanschaffen en iedereen veilige toegang geven via jouw mobiele verbinding." MiFi is een los (mobiel) apparaatje om een lokaal wifi-netwerk op te zetten.

In het geval er geen andere mogelijkheid is dan het gebruik van een open en onbeveiligd netwerk is het verstandig om een VPN-dienst te gebruiken. "Je kunt een abonnement nemen bij een VPN-aanbieder (bijvoorbeeld Hamachi, private internet access of ProXPN) waarmee je een veilige verbinding maakt over de onveilige verbinding heen."

De informatie uit de factsheet is afkomstig van het Team Digitale Expertise (TDE) van de eenheid Amsterdam en is aangevuld door het Team Digitale Expertise van de Landelijke Eenheid. Klik op het logo hieronder om de factsheet in zijn geheel te lezen.

Firefox en Safari stoppen meeste phishingsites

Firefox en Safari bieden internetgebruikers de meeste bescherming tegen phishingsites, terwijl Internet Explorer de minste bescherming biedt.

Dat blijkt uit onderzoek van NSS Labs naar de detectie van phishingsites en "social engineering malware" door de vier meest gebruikte browsers.
Firefox stopt gemiddeld 96% van de phishingsites, gevolgd door Safari met 95%. Google Chrome volgt op een derde plek met 92%, terwijl Internet Explorer onderaan eindigt (83%).
Naast het gemiddelde werd er ook naar de "zero-hour" blokratio gekeken. In dit geval gaat het om detectie van net gelanceerde phishingsites.

NSS Labs stelt dat het blokkeren van deze phishingsites belangrijker is dan het gemiddelde percentage van geblokkeerde phishingsites, omdat veel phishingsites vaak korte tijd online zijn. Browsers met een laag gemiddelde maar betere zero-hour blokratio kunnen dan ook betere bescherming bieden.

Wederom presteren Safari en Firefox het best, waarbij dit keer Safari (93,4%) net voor Firefox (93,3%) eindigt. Chrome is wederom derde (81,5%) en IE weer laatste (73,3%).

Social engineering malware

Een onderdeel waar IE de overige browsers wel verslaat is met de detectie van social engineering malware. Dit is malware die gebruikers zelf downloaden. Het gaat in dit geval niet om drive-by downloads die internetgebruikers automatisch zonder enige interactie infecteren omdat ze onveilige software gebruiken, maar om programma's waarin malware zit verstopt of die malware zijn.

Waar Firefox en Safari zo goed zijn in het stoppen van phishingsites, weten ze social engineering malware nauwelijks te herkennen. Gemiddeld wordt slechts 10% gestopt. Chrome houdt gemiddeld 83% tegen, terwijl Internet Explorer zelfs 100% detecteert. In het geval van net gelanceerde social engineering malware doen Firefox (8%) en Safari (12%) het wederom niet goed, terwijl Chrome naar een percentage van 49% zakt. IE eindigt met 98% wederom op de eerste plek.

Overigens is Apple gestopt met het doorontwikkelen van de Safari browser voor Windows gebruikers. Uit veiligheidsoverwegingen niet meer downloaden dus.

Versleutel je USB-stick voor onderweg

Een USB-stick staat soms boordevol privacygevoelige informatie.

Prima, tot je zo'n stick verliest. Dan kan je maar beter hopen dat je data stevig versleuteld zijn.

Protectorion ToGo Free zorgt daarvoor.

USB-sticks zijn best handig, want ze zijn stevig en compact. Maar net die compactheid zorgt er ook voor dat je ze sneller dreigt te verliezen of ergens onachtzaam achterlaat. Niet zo erg voor de stick, want die is goedkoop. Maar wellicht wel voor je data.

Wil je voorkomen dat derden die zomaar kunnen inkijken, dan kan je die maar beter encrypteren. Protectorion ToGo Free biedt daar alvast een gebruiksvriendelijke interface voor.

Eenvoudig verslepen

Protectorion ToGo kun je zowel op je interne schijf als op een verwisselbare schijf of stick installeren. Een echte installatie is niet nodig, aangezien het een draagbare applicatie is. Meteen nadat je het programma hebt uitgevoerd, krijg je de vraag een stevig masterpassword in te tikken. Inclusief een hint, voor het geval je het wachtwoord ooit zou vergeten.

Meteen erna kun je aan de slag. Bestanden versleutelen is niet lastiger dan die naar het venster van Protectorion ToGo te verslepen of te kopiëren, en te beslissen of je de originele en dus onversleutelde data meteen wil verwijderen. Het programma encrypteert je data met het beproefde AES 256-bits algoritme.

Uiteraard kan je op elk moment versleutelde bestanden weer ontgrendelen. De optie Unencrypted Export geeft je bovendien de mogelijkheid een reeks bestanden tegelijk te ontsleutelen en die naar een externe map te kopiëren.

Wachtwoorden beheren

Protectorion ToGo heeft bovendien een module voor wachtwoordbeheer aan boord. Hier kan je dan alle ID's van webdiensten of andere applicaties toevoegen. Met een druk op een knop maak je je wachtwoord weer zichtbaar of kopieer je het naar het Windowsklembord.

De gratis versie van Protectorion ToGo toont bij elke opstart van het programma wel een venster met een productvoorstelling. Je bent tevens beperkt tot een installatie op twee externe opslagapparaten.

HYVES STOPT. RED JE FOTO'S!

Hyves stopt als sociaal netwerk en gaat verder als spelletjessite. Pas op! Je moet voor 29 november een aanvraag doen als je je foto's, krabbels en blogs wilt downloaden.

Het is lastig om zelf je foto's en andere gegevens die op Hyves staan in veiligheid te brengen voor de deur dicht gaat, maar Hyves gaat er voor zorgen dat je je gegevens op een eenvoudige manier kunt downloaden. Hiervoor dien je tussen 15 november en 20 november een verzoek bij Hyves in te dienen. Dat kan via het webadres hyves.nl/bedankt. Uiterlijk 31 december 2013 ontvang je dan van Hyves de downloadgegevens van jouw bestanden.

Na 2 december 2013 heeft niemand meer toegang tot de profielen op Hyves. De site gaat dan uitsluitend verder als spelletjessite zoals momenteel al op hyves.nl/games het geval is. Terwijl de rest van Hyves al een tijdje stervende was werd het gedeelte met spelletjes vorig jaar nog uitgeroepen als meest populaire Nederlandse gaming-site.

HOTSPOT SHIELD BIEDT MEER DAN ALLEEN VEILIG INTERNET BUITEN DE DEUR

Hotspot Shield Free is een gratis programma waarmee je veilig via hotspots kunt internetten. Daarnaast biedt het toegang tot websites en webdiensten die normaal gesproken alleen voor Amerikanen beschikbaar zijn.

