Augustus-September 2014

JAARGANG 3

Secure Computing

Inderdaad. Nieuw layout. Beter leesbaar, meer hyperlinks, snellere navigatie mogelijkheden.

Ook meer Android en Apple gerelateerde onderwerpen.

Dit keer een dubbel nummer ivm mijn vakantie in september. Een paar items in de herhaling welke nog steeds actueel zijn.

Op verzoek is er een overzicht van cybercrime gerelateerde wetsartikelen opgenomen. Via een hyperlink is de wetstekst te lezen en waar mogelijk met jurisprudentie.

En……de schatkist is terug!

Een leuk nummer om weer te bewaren dus!

W.Bosgra Taakaccenthouder Digitale Criminaliteit Basisteam Enschede

Snel index

Klik op een link voor snelle toegang tot het artikel.

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

Bronnen:

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

Cybercrime wetsartikelen

Wetsartikelen voor computercriminaliteit in enge zin

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

Voor cybercrime in enge zin zijn de volgende wetsartikelen beschikbaar:

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

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

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

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

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

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

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

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

————————————————————

Haatzaaien.

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

Haatzaaien staat niet als zodanig in het wetboek.

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

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

————————————————————

Cyberstalking.

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

Relevante wetsartikelen zijn:

Artikel 285b WvSr: belaging.

Artikel 138a WvSr: computervredebreuk.

Artikel 266 WvSr: belediging.

————————————————————

Grooming.

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

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

————————————————————

Handel in mensen of foute goederen.

Verschijningsvormen:

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

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

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

Relevante artikelen zijn:

Artikel 273a WvSr mensenhandel.

Artikel 416 WvSr opzetheling.

Artikel 417 WvSr opzetheling (gewoonte).

Artikel 274 WvSr slavenhandel.

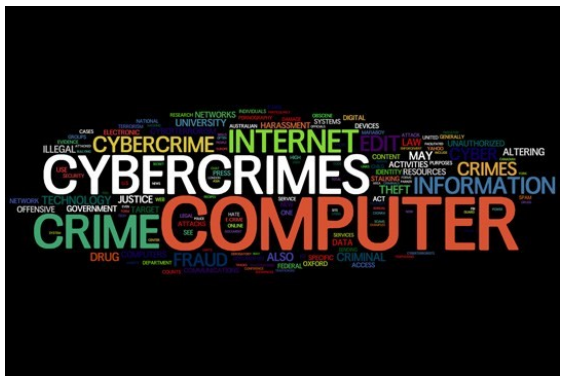
Artikel 2 Wwm: wet wapens en munitie

Artikel 31 Wwm: overdragen van wapens of munitie

Artikel 2 Ow: opiumwet

Artikel 3 Ow: opiumwet

Artikel 3b Ow: opiumwet



Index

Cybercrime wetsartikelen (2)

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

Relevante artikelen uit het wetboek van strafrecht zijn:

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

————————————————————————————————-

Kinderpornografie.

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

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

————————————————————————————————-

Illegale kansspelen.

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

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

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

op internet' .

Relevante wetsartikelen zijn:

Artikel 1 Wks: wet op de kansspelen

Artikel 1a Wks: piramidespelen

————————————————————————————————--

E-fraude.

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

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

Artikel 326 WvSr: oplichting.

Artikel 225 WvSr: valsheid in geschrifte.

Artikel 310 WvSr: diefstal.

Artikel 321 WvSr: verduistering.

Artikel 416 WvSr: heling.

————————————————————————————————

Index

Gijzelsoftware Cryptolocker is gekraakt

Twee beveiligingsfirma's hebben een website opgezet waar bestanden die met Cryptolocker geëncrypteerd zijn, weer ontgrendeld kunnen worden.

Het Amerikaanse beveiligingsbedrijf FireEye heeft samen met zijn Nederlandse branchegenoot Fox IT een website gemaakt waarop bestanden die besmet zijn met Cryptolocker bevrijd kunnen worden.

De ransomware Cryptolocker dook eind vorig jaar op in verschillende varianten. Bij computergebruikers die ermee besmet werden, encrypteerde de software belangrijke bestanden als documenten, foto's en videofilmpjes. De gebruikers hadden dan drie dagen tijd om een betaling te doen alvorens de bestanden voorgoed onbruikbaar werden. Na betaling, meestal rond de 300 dollar, kregen ze een private sleutel toegestuurd om alles weer te ontgrendelen.

Volgens FireEye en Fox It zijn ze achter een hele hoop van die private sleutels gekomen door reverse engineering van Cryptolocker. Geïnfecteerde gebruikers moeten simpelweg een besmet bestand uploaden naar decryptcryptolocker.com en krijgen, als alles goed gaat, daarna een private sleutel en een kleine softwaretool toegestuurd waarmee Cryptolocker gekraakt wordt.

Pas op met persoonlijke informatie
De twee bedrijven benadrukken dat er, buiten een mailadres, geen contactinformatie moet gegeven worden en dat de doorgestuurde bestanden niet gelezen of opgeslagen zullen worden.

Desondanks wordt gebruikers geadviseerd om niets door te sturen wat persoonlijke informatie bevat.

In december van vorig jaar schatte Dell Secureworks dat zeker 250.000 mensen door Cryptolocker geïnfecteerd zouden zijn. Volgens het Amerikaanse ministerie van Justitie is het virus nu onder controle en geneutraliseerd, maar heel wat mensen zouden nog steeds met onbruikbare bestanden op hun pc zitten omdat ze destijds weigerden te betalen.

Via deze link DECRYPT kunt u aan de slag!

Iedereen die de portal 'Decrypt Cryptolocker' bezoekt krijgt een private key voor het unlocken van hun gestolen bestanden. Alles wat zij hoeven te doen is het invullen van hun e-mailadres - die volgens de beveiligers niet bewaard wordt - en de door Cryptolocker versleutelde bestanden uploaden. Die krijgen zij vervolgens gratis en voor niets ontsleuteld terug.

FOX IT
FOR A MORE SECURE SOCIETY

FireEye

Index

Verwijder ongewenste informatie uit documenten

Stuurt u Excel-bestanden naar contactpersonen buiten de organisatie, check dan eerst of u niet per ongeluk persoonlijke informatie meestuurt.

Er zijn namelijk allerlei onzichtbare gegevens aan het bestand gekoppeld die meteen te herleiden zijn naar u. Wis voortaan de persoonlijke gegevens als u een Excel-bestand mailt.

Het is altijd oppassen geblazen bij het versturen van een Excel-bestandje naar iemand buiten de organisatie Voordat u een Word-, Excel- of PowerPoint-document als bijlage aan een e-mail hangt, zou u alle persoonlijke gegevens moeten verwijderen. Een Office-bestand staat namelijk bol van de (verborgen) gegevens die u misschien liever niet deelt. Wat dacht u van bijgehouden wijzigingen, inclusief data en tijdstippen? Of de naam van de persoon die het bestand als laatste heeft opgeslagen? Zo geeft u prijs hoe vaak het is herschreven en hoeveel mensen eraan hebben meegewerkt.

Sporen uitwissen met Documentcontrole
Met de functie Documentcontrole in de Office-programma's kunt u dit soort gegevens vinden en uw sporen uitwissen. Volg daarvoor deze stappen in Word, Excel en PowerPoint 2010 of 2013:

➡ Maak via 'Opslaan als' een kopie van het bestand. Dit omdat het niet altijd mogelijk is om gegevens te herstellen als u ze eenmaal heeft verwijderd.

➡ Ga naar tabblad 'Bestand', klik op 'Voorbereiden voor delen' en kies voor 'Document controleren'.

➡ Vink aan op welk type gegevens u wilt controleren en klik op 'Controleren'.

➡ Bekijk de resultaten en kies voor 'Alles verwijderen' als u ervan af wilt.

Microsoft® Office™

Index

Vanaf 2015 'killswitch' op smartphones

Minister Opstelten wil dat alle telefoons in Nederland een 'killswitch' krijgen. Daarmee kunnen providers een telefoon op afstand onbruikbaar maken. De nieuwe maatregel moet uiterlijk 1 februari 2015 ingesteld zijn.

Dat meldt minister Opstelten in antwoorden op Kamervragen van Van Haersma Buma. De minister wil dat telefoonproviders de unieke IMEI-nummers van telefoons kunnen blokkeren.

Aantal straatroven omlaag

Volgens Opstelten blijkt uit ervaring in andere landen dat het aantal straatroven met circa 20% daalt wanneer IMEI-blokkering wordt ingevoerd. Opstelten laat verder weten dat het proces om de verplichting door te voeren al in volle gang is. Zoals het er nu uit ziet, moet het eerste wetsvoorstel tijdens het zomerreces naar de Tweede Kamer. Voor de maatregel is een wijziging van de Telecommunicatiewet nodig.

Unieke identificatie

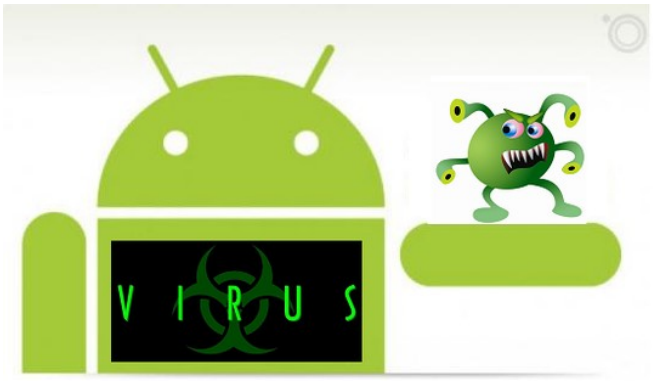
Een IMEI-nummer is een unieke identificatiecode voor de provider. Wanneer het IMEI-nummer wordt geblokkeerd, kan de telefoon niet meer op het telefoonnetwerk worden aangemeld. Het is dus nodig dat iedere provider meegaat in een blokkade, wat één van de voorwaarden was van de grote telecomaanbieders voordat zij wilden meepraten over het onderwerp.

Wanneer het IMEI-nummer is geblokkeerd, kan de gestolen telefoon nog altijd op andere manieren worden gebruikt, bijvoorbeeld via wifi. De blokkade is dus puur van toepassing op het GSM-gedeelte van de telefoon.

Index

Een op tien Android-apps bevat virus

Een op de tien apps voor het Android-besturingssysteem bevat een virus of linkt naar malware. Dat blijkt uit een onderzoek van Cheetah Mobile over de eerste helft van 2014.



Virussen en malware komen telkens vaker voor op Android: twintig keer zo veel als in 2012. Die groei is echter ook te linken aan de explosieve groei van het aantal apps op de Android-markt zelf. Er zijn nu simpelweg veel meer apps dan twee jaar geleden, dus het aantal geïnfecteerde apps is ook groter.

Apps die een virus of malware bevatten komen zo goed als altijd (99,86 procent) van andere App Stores dan Google Play, aldus Cheetah Mobile.

App Stores

Volgens de onderzoekers zijn de appwinkels van derde partijen erg laks in het controleren van beschikbaar gestelde apps, zoals de Amerikaanse Amazon Store en de Russische Yandex Store.

Dit in tegenstelling tot Google, dat juist heel streng controleert welke apps er wel en niet beschikbaar komen op Google Play. Slechts 0,14 procent van de ontdekte, geïnfecteerde Android-apps komt daar vandaan.

Betalen

Hackers hebben het daarbij telkens vaker voorzien op de portemonnee van de smartphone-gebruiker. Malafide apps sporen maar wat graag aan tot het betalen voor diensten die helemaal niet bestaan. Ook het aanzetten tot SMS'en naar dure telefoonnummers komt vaak voor.

De onderzoekers raden Android-gebruikers aan om app enkel te downloaden van betrouwbare bronnen, zoals Google Play. Ook het installeren van goede antivirussoftware kan helpen bij het detecteren van apps die naar malware linken.

Index

Ransomware gijzelt NAS-opslag

NAS-systemen van Synology zijn doelwit van nieuwe malware die de opgeslagen data versleutelt en dan losgeld eist. De zo gegijzelde gegevens moeten in Bitcoin worden betaald.

De zogeheten Synolocker-malware lijkt binnen te komen via de webinterface van de Synology NAS-apparaten (network attached storage). Het is nog niet duidelijk of het gaat om een gloednieuw gat in de webserver van het op Linux gebaseerde Synology-besturinggsyssteem (DSM). Mogelijk gaat het om een kwetsbaarheid waarvoor Synology al updates heeft uitgebracht, maar die gebruikers nog niet hadden geïnstalleerd.

Toegang vanaf internet

Op Twitter en op internetfora wordt melding gemaakt door getroffen Synology-klanten. Daarbij wordt langzaam in kaart gebracht wat de overeenkomsten zijn qua DSM-versie (vooralsnog 4.3) en de services op het gegijzelde NAS-apparaat die openstonden naar internet toe. Hierbij wordt ook de EZ-internetdient van Synology zelf aangewezen als verdachte. Die dienst maakt het makkelijker om de NAS-systemen van die fabrikant vanaf internet te benaderen.

