

Mijn geeltjes ? Kijk op compubuy.jouwpagina.nl



Mei 2015

JAARGANG 4

Secure

Computing

Meer info:
Klik op de hyperlinks!



Veel lees(r)plezier

(NB: met Ctrl+ scrolwielletje kunt u de pagina vergroten en verkleinen. U kunt dus zelf uw leesbaar formaat kiezen.)

[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 snelindex 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, Klikx, Peppermunt.net, PrivacyNieuws, HackInfo, HardwareInfo, Bright, Computerworld

[Politie vereenvoudigt doen van online aangifte](#)

[Internetoplichting via koopsites toegenomen](#)

[Minister laat burgers beelden van misdrijven online zetten](#)

[Gratis ransomware-bevrijding dankzij politie en OM](#)

[Politie gaat cybercrime actief bij hostingbedrijven aanpakken](#)

[Je autokenteken wordt getagd met een RFID-chip](#)

[Telecomgegevens Nederlanders 2 miljoen keer opgevraagd](#)

[Nederlands Foxt-IT detecteert NSA hack](#)

[Malafide Dixon-websites massaal op Marktplaats](#)

[Cybercrimineel laat Apple's OS X en iOS links liggen](#)

[Gratis virusscanners overtuigen op Mac OS X](#)

[6 nieuwe gevaarlijke hacktechnieken](#)

[Is een gemiste zelfscan bij Albert Heijn diefstal?](#)

[Zijn ouders aansprakelijk voor downloads van kinderen?](#)

[Google onthult Password Alert tegen phishingaanvallen](#)

[Nieuwe Tor Browser verbetert veiligheid en gebruiksgemak](#)

[De mythes en feiten rond Androidmalware](#)

[10 tips om je online privacy te beschermen](#)

[Bendeoorlog tussen cybercriminelen](#)

[Leg je elektronische autosleutel in de koelkast](#)

[De 9 beste alternatieven voor WhatsApp](#)

[Schatkist](#)

[Snapshots](#)

[Cops in Cyberspace](#)

[Handig](#)

[Wetsartikelen](#)

Politie vereenvoudigt doen van online aangifte

De politie gaat het eenvoudiger voor mensen maken om via internet aangifte van verschillende misdrijven te doen. Via de website politie.nl is het vanaf 30 april ook mogelijk om aangifte te doen van internetoplichting. Het Meldpunt Internetoplichting (LMIO) is namelijk onderdeel van Politie.nl geworden.



Daarmee worden alle internetaangiftemogelijkheden ondergebracht op één adres. Op dit moment verwerkt de politie al ongeveer veertigduizend internetaangiftes per maand. Dat is ongeveer veertig procent van het totale aantal aangiftes. Politie.nl wordt per maand twee miljoen keer bezocht en mensen doen er ongeveer 34.000 keer per maand online aangifte van diefstal of vernieling en circa 3500 keer van (internet)oplichting.

Volgens de politie is het daarom belangrijk dat het doen van online aangifte duidelijk is voor burgers. De afgelopen maanden is het proces daarom verbeterd, waardoor een online aangifte gemiddeld in tien minuten is af te ronden. De stappen die burgers moeten volgen zijn in een logischer volgorde geplaatst. Zo moet er eerst worden beschreven wat er gebeurd is en wordt er pas daarna naar specifieke informatie gevraagd. Verder is de vormgeving aangepast en zijn de teksten begrijpelijker.

DigiD

De politie laat weten dat de online dienstverlening sterk in ontwikkeling is. Zo wordt er op dit moment bekeken of en wanneer het mogelijk is om aangifte te doen met behulp van DigiD. En dit jaar start een proef met aangifte doen via een tablet met cameraverbinding, zodat mensen dit eenvoudig vanuit huis of werk kunnen doen. Ook kunnen burgers een uitbreiding van het aantal delicten verwachten waarvan via internet aangifte gedaan kan worden. Nu kan dat alleen nog van diefstal, vernieling en (internet)oplichting.