Wie buiten de deur internet gebruikt maakt vaak gebruik van open WiFi hotspots. Bijvoorbeeld in restaurants, winkels of van particulieren in de buurt. Hotspot Shield is een Amerikaans programma dat veilig surfen via onbekende hotspots tot doel heeft.

Veel open hotspots beveiligen het dataverkeer slecht of helemaal niet. Daardoor kunnen andere gebruikers van het hotspot vrij makkelijk de gegevens die je van en naar het hotspot stuurt aftappen.

Zo is het niet verstandig om via een onbekend hotspot te telebankieren. Je loopt daarbij veel meer risico dan thuis.

Hotspot Shield heeft tot doel dat risico te verkleinen. Als je Hotspot Shield gebruikt maak je verbinding met het VPN (Virtual Private Network) van AnchorFree. Alle gegevens die je vervolgens vestuurd lopen via dit netwerk en dat gebeurd op een veilige versleutelde manier. De gegevens die je langs het hotspot gaan zijn daardoor niet te lezen voor anderen die via het hotspot je gegevens willen aftappen.

Zo kun je veilig buiten de deur via hotspots internetten, maar toch is dat niet de belangrijkste reden dat Hotspot Shield Free erg populair is in Nederland. Deze gratis software heeft namelijk een heel interessante nevenfunctie. Doordat je een Amerikaanse VPN surft krijg je een ander, Amerikaans, IP-adres. Hierdoor lijkt het alsof je vanuit Amerika surft en krijg je ineens toegang tot websites en webdiensten die normaal voor Nederlanders afgesloten zijn.Denk hierbij aan videosites als Hulu.com, downloadsites als The Piratebay en de gratis te bekijken video on demand series van Amerikaanse omroepen als CBS en NBC.

Omgekeerd kan het voorkomen dat je Nederlandse content niet kan zien. Maar dit is heel simpel. Hotspot Shield opent namelijk een apart tabblad in je browser waarin je het beveiligingsprogramma met één klik aan en uit kunt schakelen.

Hotspot Shield is er in een gratis en een betaalde versie. Het verschil zijn de advertenties die bij de gratis versie getoond worden. Het programma is beschikbaar voor Windows, Mac OS X en Android. Wees bij het installeren van de gratis versie wel zorgvuldig, want als je een vinkje vergeet uit te vinken krijg je veel ongewenste reclamesoftware meegeleverd.

Hotspot Shield is een prima programma om buitenshuis veilig te surfen, maar de meeste Nederlanders gebruiken het gewoon thuis.

Windows 8.1 zonder Microsoft-account installeren

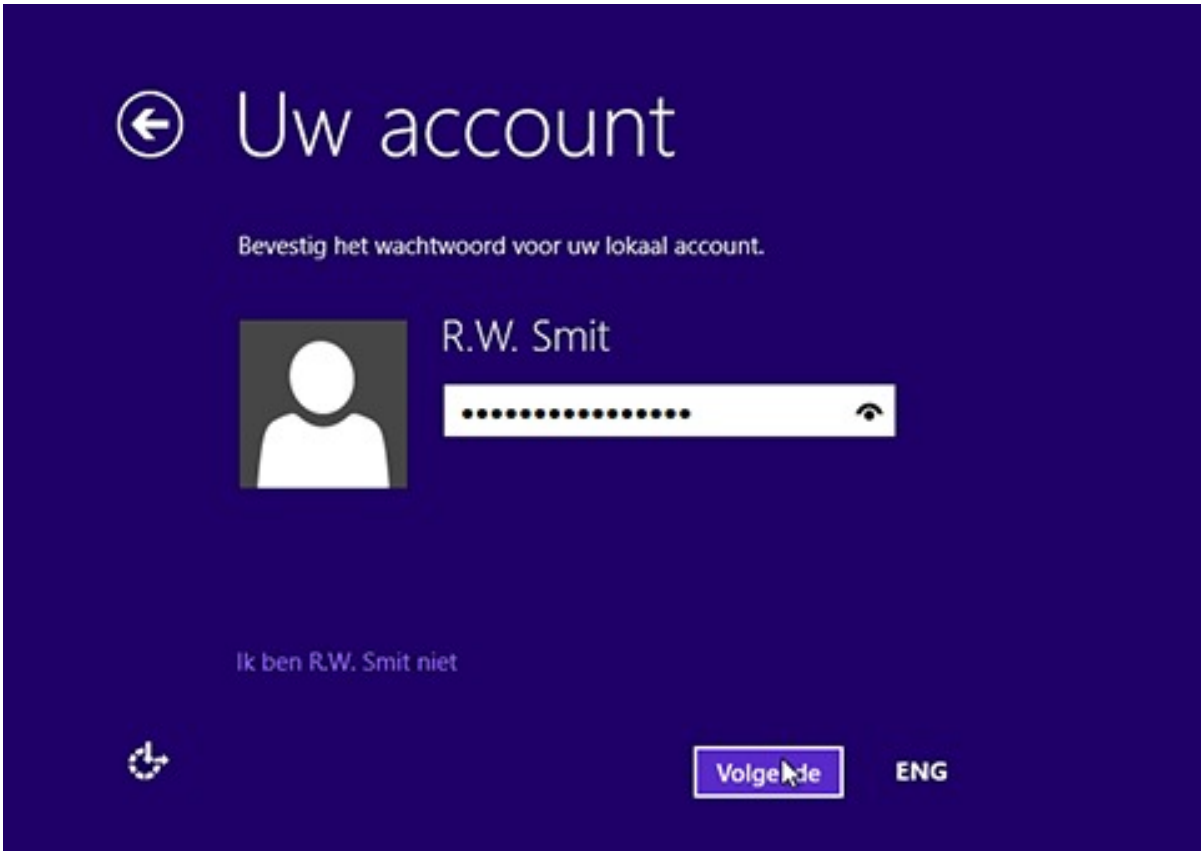
Windows bijwerken met de nieuwste update zonder verplicht Microsoft-account? Dat kan, al moet je wel even goed opletten tijdens de installatie.

Tijdens het installeren van de update van Windows 8.1 word je halverwege het installatieproces gevraagd in te loggen met je Microsoft-account. Ogenschijnlijk kun je niet om deze stap heen, wat zou betekenen dat je een nieuw account moet aanmaken als je dat nog niet hebt. Hoogst irritant als je niet van plan bent om gebruik te maken van de online diensten van de softwarefabrikant.