Als de malware eenmaal is binnengekomen, versleutelt het de data die staat opgeslagen op de NAS. Toegang tot die gegevens is dan niet meer mogelijk; noch via gedeelde mappen op het netwerk, noch via de beheerinterface. Vervolgens wordt de beheerpagina van het opslagapparaat vervangen door de gijzelingsmelding waarbij het losgeld wordt geëist. Momenteel eisen de datagijzelaars 0,6 Bitcoin (ongeveer 260 euro), wat betaald dient te worden via anonimiseringsnetwerk Tor. Fabrikant Synology is ingelicht en onderzoekt de zaak.

Data redden

Volgens securitynieuwssite CSO worden de bestanden stuk voor stuk versleuteld, dus zou snel uitschakelen van het NAS-apparaat de schade kunnen beperken. Synology-gebruikers moeten dat dan doen zodra ze ontdekken dat de malware bezig is, wat al zou kunnen doordat de gekaapte beheerpagina meldt dat Synolocker bezig is de opgeslagen data te versleutelen. Het geheel uitschakelen van de NAS ‘bevriest’ die operatie dan, waarna de nog niet gegijzelde gegevens nog zijn te redden middels herinstallatie van het Synology-OS zónder de geïnfecteerde harde schijven om die daarna dan toe te voegen zodat de data gekopieerd kan worden.

Index

Nieuwe drugssites als paddenstoelen uit de grond

‘Vergeet de overlast veroorzakende dealer op de hoek’, de handel in drugs is verplaatst naar internet. Onderzoeksjournalist Mick van Wely schrijft in Dagblad van het Noorden over de ‘Drugs Online BV’ waar je ‘vanuit je luie stoel steengoede drugs en wapens’ koopt.

Van Wely schrijft naar aanleiding van de zaak tegen ‘sinterklaas’ uit Emmen, oftewel Theo van G. (63) die met enkele compagnons vanaf 2009 via internet in xtc handelde. De pillen werden verstuurd in dvd’s met hoesjes van kerkmuziek, die in Duitsland werden verstuurd; naar adressen over de gehele wereld. Theo en zijn bendeleden zijn november 2012 de eerste Nederlanders die worden opgepakt op verdenking van drugsverkoop via de ondergrondse website Silk Road. Dat was geheel nieuw, zegt woordvoerster Manon Hoiting van het OM. ‘We vonden een usb-stick bij de doorzoeking van de woning van één van de verdachten. Daar stonden bitcoins op’ en daar hadden toen nog maar weinigen bij het OM van gehoord. Het oprollen van Silk Road heeft weinig opgeleverd. Van G. is uiteindelijk veroordeeld tot dertig maanden, waar het OM acht jaar had geëist.

De online drugshanden heeft veel voordelen, schrijft Van Wely verder. De koper blijft anoniem, hoeft niet met louche types op straat te onderhandelen en kan in recensies lezen hoe goed het spul is. ‘Zou alle drugshandel online gaan, dan zou het fenomeen drugsoverlast in woonwijken voor een groot deel verleden tijd zijn’, veronderstelt Van Wely. Volgens woordvoerder Wim de Bruin van het landelijk parket heeft online drugshandel ‘zeker onze prioriteit’. Handel in drugs is strafbaar, online of niet. Maar online kost het meer tijd en capaciteit. Van Wely schrijft ook over ict-specialist ‘Maikel’ S. (21, uit Woerden) die onder het alias Super Trips rijk werd met online drugshandel via tor-netwerken. Als hij per ongeluk een keer niet op tor werkt, loopt hij tegen de lamp. De FBI blijkt hem al maanden te volgen. Hij wordt opgepakt op het vliegveld van Miami waar hij zijn netbestelde Lamborghini wil ophalen. Volgens berekeningen van de FBI verdiende S. in een anderhalf jaar tijd ongeveer vijf miljoen euro. Er wordt veertig jaar celstraf tegen S. geëist maar hij bekent en krijgt nu waarschijnlijk vijftien jaar. De FBI riep na de arrestatie van S. dat de online drugshandel gestopt was, maar niets is minder waar. Nieuwe websites schieten als paddenstoelen uit de grond, aldus het artikel: Silk Road 2 (15 duizend drugstransacties sinds de lancering), Evolution, Agora, Pandora, Blue Sky, Cloud Nine, Tor Bazaar, Cannabis Garden en Alcapa – allemaal sites die beter beveiligd zijn en hun eigen specialiteiten hebben. En uit het Global Drugs Survey bleek begin 2014 dat 22% van de drugsgebruikers al eens online drugs kocht. De helft daarvan deed dat voor het eerst na het oprollen van Silk Road, wat Van Wely doet concluderen dat de ‘Drugs Online BV’ springlevend is.

Index

Malware ook te verspreiden via USB-toetsenborden en muizen

Beveiligingsexpert Karsten Nohl waarschuwt voor potentieel malware-gevaar in USB-apparaten als toetsenborden, muizen, USB-sticks en smartphones. De chips die hier in zitten gebruiken software die hackers kunnen injecteren met virussen.

De onderzoeker van techbedrijf SR Labs geeft daarover volgende week een presentatie op de hackersconferentie Black Hat in Las Vegas, zo meldt persbureau Reuters.

Niet te ontdekken

Eens een USB-chip is geladen met een virus, is het lastig te ontdekken voor virusscanners omdat deze enkel de content scannen die er óp staat, niet wat er in de 'firmware' is geladen, zo legt Nohl uit.

Nolh testte dit zelf door hackingsoftware te injecteren in USB-chips van de Taiwanese fabrikant Phison Electronics.

Zodra het USB-apparaat in de computer wordt gestoken, heeft de malware vrij spel om bijvoorbeeld communicatie af te tappen, toetsaanslagen bij te houden en data te vernietigen.

Volledige toegang

Ook slaagde Nolh er in volledige toegang te krijgen tot de pc door via de USB een malafide programma te downloaden, waarbij de computer zelf veronderstelde dat de instructies gewoon van het toetsenbord zelf afkwamen.

Volgens Nohl zijn ook chips van andere fabrikanten in theorie te injecteren, ook al heeft de onderzoeker dat zelf niet getest. "The sky is the limit," verklaart hij.

"Je kan alles doen wat je wilt."

Als de computer eenmaal is geïnfecteerd, kan het virus zich tevens verspreiden naar alle andere USB-appaten. "En dan kom je er nooit meer vanaf," aldus Nohl.

Index

Zet een versleutelde VPN-verbinding op

Wanneer je surft weet je eigenlijk nooit helemaal zeker dat geen enkele hacker of regering je data afluistert. En al helemaal niet wanneer je surft via een openbare hotspot. Een versleutelde VPN-verbinding is dan een oplossing. Dat kan gratis met OpenVPN Client, in combinatie met bijvoorbeeld VPNBook.

Als je surft, loop je altijd wel het risico dat derde partijen (hackers, snoopers, regeringsinstanties…) op een of andere manier je datacommunicatie afluisteren. Zeker ook wanneer je daarvoor een draadloze hotspot aanspreekt.

De beste manier om snoopen te voorkomen is een stevig versleutelde verbinding opzetten. Dat kan met een VPN-verbinding (virtual private network) en een van de betere protocollen daarvoor is OpenVPN. Dat maakt meteen dat je een OpenVPN-client nodig hebt.

OpenVPN Client bestaat voor diverse platformen, waaronder iOS en Android. We focussen ons hier echter op de Windows-variant. Of liever: varianten, want er zijn versies voor Windows 32-bits en 64-bits. De installatie stelt weinig voor en je kunt gerust de standaard instellingen aanvaarden. Noteer alvast wel het installatiepad, want deze informatie heb je nog nodig. Standaard is dat c:\program files\openvpn.

Nu heb je dus wel al OpenVPN Client, maar zolang je die geen OpenVPN-profiel voedt waarmee die een correcte verbinding met een welbepaalde VPN-server kan opzetten, kun je er weinig mee. Je zou bijvoorbeeld een van de gratis certificaatbundels van VPNBook kunnen gebruiken. Die vind je op www.vpnbook.com, op het tabblad OpenVPN. Noteer hier meteen ook het account-ID.

Pak het gedownloade zipbestand uit en kopieer een van de ovpn-profielbestanden naar de submap \config van de installatiemap van OpenVPN Client. Nu kun je de OpenVPN Client-GUI opstarten, weliswaar als administrator. In het contextmenu van het bijhorende pictogram (in het systeemvak van de Windows-statusbalk) kun je de verbinding met de gekozen VPN-server nu initiëren. Je hebt er dus wel het genoteerde ID voor nodig. Als de verbinding is geslaagd, kleurt het pictogram groen en vertelt een site als www.whatismyip.com je inderdaad dat je nu via zo'n VPN-server (van VPNBook) aan het surfen bent.

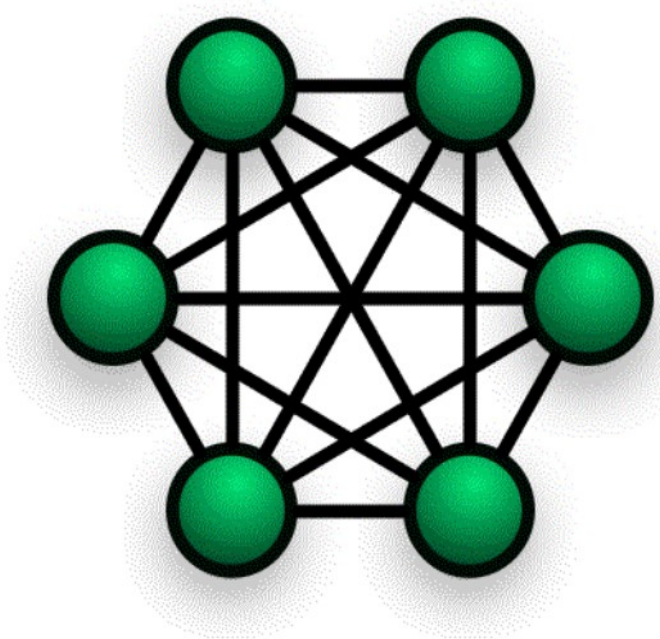
Kortom, OpenVPN Client in combinatie met de certificaatbundels van VPNBook is een gratis, gebruiksvriendelijke en betrouwbare oplossing om snel een VPN-connectie op te zetten, voor diverse platformen.

Open VPN download je via deze link OPEN VPN

Index

Communicatie via mesh-netwerk steeds populairder

Chat-apps zijn uitermate populair, maar als je even tijdelijk geen internet hebt, kun je niet met anderen op je smartphone chatten. mesh-netwerken kunnen hierbij een uitkomst bieden. Maar er zijn ook gevaren.



Een mesh netwerk is een draadloos netwerk waarbij het mogelijk is om direct - buiten het internet om - met andere mobiele apparaten kunt communiceren. Je smartphone of tablet maakt zo via andere apparaten - die op dat moment wel een internetverbinding hebben - contact, zodat je altijd ongestoord kunt blijven chatten, ook al is de mobiele verbinding onstabiel. Je kunt een mesh-netwerk het beste vergelijken met een wiel. De spaken in een wiel maken geen contact met elkaar, maar zijn via een centrale hub - de naaf - verbonden, waardoor ze toch met elkaar in verbinding staan, zij het niet direct.

Een mesh-netwerk kan ook gebruikt worden voor groepen mensen die onderling met elkaar willen chatten, zonder gebruik te maken van een centraal netwerk op internet. iOS 7 heeft mesh-technologie ingebakken in het besturingssysteem. Apple noemt dit zelf multi-peer connectivity. Ontwikkelaars van chat-software kunnen deze functionaliteit in het besturingssysteem gebruiken om software te ontwikkelen, die direct met andere apparaten communiceert, zonder dat de data via het internet naar een centrale server wordt gestuurd.

Firechat

Een van de chatapplicaties die gebruik maakt van een mesh-netwerk, is Firechat Deze app is beschikbaar voor zowel Android als Apple, en stelt gebruikers (groepen) in staat om direct met elkaar buiten het internet om met elkaar te chatten.

Gevaren

Het gebruik van een mesh-netwerk heeft voordelen, omdat je buiten een gecontroleerde omgeving met elkaar kunt chatten. Ook kan het handig zijn in geval van nood, als het internet niert bereikbaar is, bijvoorbeeld in oorlogs- of rampgebieden. Het kan echter ook nadelig werken: groepen gebruikers kunnen buiten het internet om - en zonder dat bijvoorbeeld politie of justitie kan ingrijpen - met elkaar afspreken, om bijvoorbeeld rellen te starten of onvredige demonstraties. In Taiwan gebruikten demonstranten onlangs nog een mesh-netwerk om anderen op te roepen te protesteren tegen de bouw van een kerncentrale.

