



W.Bosgra taakaccenthouder digitale criminaliteit

December 2013

Dit digitale magazine wordt verzorgd door Secure Computing.

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

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

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

[E-mail? klik hier !](#)



Speciale December schatkist

Nieuwe eisen banken voor internetbankieren

Diensten afnemen zonder te betalen

Internetverslaving

Online beveiligingstesten

Spyware in Windows Media Player



De Wet Computercriminaliteit: Diensten afnemen zonder betalen

Aanbieden en bewaren

Het aanbieden en verspreiden van hulpmiddelen of gegevens om gratis toegang te krijgen tot betaaldiensten is verboden: hierop staat een straf van maximaal een jaar cel (art. 326c lid 2). Hetzelfde geldt voor het maken of bewaren van dergelijke middelen, alleen moet dat dan wel uit winstbejag gebeuren. En wie van dit maken of verspreiden zijn beroep maakt, kan zelfs tot drie jaar de gevangenis in gaan (art. 326c lid 3).

Apparaten om te kraken

Hulpmiddelen voor gratis toegang zijn meestal software, maar ook speciaal ontworpen apparaten worden wel gebruikt. Het oudste voorbeeld van zo'n apparaat is waarschijnlijk het fluitje dat als kadootje in de Cap'n Crunch cornflakes zat. Het bleek dat met het geluid van dit fluitje gratis gebeld kon worden in de hele VS.

Ook een apparaat waarmee verbruikte telefoonkaarten konden worden opgewaardeerd was een dergelijk hulpmiddel, zo vond de Hoge Raad in 2003. Overigens staat op namaak van betaalpassen of waardekaarten (bijvoorbeeld beltegoedkaarten) zes jaar cel of een boete van 67.000 euro (art. 232 lid 1). Hetzelfde geldt voor het gebruiken, hebben of verkopen van dergelijke kaarten als je weet dat ze vervalst zijn (art. 232 lid 2).

Instructies om te kraken

Ook instructies of een handleiding hoe de beveiliging van een dienst gekraakt kan worden, kunnen strafbaar zijn.

Artikel 326c spreekt van "een voorwerp of gegevens". En uit art. 80quinquies blijkt dat "onder gegevens" wordt verstaan iedere weergave van feiten, begrippen of instructies, al dan niet op een overeengekomen wijze, geschikt voor overdracht, interpretatie of verwerking door personen of geautomatiseerde werken."

IDe Hoge Raad oordeelde dan ook dat een tijdschriftartikel een "verboden voorwerp" was. In deze zaak was een artikel in een tijdschrift gepubliceerd met als titel "gekraakt, Canal+ kijken op uw PC". Met de instructies uit dit artikel kon de beveiliging van betaalzender Canal+ gekraakt worden. Dit artikel werd dus gezien als een weergave van instructies geschikt voor interpretatie of verwerking door personen.

Veel telecommunicatiediensten worden tegen betaling aangeboden. Denk bijvoorbeeld aan betaaltelevisie, mobiele telefonie of gewoonweg toegang tot Internet. Het is soms mogelijk om met een speciaal kastje of door speciale software te gebruiken van zo'n dienst gebruik te maken zonder te betalen. Gratis betaaltelevisie kijken lijkt aantrekkelijk, maar is een misdrijf: maximaal drie jaar cel of een geldboete van 67.000 euro (art. 326c lid 1). Dit wordt soms "diefstal" (van de dienst) genoemd, alhoewel dit formeel juridisch onjuist is. Een dienst kan niet worden weggenomen zoals een fiets. Vandaar de aparte strafbaarstelling als "afnemen zonder betalen". Opsporen van dit misdrijf is lastig, omdat het immers heel moeilijk is om na te gaan wie de dienst ontvangt en of zijn aansluiting terecht is. Vandaar dat de bestrijding van dit misdrijf meestal gebeurt door verspreiders van hulpmiddelen aan te pakken. Die zijn verboden op grond van art. 326c lid 2.

Kraken van beveiliging van werken

Naast diensten zoals telefonie of televisie worden ook wel producten zoals elektronische boeken of muziek en films voorzien van beveiligingen. Het omzeilen van dergelijke beveiligingen kan onrechtmatig zijn (art. 29a lid 2 Auteurswet), maar dit is geen strafbaar feit in de zin dat er gevangenisstraf of een boete op staat. De maker van het werk kan wel in een civiele procedure schadevergoeding eisen.

Hetzelfde geldt voor iemand die apparaten verkoopt om dit te vergemakkelijken (art. 29a lid 3 Auteurswet), of die beroepsmatig beveiligingen van werken verwijdert.

Banken stellen nieuwe regels voor internetbankieren



Nederlandse banken hebben nieuwe regels voor internetbankieren opgesteld waar klanten aan moeten voldoen als ze in het geval van fraude hun geld terug willen krijgen. Zo mag er geen illegale software zijn geïnstalleerd, moet de computer up-to-date zijn en moet de rekening regelmatig worden gecontroleerd.

Dat laat de Nederlandse Vereniging van Banken (NVB) weten. Tot nu toe hanteerde iedere bank zijn eigen veiligheidsvoorwaarden. Banken bepalen zelf wanneer ze de nieuwe uniforme regels aan hun klanten communiceren. Tot dat moment zullen banken bij de behandeling van nieuwe claims van klanten vanaf 1 januari 2014 in de geest van de nieuwe regels handelen.

Mocht een klant schade lijden en het blijkt dat hij zich niet heeft gehouden aan de veiligheidsregels, dan kan een bank op basis van haar coulerbeleid overigens alsnog besluiten om een deel van de schade voor haar rekening te nemen.

Veiligheidsregels

De NVB heeft de nieuwe veiligheidsregels samen met de Consumentenbond opgesteld. Ze gaan voor particuliere klanten gelden. "Als consumenten zich aan de volgende veiligheidsregels voor elektronisch bankieren en - betalen houden, vermindert de kans sterk dat om slachtoffer te worden van fraude. Ook weten ze dan zeker dat de bank de schade vergoedt", stelt de NVB. Het gaat in totaal om vijf regels.

Houd beveiligingscodes geheim. Klanten mogen beveiligingscodes alleen zelf gebruiken. Daarnaast mogen ze niet worden opgeschreven. In het geval dit echt niet anders kan moet de code in een onherkenbare vorm voor anderen worden opgeschreven. Als klanten zelf hun beveiligingscode kiezen mag die niet eenvoudig te raden zijn. Bijvoorbeeld geen geboortjaar of naam van een familielid of een postcode. Klanten mogen de beveiligingscode ook nooit per telefoon of e-mail doorgeven.

Anderen mogen de bankpas niet gebruiken. Klanten moeten zich tijdens het gebruik van de bankpas niet laten afleiden en de bankpas altijd op een veilige plaats opbergen waar die niet eenvoudig verloren kan worden. Ook moet de klant regelmatig controleren of hij de bankpas nog in zijn bezit heeft.