Gelukkig is er een mogelijkheid ingebouwd je bestaande, lokale account te blijven gebruiken. Die optie is echter goed verstopt, dus hebben we de daarvoor relevante stappen er even tussenuit geplukt.

Stap 1.

In het venster Uw account log je in met de gegevens die je tot nu toe gebruikte voor je lokale account, waarna je klikt op Vol-

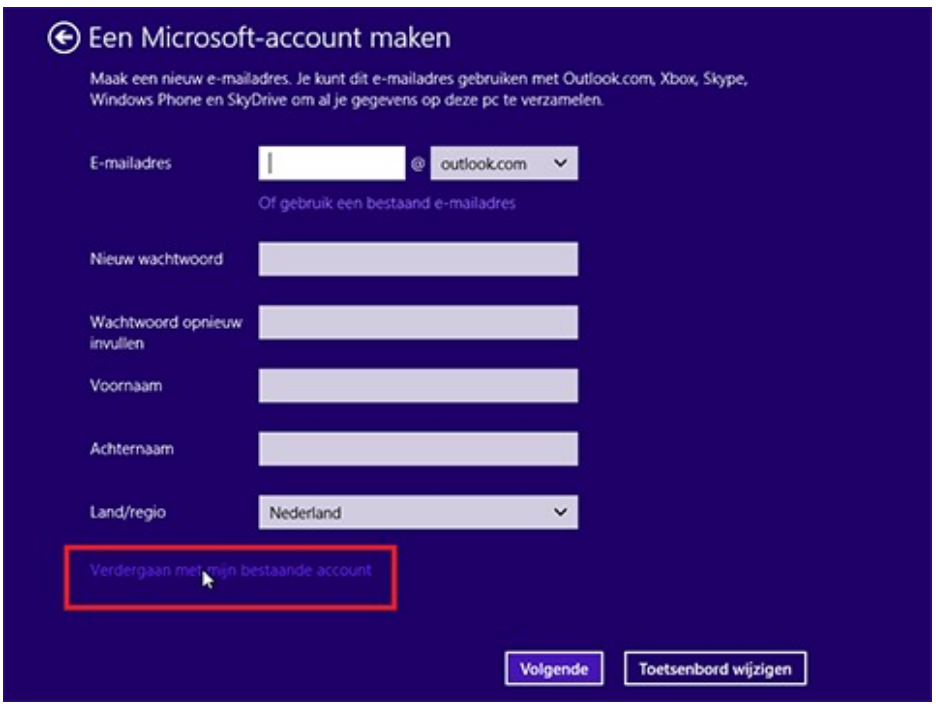


Stap 2.

Het volgende venster is bedoeld om je aan te melden bij je Microsoft-account. Heb je dat niet, dan is daarvoor een duidelijk zichbaar linkje aangebracht. Veel minder goed te zien is de link 'Een nieuw account maken' en juist die heb je nodig, dus klik

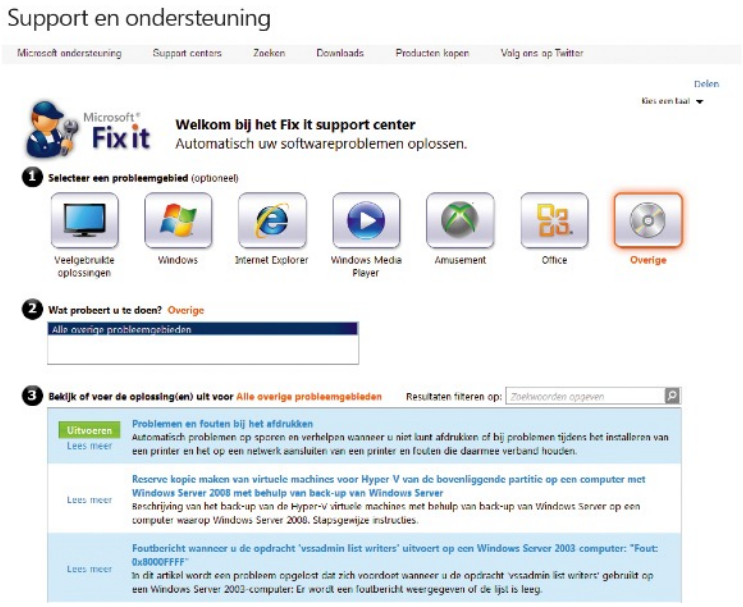
Stap 3.

In het nu getoonde venster kun je een e-mailadres aanmaken voor je nieuwe Microsoft-account. Dat wil je niet, daar is het immers allemaal om begonnen. Klik daarom op de bijna onzichtbare link 'Verdergaan met mijn bestaande account' helemaal onderaan, waarmee je het doel hebt bereikt!



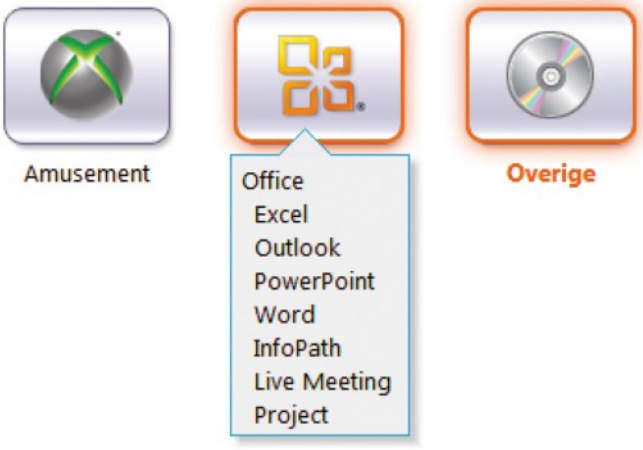
Fixit: Online fixer van Microsoft

Computerproblemen oplossen kan knap lastig zijn, vooral als u niet goed weet waar u aan begint. Microsoft heeft een online reparatiecentrum klaargezet, waarmee u in enkele muisklikken en zonder enige voorkennis een hoop ellende oplost.