Ook zou een mesh-netwerk gebruikt kunnen worden voor terrorisme, omdat berichten niet kunnen worden onderschept, en er dus geen actie kan worden ondernomen bij een eventuele dreiging. Berichten via een mesh-netwerk kunnen immers ook niet worden gefilterd op eventueel potentieel gevaarlijke inhoud.

Index

Verberg-apps verbergen bestanden niet

Apps die claimen bestanden te verstoppen op smartphones, maken er een potje van. Ze zijn makkelijk terug te vinden en apps die versleuteling bieden, leveren het ontsleutelmechanisme mee.

Een app als File Hide Pro 'verbergt' bestanden door een punt voor de bestandsnaam te zetten en File Locker door ze te verplaatsen naar de sd-kaart. Maar goed, dat is misschien wat gebruikers willen, zodat bijvoorbeeld gevoelige afbeeldingen niet direct te zien zijn door iemand die de smartphone bekijkt. Het wordt erger als apps versleuteling bieden.

Trend Micro bekeek onder meer de app AppLock die door meer dan een miljoen gebruikers is geïnstalleerd. Deze versleutelt bestanden weliswaar, maar gebruikt daar een vaststaand algoritme voor. Een aanvaller hoeft enkel het apk-bestand te decompileren om dit algoritme aan te spreken, waarna er geen verschil is tussen versleutelde bestanden en bestanden die in platte tekst worden opgeslagen.

Beveiligingsonderzoeker Simon Huang van Trend Micro stelt dat dit niet het grootste issue is, maar dat het erger is dat deze data kunnen worden aangesproken door andere apps. "Zelfs niet-malafide applicaties kunnen bij deze bestanden", waarschuwt Huang.

Uiteraard raadt de beveiligingsleverancier apps van beveiligingsleveranciers aan, maar het is waarschijnlijk beter om gevoelige gegevens simpelweg niet overal mee te dragen op mobiele apparaten.

Index

Politie gebruikt mogelijk omstreden spionagesoftware

Digitale activisten hebben een Duits-Brits bedrijf gehackt dat geheime spionagesoftware aan overheden en opsporingsautoriteiten verkoopt. De Nederlandse politie lijkt ook tot de klanten te behoren.

Bekijk de video

Recentelijk verscheen op internet een enorme berg aan technische en klanteninformatie van het bedrijf Gamma International. Dat is de maker van FinFisher, een softwareprogramma waarmee computers kunnen worden geïnfecteerd om op afstand bestanden te kopiëren, beeldschermkopieën te maken en toetsaanslagen te registreren. Spionagesoftware dus, die alleen wordt verkocht aan overheden.

'Het is raar dat de politie die producten nu al in gebruik heeft'

De hack is een grote overwinning voor burgerrechtenactivisten. FinFisher werd onder meer door de overheid van Bahrein gebruikt om de computers van dissidenten te bespioneren gedurende de Arabische Lente. Sindsdien liggen het programma en het bedrijf onder vuur. Er wordt onder meer gepleit voor exportregels voor dergelijke software.

Politie mogelijk ook klant

Ook de Nederlandse politie lijkt gebruik te maken van het programma. In de gehackte klantenbestanden werd een versleutelingscode gevonden die toebehoort aan een lid van de Nationale Eenheid, de landelijke politie in Driebergen. De match werd gevonden door de Nederlandse hacker Jurre van Bergen, die zich met andere digitale experts op de geopenbaarde informatie had gestort.

Vervolgens werd duidelijk dat deze klant, waarschijnlijk de Nederlandse politie dus, gebruik maakt van drie van Gamma's softwareprogramma's. De licentie zou lopen van 2012 tot 2015.

In Nederland is het op afstand hacken en overnemen van verdachte computers door de politie niet toegestaan. Er is een nieuwe wet in de maak (Wet Computercriminaliteit III), die daar verandering in moet brengen.

Wob-verzoek

'Het is raar dat de politie die producten nu al in gebruik heeft', zegt Rejo Zenger van digitale burgerrechtenorganisatie Bits of Freedom. 'Bovendien hebben ze dat altijd verzwegen.' Zenger diende in 2012 een Wob-verzoek in om te vragen naar het gebruik van spyware. Toen kreeg hij als antwoord dat er geen documenten over waren gevonden.

Een woordvoerder van het ministerie van Veiligheid en Justitie benadrukt dat het gebruik van spyware onder voorwaarden al is toegestaan. Dan gaat het om de installatie van deze software ter plekke, niet om het van afstand overnemen (en live volgen) van de activiteiten op de com-

Index

30 virusscanners voor Android getest

Mobiele virusscanners voor het Android-platform hebben weinig moeite met kwaadaardige apps, zo blijkt uit een test van het Duitse testorgaan AV-Test.org, dat 30 verschillende anti-virus apps vergeleek. In totaal werden de 30 virusscanners met 2627 kwaadaardige apps uit de afgelopen vier weken getest

Slechts vijf virusscanners scoren lager dan 98%, namelijk Whitegate (69,3%), Lookout (92,9%), Ikarus (94,1%), Bornaria (96,8%) en Tencent (96,9%). Elf scanners scoren zelfs de maximale 100%. Zeven apps veroorzaakten false positives, waarbij legitieme apps van zowel Google Play als andere stores voor malware werden aangezien.

Uitslag

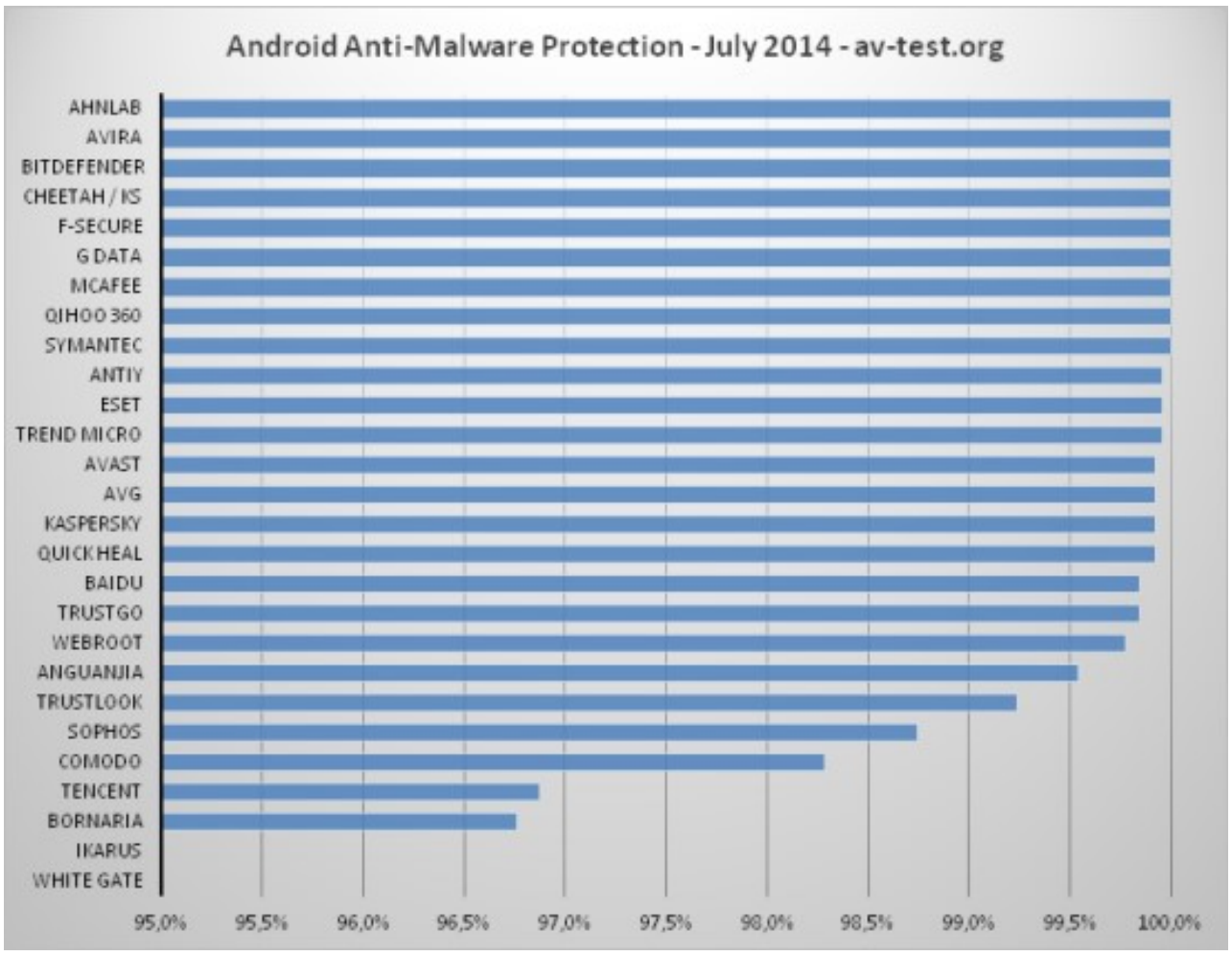
In totaal konden de virusscanners 13 punten verzamelen. Zes punten waren te behalen voor het detecteren van kwaadaardige apps. Hetzelfde aantal punten werd verdeeld voor de bruikbaarheid, zoals het batterijverbruik, systeembelasting, het genereren van veel dataverkeer en het onterecht alarm slaan bij schone applicaties van Google Play. Als laatste was er nog één punt voor aanvullende beveiligingsmaatregelen, zoals anti-diefstal, encryptie en back-up.

AhnLab, Avast!, Avira, BitDefender, ESET, G Data, Cheetah Mobile, McAfee, Qihoo en Quick Heal scoorden de maximale 13 punten.

Om gecertificeerd te worden moesten de scanners meer dan 8 punten scoren. Alleen Whitegate lukte dit niet, dat op 4 punten bleef steken.

Overzicht

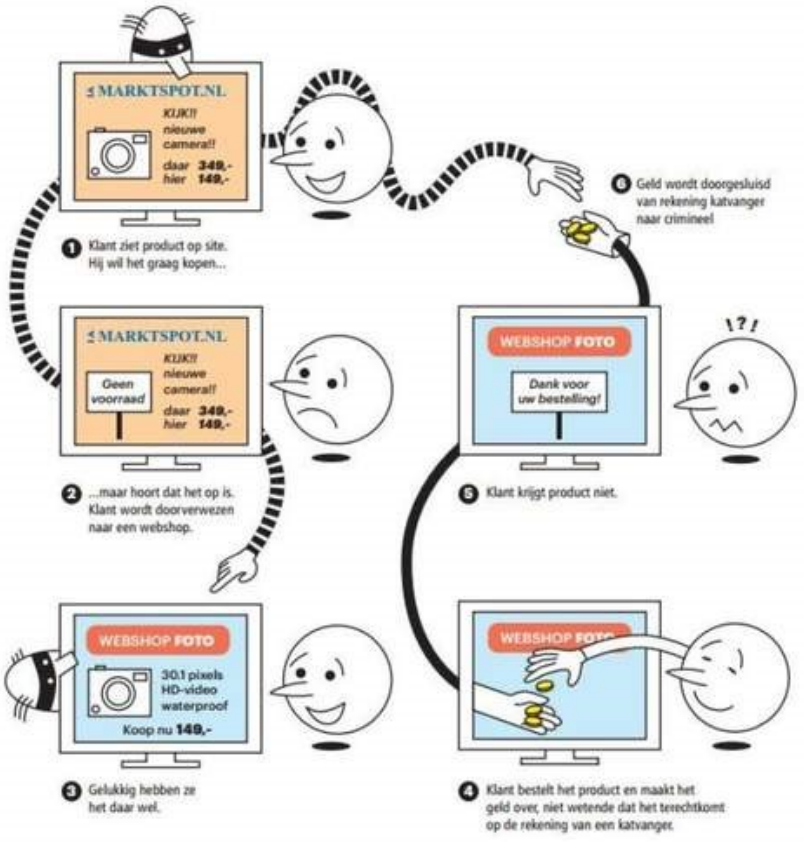
In het onderstaande overzicht staan 29 scanners vermeld, waarbij er specifiek is ingezoomd op de detectie vanaf 95%. Lookout werd op verzoek van Security.NL apart door AV-Test getest. Dit is een vrij grote speler op de mobiele markt, waarvan de virusscanner inmiddels standaard door AT&T op toestellen wordt geïnstalleerd.
Ook Samsung gebruikt de technologie van Lookout. Volgens Andreas Marx van AV-Test.org biedt Lookout interessante beveiligingsfeatures die vaak beter geïmplementeerd zijn dan de concurrentie. "De gemeten testresultaten bieden echter ruimte voor verbetering", aldus Marx.