Goede beveiliging van de apparatuur die wordt gebruikt voor bankzaken. Hierbij geldt dat de geïnstalleerde software op de apparatuur, zoals computer, tablet en/ of smartphone, die voor het regelen van de bankzaken wordt gebruikt, is voorzien van actuele (beveiligings)updates. Geïnstalleerde software is bijvoorbeeld het besturingssysteem en beveiligingsprogramma's, zoals virusscanner en firewall.

Ook mag er geen illegale software zijn geïnstalleerd. Verder moet de apparatuur die wordt gebruikt voor het regelen van bankzaken met een toegangscode beveiligd zijn. Klanten moeten er daarnaast voor zorgen dat de toepassingen van de bank op hun apparatuur niet door onbevoegden zijn te gebruiken. Als laatste moeten klanten na hun bankzaken uitloggen.

Controleer de bankrekening. Klanten moeten in ieder geval elke twee weken hun rekeninginformatie controleren. Alleen als klanten rekeninginformatie op papier ontvangen moeten ze deze twee weken na ontvangst controleren. Als er schade voor de bank ontstaat doordat de klant enige tijd zijn rekeninginformatie niet heeft kunnen controleren, kan de bank de klant vragen aan te tonen waarom dit niet mogelijk was.

Meld incidenten direct aan de bank en volg aanwijzingen van de bank op. Het gaat dan om zaken als klanten weten of vermoeden dat iemand anders hun beveiligingscode kent of heeft gebruikt, of dat er transacties op de bankrekening hebben plaatsgevonden waarvoor geen toestemming is gegeven. Ook moet er direct contact met de bank worden opgenomen als de klant iets vreemds of ongebruikelijks ervaart, zoals een andere manier van inloggen.

In het geval banken fraude vermoeden kunnen ze daarnaast de klant blokkeren om (verdere) schade te voorkomen. Als de bank in dit geval aanwijzingen geeft, bijvoorbeeld om nieuwe incidenten te voorkomen, dan moet de klant deze aanwijzingen opvolgen. "Ook hierbij zal de bank u nooit om beveiligingscodes vragen", aldus de NVB. Die laat verder weten dat de schade als gevolg van fraude met internetbankieren daalt.

Juridische vraag: wie is aansprakelijk voor fraude met internetbankieren?

Door Arnoud Engelfriet De banken hebben nieuwe regels voor internetbankieren opgesteld waar klanten aan moeten voldoen als ze in het geval van fraude hun geld terug willen krijgen. Zo mag er geen illegale software zijn geïnstalleerd, moet de computer up-to-date zijn en moet de rekening regelmatig worden gecontroleerd. Als ik het goed begrijp, dan ben ik aansprakelijk voor fraude als ik die regels overtreed. Mag dat zomaar?

Deze veiligheidsregels zijn door de banken opgesteld (in overleg met de Consumentenbond) maar ze kunnen natuurlijk de wet niet wijzigen. Hoofregel bij fraude met betaalmiddelen is dat de bank het risico draagt (art. 7:529 BW).

De bank heeft het beste overzicht op wat er gebeurt, zij kunnen beveiligingsmaatregelen invoeren en zij kunnen typische fraudezaken vaak volautomatisch detecteren. De bank mag de klant een eigen risico geven van €150 bij bij verlies en diefstal (tot het moment van melding) en bij ongeautoriseerd gebruik wanneer de klant de veiligheidsmaatregelen heeft verwaarloosd.

Lid 2 van art. 7:529 BW bepaalt dat bij fraude, opzet en grove nalatigheid van de klant deze zelf het risico moet dragen. Bij fraude en opzet is dat logisch: wie dat soort dingen doet, kan toch niet verwachten dat de gevolgen vergoed gaan worden. Maar bij "grote nalatigheid" is dat toch moeilijker. Wanneer is iemand nalatig? Wanneer is dat grof?

Uit de (schaarse) rechtspraak blijkt dat grove nalatigheid bepaald moet worden aan de hand van alle omstandigheden van het geval. Er zijn geen algemene regels zoals "als je dagelijks controleert of je je pas nog hebt, is het nooit nalatig" of juist "stop je je creditcard in je tas dan is dat altijd nalatig". Zo achtte het Gerechtshof Arnhem het niet grof nalatig dat een klant na een vermoeden van zakkenrollen wél naging of zij haar portemonnee nog had, maar niet of de pinpas daar nog in zat. Dit maakt het moeilijk om op voorhand te zeggen of in een concrete situatie sprake is van grove nalatigheid.

De bewijslast dat sprake is van grove nalatigheid (of opzet/fraude) ligt bij de bank. En die bewijslast houdt meer in dan zeggen "er is gepind met de pas van klant dus is sprake van grove nalatigheid." Er moeten feiten of omstandigheden worden aangedragen door de bank waaruit blijkt dat de klant meer dan normaal slordig was.

*Arnoud Engelfriet is ICT-jurist, gespecialiseerd in internetrecht waar hij zich al sinds 1993 mee bezighoudt. Hij werkt als partner bij juridisch adviesbureau ICTRecht. Zijn site [Ius mentis](#) is één van de meest uitgebreide sites van Nederland over internetrecht, techniek en intellectueel eigendom. Hij schreef twee boeken, *De wet op internet en Security: Deskundig en praktisch juridisch advies*.*

Veiligheidsvoorwaarden staan apart in de wet genoemd. Er staat expliciet dat je verplicht bent als klant deze voorwaarden op te volgen (art. 7:524 BW). Doe je dat niet, dan kan de rechter (art. 7:529 lid 3 BW) besluiten dat je een groter eigen risico draagt dan de normaal geldende 150 euro bij frauduleuze transacties. Hij kan ook besluiten dat het eigen risico toch gewoon geldt, of zelfs het eigen risico omlaag doen, afhankelijk van de aard van het misbruikte beveiligingsprobleem.

Bij een zeer geavanceerde Trojan helpt zelfs de beste virusscanner niet, dus om dan te zeggen "u had géén enkele virusscanner en daarom bent u volledig zelf aansprakelijk voor het verlies" gaat wat ver. De bankvoorwaarden moeten natuurlijk wel redelijk zijn (art. 6:233 BW).

Wat de banken met deze nieuwe regels proberen te doen, is allereerst de regels gelijktrekken, wat op zich prima is. Maar het lijkt óók een poging om eerder te kunnen zeggen "u overtrad de veiligheidsvoorwaarden dus u bent grof nalatig". Bij de rechter is dat echter geen automatisme, hoewel je met deze nieuwe regels denk ik wel meer uit te leggen hebt.

Een punt hierbij is in ieder geval wel dat er een link moet zijn tussen de overtreding en de fraude. Zo is er een regel die installeren van illegale software verbiedt. Maar het enkele feit dat ik een gekraakte Photoshop op mijn Windowslaptop heb, betekent niet dat schade door een Android-trojan automatisch voor mijn rekening moet komen. Echter, kwam een Windowstrojan mee met die gekraakte Photoshop, dan ga ik wél voor de bijl.