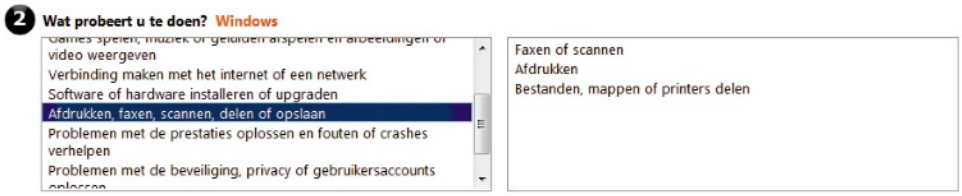
1. Welkom

Microsoft brengt éénkliksoplossingen voor een heel brede waaier aan problemen die u als gebruiker met Microsoft-software kunt ondervinden. De meeste van die oplossingen zitten vervat in kleine programmaatjes (exe-bestanden) die u binnenhaalt via een slim opgestelde webpagina, waar de automatische online reparateur zo exact mogelijk zal proberen achterhalen wat het probleem is. Daarvoor surft u eerst naar support.microsoft.com/fixit. Zo komt u bij het Fix it support center, het diagnosecentrum en walhalla van Microsoft-oplossingen. Wanneer de webpagina zich opent in een vreemde taal, zet u de interface rechtsboven via de knop Kies een taal in het Nederlands



2. Probleemgebieden (1)

In vak 1 bevinden zich zeven probleemgebieden: Veelgebruikte oplossingen, Windows, Internet Explorer, Windows Media Player, Amusement, Office en Overige. Weet u niet goed in welke categorie uw probleem past, dan doet u er goed aan niet lukraak op deze knoppen klikken. Beweeg liever uw muisaanwijzer over iedere rubriekknop; op die manier verschijnen de toepassingen waarvoor er oplossingen onder de knop zitten. Vooral de knoppen Amusement en Overige kunnen meerdere ladingen dekken. Bij Amusement vindt u bijvoorbeeld ook oplossingen voor de Windows Phone, en bij Overige voor Microsoft Exchange en allerlei serverproblemen.



3. Probleemgebieden (2)

Laten we ervan uitgaan dat u problemen ondervindt met het afdrukken van bestanden. Hiervoor selecteert u het probleemgebied Windows. In het tweede vak moet u aangeven wat u precies probeerde te doen wanneer de ellende begon. Aan de linkerkant verschijnt een lijstje van mogelijke acties die problemen met zich meebrengen. In dit voorbeeld zijn dat: Afdrukken, Faxen, Scannen, Delen of Opslaan. In het vakje daarnaast kunt u deze selectie verfijnen, dus hier kiest u Afdrukken.

4. Oplossingen

In het derde vak verschijnen de oplossingen die deze Microsoft-wizard voor u in petto heeft. De blauwe titels zijn duidelijk, en in één oogopslag weet u of de oplossing die u zoekt erbij zit. Omdat het nooit kwaad kan om écht zeker te zijn van uw zaak, klikt u wanneer u denkt dat u bij de juiste fix bent beland eerst op de knop Lees meer. Hierdoor opent zich een nieuwe webpagina van de Microsoft support-site waarop het probleem en de oplossing beschreven worden. Als u zeker bent dat dit het euvel is dat u wilt aanpakken, gaat u terug naar het Fix it center en klikt u op de groene knop Uitvoeren. Hierdoor zal het programma een exe-bestand downloaden.

5. Exe-tools

Als dit exe-bestand gedownload is, opent u de map waarin de downloadbestanden staan en dubbelklikt u op dit bestand. In het volgende dialoogvenster vraagt het systeem of u het zelfuitvoerbare bestand wilt activeren. Klikt u op Ja, dan opent er een specifieke Fix it-tool. Die zal automatisch uw systeem scannen en achteraf vragen of hij ineens ook de nodige reparaties mag uitvoeren. Een tweede optie is dat hij eerst de problemen opsomt en dat u daarna handmatig de reparaties selecteert die u wilt toepassen.

Microsoft® Fix it

De eigenaar van een domeinnaam achterhalen

De eigenaar van een website is snel te vinden via de registratie van de domeinnaam. Nederlandse en Belgische domeinnaamhouders kunnen online worden opgezocht bij SIDN en DNS Belgium.

Geen contactgegevens?
Websites vermelden soms geen juiste contactgegevens. Wie - om welke reden dan ook - contact wil opnemen met de persoon achter een website, kan in een *Whois* register opzoeken op wiens naam de domeinnaam staat. Vaak is dit de eigenaar zelf, of een bedrijf dat in contact staat met de eigenaar (zoals de webhoster of de webdesigner).

Nederlandse domeinnamen opzoeken

SIDN
Typ de domeinnaam in het zoekveld, en klik op **OK**. Vink in het volgende scherm het vakje**Accoordverklaring** aan, en klik op **OK**. De **houder** van de domeinnaam is de eigenaar, de**registrar** is het bedrijf dat de domeinnaam voor de eigenaar heeft geregistreerd.

Belgische domeinnamen opzoeken

DNS
Typ de domeinnaam in het veld, en klik op **Check**. Na het opzoeken van de domeinnaam is informatie over de domeinnaamhouder te verkrijgen door te klikken op
Meer info.

Internationale domeinnamen opzoeken

Who Is The Owner
Deze dienst zoekt wereldwijd in 350+ *Whois* registers.

Laptop op internet via een Android mobiel

Via *tethering* kun je een laptop op internet laten gaan met een Android mobiel. In deze handleiding wordt gebruik gemaakt van WiFi: er wordt een draadloze hotspot ingesteld.

Op internet via een Android mobiel

Hoe werkt het?
Je kan een laptop of iPad op internet laten gaan via een smartphone met een internetverbinding. Dit heet *tethering*: één internetverbinding delen met meerdere apparaten. Tethering kan via een USB kabel, of draadloos met Bluetooth of WiFi. In deze handleiding wordt de verbinding gemaakt via WiFi: er wordt een draadloze hotspot ingesteld.

Wat heb je nodig?
Een smartphone met Android 2.2 of hoger.
Een mobiel abonnement met databundel.
Een iPad of laptop met WiFi.

Mag dit van mijn provider?
In de nieuwe Telecomwet - ingegaan in mei 2012 - wordt de netneutraliteit gewaarborgd. Dit betekent dat telecomaanbieders geen internetdiensten mogen blokkeren, belemmeren of afknijpen. Online gaan via tethering valt hier onder: providers mogen het niet verbieden of verhinderen.

Dataverbruik bijhouden
De kosten van mobiel internet zijn hoog, dus ook bij het internetten via de mobiel. Let dus op hoe groot je databundel is, en wat je verbruik is. Door het installeren van een app kun je gemakkelijk je dataverbruik bijhouden, bijvoorbeeld met **Traffic Monitor** of **3G Watchdog**.