Index

Nepshops leveren criminelen goud op

Het is criminelen niet ontgaan dat steeds meer mensen hun producten via internet bestellen. Met namaak webshops pikken zij een graantje mee van de toegenomen handel.



Oplichters kijken vooral naar particulieren die al jaren spullen op Marktplaats verkopen en daar een goede naam hebben opgebouwd. De oplichter stuurt die persoon een mailtje uit naam van Marktplaats met de vraag: 'We zien dat u uw wachtwoord heeft veranderd. Klopt dat, dan hoeft u niets te doen. Klopt dat niet, klik dan op deze link.' De Marktplaatsverkoper komt dan uit bij een namaak-Marktplaats waar hij zijn echte wachtwoord moet bevestigen. Zo krijgen oplichters toegang tot zijn account.

Via dit account plaatsen de criminelen zo'n duizend advertenties met een link naar de nepshop, het liefst eentje met een vertrouwde naam. In plaats van Bcc gebruiken zij bijvoorbeeld Bcc-winkel . "Wij proberen die advertenties snel van Marktplaats af te krijgen, maar toch trappen honderden mensen erin", zegt Ketelaars. "Criminelen hebben maar een paar dagen nodig om tot 50.000 euro binnen te roven." Daarom plaatsen ze het liefst op vrijdag hun advertenties. Dat geeft hen extra tijd voordat de site wordt geblokkeerd en de banken actie ondernemen.

Katvangers

De oplichters maken uiteraard geen gebruik van hun eigen betaalrekening. Daarvoor gebruiken ze katvangers. "Ze ronselen bankpasjes", zegt Ketelaars, "vaak van mensen in kwetsbare posities. Die bieden ze geld in ruil voor toegang tot hun bankrekening. Het liefst hebben ze een ING-nummer. Dan is een pasje niet nodig. De TAN-code (eenmalig wachtwoord in cijfers voor overboekingen, red), de pincode en een mobiel nummer: dan kun je geld overmaken zonder steeds contact te maken met je slachtoffer."

De banken zijn alerter geworden op internetfraude, toch blijven zij volgens Ketelaars te terughoudend met blokkeren. Banken ondernemen niets zonder aangiftes. Voordat de aangiftes binnen zijn, zijn er al snel een paar dagen voorbij. Criminelen hebben dan hun slag al geslagen.

Aangiftes waar je weinig aan hebt

Komen de aangiftes binnen, dan blijven banken terughoudend, zegt Ketelaars. "Soms verschenen voor een bankrekeningnummer honderd aangiftes en dan nog aarzelde de bank een blokkade te zetten. We hebben de banken aangesproken op hun eigen voorwaarden. Die stellen dat bij een vermoeden van oplichting een nummer geblokkeerd kan worden. Dat ligt juridisch erg moeilijk, kregen we te horen. Met het tv-programma 'Kassa' hebben ze daarop een uitzending gemaakt. Dat bracht enige verbetering. Toch blijft het moeizaam. Hun starre houding stuit ons wel eens tegen de borst."

Soms hebben katvangers niet eens door dat hun rekening wordt gebruikt door criminelen. Die lokken via advertenties thuiswerkers. Maar 'om snel geld te verdienen', moet er bijvoorbeeld speciale software op de computer van de thuiswerker geïnstalleerd worden. Het laat zich raden dat die software vooral oog heeft voor de bankgegevens.

Die advertenties voor thuiswerken waren te vinden op sites als Speurders en Marktplaats, maar ook op de vacaturesite van het UWV: Werk.nl. De dienst heeft er een team op gezet om de echtheid van vacatures te controleren. Sindsdien is het aantal meldingen van fraude sterk teruggelopen.

Jonkies

De oplichters die via vacatures, advertenties op Marktplaats en nepshops voor tienduizenden euro's incasseren, zijn voor Ketelaars geen onbekenden. "Jongens tussen de 18 en 25, vaak met een mbo-opleiding, afstudeerrichting ICT. Ze hebben allemaal een eigen functie in de organisatie. De één zorgt voor de bankpasjes, de ander maakt de webshop. De politie weet wie het zijn, maar het harde bewijs ontbreekt. Wij kunnen mensen uit de tent lokken met valse mailtjes, maar die gelden bij de rechter niet als bewijs."

Te mooi? Dan checken!

Hoe voorkomt u oplichting via nepshops?
De webshop moet bereikbaar zijn via een telefoonnummer. Alleen een mailadres is onvoldoende.

Controleer of er een KvK-nummer is en check dat op de site van de Kamer van Koophandel.

Controleer of het keurmerk klikbaar is en of u via de link uitkomt bij de pagina van een echt keurmerk. Een overzicht is te vinden op de website van ConsuWijzer.

Kijk via Google, Opgeletopinternet.nl of mijnpolitie.nl of de naam van de webshop bekend is.

Het belangrijkste: klinkt het te mooi om waar te zijn, dan is het ook vrijwel zeker niet waar.

Index

E-mailheaders zichtbaar maken

Log in op uw Gmail account

- Open het bewuste bericht
- Klik op de blauwe pijlpunt rechts naast de knop “Beantwoorden”
- Klik in het geopende menu op “Origineel weergeven”
- Selecteer alle getoonde tekst (Ctrl + a) en kopieer (Ctrl + c) dit
- Plak (Ctrl + v) gekopieerde gegevens in het programma Kladblok, Wordpad of Word
- Sla het bestand op of print dit bestand en neem dit mee wanneer u aangifte gaat doen

Gmail (eenvoudige HTML weergave)

- Log in op uw Gmail account
- Open het bewuste bericht
- Klik op “Origineel weergeven”
- Selecteer in het geopende menu alle getoonde tekst (Ctrl + a) en kopieer (Ctrl + c) dit
- Plak (Ctrl + v) gekopieerde gegevens in het programma Kladblok, Wordpad of Word
- Sla het bestand op of print dit bestand en neem dit mee wanneer u aangifte gaat doen

Hotmail / Windows Live

- Log in op uw Windows Live Hotmail account
- Klik met de rechtermuisknop op het bewuste bericht en kies “Berichtbron weergeven"
- Selecteer alle getoonde tekst (Ctrl + a) en kopieer (Ctrl + c) dit
- Plak (Ctrl + v) gekopieerde gegevens in het programma Kladblok, Wordpad of Word
- Sla het bestand op of print dit bestand en neem dit mee wanneer u aangifte gaat doen

Windows Live Mail (als programma geinstalleerd)
Start het programma Windows Live Mail

Selecteer het bewuste bericht.

Klik met de rechtermuisknop op het bewuste bericht en kies “Eigenschappen"

Klik bovenin het geopende scherm op de tab “Details”

Klik onderin in de tab “Details” op de knop “Bron van het bericht…”

Ga met de cursor (pijltje) in het nieuw geopende venster staan en selecteer alle getoonde tekst (Ctrl + a) binnen dit venster en kopieer (Ctrl + c) dit

Plak (Ctrl + v) gekopieerde gegevens in het programma Kladblok, Wordpad of Word

Sla het bestand op of print dit bestand en neem dit mee wanneer u aangifte gaat doen

Mail (Apple)

- Start het programma Mail
- Selecteer het bewuste bericht.
- Selecteer binnen de tap “Weergave” de subtap “Bericht”
- Selecteer binnen subtap “Bericht” “Lange kopteksten”
- Of druk na het selecteren van het bericht op de toetsen cmd + u
- Selecteer (cmd + a) alle getoonde tekst in het tekstvenster en kopieer (cmd + c) dit.
- Plak (cmd + v) gekopieerde gegevens in het programma Teksteditor, Pages of Word.
- Sla het bestand op of print dit bestand en neem dit mee wanneer u aangifte gaat doen.

Entourage 2008 (Apple)
Start het programma Entourage

Selecteer het bewuste bericht

Selecteer binnen de tap “Bericht” onderaan de lijst “Internetheaders”

Of druk na het selecteren van het bericht op de toetsen cmd + SHIFT + h

Selecteer (Command + a) alle getoonde tekst en kopieer (cmd + c) dit

Plak (Command + v) gekopieerde gegevens in het programma Teksteditor, Pages of Word

Sla het bestand op of print dit bestand en neem dit mee wanneer u aangifte gaat doen

Index

E-mailheaders zichtbaar maken (2)

Yahoo (Nieuwe lay-out)
Log in op uw Yahoo account

Selecteer het bewuste bericht

Klik met de rechtermuisknop op het bewuste bericht en kies “View Full Headers"

Ga met de cursor (pijltje) in het nieuw geopende venster staan en selecteer alle getoonde tekst (Ctrl + a) binnen dit venster en kopieer (Ctrl + c) dit

Plak (Ctrl + v) gekopieerde gegevens in het programma Kladblok, Wordpad of Word

Sla het bestand op of print dit bestand en neem dit mee wanneer u aangifte gaat doen

Yahoo (Classic lay-out)
Log in op uw Yahoo account

Open het bewuste bericht

Klik rechtsonder op de pagina, achter de meerkeuzelijst “Select `message Encoding” op “Full Headers"

De regel met het onderwerp en afzender wordt nu vergroot en de headers van het bewuste bericht wordt zichtbaar in een lichtgekleurd kolom

Selecteer alle tekst in deze kolom vanaf de eerste tot en met de laatste regel. Doe dit met je muis en houd daarbij de linkermuisknop ingedrukt zodat de tekst blauw gearceerd wordt.

Wanneer de tekst blauw gear-

Thunderbird (Apple)
Start het programma Thunderbird

Selecteer het bewuste bericht.

Selecteer binnen de tab “Beeld” de regel “Berichtbron”

Of druk na het selecteren van het bericht op de toetsen cmd + u

Ga met de cursor (pijltje) in het nieuw geopende venster staan en selecteer alle getoonde tekst (cmd + a) in het tekstvenster en kopieer (cmd + c) dit.

Plak (cmd + v) gekopieerde gegevens in het programma Teksteditor, Pages of Word.

Sla het bestand op of print dit bestand en neem dit mee wanneer u aangifte gaat doen.

Thunderbird (Windows)
Start het programma Thunderbird

Selecteer het bewuste bericht.

Selecteer binnen de tab “Beeld” de regel “Berichtbron”

Of druk na het selecteren van het bericht op de toetsen Ctrl + u

Ga met de cursor (pijltje) in het nieuw geopende venster staan en selecteer alle getoonde tekst (Ctrl + a) binnen dit venster en kopieer (Ctrl + c) dit

Plak (Ctrl + v) gekopieerde gegevens in het programma Kladblok, Wordpad of Word

Sla het bestand op of print dit bestand en neem dit mee wanneer u aangifte gaat doen

Outlook
Start het programma Outlook

Selecteer het bewuste bericht.

Klik met de rechtermuisknop op het bewuste bericht en kies “Opties"

Ga met de cursor (pijltje) in de kolom staan achter “Internetheaders” en selecteer alle getoonde tekst (Ctrl + a) binnen deze kolom en kopieer (Ctrl + c) dit

Plak (Ctrl + v) gekopieerde gegevens in het programma Kladblok, Wordpad of Word

Sla het bestand op of print dit bestand en neem dit mee wanneer u aangifte gaat doen

Outlook Express
Start het programma Outlook Express

Selecteer het bewuste bericht.

Klik met de rechtermuisknop op het bewuste bericht en kies “Eigenschappen"

Klik bovenin het geopende scherm op de tab “Details”

Klik onderin in de tab “Details” op de knop “Bron van het bericht…”

Ga met de cursor (pijltje) in het nieuw geopende venster staan en selecteer alle getoonde tekst (Ctrl + a) binnen dit venster en kopieer (Ctrl + c) dit

Plak (Ctrl + v) gekopieerde gegevens in het programma Kladblok, Wordpad of Word

Sla het bestand op of print dit bestand en neem dit mee wanneer u aangifte gaat doen

Overige e-mailprogramma's
Mocht uw e-mailprogramma hierboven niet vermeld staan dan kunt u mogelijk op deze site de uitleg om e-meilheaders van uw e-mailprogramma veilig te stellen uw vinden. Deze site is engelstalig.

Index

Belangrijk in de header is het X-originating IP

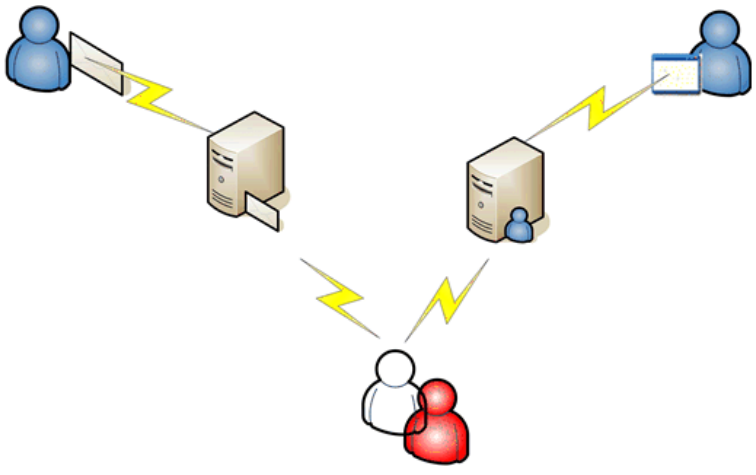
Hiermee is de provider en gebruiker te achterhalen.