Internetoplichting via koopsites toegenomen

Volgens de [VeiligheidsMonitor](#) van het CBS zijn koopjesjagers op internet 'nog nooit zo vaak bedonderd' als in 2014. Niet alleen zijn er meer websites waarop tweedehands spullen worden aangeboden, fraudeurs gebruiken ook steeds slimmere trucs.

MARKTPLAATS

Het [CBS](#) meldt dat in 2014 maar liefst 490 duizend mensen naar hun geld konden fluiten, 85 duizend meer dan in 2012. Het aantal gedupeerden blijft dus stijgen, ook al doen verkoopsites er van alles aan om oplichting tegen te gaan. Bij Marktplaats zijn 24 mensen in dienst die niks anders doen dan frauduleuze advertenties zoeken en verwijderen. Woordvoerder Jasper Teijsse zegt dat dat helpt. 'Elke dag delen we meldingen van gebruikers met de politie. Advertenties van oplichters kunnen we zo heel snel verwijderen.' Per dag gaat het om 35 foute advertenties, ofwel 0,01% van het totaal. Maar behalve Marktplaats zijn er zo veel andere sites waarop oplichters hun gang kunnen gaan. En omdat veel gedupeerden geen aangifte doen, blijven veel daders ongestraft. In 2014 deden 43 duizend van de genoemde 490 duizend aangifte – overigens ook zonder veel resultaat omdat het Landelijk Meldpunt Internetoplichting (LMIO) niet de capaciteit heeft om alle zaken op te pakken. 'We moeten keuzes maken', aldus meldpunt-projectleider Gijs van der Linden. Het LMIO loste in 2014 in totaal 170 zaken op, vooral grote.

Tips:

De advertentie. Wanneer u een interessante advertentie aanklikt en overweegt om contact op te nemen met de verkoper, moet u een aantal zaken in de gaten houden. Kijk of er foto's aanwezig zijn die het product tonen. Advertenties zonder foto's

mogen gerust als minder betrouwbaar beschouwd worden. Veel oplichters plaatsen wel foto's, maar kopiëren die slechts van andere sites en maken dus zelf geen foto's. Wanneer u ziet dat de foto van het daadwerkelijke product zelfgemaakt is, bevindt u zich al op veiliger terrein. Wanneer u twijfelt aan de authenticiteit van de foto's, kunt u altijd de website Tineye gebruiken. Op deze website kunt u de URL (het linkadres van de foto) invoeren en de website zal vervolgens het internet scannen om de authenticiteit te testen.

Onbetrouwbaar. Negeer te allen tijde advertenties die niet in het Nederlands zijn. Er zijn al teveel mensen door buitenlanders opgelicht. Houd de volgende simpele gedachte aan: buitenlanders hebben met eBay een ander prima platform om hun producten te verkopen. Wanneer u twijfelt aan de betrouwbaarheid van de verkoper, maar toch besluit in zee met hem of haar te gaan, maak dan altijd een 'printscreen' van de advertentie. Oplichters verwijderen nadat het geld binnen is heel vaak hun advertentie om het aantal bewijsstukken te verminderen. Wanneer u op de knop 'Prt Sc' van uw toetsenbord drukt, maakt u een printscreen die u vervolgens kunt plakken in bijvoorbeeld Microsoft Word of Paint. Blijf ook trouw aan uw gevoel: prijzen die zo ontzettend mooi lijken, zijn dat vaak ook! Er worden op Marktplaats veel games voor spotprijzen aangeboden, maar bij na-

vraag zal u vaak te horen krijgen dat het gaat om illegale gekopieerde edities, die u dus niet zomaar kunt afspelen. Ook telefoons die voor spotprijzen worden aangeboden, zijn vaak afkomstig van oplichters. Advertenties met games, telefoons en andere nieuwe mediavormen zijn gevoeliger voor oplichting dan bijvoorbeeld advertenties met boeken. Bedenk vooraf of de kans op oplichting bij het product groot is. Veel oplichters bevinden zich in de kleding- of multimediamarkt.