Handleiding: laptop of iPad op internet via een Android mobiel

- Ga op de mobiel naar **Instellingen** - **Draadloos en netwerk** - **Tethering en draagbare hotspots**.
- Vink aan: **Draagbare Wi-Fi hotspot**.
- Klik op **Draagbare Wi-Fi hotspot config**.
- Vul een naam in.
- Kies bij beveiliging: **WPA2 PSK**.
- Vul een wachtwoord in.
- **Opslaan**.**Laptop:**
- Klik op het WiFi icoon in de taakbalk om de **WiFi netwerken** te zien (of blader via het Configuratiescherm naar het Netwerkcentrum).
- Als het goed is zie je de Android hotspot in de lijst met beschikbare netwerken.
- Bij het maken van de verbinding wordt het wachtwoord gevraagd.**iPad:**
- Ga naar **Instellingen** - **WiFi**.
- Als het goed is zie je de Android hotspot in de lijst met beschikbare netwerken.
- Bij het maken van de verbinding wordt het wachtwoord gevraagd.

Profiel van een overledene verwijderen

Het is pijnlijk om een overleden vriend terug te zien in de Facebook suggesties en verjaardagsnotificaties. De nabestaanden kunnen dit vermijden door contact op te nemen met de netwerksite.

Hoe werkt het?
Je kan contact opnemen met de sociale netwerksite over wat er moet gebeuren met het profiel van een overleden persoon. Het profiel kan een herdenkingsstatus krijgen: het blijft dan op internet, maar het wordt 'bevroren'. Uiteraard kan een profiel ook helemaal verwijderd worden. Als je zelf een nabestaande bent, probeer dan bij je keuze hierin rekening te houden met de gevoelens van andere nabestaanden, waaronder de online vrienden.

Een netwerksite zal de nabestaanden altijd vragen om een bewijs dat de persoon is overleden, zoals een overlijdensakte of een overlijdensbericht uit de krant. Om privacy redenen kunnen de nabestaanden niet de logins van het profiel krijgen.

Facebook

Facebook herdenkingsstatus aanvragen
Facebook biedt nabestaanden de mogelijkheid om een profiel op **Herdenking** te zetten. Dit houdt in dat alleen vrienden het profiel kunnen zien en de persoon niet meer verschijnt in suggesties en verjaardagsnotificaties. Statusupdates en contactinformatie wordt weggehaald. Het prikbord blijft wel bestaan, met de mogelijkheid om berichten achter te laten.

Vragen om verwijdering van een Facebook profiel
Via dit formulier kun je Facebook vragen om het profiel van een overledene te verwijderen. Het profiel moet al een herdenkingsstatus hebben, en wordt dan geheel gewist.

Hyves

Contact met Hyves
Via dit formulier kun je contact opnemen met Hyves over het profiel van een overledene. Je kan het profiel een **In Memoriam** status laten geven. Dit houdt dat er een overlijdensdatum wordt geplaatst, en de persoon niet meer verschijnt in de chat en de verjaardagsnotificaties. De privéfoto's en berichten worden afgeschermd. Uiteraard kun je Hyves ook vragen om het profiel helemaal te verwijderen.

Twitter

Contact met Twitter
Je kan contact opnemen met Twitter per e-mail - en gewone mail - over het account van een overledene. Het Twitter account van de persoon kan worden verwijderd, en de nabestaanden kunnen assistentie krijgen bij het maken van een backup van de Tweets.

Beschadigde bestanden herstellen

Soms zijn beschadigde bestanden na een computercrash nog te redden. Deze speciale software herstelt Word documenten en MP3's die niet meer geopend kunnen worden.

Een bestand dat een foutmelding geeft - "Dit bestand is ongeldig" - is mogelijk beschadigd door een computercrash, virus, of afgebroken download. Er zijn programma's die deze bestanden kunnen repareren door ze te analyseren, en fragmenten in de juiste volgorde te plaatsen. Het resultaat hangt af van de mate van beschadiging: lichte beschadigingen zijn goed te herstellen.

Word documenten herstellen

Word Repair
Eenvoudig programma om beschadigde Word documenten te herstellen. Bestanden worden gerepareerd, of zonodig wordt de tekst die nog te redden uit het bestand gehaald, om op te slaan in een nieuw document. Word Repair werkt met .doc, .docx, dot, .dotx, .docm en .dotm bestanden.
Platform: Windows NT, ME, 95, 98, 2000, 2003, XP, Vista, Windows 7.
Nederlands: Nee.
Gratis: Nee, er is wel een gratis probeerversie.

MP3's herstellen

MP3 Diags
Dit programma repareert kapotte MP3's: door bitrate, headers en tags te herstellen worden bestanden weer afspeelbaar. Zonodig wordt je hele collectie gecheckt op fouten, maar je kan ook één bestand repareren.
Platform: Windows NT, ME, 98, 2000, 2003, XP, Vista, Windows 7.
Nederlands: Nee.
Gratis: Ja.

Bestanden herstellen van een beschadigde geheugenkaart

ArtPlus Digital Photo Recovery
Klein programma om foto's te herstellen van een kapotte, gewiste of beschadigde geheugenkaart. Ook van kaarten die niet herkend worden door Windows zijn soms foto's te redden. Er kunnen JPEG, TIFF en RAW bestanden worden hersteld.
Platform: Windows 8, Windows 7, XP, Vista met alle geheugenkaarten.
Nederlands: Nee.
Gratis: Nee (de gratis versie biedt alleen preview van bestanden).

Bestanden herstellen van een beschadigde CD of DVD

CDCheck
CDCheck kan bestanden op CD-roms en DVD's controleren en herstellen. Het programma test schijven op fouten en repareert beschadigde bestanden. Het scoort hierin goed in vergelijking met andere programma's.
Platform: Windows (alle versies).
Nederlands: Nee.
Gratis: Ja, voor privé-gebruikers. Wel registreren.

IsoPuzzle
Dit programma redt bestanden van beschadigde CD's en DVD's. Het werkt alleen met gegevens, dus niet met muziek CD's. Ook als de schijf niet meer afleesbaar is zal IsoPuzzle proberen om zoveel mogelijk bestanden over te zetten naar de harde schijf. De geredde bestanden worden opgeslagen als een ISO image. Zo'n bestand kan op een lege CD of DVD worden gebrand.
Platform: Windows (alle versies).
Nederlands: Nee.
Gratis: Ja.