(zie afbeelding)

Return-Path: <bogdan@fx.ro>
Received: from srv01.advenzia.com (root@localhost)
by emailaddressmanager.com (8.11.6/8.11.6) with ESMTP id i2OApwQ14083
for <support@emailaddressmanager.com>; Wed, 24 Mar 2004 10:51:58 GMT
X-ClientAddr: 193.231.208.29
Received: **from** corporate.fx.ro (corporate.fx.ro [193.231.208.29])
by srv01.advenzia.com (8.11.6/8.11.6) with ESMTP id i2OApvs14078
for <support@emailaddressmanager.com>; Wed, 24 Mar 2004 10:51:57 GMT
Received: from mail.fx.ro (mail3.fx.ro [193.231.208.3])
by corporate.fx.ro (8.12.11/8.12.7) with ESMTP id i2OAtxBr025924
for <support@emailaddressmanager.com>; Wed, 24 Mar 2004 12:55:59 +0200
Received: from localhost.localdomain (corporate2.fx.ro [193.231.208.28])
by mail.fx.ro (8.12.11/8.12.3) with ESMTP id i2OAtoQe006624
for <support@emailaddressmanager.com>; Wed, 24 Mar 2004 12:55:50 +0200
Date: Wed, 24 Mar 2004 12:55:50 +0200
Message-Id: <200403241055.i2OAtoQe006624@mail.fx.ro>
Content-Disposition: inline
Content-Transfer-Encoding: binary
MIME-Version: 1.0
To: support@emailaddressmanager.com
Subject: How to read email headers
From: bogdan@fx.ro
Reply-To: bogdan@fx.ro
Content-Type: text/plain; charset=us-asci
X-Originating-Ip: [80.97.5.101]
X-Mailer: FX Webmail webmail.fx.ro
X-RAVMilter-Version: 8.4.3(snapshot 20030212) (mail)
Status:

Index

E-mail spoofing



"Mijn e-mail account is gehackt. Mensen ontvangen e-mail van mij, welke ik niet heb opgesteld en heb verstuurd".

Vervolgens wordt een aangifte opgenomen ter zake Computervredebreuk. U herkent dit vast wel. Echter hoeft er geen sprake te zijn van Computervredebreuk. Een nieuw fenomeen wat de kop opsteekt is E-mail spoofing. E-mail spoofing is een term die gebruikt wordt om frauduleuze e-mailactiviteiten te beschrijven. Deze activiteiten houden in dat specifieke eigenschappen van het e-mail bericht, zoals From (Van), Return- Path (Afzender) en Reply-To (Antwoorden naar) worden gewijzigd, waardoor het lijkt dat de e-mail bij een andere bron vandaan komt. E-mail spoofing is een veelgebruikte techniek voor het versturen van spam.

Ook zijn er computervirussen welke e-mail spoofing gebruiken om zichzelf te verspreiden. Het virus gebruikt een ander adres dat het op de geïnfecteerde computer heeft aangetroffen als afzender. In sommige gevallen maakt het virus ook zelf een e-mailadres aan. Mensen van wie de computer geïnfecteerd is, kunnen moeilijk worden gewaarschuwd, omdat hun e-mailadres voor de meeste ontvangers onbekend is.

Wie maakt er gebruik van e-mailspoofing en waarom? E-mailspoofing wordt voornamelijk-gebruikt om twee redenen: Om een onbestaand afzendadres mee te geven. In veel gevallen van spam wordt gebruik gemaakt van een onbestaand afzendadres. De afzender van de

spam heeft dus niet alleen een ander adres meegegeven als afzendadres, maar zelfs een adres dat helemaal niet bestaat. De reden hiervoor is dat spammers vaak absoluut niet geïnteresseerd zijn in antwoorden per e-mail, maar zoveel mogelijk mensen willen leiden naar hun website waarop zij hun producten aanbieden.

Om een bestaand adres van een ander mee te geven. Het meegeven van een bestaand adres van een ander heeft natuurlijk als voornaamste doel de ontvanger te laten denken dat de e-mail ECHT van die ander vandaan komt. Dit kan autoriteit uitstralen of vertrouwen inboezemen. Er zijn twee vaak voorkomende gevallen waarbij een bestaand adres van een ander wordt gebruikt: Virussen die zichzelf via e-mail versturen geven er de voorkeur aan om bestaande e-mailadressen als afzendadres te gebruiken. Sommige virussen gebruiken telkens hetzelfde adres (bijvoorbeeld eenvirus dat zichzelf als Microsoft verzendt), sommige virussen maken met behulp van informatie van de geïnfecteerde computer een afzendadres (bijvoorbeeld) en weer andere virussen zoeken op de geïnfecteerde computer naar adressen en gebruiken die. Het doel is hier om vertrouwen in te boezemen. Als u erin trapt en denkt dat de e-mail echt bij Microsoft vandaan komt, dan is de kans groter dat u de e-mail en eventuele bijlage opent. De kans dat het virus zichzelf verder kan verspreiden wordt op die manier dus groter. Phishers gebruiken e-mailadressen van de organisaties die ze imiteren, met als doel autoriteit en vertrouwen uit te stralen. Als een phisher uw creditcardgegevens wil achterhalen dan is het van belang dat u gelooft dat de e-mail ook echt van uw creditcardverstrekker vandaan komt.

Kortom: e-mailspoofing wordt op grote schaal gebruikt door virussen, spammers en phishers, met als doel om vertrouwen en autoriteit uit te stralen.

Hoe herken je e-mailspoofing en wat kun je ertegen doen?

Als individuele gebruiker kunt u weinig doen tegen e-mailspoofing. Als u een e-mail heeft ontvangen dan heeft hetfeitelijke spoofen al plaatsgevonden. In deze gevallen is het belangrijk dat u gespoofde e-mail kunt herkennen. E-mailspoofing is in sommige gevallen te ontdekken door naar de zogenaamde headers te kijken van de e-mail (zie ander artikel).

Hoe herken je een daadwerkelijk gehackt e-mailaccount.

1. vraag of er e-mail berichten zijn verwijderd

2. staan er te verzenden e-mail berichten klaar die geweigerd zijn door ontvangers?

3. men kan niet meer met het eigen wachtwoord inloggen

4. persoonlijke instellingen zijn veranderd

Indien hier sprake van is heeft men daadwerkelijk het e-mail account gehackt.

Index

Prullenbak voor Android

Verwijder je per ongeluk een bestand van je smartphone of tablet, dan ben je het onherroepelijk kwijt. Tenzij je Dumpster hebt geïnstalleerd.

De prullenbak op je pc vormt een veiligheidsnet voor bestanden die je per ongeluk verwijdert. Met een klik op de knop kan je een bestand opnieuw herstellen naar de oorspronkelijke locatie op je computer. Dumpster brengt die functionaliteit naar je Androidsmartphone of -tablet. Je kan de applicatie downloaden uit de Play Store via deze link. De app is gratis, maar wordt ondersteund door advertenties. Met een in-app-aankoop van 2,99 euro ben je verlost van de reclame indien je dat wenst. In de instellingen geef je aan welke types bestanden moeten worden bijgehouden in Dumpster en voor hoe lang. Met een schuiver kan je een tijdsbestek van een week tot enkele maanden instellen of ervoor kiezen om de prullenbak alleen handmatig te legen.

Wanneer je nu per ongeluk een bestand op je smartphone of tablet verwijderd, kan je Dumpster openen om het bestand te herstellen. De prullenbak bewaart je verwijderde bestanden in volledige grootte. Ben je bewust bestanden aan het verwijderen om plaats te maken op je toestel, dan zal je ze dus ook uit Dumpster moeten verwijderen om ze volledig van je apparaat te wissen.

Index

Google verhelpt Fake ID-lek in Android

Bluebox Security bracht recent een gevaarlijk lek in Android aan het licht dat malafide apps in staat stelt om zich als andere apps voor te doen.

Bluebox Security, een bedrijf gespecialiseerd in mobile security, heeft een gevaarlijk lek in Android aan het licht gebracht dat aanwezig is op alle versies sinds Android 2.1. Google werd op de hoogte gebracht en heeft intussen een patch beschikbaar gemaakt.

Het lek, dat Fake ID werd gedoopt, kan door een malware-app worden misbruikt om zich als een reeds vertrouwde applicatie voor te doen. De malware kan zich via het lek meer rechten toeëigenen, zonder medeweten van de gebruiker. Op die manier kan onder meer toegang tot betaalgegevens van de gebruiker of de instellingen van het toestel worden verkregen.

“Je kan zelf nagaan of jouw toestel gepatcht is door de-Bluebox Security Scanner te installeren”

Volgens BlueBox komt het lek voort uit een probleem met de Android package installer. Dat is het deel van het besturingssysteem dat instaat voor de installatie van apps. Applicaties beschikken over een beveiligignscertificaat, waarvan de authenticiteit door de package installer moet worden gecontroleerd. Dat gebeurt echter niet correct, waardoor malafide certificaten kunnen laten uitschijnen dat ze door een vertrouwde partij - zoals bijvoorbeeld Google of Adobe - worden uitgegeven, terwijl dat helemaal niet het geval is.

Google werd in april op de hoogte gebracht van het lek en heeft tegenover de BBC bevestigd dat het ondertussen een patch heeft uitgerold naar zijn partners en via het Android Open Source Project. Het is niet helemaal duidelijk welke toestellen de patch reeds hebben ontvangen, maar een snelle steekproef op de redactie leert ons dat apparaten die draaien op Android 4.4.2 of hoger alvast gepatcht zijn. Je kan zelf nagaan of jouw toestel gepatcht is door deBluebox Security Scanner te installeren.

Maar zelfs als jouw toestel nog niet gepatcht is, betekent dat gelukkig niet dat je onbeschermd bent. Google heeft een tijd geleden Google Play Services geïntroduceerd om snel nieuwe functies naar alle Androidapparaten te kunnen uitrollen, ongeacht op welke Androidversie ze draaien. Zo werd onder meer de functionaliteit “Apps verifiëren” toegevoegd om apps te scannen op malware voordat ze geïnstalleerd worden. Google heeft die functionaliteit geüpdatet om gebruikers tegen het Fake ID-lek te beschermen. Op die manier werd het probleem snel in de kiem gesmoord, ook al is het lek nog niet op elk toestel gepatcht. Volgens Google werd het lek niet in het wild misbruikt.

Index

Ransomware voor Android maakt sprong naar pc

De ransomware die eerder dit jaar op Androidtoestellen opdook, heeft nu ook zijn weg gevonden naar de pc.

De ransomware Koler.A, die eerder dit jaar op Androidtoestellen opdook, heeft nu ook zijn weg gevonden naar de pc. Dat meldt beveiligingsexpert Kaspersky.

Het onderzoekslab van de Russische beveiliger heeft browser-gebaseerde ransomware en een exploit kit ontdekt waarmee de malwarecampagne nu ook zijn weg naar de pc heeft gevonden. De gijzelende software - ook wel gekend als het 'politievirus - wordt net als op Android geïnstalleerd na het bezoeken van één van minstens 48 besmette pornowebsites.

> "Sinds de campagne is begonnen op Android in april van dit jaar, werden er al bijna 200.000 gebruikers gebruikers door besmet

Het gebruik van pornowebsites voor dit soort doeleinden is geen toeval, weten ze bij Kaspersky. "Slachtoffers voelen zich schuldig over het bezoeken van dergelijke websites en zijn sneller geneigd om het door de 'autoriteiten' vastgestelde bedrag te betalen," klinkt het in eenpersbericht.

Sinds 23 juli is de mobiele component van de campagne onderbroken, nadat de command-and-control-server 'Uninstall'-commando's begon uit te sturen waarmee de kwaadaardige applicatie effectief van besmette Androidtoestellen werd verwijderd, maar de nieuwe pc-component blijft wel actief.

De aanval gebeurt als volgt. Bezoekers van een besmette pornosite worden doorgestuurd naar één van twee websites, afhankelijk of ze al dan niet gebruik maken van Microsofts webbrowser Internet Explorer. Wordt gebruik van IE gedetecteerd, dan wordt het slachtoffer doorverwezen naar een webpagina met de Angler Exploit Kit. Die bevat exploits voor Silverlight, Flash en Java. Werkt het slachtoffer via een andere browser, dan wordt zijn systeem niet besmet, maar krijgt hij wel een scherm te zien met de boodschap dat zijn pc geblokkeerd is en hij losgeld moet betalen. Dat scherm is echter eenvoudig af te sluiten met de combinatie Alt+F4.