Omgekeerd staat er echter ook dat als je je aan alle gestelde regels houdt, je per definitie *niet* grof nalatig was. Dat is immers wat men bedoelt met "weten [consumenten]" dan zeker dat de bank de schade vergoedt."



Kapen online-identiteit is onderschat probleem

Kinderombudsman Marc Dullaert stelt een onderzoek in naar privacyschending van kinderen op sociale netwerken. Volgens hem moeten de sociale media werken aan hun zelfreinigend vermogen. Als ze dat niet voldoende doen, moet er een onafhankelijke waakhond komen die bedrijven als Facebook en Twitter op de vingers kan tikken.

Aanleiding voor het onderzoek van de Kinderombudsman is een noodkreet van stichting Mijn Kind Online, die vier jonge slachtoffers van online-identiteitsdiefstal bijstond. 'Toen ik een voorbeeld van dergelijk misbruik hoorde, was ik ronduit geschokt', zegt Dullaert. 'Ik ga onderzoeken hoe dit mogelijk was en hoe zo iets in de toekomst kan worden voorkomen.'

Het voorbeeld van Mijn Kind Online gaat over de nu 13-jarige jongen Freek (een gefingeerde naam). Hij maakte eind 2012 een Twitteraccount aan om met vrienden en familieleden te kunnen communiceren. Een paar weken later circuleerde zijn foto plots op internet. Niet alleen op sociale media als Facebook en Tumblr, ook op buitenlandse websites.

'Hij moet dood'

Het karakteristieke uiterlijk van Freek - hij kijkt scheel en heeft sproeten - werd onderwerp van internationale spot. Zijn gezicht werd op afbeeldingen en in filmpjes gemonteerd. 'Daarbij stonden teksten als: Deze jongen had nooit geboren mogen worden, en: Hij moet dood', zegt Remco Pijpers, directeur van Mijn Kind Online. 'Ik heb nog nooit eerder zo iets meegemaakt.'

De ouders van Freek waren ten einde raad toen de internetbedrijven niet reageerden op verzoeken de foto's offline te halen. Zelfs nadat moeder Linda liet weten dat ze het hoofd van haar zoon boven het lichaam van naakte vrouwen zag gemonteerd, kwam er geen reactie. Ze vond het verschrikkelijk, maar andere internetters smulden ervan. Tienduizenden mensen wereldwijd volgden de karikatuur van Freek op de voet.

Toen de ouders van Freek aangifte wilden doen, weigerde de politie die in eerste instantie op te nemen. Uiteindelijk lukte het bij een politiebureau in een andere stad alsnog. Met behulp van Mijn Kind Online slaagden ze er bovendien in veel foto's en filmpjes te laten verwijderen. Maar zelfs nu, een jaar later, duiken de ongewenste alter ego's van Freek nog geregeld op.

"We hebben meer signalen gekregen van kinderen die het slachtoffer zijn van online-privacyschending. Als er niet snel iets gebeurt, zou het me niet verbazen als het tot een internationale rechtszaak komt."

Kinderombudsman Dullaert

Moeilijk tegen op te treden

'Het lukt bedrijven als Facebook en Google maar niet om Freek's foto uit te bannen', zegt Remco Pijpers, directeur van Mijn Kind Online. 'Het geval van Freek is extreem, maar het legt wel bloot hoe moeilijk het is om hiertegen op te treden. Als het om kinderporno gaat is het binnen enkele uren verwijderd, gaat het om online-identiteitsdiefstal dan is het kennelijk geen prioriteit. Het is tijd om hierover een flinke discussie te beginnen.'

De aanstichter van de onlinepestcampagne - een minderjarige Nederlander - is inmiddels gevonden. Volgens Mijn Kind Online handelde de jongen doelbewust. Hij verwees mensen door naar de echte Freek en vertelde op internet dat hij vaker dit soort grappen uithaalt. De jongen is in afwachting van de strafeis van de officier van Justitie.

Het is nog maar de vraag in welke mate het strafbaar is wat hij, en anderen die zich bezighouden met onlinepesten, doen. 'Je zult juridische pleisters moeten plakken', zegt Simone van der Hof, hoogleraar recht en informatiemaatschappij aan de Universiteit Leiden. Volgens haar heeft een strafzaak niet het gewenste effect, omdat de beelden gewoon online blijven staan. 'Ik denk eerder aan Europese regelgeving die het gemakkelijker maakt om data van internet te verwijderen.'

Mogelijk internationale rechtszaak

Providers en internetbedrijven moeten op de stoel van de rechter gaan zitten als ze bepalen welke zaken worden verwijderd. Een ongezonde situatie, vindt Van der Hof. 'Vooral de grijze gebieden zijn lastig. Soms is het overduidelijk dat er iets moet gebeuren, zoals in het geval van Freek, maar wat doe je als iemand belt met het verzoek een onflatteuze foto te verwijderen?'

Kinderombudsman Dullaert gaat contact opnemen met eurocommissaris Neelie Kroes (digitale agenda) om te kijken wat er aan de regelgeving moet worden veranderd. 'We hebben meer signalen gekregen van kinderen die het slachtoffer zijn van online-privacyschending. Als er niet snel iets gebeurt, zou het me niet verbazen als het tot een internationale rechtszaak komt.'

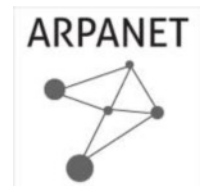


Spam verschuift naar sociale netwerken

Het is 35 jaar geleden dat de eerste spam-mail werd verstuurd. En ook al daalt het aandeel van spam, het blijft een hardnekkig fenomeen. Zeker nu spam meer en meer verschuift naar sociale netwerken.

69 procent. Dat is volgens het gespecialiseerde bedrijf Pingdom het aandeel van spam in het totale e-mailverkeer. Dat lijkt veel, al zit dat cijfer in dalende lijn. Twee jaar geleden was het nog 89 procent.

En dat terwijl weet dat het eerste spambericht al 35 jaar geleden werd verstuurd. Zowat 400 van de destijds 2.600 gebruikers van internet-voorloper ARPANET kregen een ongevraagde mail van marketing manager ene Gary Thuerk van een Amerikaanse computerfabrikant. Hij gaf in de mail informatie over open dagen waar men zijn computersysteem kon bekijken.



Spam beleefde zowat drie à vijf jaar geleden een hoogtepunt, maar lijkt dus op retour. Verfijnde en betere spamfilters en juridische acties hebben ertoe gebracht dat bedrijven spam min of meer onder controle krijgen. Toch is het opletten voor een nieuwe trend: spam die steeds vaker te vinden is op sociale media, als Facebook, Twitter en zelfs Instagram.