Op dit moment in de schatkist:
(Klik op de kist om het te downloaden)

Wet Computercriminaliteit III

PC Decrapifier

Memorie van Toelichting

Asus Ai charger

Blackberry Desktop Software

Recuva

Bootkit Removal Tool

Format Factory

Twitter handleiding

Revo Uninstaller

UnstoppableCopier

BLOG

Minder blauw op straat en meer online graag, betoogde microbioloog Rosanne Hertzberger deze week in NRC. Aanleiding was de arrestatie van grooming-verdachte Frank R. uit Cuijk. ‘Weer een pedofiel die online straffeloos zijn gang kon gaan’, aldus Hertzberger die de schuld daarvoor min of meer bij burgerrechtenorganisatie Bits of Freedom legt. Die zijn er immers verantwoordelijk voor dat de politie nog steeds ‘nauwelijks een rol speelt op het internet’, doordat ze elke poging om de opsporingsbevoegdheden online uit te breiden, frustreren. ´Nederlandse pedofielen blijken keer op keer volledig vrij om terabytes aan beeldmateriaal te up- en downloaden´, schrijft Hertzberger. ‘Enig idee hoeveel onderzoeken naar cybercriminaliteit er werden afgerond in de recente prestatiecijfers van de politie? Nul’. En dat komt omdat er te veel privacy is. In Computerworld gaat columnist Maarten Reijnders tegen die mening in. Volgens Reijnders heeft de politie juist heel veel online bevoegdheden gekregen, zoals de bewaarplicht van providers. Dat Frank R. al in 2009 op de politieradar opdook en niet werd gepakt, heeft volgens hem dan ook niks met te weinig bevoegdheden te maken, maar veel meer met ‘weinig daadkrachtig optreden van de politie’.

Nederland anno 2013: zo’n vijf miljoen tweets per dag, waarvan 35 duizend met een bedreiging, waarvan weer zo’n tweehonderd met een serieuze bedreiging. Zo ernstig dat de politie ze natrekt. Met als resultaat dat er elke dag wel iemand in Nederland wordt opgepakt of berispt voor bedreiging. Dat stelt Martine Vis die binnen de Nationale politie de portefeuille sociale media heeft. Ze spreekt van een sociaal probleem: ‘vroeger moest je een envelop kopen, een brief schrijven en hem posten. Nu tik je wat woorden en bedreig je iemand. Dat is erg makkelijk en gebeurt dus ook veel.’ Dat bevestigt sociale-media-expert Thomas Boeschoten. Niet de maatschappij is gevaarlijker geworden, ‘het is nu simpelweg mogelijk een echo van onderbuikgevoelens te maken’. En daarom monitoren veertig agenten dag en nacht al het internetverkeer, soms met hulp van ‘experts binnen bepaalde sociale groepen’ die tweets analyseren, en soms zelfs met buitenlandse collega’s als de tweets in vreemde talen staan. ‘Twitterarrestanten’ zijn er in alle groepen van de samenleving. Soms zijn het hevig geëmotioneerde tieners, soms leden van belangengroepen, soms geradicaliseerde eenlingen. En waar de een in de cel beland, wordt de ander (stevig) aangesproken. Zoals de twee tienermeisjes die met hun ouders op het bureau moesten komen nadat ze getwitterd hadden over het opblazen van hun scheikundelokaal. De plek waar die tweets trouwens worden onderzocht, is volgens Vis het real time intelligence center. Agenten ‘koppelen daar de tweets aan andere informatie’.
Bij Pauw en Witteman vertelde Vis heel transparant hoe haar team te werk gaat bij het opsporen van de afzenders van deze dreigtweets.

Volgens het CBS is vorig jaar 3% van alle Nederlanders boven de 15 jaar slachtoffer geworden van fraude bij aan- of verkopen via internet. Het gaat om zo’n 370 duizend personen. Jongeren (18-35) werden vaker slachtoffer dan ouderen, middelbaar- en hoogopgeleiden vaker dan laaggeschoolden, aankoopfraude komt vaker voor dan verkoopfraude. Volgens Thuiswinkel.org zal rond 2020 ongeveer eenderde van alle consumptieve bestedingen via internet gedaan worden, zo’n 27 miljard euro. Bestedingen in fysieke winkels zullen rond 2020 nog maar 47 miljard bedragen (-15%).

Bij de grote landelijke kinderpornoactie van half oktober (144 zoekingen, 1753 inbeslaggenomen gegevensdragers) werd ook een man als verdachte aangemerkt die zei van niks te weten. Het bleek dat hij zijn internetwachtwoord deelde met de buren en dat zijn router onvoldoende beveiligd was. De buurman bleek de downloader te zijn, op het ip-adres van de onschuldige. Het voorval toont volgens het OM aan dat sommige mensen ‘knap stom’ zijn als het gaat om de beveiliging van hun computer. ‘Draadloos internet is thuis eenvoudig te beveiligen en je bent een sukkel als je dat niet doet’, aldus een woordvoerder. ´Meeliften is hetzelfde als je huisdeur open laten staan’.

De politie op Terschelling waarschuwt voor oplichters die op handelssites als Marktplaats.nl vanaf een waddeneiland spullen proberen te verkopen. Volgens woordvoerder Kalina Pruntel worden vooral telefoons en elektronica aangeboden door mensen die zich voordoen als bewoner van Terschelling, Vlieland of een van de andere eilanden. Kopers die wel betalen maar niets krijgen, ‘komen toch niet zo snel verhaal halen op een eiland’, aldus Pruntel, die spreekt van weken met wel drie meldingen van slachtoffers.

De politie heeft in Alkmaar, Haarlem, Woubrugge en Roden vier mannen aangehouden op verdenking van phishing, digitale fraude en witwassen. De mannen zouden malware op computers van argeloze rekeninghouders hebben geïnstalleerd en via die rekeningen zo’n 150 betalingsopdrachten hebben uitgevoerd en daarmee mogelijk een miljoen euro hebben buitgemaakt. Ze maakten, schrijft De Telegraaf, gebruik van het Tor-netwerk. Het geld werd overgemaakt naar ‘moneymules‘ en vandaar naar rekeningen in binnen- en buitenland. Een deel van de buit werd in bitcoins overgezet. Het OM legde beslag op 77 bitcoins, omgerekend 7700 euro.

De politierechter in Zwolle heeft een man en een vrouw (29 en 30, uit Kampen) veroordeeld tot 140 uur werkstraf voor uitkeringsfraude. De gemeente Kampen vond op facebook dat het stel de fraude pleegde. De vrouw verzweeg dat ze samenwoonde met de man, vader van haar kinderen. Berichten en foto’s op facebook bevestigden het gemeentelijke vermoeden dat het stel fraude pleegde. Toen de man zich in 2008 inschreef bij zijn ouders, omdat de relatie zou zijn beëindigd, startte de gemeente een onderzoek. Oktober 2011 was zoveel ‘bewijs’ verzameld dat de twee toch samenwoonden en volgde aangifte.