Sinds de campagne is begonnen op Android in april van dit jaar, werden er al bijna 200.000 gebruikers gebruikers door besmet. Het grootste deel van die besmettingen - zo'n 80 procent - gebeurde in de Verenigde Staten, maar volgens Kaspersky zijn ook Belgen en Nederlanders slachtoffer gevallen. Kaspersky heeft zijn bevindingen doorgegeven aan Europol en Interpol, en werkt samen met deze instanties om de campagne neer te halen.

Index

Acht tips om meer uit Apple Airplay te halen

Met AirPlay kan je je media tussen verschillende (Apple-)toestellen streamen. Film kijken, presentaties geven of gamen: met deze tips gaat het vanzelf.

AirPlay bestaat in zijn huidige vorm al sinds 2010, maar het is een stukje technologie dat door veel Mac-gebruikers over het hoofd wordt gezien. Met AirPlay kan je je media tussen verschillende (Apple-) toestellen streamen. Film kijken, presentaties geven of gamen: met deze tips gaat het vanzelf.

1. AirPlay op iOS en OSX

AirPlay laat je toe om foto's, films, muziek en games door heel je huis te verdelen. Je Mac of iOS-toestel is daarbij de zender; een Apple TV, Airport Express of ondersteunde luidspreker fungeert als ontvanger. Om met AirPlay content te streamen, moeten alle toestellen – zender en ontvanger – op hetzelfde wifi -netwerk aangesloten zijn.

Op Mac vind je AirPlay in eerste instantie in iTunes: als je Apple TV of AirPlay-speaker aangesloten is op wifi, zal je daar rechts naast de volumeregelaar het AirPlay-icoontje zien verschijnen. Klik erop en je krijgt een lijst met ondersteunde toestellen waarnaar je kan streamen. Deze optie werkt overigens ook in iTunes voor Windows. Wil je je scherm of systeemgeluid streamen, dan zal je het icoontje zien verschijnen in de menubalk van OS X.

In iOS 7 vind je de optie dan weer in het Control Center; veeg naar boven op je scherm, en je ziet AirPlay staan naast AirDrop. Als je hierop klikt, krijg je opnieuw een lijstje met mogelijke ontvangers.

2. Streaming en mirroring

Kort gezegd kan je twee dingen doen met AirPlay: streamen en spiegelen. Streaming spreekt grotendeels voor zich: je speelt filmpjes, muziek, of foto's – uit iTunes of de iOS-equivalenten – af op een ander scherm of luidspreker.

Mirroring (of AirPlay Display op je Mac) geeft dan weer exact weer wat er op het scherm van je Mac, iPhone, of iPad gebeurt op het grote scherm van je tv met Apple TV. Zo kan je je flatscreen als externe monitor gebruiken zonder geknoei met kabeltjes; handig voor presentaties of als 21ste-eeuwse vervanging voor de vakantiefotodiashow.

3. Een beetje valsspelen

Hierboven legde ik de basisfunctionaliteiten van AirPlay uit, maar daarmee ook de beperkingen: je kan het scherm van je Windows-pc niet mirroren naar je Apple TV, en je kan een computer nooit gebruiken als ontvanger voor, bijvoorbeeld, de AirPlay-stream van je iOS-toestellen.

Er bestaan echter – uiteraard – applicaties die daar wat aan verhelpen. Zo kan je met AirParrot wél het scherm spiegelen van op een Windows-computer . Daarnaast voegt de app (ook op Mac) een aantal extra features toe, zoals de mogelijkheid om je Apple TV als tweede scherm te gebruiken, of om maar één bepaalde applicatie te spiegelen. AirServer tovert op zijn beurt je Mac of Windows-pc om tot ontvanger voor AirPlay-streams of mirroring, zodat je nog meer opties krijgt om draadloos je ding te doen.

4. Streamende speakers

Eén van de handigste toepassingen voor AirPlay is ongetwijfeld het streamen van muziek: met je muziekcollectie op je Mac kan je - in tegenstelling tot bluetooth - zonder kwaliteitsverlies je hele huis van muziek voorzien, zolang je wifi-netwerk maar sterk genoeg is. De makkelijkste, maar helaas niet de goedkoopste, manier om dat te doen is het aanschaffen van AirPlay-ondersteunde muziekspeakers. Die verschijnen zonder gedoe rechtsreeks in het lijstje apparaten op je Mac of iOS-toestel. Wel even opletten: van een Mac kan je meerdere speakers met één stream aanspreken, op iOS is dat beperkt tot één toestel.

5. Airport Express als muziekmachine

Een andere manier om je muziek naar je speakers te brengen, is het aanschaffen van een AirPort Express, Apples goedkoopste wifi-access point. Dat toestel is namelijk voorzien op AirPlay. Al wat je dan nog rest te doen, is je doodnormale speakers in de audio-poort van de AirPort pluggen, en ook zij verschijnen als AirPlay-apparaat op je netwerk. Een AirPort Express koop je voor 99 euro.

6. Dubbel spelplezier

Aangezien je met AirPlay alles op het scherm van je iOS-toestel kan tonen op je tv, kan je op die manier ook gamen. Dat kan leuk zijn – het opent mogelijkheden om met vrienden samen te spelen, bijvoorbeeld – maar niet wereldschokkend. Apple geeft ontwikkelaars echter ook de mogelijkheid om hun spellen in dual screen te ontwikkelen. Daarmee kan je andere content weergeven op het iOS-toestel dan op de tv, gewoon via Airplay. Denk aan een kaart of andere controls op het kleine scherm. Een paar spellen met deze optie: Real Racing 2, N.O.V.A. 3, Sky Gamblers: Rise of Glory, Asphalt 7: Heat, en Modern Combat 4: Zero Hour.

7. De muzikale kwaliteiten van je Apple TV

Als je AirPlay-ondersteunde speakers en een Apple TV hebt, dan hoef je zelfs niet per se een computer te gebruiken om je muziek af te spelen – tenminste als je muziek zich in de iTunes-cloud bevindt. Al die content is namelijk rechtstreeks beschikbaar op je Apple TV, en sinds softwareversie 5.1 kan die via AirPlay muziek streamen. Je kan de AirPlay-opties vinden in de instellingen, maar er is een snellere manier: hou de centrale Select-knop ingedrukt op je afstandsbediening, en je krijgt een pop-upmenu met een optie Speakers. Je kan ook het volume van die externe speakers bedienen met de afstandbediening van je Apple TV.

8. Weg met de afstandsbediening

Als je Apples eigen Remote-app (gratis in de App Store) downloadt op je iPad of iPhone, kan je je video of muziek bedienen vanuit je iDevice – ook als je die content niet aan het afspelen bent van dat toestel. Zeker handig als je je telefoon toch altijd naast je hebt liggen in de zetel.

Index

Apple blokkeert verouderde versies van Flash

De Mac-fabrikant dwingt gebruikers de laatste versie van Flash te installeren om te voorkomen dat ze slachtoffer worden van een kritiek lek in de software.

Mac-gebruikers die over internet surfen met Safari hebben vanaf nu geen toegang meer tot Flash-websites totdat ze hun Flash Player upgraden.

In een bericht van Apple staat te lezen dat mensen met verouderde versies van Flash kans hebben een foutbericht te krijgen wanneer ze een website bezoeken met Flash-content. De melding is iets in de trant van Blocked plug-in, Flash Security Alert of Flash out-of-date. Hierdoor krijgen ze niets te zien.

“Veel mensen gaan nonchalant om met het updaten van hun software”

Apple heeft altijd al een vervelende relatie gehad met Adobe Flash. Dat ging op een gegeven moment zelfs zover dat Flash verbannen werd van iPhones en iPads. In dit geval is de voorzorgsmaatregel van Apple er juist op gericht de klant te beschermen.

Kritieke update

Vorige week dinsdag heeft Adobe een kritieke update voor Flash vrijgegeven om een lek te dichten dat hackers in staat stelt cookies ter authenticatie te stelen van gebruikers voor populaire websites. Veel mensen gaan nonchalant om met het updaten van hun software. Daarom is het soms nodig een veiligheidsupdate door de strot te drukken om ergere problemen te voorkomen.

Safari-gebruikers die een bericht krijgen dat Flash niet langer up-to-date is kunnen op de downloadknop klikken om de laatste versie binnen te halen. Belangstellenden kunnen meer details vinden over de veiligheidsupdate opAdobes Security Bulletin-pagina. Ook mensen die Windows, Linux en Adobe AIR-producten gebruiken, worden geadviseerd zo snel mogelijk hun Flash Player te updaten.

Index

Gratis online virusscanners

Hoewel het verstandig is om continue virusbescherming op je computer te draaien kan het handig zijn om gebruik te maken van een online virusscanner. Bijvoorbeeld als second opinion of als een normale virusscanner niet goed draait op je (oude) computer.

Virusscanners vragen namelijk dusdanig veel van een computer dat sommige gebruikers, met name van oude trage computers, er voor kiezen de virusscanner achterwegen te laten. Niet verstandig, maar wel de realiteit.

“HouseCall draait vrijwel geheel op internet.”

Heb je zo'n trage computer, dan kun je Panda Cloud Anti Virus gebruiken. Dit programma draait grotendeels op internet en vraagt dus weinig van je PC, maar geeft wel continue bescherming

Daarnaast zijn er online virusscanners die je gebruikt om alleen een scan uit te voeren. Bescherming bieden deze scanners niet, je kunt er alleen een scan mee draaien en krijgt dan te horen of je virussen, wormen, Trojaanse paarden of spyware op je computer hebt staan.

Een goede online virusscanner is HouseCall van Trend Micro. HouseCall is gratis, snel en je kunt er ook virussen en andere besmettingen mee weghalen. Dit in tegenstelling tot met veel andere grats virusscanners waarmee je alleen kun scannen. TrendMicro HouseCall is snel, krachtig en browseronafhankelijk.

HouseCall draait vrijwel geheel op internet. Als je de scanner voor het eerst gebruikt dien je een piepklein bestandje te downloaden, maar daarna kun je meteen gaan scannen. Dat gaat razendsnel. Een gemiddelde scan duurt zo'n 15 minuten. Heb je veel bestanden op je computer staan dan kan het wel wat langer duren. Ook duurt de allereerste scan langer. Naast een volledige scan (Full Scan) beschikt het programma ook over een Quick Scan en een Folder Scan. Met de laatste optie kun je een deel van een schijf scannen.

Trend Micro
Trend Micro Inc is een Taiwanees beveiligingsbedrijf dat is opgericht in de USA en zijn hoofdkantoor in Japan heeft. Dit internationale bedrijf maakt beveiligingssoftware voor particulieren en grote en kleine bedrijven. Andere bekende antivirus programma's voor thuisgebruik van Trend Micro zijn Hijack This en de CWShredder.

Index

Gratis Office online gebruiken

Microsoft biedt tegenwoordig Office Live aan. Een online versie van het kantoorprogrammapakket Office, waarmee u overal gratis aan de slag kunt.

Het gratis pakket heeft iets minder opties dat de standaard Officeversie die te koop wordt aangeboden, maar u kunt er overal mee werken én een bijkomend voordeel is dat meerdere mensen aan eenzelfde bestand kunnen werken. Enige voorwaarde natuurlijk is dat u over een internetaansluiting beschikt.

Welke mogelijkheden biedt Office Live (ook Office Web Apps genoemd) u?

Word: u wilt even een kleine wijziging aanbrengen in een rapport of snel een document afdrukken? Met Microsoft Word Web App is dat zo gepiept, dankzij vertrouwde hulpmiddelen die u al kent uit Microsoft Word zoals AutoCorrectie, spellingcontrole en teken- en alineaopmaak. Ook het toevoegen van een tabel of figuur, hetzij afbeeldingen uit uw eigen bestanden of illustraties van Office.com, kan rechtstreeks vanuit uw browser.

Excel: met Microsoft Excel Web App kunt u onderweg moeiteloos een budget bijwerken met leden van uw team of uw oefenschema bijhouden. U kunt tegelijk met anderen aan dezelfde map werken, waar ook ter wereld. Daarbij kunt u diagrammen, voorwaardelijke opmaak en zelfs de nieuwe sparkline-update weergeven wanneer u kolommen sorteert en formules bewerkt.