Omdat social media vaak nog persoonlijker lijken dan e-mail, spelen spammers daar handig op in. Ze misbruiken het vertrouwen, vermits sociale media-gebruikers vaak een 'echt' bericht denken te zien van een vriend. Sociale media zien het fenomeen met lede ogen tegemoed. Zo sloegen Facebook en Trend Micro al de handen in mekaar en worden posts gefilterd, waardoor spam zoveel mogelijk wordt onderschept.

Voorals Twitter lijkt moeite te hebben met het fenomeen van spam. Het sociale netwerk lijkt niet altijd in staat om kordaat op te treden tegen alle soorten spam die we er tegenkomen. Erg prominent zijn de zogenaamde direct mail-berichten van bekenden met links die u naar bepaalde websites willen leiden, en die eigenlijk als phishing kunnen worden bestempeld.



Twitterspam - te voorkomen?

Beware of Spam Tweets



Uit onderzoek van Fisheye Analytics is op dit moment 7 procent van alle Twittergebruikers een spambot. Waarvoor veel twitteraars door een spambot kunnen worden misleid. Ze denken echt dat ze met een mens te maken hebben. Niet alleen in uw mailbox, maar ook op Twitter en Facebook is het dus opletten voor spam.

E-mail & spam in cijfers

2,2 miljard: aantal e-mailgebruikers wereldwijd,
144 miljard: aantal e-mails dat wereldwijd dagelijks wordt verstuurd,
4,3 miljard: aantal e-mailclients wereldwijd in 2012,
425 miljoen: aantal actieve Gmail gebruikers wereldwijd, 's werelds grootste e-mailprovider is,
69%: percentage van het e-mailverkeer dat als spam gemarkeerd kan worden (was nog 89% in 2010)
50,76%: percentage van de spam afkomstig van pharmaaanbieders, de grootste categorie van alle verstuurde spam.
0,22%: percentage van het e-mailverkeer dat als phishing gemarkeerd kan worden.

Europa begint aan eigen, spionvrije cloud

De blootgelegde af luisterpraktijken van Amerikaanse en Britse inlichtingendiensten hebben geleid tot een groter bewustzijn van cloudsecurity in Europa. In Duitsland zijn de eerste verkenningen gedaan voor een Europese cloud.

In Berlijn is een begin gemaakt met een nieuw EU-project: de ontwikkeling van een eigen Europese cloud die niet toegankelijk is voor de nieuwsgierige neuzen van de NSA.

“Recente beschuldigingen van spionage hebben ons geschokt. Maar ze mogen onze kansen in de cloud niet ontregelen”, zo zei eurocommissaris Neelie Kroes bij de eerste besprekingen voor het EU-project in Berlijn, dat voorlopig de naam Cloud for Europe draagt.

Europees toezicht

Het hoofdidee achter het project is dat er een gereguleerd en beveiligd, continentbreed systeem voor dataopslag komt dat Europese regeringen en consumenten kunnen vertrouwen. Er zal dus een toezichthouder voor moeten worden aangesteld. Deze toezichthouder kan zorgen voor grensoverstijgende privacyregels, die tegelijk ook beter aansluiten op Europese wetgeving.

“95 procent van de clouddiensten die nu worden gebruikt in Europa komt uit een andere juridische omgeving, zonder enige Europese deelname hierin”, zegt president Toomas Hendrik Ilves van Estland, een van de gangmakers achter het project. “Dan geldt het soort security dat andere landen belangrijk vinden, maar niet de beveiliging die voldoet aan de Europese behoeften.”

Elf lidstaten doen mee

Maar makkelijk zal het niet worden om één Europese cloud van de grond te krijgen. Huidige beleid van lidstaten zal geharmoniseerd moeten worden. En wil elke lidstaat eigenlijk wel meedoen? Tot nu toe hebben nog maar 11 van de 28 lidstaten ingetekend voor Cloud for Europe.

Maar Neelie Kroes ziet in dat laatste geen probleem. Ze maakt een vergelijking met de invoering van de euro. “Toen zijn we ook maar met een paar lidstaten gestart. Nu staan de andere nog steeds te kloppen om mee te doen.”



Politie: opbouw Windows XP-exploits in underground



Het Team High Tech Crime van de politie adviseert gebruikers van Windows XP om het besturingssysteem te 'dumpen', gezien er een opbouw van Windows XP-exploits in de 'underground' plaatsvindt. De reactie volgt op berichtgeving dat China wil dat Microsoft XP langer blijft ondersteunen.

"In ons land blijft het advies: dump XP, kies elk ander nieuw systeem", zo laat het Team High Tech Crime via Twitter weten. "Dit is de tijd om te gaan migreren. Wij bespeuren net als China een opbouw van XP-exploits in de underground. Nog 4 maanden te gaan."

Microsoft stopt op 8 april 2014 de ondersteuning van het besturingssysteem. Beveiligingslekken worden daardoor niet meer verholpen. Exploits die na 8 april volgend jaar verschijnen zijn daardoor in principe oneindig houdbaar. "Het is voor veel gebruikers een vervelende situatie", zo laat het politieteam weten.

In oktober riep de politie Windows XP-gebruikers al op Windows XP te verlaten.



Team High Tech Crime
@PolitieTHTC

 Follow

@DennisVNL Wij hielden ook van XP, maar het is een gedoemde liefde.

← Reply ↗ Retweet ★ Favorite ... More

1

RETWEET



5:05 AM - 4 Dec 13

Wordt het versleutelde Syme de Facebook-killer?



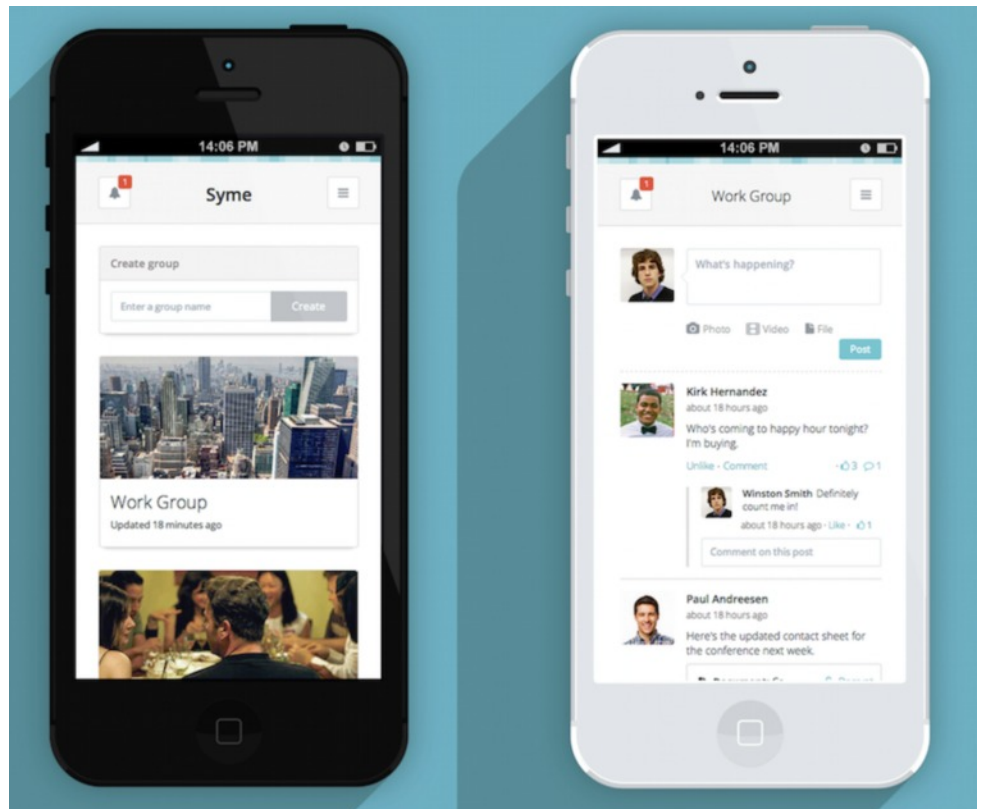
Syme past encryptie toe op alle content, waaronder status-updates, foto's en gedeelde bestanden. Het sociale netwerk slaat zijn data op in Canada en zegt ook zelf geen toegang te hebben.