Waar de politie in veel landen steeds actiever wordt op sociale media, zijn er ook landen waar ‘transparantie’ met een heel dun potloodje geschreven wordt. Zo mogen politieagenten in Marokko sinds kort geen sociale media meer gebruiken. Volgens de Directie voor de Nationale Veiligheid (DGNS) hebben agenten regelmatig de neiging ‘dingen te uiten die binnenskamers moeten blijven’. Het verbod levert dan ook een bijdrage aan de nationale veiligheid, hoopt men. In 2011 legde DGNS al een verbod op aan soldaten en burgerpersoneel in het leger: geen facebook en twitter meer. Binnen de DGNS is, om het verbod te handhaven, een eenheid met computerspecialisten opgezet die vanuit Frankrijk opereert en Marokkaanse politieagenten in de gaten houdt. De directie zegt ook depressieve en ontevreden agenten te kunnen opsporen die onder een valse naam op sociale media actief zijn.

Hoe gemakkelijk het is om online iemands identiteit over te nemen, ondervond Michelle Vreulink (23, uit Enschede) onlangs toen haar foto werd misbruikt om zangeres Anouk op facebook uit te schelden voor ‘negerhoer’. Vreulink zegt zich rotgeschrokken te zijn. ‘Ik vraag me de hele tijd af: wie zou mij zoiets willen aandoen? Ik vind het echt heel erg’. Ze zegt dat de politie haar niet serieus neemt toen ze het voorval meldde. ‘Ze zeiden dat ze niets voor me konden doen’. Facebook maakte onlangs bekend dat er wereldwijd ruim veertien miljoen nepprofielen bestaan. Met één daarvan kwam studente Natalja Laurey in de problemen toen iemand onder haar naam antimoslimberichten verstuurde. Ook slachtoffer werd de Belgische advocaat Bart de Maeseneir. Een oud-cliënte maakte een facebookprofiel op zijn naam en postte daar kinderporno, liefdesverklaringen naar kantoorgenoten en scheldkanonnades naar cliënten van de advocaat. De vrouw is inmiddels tot achttien maanden voorwaardelijk veroordeeld. Om zulke zaken te voorkomen, moet je jezelf regelmatig googlen, adviseert advocaat Paul Visser die enkele slachtoffers van dit soort trucs bijstaat. ‘Houd in de gaten hoe je naam op internet verschijnt’. En meldt het direct bij de site waarop je een nepprofiel vindt. Nepaccounts worden dan snel geblokkeerd, is zijn ervaring. Met de identiteitsgegevens van de maker van het nepprofiel is het ook mogelijk deze fraudeur voor de rechter te slepen, stelt hij, hoewel lang niet iedereen die moeite neemt. De ‘dader’ is volgens Visser meestal een wraakzuchtige ex of iemand waarmee het slachtoffer een (zakelijk) conflict heeft. Juridisch gezien is identiteitsdiefstal alleen strafbaar als het leidt tot financiële schade. Volgens PvdA-Kamerlid Astrid Oosenbrug is dat echter lastig aan te tonen. Bij de Eerste Kamer ligt momenteel een wetsvoorstel dat vervolging (maximaal vijf jaar celstraf) gemakkelijker moet maken. ‘Mensen moeten leren waar de grenzen liggen en daar hoort een forse straf bij’, aldus Oosenbrug.

Bij de terechtzitting in de strafzaak tegen ‘schooldreiger’ Janoek V. (19, uit Leiden), die april jl via website 4Chan doodsbedreigingen uitte richting een leraar en leerlingen van zijn oude school in Leiden, werd gesteld dat het Team High Tech Crime ingebroken heeft op een router in Costa Rica. Uit het proces-verbaal blijkt volgens internetjurist Arnoud Engelfriet, die als getuige-deskundige werd gehoord, dat het ip-adres van de bedreiging leidde naar een adres in Costa Rica. Daar werd vervolgens nader onderzoek gedaan en daarbij is een rechercheur met het ‘algemeen bekende wachtwoord’ admin die router binnengegaan. Dat valt juridisch gezien onder hacking, aldus Engelfriet. ‘Het gebruik van standaardwachtwoorden is net zo goed binnendringen. Formeel is er sprake van computervredebreuk’. Volgens Engelfriet logde de agent op eigen houtje in. Later werd samengewerkt met de internetprovider in Costa Rica. De agent vertelde de rechters dat hij onder meer kon zien dat de router de dag ervoor opnieuw was opgestart, wat uiteindelijk belangrijk bleek bij het achterhalen van de dreiger. Engelfriet stelt ook dat het binnendringen ‘waarschijnlijk weinig uitmaakt’ voor de loop van de rechtszaak. De politiewet biedt volgens hem ‘redelijk veel ruimte’ om ergens naar binnen te gaan als er een bepaalde dreiging is, hoewel er bij huizen strengere regels gelden dan bij computers. Dat de router in Costa Rica staat, roept wel de vraag op of er geen wetgeving in Costa Rica is overtreden, stelt Engelfriet.

Dit magazine verschijnt maandelijks.
De inhoud bestaat uit verzameld werk uit openbare internetbronnen.
Voor zover mogelijk zal de bron worden vermeld.

Opmerkingen kunt u mailen naar de redacteur.

Onderwerpindex edities 2012: (wilt u een magazine opnieuw / alsnog toegezonden krijgen, volstaat een e-mail)

12-01 > Computercriminaliteit, Definitie van Cybercrime, Strafbare gedragingen, Aftappen van gegevens, MSN chat via Windows, E-mail headers zichtbaar maken, Botnet, Hacking, Spyware,

12-02 > Kwaadaardige software, Phishing, Keyloggers, DNS aanval, Politiemethodes voor bewijs

12-03 > Man in the Middle, ID alert, Meldingsformulier identiteitsfraude, Meldpunten, Wetsartikelen voor computercriminaliteit in enge zin, Cyberstalking, Grooming

12-04 > E-mail spoofing, Elektronisch briefgeheim, Afgeven klantgegevens, Gebruik een live cd/dvd voor veilig internetbankieren, Cloudcomputing

12-05 > Van password naar passphrase, Nieuwe phishing scams, E-mail blunder, Word documenten kunnen virussen bevatten, Hoe hackers u misleiden, Cyberkatvanger, Gratis Windows-tool voor veilig internetbankieren, HP USB disk storage format tool, Muis smeriger dan wc bril

12-06 > Microsoft calling?, Computer in slaapstand of uitschakelen, EU wil internetidentiteitskaart, BVH kan het nog slechter, Wat is Facebook echt waard, Browser voor liefhebber social media, Politievirus, Wardriving, Vind gratis wi-fi op je vakantiebestemming

12-07/08 > Facebook: Nieuwe tactiek om verblijfsvergunning te krijgen, Facebook scant chatconversaties van gebruikers, Lokpuber ontmaskert pedofiel in chatbox, Uw smartphone virusvrij, Facebook Hyves Twitter: zo komt u van uw accounts af, Hoe hackers hacken, Vakantie? Smartphone mee, Beelden bewakingscamera's sneller online, Nederland mist urgentie in aanpak cyberdreiging, Antivirus bedrijf AVG lanceert social media beheertool