PowerPoint: met Microsoft PowerPoint Web App kunt u op elk gewenst moment uw presentatie geven. Het maakt daarbij niet uit of u onderweg bent of even niet aan uw bureau. Via een webbrowser kunt u uw diavoorstelling met hoge beeldkwaliteit afspelen en op het laatste moment wijzigingen aanbrengen. De vertrouwde functies die u kent uit PowerPoint, waaronder de mogelijkheid dia´s toe te voegen of te verwijderen, teken- en alineaopmaak te wijzigen en een figuur in te voegen en afbeeldingstijlen toe te passen, zijn ook online beschikbaar. Bovendien kunt u met SmartArt-afbeeldingen zelfs snel diagrammen of organogrammen maken. Dat gaat net zo makkelijk als het typen van een lijst met opsommingtekens

OneNote: bent u bezig met de organisatie van een project? Met Microsoft OneNote Web App beschikt u over een handige onlinelocatie waar u al uw ideeën en informatie kunt bewaren. Iedereen die bij het project betrokken is, kan meewerken aan een gedeeld notitieblok via OneNote Web App. Daarbij kunt u uw informatie structureren met een aantal van de functies die ook beschikbaar zijn in OneNote op uw pc, zoals labels, tekststijlen, spellingcontrole terwijl u typt en AutoCorrectie. En omdat u met OneNote Web App kunt zien wie de laatste wijziging heeft aangebracht en zelfs eerdere versies van notitieblokpagina´s kunt bekijken, blijft u moeiteloos op de hoogte van alle belangrijke informatie.

Hoe gaat u te werk?

Surf naar http://office.live.com. U krijgt dan in eerste instantie het inlogvenster van Windows Live te zien. Om met de online-versie van Office te werken hebt u namelijk een Live-account nodig. Misschien bezit u die al omdat u bijvoorbeeld een hotmail-adres hebt. In dat geval kunt u zich meteen aanmelden. Is dat niet het geval, dan moet u op de knop Registreren klikken en de instructies volgen.

⇒ Na het aanmelden komt u terecht in uw persoonlijke kantoorruimte, die op dit ogenblik nog leeg is.

⇒ In het middelste deel van het scherm bij 'Recente documenten op OneDrive' zullen de documenten verschijnen die u het laatste hebt aangemaakt of bewerkt. Om al uw documenten te bekijken klikt u links op 'Alles weergeven' onder het kopje 'Persoonlijk'.

⇒ Daaronder hebt u eventueel ook nog de kopjes 'Gedeeld' en 'Gedeeld met mij'. In de eerste rubriek komen alle documenten die u met anderen hebt gedeeld, in de rubriek daaronder alle documenten die anderen met u hebben gedeeld.

⇒ Rechts staan de icoontjes van de verschillende kantoorprogramma's die u online kunt gebruiken: Word, Excel, PowerPoint en OneNote.

Word online video uitleg

Powerpoint online video uitleg

Index

Gratis Office online gebruiken (2)

Een Word-document maken

⇒ Klik op het Word-logo.

⇒ In het volgende venster geeft u uw document een naam en klikt u op Opslaan.

⇒ Het programma start nu op en u krijgt een scherm te zien dat sterk gelijkt op het vertrouwde Word 2010-venster. U zult meteen merken dat de mogelijkheden haast gelijk zijn. U kunt knippen, plakken en kopiëren, lettertypes en -groottes aanpassen, uw tekst in vet of schuin zetten, alinea's aanpassen, stijlen gebruiken, de spelling controleren, grafieken, tabellen en illustraties invoegen enz.

⇒ Werken met Excel, PowerPoint of OneNote

⇒ Ook voor deze programma's zijn de verschillen met de betalende versie die u op een computer kunt installeren niet erg groot. Enkel de meest geavanceerde functies zijn niet beschikbaar

Een document bewerken

⇒ Sluit alle online-programma's af, dan komt u terug op uw persoonlijke startpagina terecht. Daar staan al uw documenten netjes onder elkaar weergegeven. Wanneer u met uw cursor op één van deze documenten gaat staan, dan krijgt u de keuze 'Openen in browser' of 'Openen in Word' (als het om een Word-document gaat). Kiest u voor 'Bewerken in browser' dan wordt het document geopend in Word Web app en kunt u rustig verder werken aan uw document.

⇒ Staat u met uw cursor op een document op uw startpagina dan krijgt u ook de keuzemogelijkheid 'Meer'. Door daarop te klikken krijgt u een aantal bijkomende mogelijkheden aangeboden zoals het bekijken van de versiegeschiedenis, de naam wijzigen of het document downloaden.

Een document delen

⇒ Op dezelfde manier kunt u onder 'Meer' ook op 'Delen' klikken.

⇒ U moet nu eerst klikken op 'Machtigingen aanpassen'.

⇒ U ziet nu een schuifbalk die gaat van 'mezelf' tot 'iedereen'. Hier bepaalt u wie allemaal aan uw documenten kan. Voor uw vrienden of geselecteerde vrienden kunt u bovendien bepalen of ze de bestanden enkel kunnen raadplegen of ze ook kunnen bewerken.

⇒ Via 'Bepaalde personen toevoegen' gaat u nog selectiever tewerk en geeft u de e-mailadressen op van die mensen die aan uw documenten mogen komen.

⇒ Klik op 'Opslaan'.

⇒ Nu moeten de mensen met wie u uw documenten wil delen daar nog van op de hoogte gebracht worden en weten waar ze het document kunnen vinden. Ga opnieuw met de cursor op het document in kwestie staan. Klik op 'Meer' en 'Delen' en vervolgens op 'Link verzenden'. U kunt daarbij nog een boodschap meegeven.

⇒ Een andere mogelijkheid is 'Link ophalen'. Klik op de link in het venstertje onder 'Delen met vrienden' typ CTRL C om de link te kopiëren. Open nu uw e-mailprogramma, schrijf een mail naar de mensen met wie u het document wil delen en plak de link hierin door CTRL V te typen.

Documenten overal voor uzelf beschikbaar maken

Bent u op kantoor aan een document aan het werken en wilt u daar graag thuis aan verder werken, dan kunt u het document op een USB-stick zetten of naar uzelf mailen. Het gevaar daarbij bestaat echter dat u het achteraf in omgekeerde richting vergeet te kopiëren of niet meer weet waar de meest recente versie zich nu precies bevindt. Dat gevaar bestaat niet als u het document oplaadt naar Office Live.

⇒ Ga opnieuw naar uw persoonlijke startpagina

⇒ klik op 'Bestanden toevoegen'.

⇒ Selecteer de map waar de documenten terecht moeten komen.

⇒ Of sleep de documenten naar het venster dat nu wordt geopend

⇒ Of klik op 'Selecteer documenten op de computer' en haal het document in kwestie op.

⇒ Klik vervolgens op 'Doorgaan'. Het bestand wordt nu opgeladen en u kunt het voortaan online terugvinden in de door u gekozen map.

Index

Windows Store zit vol met apps van oplichters

De Windows Store, de appstore van Windows 8.1 en Windows RT 8.1, bevat talloze nep-apps die gebruikers geld uit de zak kloppen voor niks, zegt website How to Geek na een eigen onderzoek.

Volgens een empirisch onderzoek van website How to Geek zit de Windows Store, waar je apps kan downloaden die werken op Windows 8, vol met apps van oplichters. Als voorbeeld noemt de site het fikse aantal apps die VLC beloven, waarvan er slechts 1 de officiële app is en de rest meuk. De meeste zijn tegen een prijs van 2 tot 8 dollar te koop en hebben vervolgens slechts een downloadlink naar de verder gratis VLC.

Nepversies van Flash Player, Minecraft, WeChat

VLC is als voorbeeld genomen omdat daar de oplichterstruc zo apert duidelijk is. Maar verder graven laat nog meer zien, meldt How to Geek. Zoeken op iTunes of Firefox levert hetzelfde resultaat op. Daarnaast zijn er betaalde nepversies van Adobe Flash Player, Candy Crush Saga, WeChat, WhatsApp, Minecraft, Spotify, Google Hangouts en veel meer.

Soms zijn de verschillen moeilijk te zien, omdat onder meer hetzelfde logo wordt gebruikt. Her en der zijn er bij reviews van apps dan ook klachten van boze consumenten te lezen, die niet kregen waarvoor ze hebben betaald.

Microsoft wordt erop aangekeken

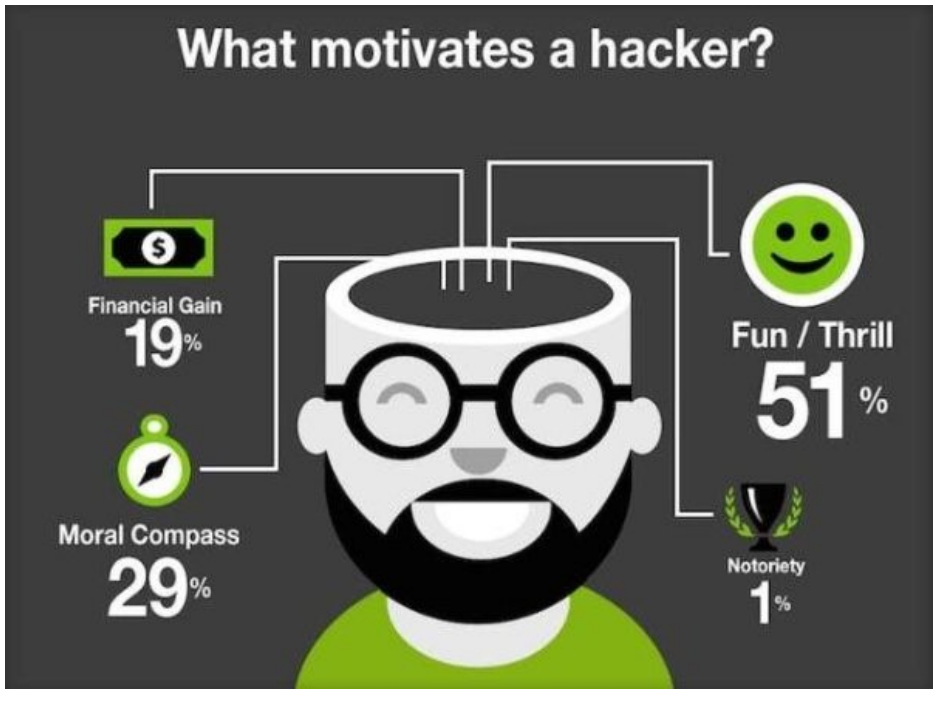
How to Geek gaat vervolgens tekeer tegen de integratie van de app-winkel met de zoekfunctie op de desktop omdat een zoekopdracht niet alleen je al geïnstalleerde programma oplevert, maar ook de eerder genoemde meuk uit de winkel.

Microsoft wordt door de schrijver van het artikel op How to Geek aangewezen als grootste schuldige, doordat het kwantiteit over kwaliteit zou verkiezen, en mensen in dienst heeft die die apps blijkbaar hebben getest en goedgekeurd. Webwereld heeft Microsoft gisteren om een reactie gevraagd, maar nog geen inhoudelijke reactie gekregen.

Index

Waarom hackers hacken

Het laatste waar hackers aan denken op het moment dat ze ergens proberen in te breken, is dat ze mogelijk gesnapt worden. Dit blijkt uit nieuwe gegevens. Sterker nog: 86 procent van de hackers denkt nooit gestraft te worden voor wat ze uitgespookt hebben.



Thycotic, een bedrijf dat software maakt om je wachtwoord te beschermen, publiceerde donderdag de resultaten van een onderzoek naar de motivatie van hackers. Het bedrijf ondervroeg 127 zelfverklaarde hackers tijdens de beurs Black Hat 2014 eerder deze maand. Dit leverde verrassende resultaten op.

Vooral om de lol

Om te beginnen lijkt de drang van hackers niet financieel gemotiveerd te worden. Meer dan de helft van de ondervraagde personen geeft aan dat ze doen wat ze doen omdat ze het leuk vinden, of vanwege de kick die ze ervan krijgen. Slechts achttien procent wil geld en één procent wil bekendheid.

Negenentwintig procent van de geïnterviewde hackers identificeert zichzelf als hacktivist met als doel het onthullen van de waarheid. Zo brak eerder deze week een groep hackers in op de computers van de St. Louis County Police. Vervolgens publiceerden ze de opnames die gemaakt zijn rond het neerschieten van de ongewapende tiener Michael Brown.

Goede intenties

Met 86 procent van de hackers die denkt nooit gepakt te worden en vier op de vijf hackers die het voor de lol doen of om de waarheid boven tafel te krijgen, denkt Thycotic-oprichter en CEO Jonathan Cogley dat veel van deze hackers geloven dat wat zij doen niet verkeerd is.

Cogley: “Ze denken waarschijnlijk: 'ik heb geen schade aangericht en ik ben er zelf niet beter van geworden'. En zelfs als ze gepakt worden dan verdedigen ze zich door te zeggen dat ze alleen maar nieuwsgierig waren.”

Methodes

Welke tactieken gebruiken de hackers? Volgens Thycotic borduren ze vooral voort op reeds bestaande en bewezen methodes, zoals phishing en spoofing. In het onderzoek gaf 99 procent van de respondenten aan dat dit nog steeds erg effectief werkt.