Het ligt in de lijn der verwachting dat ook het extreem populaire Facebook een opvolger krijgt. Drie Canadese studenten denken het antwoord te hebben op het privacy-inlevermodel van Mark Zuckerberg. Syme is een sociaal netwerk dat alle content versleutelt, zonder dat hiervoor een expertise in encryptie nodig is.

Het platform oogt als Google+ en heeft veel bekende Facebook-elementen, waaronder een eigen variant van de Like-knop. Tot dusver is er een [Chrome-extensie](#) gebouwd en zijn die voor Firefox en Safari in de maak. Hetzelfde geldt voor iOS en Android-apps. Inschrijven werkt via een e-mailadres.

Groepsberichten zoals WhatsApp

Net als ooit op het sociale netwerk van Google moeten Syme-gebruikers eerst worden uitgenodigd. Het platform, vernoemd naar het vrijgevochten karakter uit George Orwells 1984, is nog in bèta. De functionaliteit is nog vrij basic, en doet in veel opzichte ook denken aan die andere Facebook-killer: WhatsApp. Gebruikers kunnen groepsberichten starten en daarbij contacten uitnodigen, die op hun beurt de noodzakelijke de-encryptie-sleutels ontvangen.



De AES-256 en ECC-384 encryptie verloopt via een op JavaScript-gebaseerde browserextensie. Die versleutelt content voordat het gepost wordt. Syme gebruikt daarbij de Stanford JavaScript Crypto Library, een bekende open source-cryptografie component. De inhoud van berichten kan daardoor niet worden onderschept, een deel van de metadata nog wel. De makers benadrukken dan ook dat Syme (nog) niet bedoeld is voor extreem gevoelige berichtgeving.

Voor Obama is BlackBerry nog lang niet passé

(voor ons ook niet.....)

Obama mag nog steeds geen iPhone van de Amerikaanse veiligheidsdiensten gebruiken. Hij is daarom nog steeds van zijn extra veilig gemaakte BlackBerry afhankelijk. Uitzonderlijk omdat BlackBerry Canadees is en Apple Amerikaans.

De Amerikaanse president heeft hard moeten knokken om aan het begin van zijn ambtsperiode in 2009 zijn BlackBerry te mogen behouden. Voor de zekerheid werd deze smartphone toen wel aangepast door beveiligingsexperts. Het als veilig te boek staande apparaat viel aanvankelijk onder de norm voor een president.

Zijn dochters wel

Maar ook Obama wil met zijn tijd mee en wil net als zijn dochters graag een iPhone. Een iPad heeft hij al, dus bekend is hij wel met Apple's iOS. Tijdens een praatje voor een groep jeugdige gasten in het Witte Huis moest hij toch even zijn teleurstelling kwijt. Hij mag geen iPhone. Die is te onveilig, zegt zijn beveiligingsapparaat. Deze publieke bekentenis wordt gemeld door onder meer persbureau AFP en zakenkrant de Wall Street Journal.

Blackberry vs Apple

De Amerikaanse overheid is extra op zijn hoede nadat bekend werd dat de mobiele telefoon van de Duitse Bondskanselier Merkel werd afgeluisterd door de NSA. Misschien heeft de Amerikaanse inlichtingendienst andere mogelijkheden hierdoor wel op ideeën gebracht.

Het blijft opmerkelijk dat de Amerikaanse regering het Canadees, door faillissement bedreigde BlackBerry, prefeert boven het Amerikaanse Apple. Dat bedrijf van wijlen Steve Jobs gaat juist prat op de beveiliging van zijn toestellen. BlackBerry heeft hoe dan ook weer wat street-credit.



Website down of ligt het aan mij?

Iedereen vraagt zich wel eens af: is die website uit de lucht, of ligt het aan mijn verbinding? Deze diensten zoeken onmiddellijk uit of een website voor iedereen onbereikbaar is.



Testen of een website uit de lucht is

Down Or Just Me

Plak het webadres in de balk, en de website wordt getest. DOJ heeft ook een button voor de browser - bookmarklet - om de test altijd bij de hand te hebben.

DOJ.me

Google Apps Status Dashboard

Overzicht van de online diensten van Google, zoals Gmail, Drive, Talk, Agenda en Google Sites. Het wordt vermeld als een dienst uit de lucht is door onderhoud of storing.

Social Down of Not

Overzicht van de *uptime* van grote sociale netwerken, zoals Facebook, Hyves, Twitter en Flickr. Om snel te checken of traagheid of slechte bereikbaarheid aan de website ligt, of aan je internetverbinding.

SOCIAL
DOWN?ORNOT

Dingitsup

Deze website stuurt een e-mail of Twitter bericht als een website weer online is.

Online beveiligingstesten

Is de computer goed beveiligd? Deze gratis tools gaan na of indringers buiten worden gehouden, en controleren bestanden op virussen en malware.



Test de computer

Microsoft Safety Scanner

Deze beveiligingsscanneer gaat na of er virussen, spyware en malware op de computer aanwezig zijn, en kan deze direct verwijderen.

Nederlands: Ja.

Gratis: Ja.

Symantec Security Scan

De Security Scan test de computer op openstaande poorten, veiligheidslekken in Windows en Trojaanse paarden. Ook wordt gecontroleerd of je antivirus programma in orde is.

Nederlands: Ja.

Gratis: Ja.



Update checkers

OutdateFighter

Handig programma dat nagaat of van alle programma's - en Windows - de nieuwste versie draait. Als er nieuwe updates zijn kunnen deze meteen worden geïnstalleerd.