12-09 > Veilig WiFi, ID alert, Versnel je windows PC, Windows 7 administrator account activeren, Anders knippen en plakken, Open DNS, Beter geluid uituw PC, Instellingen makkelijk terug vinden, XBMC het alternatief voor Windows media center, Windows 7 sneltoetsen, De windows toets, Free Video Converter, Je gegevens zijn op internet gelekt, wat nu, PC gekaapt, Money mules, I-frame injection, Zoekmachine misbruik, Hardware printers, Opinie: Cybercrime, Social engeneering, WhatsApp berichten veiligstellen, E-boeken downloaden, Beter zoeken met Google, Studeren doe je met YouTube, Handige freeware, I-doser, Tablet kopen, Smartphone beveiliging, Find my Phone

12-10 > Is spyware illegaal, Wanneer valt website onder cookiewet, Wapen uit 3d printer, Facebook plug-in beschermt foto's tegen pottenkijkers, Hackpreventie, Libre Office, Hardware videokaart, Apps: wat moet je weten, Variaties op de Nigerian scam, Handige hulpprogramma's voor je PC, Tips om je smartphonebatterij te sparen, Meeste Torrent-downloaders gemonitord, Populaire vingerafdruklezer lekt Windows wachtwoord, Grote bestanden verzenden, De Russen komen, Digitaal onderzoek politie schiet tekort, Facebookfoto's beschermd met plug-in, Nederlanders doelwit valse Rechtspraak.nl e-mails

12-11 > Politievirus waarchuwt slachtoffers via Mp3, Trusteer voor veilig internetbankieren, Veilig internet: behaal het certificaat, Cameratoezicht: mag wel/ mag niet, Panopticon, Laat u niet volgen, Key generators, Opt-in botnet probleem voor banken en landen, Zo redt u foto'd, Facebook: geen toegang voor spammers, Backup van uw online data, repareer je internet explorer, Herken een besmette PC en doe er wat aan, Illegale torrents: wat zijn de gevolgen

12-12 > Ontsleutelen, Malafide webwinkels, Romance scam, Phiishing mail vraagt om foto van TAN-codes, HTTPS Everywhere, Metadata Cleaner

Onderwerpindex 2013

2013-01 > Voorspellingen 2013: maatschappelijke trends, Herken jij alle nep-virusscanners, Overheid onthult richtlijnen voor hackers, Anti-virus boot cd/dvd's, Browser plug-ins, Hoe weet je dat je smartphone is gehackt,
Hoe gezond is je harde schijf, Halkf miljoen wifi routers lek, Telefoneren via Facebook, Voicemails sturen met Facebook messenger, Data verbergen, USB sneller verwijderen, Beter zoeken met Google, Tips voor Windows 8,
Internetprovider, De gevaren van een enkele Net identiteit

2013-02 > Nederlandse politie worstelt met TOR, Nieuwe versie Police Ransomware, Cloudopslag vereist nieuwe wetgeving, Drugs bestellen via de post: sure we can, Cybercrises in aantocht, Ultieme dataredder bij stervende schijf, Virusdoder vermomt zicht om besmette pc's te ontsmetten, Microsoft bestrijdt processor-dief op Windows pc's, WiFi Protector beschermt je WiFi buiten de deur, Politie en NCSC laks na hack duizenden bedrijven, Opinie: opofferen privacy helpt niet tegen cybercrime

2013-03 > Toename phishingmails, Angifte phishing: stel de volgende vragen, Cybertaal,: bezemen - Vishing _ Sexting, SSID, Valse Flash player update verspreidt politievirus, Een veilige smartphone in toe stappen, Opinie: het neerhalen van botnets is zinloos

2013-04 > Wat is een Ddos aanval, Cybercriminelen zetten buitenwipper in, Antiwaskist mobiele telefoons, Inbreken op router wel strafbaar, Vaker kinderporno op Nederlandse servers, Meeste mailmalware verstopt in ZIP bestanden, Gestolen mobiel voor de zomer onklaar, Visie rapport Trends in Veiligheid 2013, Zoeken op internet in alle privacy, Sociale media vast onderdeel van politiewerk, Glasvezel internet, PhoXo gratis forobewerking,
Geen downloadverbod voor particulieren, 20% websites bevat kwaadaardige code, Nep muiscursor beschermt t wachtwoord tegen gluurders, Zo maakt u sterke wachtwoorden, In de schatkist, Opinie: wij sturen online criminelen de verkeerde boodschap

2013-05 > VPN, PGP, Malware in BING, Notice & Takedown, uKAsh politievirus verwijderen, Wachtwoord kwijt?, Identiteit uitfilteren, Facebookprofiel gekaapt, Beschadigde bestanden leesbaar maken, Steganografie, HOAX, Netneutraliteit

2013-06 > Wet Computercriminaliteit III, Darknet, NSA tapt servers, TOR adviseert privacycocktail, Virusinformatie, Alles over een bootsectorvirus, Klaar voor Ipv6, Marktplaatsoplichting vrijspraak, Zoek je eigen digitale sporen, Herstart gecrashte computer

2013-07/08 > Internetoplichting verschuift naar webshops, Een geautomatiseerd werk, Ransomware dwingt gebruiker tot enquete, Straffen cybercriminaliteit verhoogd in Europa, Hoe wachtwoorden gekraakt worden, Stop je wachtwoorden in een kluis, In 6 stappen buiten bereik van PRISM, Is jouw Ipadres onderdeel van een Botnet, Beveiliginsgtips voor vakantiegangers, Veilig onderweg surfen

2013-09 > Vernielen volgens de Wet Computercriminaliteit, Internettaps verfijfvoudigd, Cloud computing, Cloudopslagdiensten verbinden, Twitter, Aangifte doen van banking trojans, Typosquatting, Cyberpesten, Industriële bestuursystemen hacken, Een 0 voor Security Essentials, Anti-virus test 2013, JonDoNym, Maak bestanden onzichtbaar, De nieuwe Google Maps, Ddos aanval, SOPA

2013-10 > Binnendringen, Sterke stijging politievirussen, Cybercrimineel verkoopt besmette Nederlandse PC,s, Zet foto's smartphonedief niet op internet, Geen wetswijziging voor Stealth-sms, Hackersoftware laat Overheid inbreken, Java besmettingsgevaar neemt toe, Virus vermomt als Google Chrome, Tor bouwt anonieme chatclient, Welke browser crasht het vaakst e.a.

2013-11 >