Contact. U besluit om contact te zoeken met de adverteerder wanneer u in de advertentie geen vreemde zaken heeft opgemerkt. Wanneer u contact met de verkoper hebt, let dan goed op het e-mailadres: adressen van Yahoo, Gmail en Hotmail zijn lastiger te traceren dan e-mailadressen van KPN en UPC. Het is absoluut niet nodig om bij elk lastig verifieerbaar adres het contact te verbreken, maar wanneer u twijfels heeft over de verkoper, zou dit een reden kunnen zijn om er nog eens goed over na te denken.

Het is wijs om zoveel mogelijk informatie over uw verkoper te achterhalen. Vraag naar een telefoonnummer, naam en (zeker bij een groot bedrag) adresgegevens. Achterhaal deze gegevens ook.

Probeer ook zoveel mogelijk face-to-face af te spreken: op deze manier bent u in staat om het product met eigen ogen te aanschouwen en 'gelijk over te steken', waardoor de kans op oplichting vrijwel nihil is.

Verzending. Het is vanzelfsprekend niet altijd mogelijk om af te spreken. Een groot verschil in afstand kan daar een oorzaak van zijn, maar er zijn meerdere redenen te bedenken. Wanneer u besluit dat u het product op laat sturen, onderneem dan de volgende stappen:

Google op de naam van de verkoper. Wanneer u bij één van de sites over oplichting uitkomt, wees dan op uw hoede.

Google ook het bankrekeningnummer van de verkoper. Dit kan waardevolle informatie verschaffen. Het is op Marktplaats de conventie om eerst het bedrag over te maken naar het bankrekeningnummer of het [PayPal](#) adres van de verkoper. Wanneer het geld definitief overgeschreven is, zal de verkoper het product zo snel mogelijk opsturen. PayPal biedt overigens kopersgarantie, waardoor u haast niet opgelicht kan worden!

Vraag het Track & Trace nummer wanneer het product per pakketdienst verzonden is. Het doorgeven van de Track & Trace code voorkomt onduidelijkheid wanneer u onverhoopt niets ontvangt.

Veel oplichters in dit circuit zijn mensen die in gebrekkig Engels de verkoper contacteren en willen betalen aan de hand van een creditcard of via Western Union. Laat de koper via internetbankieren of PayPal betalen en begin niet aan cheques of andere alternatieve betaalmethoden.

Minister laat burgers beelden van misdrijven online zetten

Het is straks toegestaan voor burgers en bedrijven om camerabeelden van een diefstal, inbraak of vernieling op internet te plaatsen. Dat blijkt uit een wetsvoorstel dat minister Van der Steur van Veiligheid en Justitie vandaag naar verschillende adviesinstanties heeft gestuurd.



De verspreiding van camerabeelden is dan niet langer in alle gevallen een zaak van politie en Openbaar Ministerie. Het ministerie van Veiligheid en Justitie verwacht dat door de inzet van deze "extra ogen en oren" de pakkans toeneemt. Nu is het particulieren en ondernemers wettelijk nog niet toegestaan om camerabeelden van verdachten te publiceren. Van der Steur komt met het wetsvoorstel tegemoet aan een wens van de meerderheid in de Tweede Kamer.

Belangrijke rol

Camerabeelden van strafbare feiten kunnen een belangrijke rol spelen bij de opsporing, zo stelt het ministerie. "Dat blijkt ook uit de opsporingsprogramma's van de overheid, die een selectie van camerabeelden gebruiken. Daar staat tegenover dat bedrijfsleven en particulieren in ruime mate beschikken over bewakingscamera's en smartphones." De gemaakte opnamen zouden goede aanknopingspunten bieden om misdrijven op te lossen.