Nederlands: Nee.

Gratis: Ja.



Internetverslaving

Internet heeft zuigkracht: soms is het moeilijk om te stoppen. Maar er zijn goede hulpmiddelen om internetgebruik onder controle te krijgen, en zonodig te beperken.



Zelftest internetverslaving

Zelftest internetverslaving

Online test van Brijder die aangeeft of je internetgebruik riskant is. Afhankelijk van de score in de test worden er adviezen gegeven.

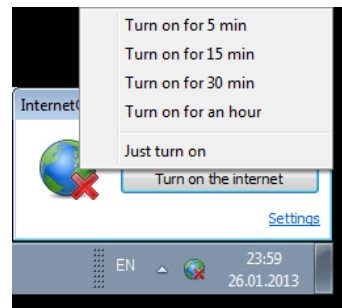
Internet tijdelijk uitschakelen

InternetOff

Dit kleine programma zorgt ervoor dat je internet gemakkelijk aan en uit kan zetten met een knop in de Windows Taakbalk. Je kan ook een periode kiezen - van vijf minuten tot een uur - waarna het internet automatisch wordt uitgeschakeld. Er zitten geen verdere restricties op: je kan het internet met één klik weer inschakelen.

WebCurfew

Deze online dienst geeft een overzicht van alle apparaten met een internetaansluiting in je huishouden, en maakt het mogelijk om daarop het internet te blokkeren. Op elk apparaat afzonderlijk kun je dus het internet aan- en uitzetten.



Monitoren van het internetgebruik

ManicTime

Programma voor *time management* dat bijhoudt welke programma's worden gebruikt, en of je actief bent op de computer. Je kan er ook je werkzaamheden in bijhouden.

Platform: Windows 7, Vista, XP.

Nederlands: Nee.

Gratis: Ja.

MeeTimer

Plugin voor de **Firefox** browser die je internetgebruik in kaart brengt. Je krijgt inzicht in de hoeveelheid tijd die op bepaalde websites wordt doorgebracht.

Platform: Firefox.

Nederlands: Nee.

Gratis: Ja.

Spyware in Windows Media Player

Windows Media Player stuurt gegevens over je kijk- en luistergedrag door naar Microsoft, als je dit niet hebt uitgezet tijdens de installatie. Je kan dit ook later nog uitzetten.



In Windows Media Player 12

Deze mediaplayer is standaard aanwezig in Windows 7 en Windows 8.

- Open Windows Media Player.
- Klik met de rechtermuisknop in de menubalk, en ga naar **Extra - Opties**.
- Ga naar het tabblad **Privacy**.
- Haal alle vinkjes weg, behalve bij 'Rechten voor mediagebruik automatisch downloaden' en 'Klok op apparaten automatisch instellen'.



In Windows Media Player 11 (in Windows Vista en XP)

Deze mediaplayer is standaard aanwezig in Windows Vista en XP.

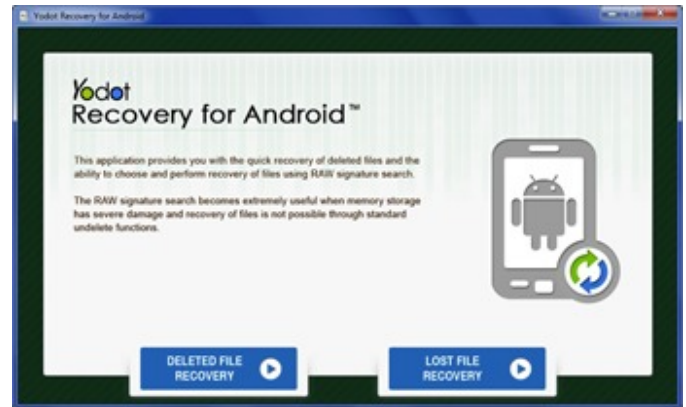
- Open Windows Media Player.
- Klik met de rechtermuisknop in de menubalk, en ga naar **Extra - Opties** of **Meer opties**.
- Ga naar het tabblad **Privacy**.
- Haal alle vinkjes weg, behalve bij 'Rechten voor mediagebruik automatisch downloaden' en 'Klok op apparaten automatisch instellen'.



Oeps, smartphone gegevens gewist.....

Denk aan een scenario waarin u kunt uw SD-kaart van je Android-telefoon verwijderd of geformatteerd door een ongeval? De gegevens van deze is volledig verdwenen en u zich afvraagt hoe ze terug te krijgen. Geen zorgen te maken! Yodot herstel voor Android is een software die je gemakkelijk kan helpen in dit soort situaties.

Yodot herstel for Android is speciaal ontwikkeld om gegevens, zoals muziek, video, audio, .Apk en andere bestanden van uw Android-smartphones te herstellen. De software scant en toont al uw verloren / verwijderde gegevens van je Android-telefoon (tenzij overschreven) met gemak. Bovendien haalt niet alleen de gegevens van de SD-kaart, maar ook van telefoons interne geheugen. Dit programma kan uw verloren gegevens te herstellen binnen enkele minuten.



Hoe de software werkt?

Stap 1: Download en installeer de gratis trial versie van [Yodot herstel](#) for Android in je laptop / pc

Stap 2: Bevestig uw Android-apparaat aan op de PC via USB-kabel

Stap 3: Start de software en volg de commando's op het scherm om de gegevens van je Android-telefoon te herstellen

Stap 4: Kies uit de twee mogelijkheid van herstel; "Deleted Bestand herstel" of "Lost Bestand herstel"

Stap 5: Selecteer het station dat je Android toestel vertegenwoordigt

Stap 6: Wacht tot de software voltooit het scanproces

Stap 7: Nu zal de software alle herstelbare bestanden weer te geven

Stap 8: Voorbeeld van hen naar de gewenste berichten die u wilt herstellen selecteren

Stap 9: Blader naar de plaats van bestemming om uw back-upbestanden

Mijn PC: In deze nieuwe rubriek vertelt een collega welke softwareprogramma's hij of zij gebruikt. Mogelijk zit er een tip voor u bij. Om te beginnen maar mijn eigen PC. Buiten het 'normale computergebruik', gebruik ik hem voor het produceren, mixen en remixen van dance / trance muziek.. Vooral mijn kinderen stellen dit op prijs (mijn vrouw wat minder....)
Productionenamen: DJ Siësta („lijkt mij duidelijk...), DJ Fuego (.. voor het wat steverige werk...) , DoubleYouAB (...mijn initialen....). Via de schatkist kunt u wat voorbeelden downloaden! Gratis natuurlijk....