“Ze gaan voornamelijk terug naar de basis. Slechts weinigen zijn op zoek naar de volgende massale zero-day-aanvallen”, stelt Cogley. “Velen zijn prima tevreden met het gebruik van tien jaar oude technieken.”

Hackers vrezen elkaar

Een andere conclusie uit Thycotics onderzoek is dat hackers elkaar vrezen. Negen op de tien ondervraagden zeggen bang te zijn slachtoffer te worden van online diefstal of dat er ingebroken wordt in hun eigen data.

De wereld is de afgelopen jaren steeds verder gedigitaliseerd. Dit heeft als gevolg dat er ook meer aanvallen en inbraken plaatsvinden. Niet alleen overspoelen de hacktivisten het web met gevoelige informatie van overheden en corporaties, maar ook grote websites en (online) winkels zijn het slachtoffer geworden van het stelen van gegevens.

Index

Cybercriminelen maken jacht op gamers

Nederland telt 8 miljoen gamers. Hoewel 55 procent van deze gamers zich beperkt tot gratis games, maar 3,6 miljoen Nederlanders besteden dus wel geld aan hun games. Dit maakt van gaming een industrie waarin veel geld om gaat en daarom trekt het steeds meer de aandacht van cybercriminelen.

Phishingaanvallen beperken zich niet tot internetbankieren. Het wordt ook ingezet om accounts voor online games te stelen. Cybercriminelen proberen inloggegevens in handen te krijgen voor populaire platformen als Steam en Origin, door exacte kopieën van deze sites te maken en gebruikers daar met een smoes naartoe te lokken.

“Dat is de meest lucratieve handel,” legt Ralf Benzmüller, hoofd van het G DATA SecurityLab, uit. “Gamers schakelen vaak hun beveiligingsoftware uit om zo hun computer nog sneller te laten werken, maar daarmee stellen ze hun pc dus wel open voor dit soort aanvallen. Het is veel verstandiger voor gamers om te kiezen voor een beveiligingspakket met een gamervriendelijke firewall."

Daarnaast is er momenteel een levendige handel in illegale gamesleutels voor de populaire games als Call of Duty, Battlefield 4 en Titanfall. Een sleutel voor Battlefield 4 Premium Edition kan voor €10 worden gekocht: een kwart van de officiële prijs. Echter, gamers die dit doen riskeren wel een blokkade van hun account als de sleutel door Steam of Origin als illegaal wordt bestempeld.

Index

Handig

Phishing- / valse e-mails melden

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

Rabobank: valse-email@rabobank.nl

SNS Bank: valse-email@sns.nl

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

opgelet op internet.nl

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

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

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

Antwoord

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

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

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

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

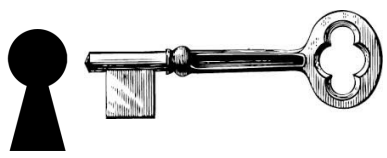
---

POLITIE Meldpunt internetoplichting

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

Index

Software schatkist



Browser Hijack Recover

Trusteer Rapport

Blackberry Desktop Software

PC Transfer

DVD Flick

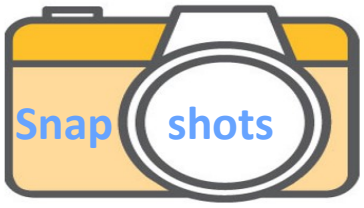
EaseUs Partition Master

EmsiSoft Emergency Kit

Any Burn

Freemake Video Converter

Index



Met de vernieuwde Politie app kun je ook pushberichten ontvangen op je smartphone, bij brand, gevaar of vermissingen in de gemeente waar je woont/werkt. De berichten kunnen weer gedeeld worden. Ook vernieuwd is de manier waarop je informatie over je eigen buurt kunt opzoeken. De politiebureaus zijn nu voorzien van openingstijden en route-informatie op basis van je eigen gps. De Politie app is sinds eind 2013 beschikbaar, najaar 2014 volgt een update waarmee je meldingen kunt doen. De app is te vinden in de app stores van Apple, Google en Microsoft. Info over de app staat op Politie.nl.

Sinds kort is Crimikaart.nl actief. De site geeft volgens de makers, Semlab, een overzicht van 'alle strafbare feiten in Nederland op straatniveau' en is behalve 'iedereen gratis toegankelijk' ook geschikt 'bij het plannen van de aankoop van een huis of bij het bepalen van een veilige route naar school'. Crimikaart gebruikt voor de kaarten 'betrouwbare informatie die bevestigd is door de Nederlandse politie'.

Oplichters hebben facebook ontdekt, schrijft Metro. De rest van de wereld had dat al eerder gedaan, maar volgens het artikel duiken er steeds meer facebookpagina's op van mensen die zogenaamd kaartjes aanbieden voor feesten, concerten en andere evenementen. De accounts verdwijnen weer als de kaartjes – die natuurlijk niet bestaan – zijn verkocht. Woordvoerder Bas Ketelaars van de Stichting Stop Internetoplichters spreekt van 'een explosieve stijging' van zulke zaken. Ook de beheerder van de facebookpagina Ticketoplichters Ontmaskerd zegt een toename te zien. Een van de slachtoffers is Nikki uit Amsterdam, die een kaartje kocht bij 'Nathalien Kurt', 52 euro overmaakte maar nooit iets kreeg. Kort na het overmaken verdween de facebookpagina. 'Ze stuurde mij een link die ik moest gebruiken om het geld over te maken. Dan zou het direct op haar rekening staan, zei ze. Er ging wel een belletje rinkelen, maar door mijn enthousiasme wilde ik het gevaar niet zien'. Ook Frank werd opgelicht, twee keer zelfs. Hij maakte ruim honderd euro over aan 'Maria Rutte' en later ook aan 'Eva Louise Langelaan'. De politie adviseert in dit soort gevallen goed na te denken voor je geld overmaakt. Een facebookpagina die een paar dagen bestaat, met één berichtje, nauwelijks vrienden of likes? Enfin, aangifte doen kan onder meer via een internetformulier.

Opgelet: er zit een addertje onder het gras bij de nieuwe Messenger-app op uw smartphone. Facebook mag geluid of video opnemen zonder dat u het weet, kan sms'jes lezen en kijken naar wie je gebeld hebt. Dat staat in de kleine lettertjes van de verplichte Messenger-app.

Ondertussen gebruiken ongeveer 1 miljard mensen de Messenger-app, al is dat logisch, want Facebook laat je geen keuze. De meeste gebruikers weten niet wat er in de kleine lettertjes staat.

Vrijwel dagelijks verschijnen er op internet foto's, filmpjes en signalementen van verdachten. De ene keer een winkeldief, dan iemand die ergens eet zonder te betalen, dan weer een oplichter. De afgelopen weken werden verscheidene verhuurbedrijven van audioapparatuur opgelicht; diens naam en foto kwamen dan ook snel online. Onder meer bij Dichtbij.nl, dat het voorval aangreep om een stelling van de week te poneren: 'wie steelt, verspeelt zijn recht op privacy'. De uitslag tot nu toe? Maar liefst 93% is het er mee eens!

Een inwoner van Heemskerk is het slachtoffer van identiteitsfraude geworden nadat hij zijn rijbewijs inclusief foto op zijn Facebookpagina had geplaatst. Onbekenden kopieerden de afbeelding en gebruikten die om zich te legitimeren bij de verkoop van valse festivalkaarten.

Een aantal mensen kocht de betreffende festivalkaarten via internet en maakten van tevoren geld over. Toen ze de kaarten niet kregen toegestuurd gingen ze verhaal halen bij de persoon die op het rijbewijs stond. De man bleek er echter niets mee te maken te hebben. De inwoner van Heemskerk deed vervolgens aangifte dat zijn identiteit valselijk werd gebruik bij de verkoop van tickets.

Index

De politie in Groningen heeft ‘afstand genomen‘ van een tweet van rechercheur Remco de Jong. Deze ‘rechercheur in de binnenstad van Groningen’ twitterde over de GayPride: ‘Ik blijf het een smerige vertoning vinden’. Volgens De Jong was daar geen sprake van Hollands Glorie maar van ‘Hollands Goorie’. De Jong twitterde vervolgens dat het zijn persoonlijke mening was en dat die los stond van zijn ‘ambtelijke handelen als politieman’. Maar de geest was al uit de fles. De politie Groningen twitterde de mening van De Jong niet te delen. ‘We gaan met hem in gesprek’. Even later gevolgd door de opmerking dat de politie voor diversiteit is. ‘Daarom nemen wij ook deel aan de Canal Parade’. Sites als GeenStijl maakten vervolgens gehakt van De Jong, die naast rechercheur ook ‘admissiaal student aan de Theologische Universiteit van Apeldoorn’ is. Enfin. Aanvankelijk werd alleen de tweet verwijderd, inmiddels is de hele twitterpagina van De Jong offline gehaald.

———————————————-

Het Hof in Amsterdam heeft in een slepende rechtszaak een vrouw lijfsdwang opgelegd omdat ze al jarenlang een agent van het toenmalige korps Kennemerland onterecht beschuldigd heeft van onder meer marteling en verkrachting. De vrouw werd al eerder veroordeeld voor smaad maar ging in beroep. De zaak sleept zich al een jaar of tien voort, bij elke uitspraak ging ofwel de vrouw ofwel de agent en het korps in beroep. Het Hof overweegt nu dat de door de vrouw op internet gedane uitlatingen ‘niet anders kunnen worden beschouwd dan als een aaneenrijging van ernstige verdachtmakingen en beschuldigingen, diskwalificaties en (anderszins) kwetsende opmerkingen’. Per overtreding kan de vrouw een week hechtenis krijgen, aldus het vonnis.

———————————————-

Nederland staat laag op de lijst van landen die bij Twitter accountinformatie opvragen, blijkt uit Twitters nieuwe Transparantierapport. Over de periode januari-juni 2014 diende Nederland slechts vijf verzoeken in, betreffende acht accounts. Een van die verzoeken werd gehonoreerd. De VS waren koploper: 1257 verzoeken. Omgerekend is dat 61% van het totaal aantal verzoeken (2058). Dat totale aantal steeg met 46% ten opzichte van het tweede halfjaar van 2013. Volgens Twitter heeft dat te maken met nieuwe landen (acht) die informatie opvroegen maar een trend is ook dat sociale media steeds vaker bestookt worden met opvragingen. Het aantal Nederlandse verzoeken was in het tweede halfjaar van 2013 ‘minder dan tien’, iets meer dan de helft daarvan werd toen ingewilligd.

———————————————-

De politie en steunpunt Huiselijk geweld in Midden Brabant maken zich zorgen over het groeiende aantal naaktselfies. De politieregio Zeeland/ West-Brabant noteerde onlangs in twee weken ruim dertig meldingen. De gevolgen zijn soms groot: meisjes zitten uit schaamte en angst soms wekenlang thuis, de daders, meestal ex-vriendjes, gaan gewoon naar school. Volgens Peter Rens, teamleider in ZWB, zijn de prikkelende naaktfoto’s en -filmpjes ‘een steeds grotere bron van zorg’. In Brabant is deze week de campagne We Can Young gestart, die jongeren, leerkrachten en ouders bewust moet maken van de gevaren van sexting.

———————————————-

In de VS zijn veertien bedrijven en veertien personen die zich telefonisch uitgaven als medewerker van Microsoft veroordeeld tot een boete van in totaal 5,1 miljoen dollar. De verdachten belden mensen thuis op en riepen dat er problemen met de computer waren. Of je maar even toegang wilde verlenen tot je computer. Daarop werd allerlei malware geïnstalleerd waarmee de argeloze gebruikers werden benadeeld. De ene keer weren er spullen aangeschaft op rekening van het slachtoffer, de andere keer werden bankgegevens verkregen. In totaal zouden tienduizenden computergebruikers zijn opgelicht. Volgens de Federal Trade Commission werkten de benden voornamelijk vanuit India en hadden ze het voorzien op Engelssprekenden in de VS en andere landen.

———————————————-

De Ierse politie is samen met Europol een onderzoek gestart nadat een laptop en documenten van een Ierse politieagent in een Amsterdams bordeel werden aangetroffen. De uitbaatster van het bordeel zou de tas met de computer en documenten hebben gevonden en vervolgens de politie hebben ingelicht.

De Nederlandse politie nam contact op met de Ierse politie, die inmiddels ook de hulp van Europol heeft ingeroepen, zo meldt de Irish Independent. Er zal worden gekeken hoe de tas in het bordeel terecht kwam en of de laptop als vermist was opgegeven. De angst bestaat dat de gevoelige gegevens op de laptop mogelijk gecompromitteerd zijn geraakt. Volgens een bericht in de Ierse krant de Sunday World zou de agent in kwestie zeer ervaren zijn, maar is hij nog niet over het incident ondervraagd.

Index