Besturingssysteem: Microsoft Windows 8 (voorzien van StartMenu 8 - Windows 7 layout) / Linux Mint Cinnamon



Anti-Virus: Free AVG AntiVirus 2014 (gratis)

Mallwarebescherming: Malwarebytes AntiMalware (gratis)



Beveiliging internetbankieren: Trusteer Rapport (ING)

Systeemonderhoud: Ccleaner (gratis), iolo System Mechanic (gratis), Auslogics DiskDefrag (gratis), SlimDrivers Free (gratis)



Brandsoftware: Burnaware Free (gratis), imgBurn (gratis), CloneDVD

DVD bewerken: DVD Shrink



E-mail: Mozilla Thunderbird (gratis)

Browser: Mozilla Firefox (gratis), Epic Privacy Browser (gratis), Pale Moon (gratis)



Medioplayer: VLC Medioplayer (gratis)

Bestandsbeheer: xPlorer2 Lite (gratis), Revo Uninstaller (gratis)



Bestandsconversie: Format Factory (gratis), Freemake Video Converter(g gratis)



Downloaden: Spotnet (gratis), Neswleecher, QuikPar (gratis)
 Freemake Video Downloader (gratis)

Officesoftware: LibreOffice (gratis)



CD/DVD hoezen printen: UnderCover XP (gratis)

Muziekbewerking: Audacity (gratis)



Muziek mixen: MixMeister Pro

Muziek-/video streamen: PLEX Media server (gratis)



Harde schijf indeling: EasUS Partition Master (gratis)

Opstartmanager besturingssystemen: EasyBCD (gratis)

Cloudopslag: Dropbox (gratis) , Skydrive (gratis)



Telefoonsoftware: BlackBerry Desktop Software (gratis)

Navigatie: TomTom Home



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

DoubleYouAB - Beautiful New Years Day (U2 dance-remix)

DJ Siësta - Ocean (eigen productie)

DJ Fuego - Ibiza 2007 (mix)

DoubleYouAB - Fedde LeGrand (remix)

DoubleYouAB - Missing One (mashup remix)

DoubleYouAB - Enigmanized (Enigma club remix)

Twitter handleiding



Dat de jihad steeds meer jongeren aantrekt, is al geen nieuws meer. Dat ze massaal naar Syrië vertrekken, ook niet. Maar dat ze steeds opzichtiger 'flirten' met al-Qaeda, wellicht wel. Janny Groen schrijft in De Volkskrant over het nieuwe fenomeen 'popjihad'. Via sociale media als facebook en instagram, wordt het gedachtegoed razendsnel verspreid, op facebook koop je Al-Qaeda-merchandising en steeds meer profielfoto's tonen openlijk jihadistische symbolen – jihad als lifestyle voor moslimpubers. Audio- en videoboodschappen maar natuurlijk ook foto's worden van websites geplukt, vertaald en via sociale media verspreid. Zo worden steeds meer jongeren 'buiten radicale kringen' bereikt en 'breidt de jihadboodschap zich als een olievlek uit. Groen schrijft verder dat de situatie anno 2013 bedreigender is dan in de tijd van de Hofstadgroep, toen het jihadistisch gedachtegoed nog nauwelijks zichtbaar was. 'De Hofstadjongeren hadden geen sociale media, gepimpte jihadfilmpjes lagen nog niet voor het oprapen'. Volgens de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) is het 'buitengewoon zorgwekkend'. Ook in andere landen neemt de populariteit van de jihad toe.

Uit een peiling op de Volkskrant-site blijkt dat 72% vindt dat symbolen van al-Qaeda, die de jihad verheerlijken, van internet verbannen moeten worden.

In Dresden, Duitsland is politiemann Detlev G. (55) opgepakt die een man zou hebben vermoord met de bedoeling hem op te eten. De twee mannen hebben elkaar online ontmoet op websites die draaien om kannibalisme en morbide vormen van seks. Volgens Bild droomde het slachtoffer (59) ervan te worden opgegeten. Toen hij als vermist werd opgegeven, startte de politie een zoekactie die, via de kannibalenwebsite, bij G. uitkwam. Volgens Bild heeft de politiemann, handschrift-analist bij de politie in de deelstaat Saksen, zijn seksuele fantasieën uitgeleefd en de man vermoord. Het lichaam werd binnen vijf uur in stukken gesneden en begraven op een terrein van de verdachte. Veel delen zijn nog zoek, aldus de politie. In Duitsland werd in 2001 Armin Meiwes opgepakt, de 'internetkannibaal'. Meiwes zocht via internet net zo lang tot hij een slachtoffer vond dat zich wilde laten opeten. Hij liep tegen de lamp toen hij een tweede slachtoffer zocht. Meiwes zit een levenslange celstraf uit.

De AIVD houdt zich aan de wet bij het verzamelen van gegevens van gebruikers van webfora. De dienst reageert op een artikel in het NRC waarin wordt gesteld dat de AIVD inbreekt op (servers van) internetfora en gegevens van alle gebruikers van die webfora verzamelt. 'Vaak zijn dat onbekende personen van wie nog niet is vastgesteld of zij een bedreiging zijn voor de rechtsorde', aldus NRC. Volgens de AIVD inspireert het 'jihadistisch internet' steeds meer tot gewelddadige actie en zijn webfora van jihadisten, gezien de bijzondere bevoegdheden die de dienst heeft, dus een legitiem doelwit. 'De AIVD gebruikt zijn bijzondere bevoegdheden voor het onderzoek naar dergelijke terroristische dreigingen voor onze samenleving', aldus de verklaring. In de Kamer zijn al vragen gesteld.

Het aantal aangiften van mensen die slachtoffer werden bij een nepwinkel op internet, steeg het afgelopen jaar van 2733 naar 8637. De politie traceerde 77 nepwinkels, vaak 'gelikte websites', waar de slachtoffers voor in totaal 1,3 miljoen euro aan spullen kochten maar die spullen nooit geleverd kregen. De politie waarschuwt daarom, met sinterklaas en kerst op komst, goed op te letten. Coördinator Harry Jongkind van het Landelijk Meldpunt Internet Oplichting van de politie, zegt zulke sites 'als paddenstoelen uit de grond' te zien schieten. Volgens het meldpunt haken oplichters handig in op wat veel mensen op het verlanglijstje hebben staan: telefoons, spelcomputers, flatscreens etcetera. Met spectaculaire aanbiedingen via online marktplaatsen lokken de fraudeurs kopers naar sites waar zelfs logo's van keurmerken als Thuiswinkel.org staan zonder dat de aanbieders lid zijn. Ook gebruiken ze iDeal om het vertrouwen van de kopers te winnen. 'iDeal is een betrouwbare partner, maar de verkoper hoeft dat niet te zijn,' waarschuwt Jongkind. Ook Bas Ketelaars van de stichting Stop Internetoplichting waarschuwt kopers. Hij schetst hoe simpel het soms kan zijn om webwinkels te controleren. Zo blijkt webshop HollandsGSM.nl – nieuwe iPhones 4s voor slechts 289 euro – gehuisvest in een leegstaand pand in Eindhoven, wordt hun rekeningnummer voor tal van andere webshops gebruikt en is de telefoonlijn dood. Toch staat de politie vaak machteloos. Verkopers zijn soms lastig te traceren of maken gebruik van mazen in de wet, het verschil tussen strafrecht en burgerlijk recht. Mede daarom heeft PvdA-Kamerlid Jeroen Recourt een initiatiefwetsvoorstel gemaakt dat mensen die aankopen doen via internet beter moet beschermen tegen oplichters. Recourt vindt de huidige wetgeving achterhaald en dat er te weinig instrumenten zijn om oplichters te bestraffen. In zijn voorstel wordt iemand die herhaaldelijk en opzettelijk anderen bij internetverkoop oplicht, strafbaar.

Opvallend veel gedoe rond twitterende wijkagenten deze weken. Zo veroorzaakte een tweet van wijkagent Raymond Vermeer uit Eindhoven een kleine rel op Twitter. Vermeer was kennelijk zo blij met zijn nieuwe dienstwapen, de Walther P99Q, dat hij een foto ervan op twitter zette. 'Hij is veel moderner en James Bond gebruikt hem ook', aldus een blije Vermeer. En dat viel niet bij iedereen in goede aarde, meldt Omroep Brabant. Veel volgers vonden het maar onverantwoord wat Vermeer deed. 'Als u niet beseft wat voor reactie deze tweet kan uitlokken bij jongeren, dan bent u totaal ongeschikt voor deze functie'.

'Sooooo if anything happens to me tonight just let my kids know I loved them dearly', schreef Michelle Rowling (25, uit St Louis) op haar facebookpagina toen ze hoorde dat haar ex-vriendje uit de gevangenis was gekomen. Enkele dagen later vond de politie haar lichaam, nadat burens 911 hadden gebeld vanwege geschreeuw. De ex, Montrell Cooper, was augustus jl nog veroordeeld voor huiselijk geweld. Toen Rowling haar posting deed, riepen vrienden dat ze de politie moest bellen. 'LOL', schreef Rowling terug, 'Im gone. B gone bout time they come'. Cooper heeft zichzelf aangegeven en is inmiddels aangeklaagd voor de moord.

Het CIDI (Centrum Informatie en Documentatie Israël) wil dat Marktplaats meer doet om de verkoop van nazispullen te stoppen. Het is namelijk strafbaar om relikwieën met een nazistisch gedachtegoed of een andere discriminerende boodschap te verkopen, zegt CIDI-directeur Esther Voet. Ze is geschrokken van het aantal nazi-items dat op Marktplaats te koop staat. 'Het lijkt wel een soort industrie te worden.' Ze vindt Marktplaats ook verantwoordelijk en wil graag met de sitebeheerders in gesprek over maatregelen. Een daarvan is de tipknop beter zichtbaar te maken, een ander is dat de site sneller actie onderneemt als een verboden item wordt aangeboden.

Weer een wijkagent in de problemen door een tweet. Toen de politie in Spijkenisse een melding kreeg over een mogelijke hennepkwekerij vonden agenten ... een sm-kamer, vol met seksspeeltjes. Wijkagent Sylvester Kreft meldde de vondst op twitter en kreeg talloze boze reacties. Volgens zijn volgers schond hij de privacy van de bewoners. Een voorlichter van de politie-eenheid zei tegen het AD dat hij 'dit beter niet had kunnen twitteren.' Krefts twitteraccount is onbereikbaar.

De politie Oost-Nederland vindt dat ouders te snel op sociale media melding maken van een vermissing als hun kind niet huis is gekomen. 'Ze slaan dan via facebook en twitter alarm maar vaak is dat loos alarm', aldus de politie. Niet nodig: in de meeste gevallen is de vermiste snel weer terug en bovendien worden persoonlijke gegevens overal onnodig gepubliceerd. In de provincie Gelderland worden maandelijks zeshonderd mensen vermist, vooral tieners die thuis ruzie hadden en vaak weer snel terug zijn. De politie adviseert eerst aangifte te doen en sociale media alleen als alarmering te gebruiken als er echt signalen zijn dat er iets ernstigs aan de hand is.

Na een waarschuwing van politie en OM, zijn op één na alle online-aanbieders van GBL gestopt deze stof te verkopen. GBL (gamma-butyrolacton) is een grondstof voor partydrug GHB, dat sinds vorig jaar op de Opiumlijst staat. September jl kregen 22 exploitanten van webshops waar GBL werd aangeboden een e-mail van politie en OM met het dringende advies te stoppen. Eén webwinkel gaf geen gehoor; een strafrechtelijk onderzoek is het gevolg. Justitie stelde verder vast dat de stilgevallen handel in GBL de prijs van GHB de afgelopen drie maanden flink opgedreven heeft.

Toen wijkagent Jurion Veenstra uit Harderwijk op twitter een foto publiceerde van een dronken man in een cel, waren de rapen weer eens gaar. 'Heerlijk werk met soms mindere kanten. Haha. Ja alcohol maakt meer vies dan je lief is', schreef hij onder meer. Enfin, veel commotie natuurlijk. Sommige volgers vonden de foto -man heeft in broek geplast en overgegeven maar zijn hoofd is niet te zien- maar niks, vanwege privacy en zo, waar anderen juist positief reageerden. Kom op zeg, 'het is geen account van een bloemenzaak', schreef een twitteraar. Een andere schreef 'juist deze openheid' enorm te waarderen. Hoe dan ook, Veenstra moest de foto weghalen. Politiewoordvoerder Wim Dirkx zegt dat 'dit niet de bedoeling is' en dat 'er zeker nog intern over gesproken zal gaan worden'. Veenstra beloofde op twitter vervolgens beterschap. 'Ik zal iets zorgvuldiger omgaan met dit soort situaties'. Naar eigen zeggen wilde hij alleen maar laten zien wat hij in zijn werk allemaal tegenkomt – een van de twitterdoelstellingen van de Nederlandse politie, toch?



Dit magazine verschijnt maandelijks.

De inhoud bestaat uit verzameld werk uit openbare internetbronnen.

Voor zover mogelijk zal de bron worden vermeld.

Opmerkingen kunt u mailen naar [de redacteur](#).

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

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

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

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

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

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

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

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

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

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

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

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

Onderwerpindex 2013

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

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

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

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

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

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

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

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

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

2013-11 > Smaad-Laster-belediging op internet, Stop met gebruik Windows XP, Politie waarschuwt winkeliers voor ransomware, Gebruik het schermtoetsenbord, Nieuwe privacybrowser Epic, Facebook gehackt?, Zoeken op Facebook, Documenten beveiligen, Bitcoin, Trojaans paard in RTF-document, Tool tegen Cryptolocker, Politie adviseert TrueCrypt, Versleutel je USBstick voor onderweg, Hyves stopt red je fotos, Hotspot Shield, Eigenaar van een domeinnaam achterhalen, Profiel van een overledene verwijderen, Beschadigde bestanden herstellen