De minister wil die mogelijkheden benutten door de wet aan te passen en gebruik te maken van moderne communicatiemiddelen. "We vragen al langer hulp van burgers bij de opsporing; dan moeten we ze ook de mogelijkheden bieden die bij deze tijd passen", aldus Van der Steur. Het gebruik van camerabeelden moet wel zorgvuldig gebeuren.

Van der Steur wil dan ook voorkomen dat de "verkeerde" verdachte in beeld wordt gebracht of onschuldige omstanders en slachtoffers herkenbaar zijn. Straks moet eerst aangifte zijn gedaan van het betreffende delict. Ook moeten de camerabeelden ter beschikking zijn gesteld aan de politie. Omdat de identificatie van de vermoedelijke dader vooropstaat, moeten het misdrijf zelf én de vermoedelijke dader duidelijk te zien zijn op de beelden.

Kennissen

Het is niet toegestaan om beelden op internet te zetten van kennissen of klasgenoten die zich schuldig hebben gemaakt aan bijvoorbeeld vernieling, omdat hun identiteit reeds bekend is. Ook is het niet de bedoeling dat particulieren en bedrijven beelden van zware criminaliteit als moord, doodslag en mishandeling openbaar maken. Die worden door politie en justitie zelf afgehandeld. In het geval de identiteit van de daders is achterhaald moeten de gepubliceerde beelden weer worden verwijderd, voor zover dat binnen de mogelijkheden van de publicist ligt.

Gratis ransomware-bevrijding dankzij politie en OM

Slachtoffers van een recente ransomware-variant hebben hoop op gratis redding. De gratis ontsleuteltool die Kaspersky biedt, is te danken aan actie van de Nederlandse politie en het Openbaar Ministerie (OM).



De Nederlandse politie en het Openbaar Ministerie (OM) hebben namelijk bij een inbeslagname in Nederland twee databases met decryptiesleutels in handen gekregen. De politie biedt die sleutels gratis en per gebruiker aan via een samenwerking met Kaspersky Lab. Die Russische leverancier van securitysoftware heeft een speciale site opgezet waar slachtoffers van de CoinVault-ransomware terecht kunnen. De site NoRansom vereist geen log-in maar slechts het uploaden van een van de bestanden die door CoinVault zijn versleuteld.

Upload, controle en ... bevrijding

Vervolgens controleert de database achter de website of de encryptie op dat vergrendelde bestand overeenkomt met één van de sleutels in de buitgemaakte databases. Is dat het geval, dan krijgt het slachtoffer de unieke sleutel voor zijn of haar eigen bestanden. Kaspersky biedt op de speciale reddingssite ook gratis de benodigde applicatie die het ontsleutelen verzorgt.

Kaspersky werkte al samen met het Team High Tech Crime (THTC) van de Nederlandse politie en het OM aan de opsporing van cybercriminelen. De nu net opgespoorde afperser zet CoinVault in om gegevens van gebruikers, waaronder ook Nederlanders, te versleutelen en dan losgeld te eisen. Naar schatting zijn er zeker 700 Nederlandse slachtoffers en even zoveel in het buitenland, waaronder Duitsland en de Verenigde Staten.

Vooraf op Nederland gericht

De ransomware is op mensen afgevuurd via een valse e-mail, die is verstuurd aan honderden adressen in ruim twintig landen. Daarbij lag de nadruk op Nederland, meldt de politie. De dader bleek ook servers in Nederland te benutten. Die machines en de software daarop zijn in beslag genomen, waarbij het THTC twee databases met decryptiesleutels heeft aangetroffen. Via de zogeheten smart coalition waar Kaspersky al deel van uitmaakte, zijn die reddingsgegevens gedeeld met de Russische securityleverancier.



[Index](#)

Politie gaat cybercrime actief bij hostingbedrijven aanpakken

De politie gaat cybercrime dit jaar actief bij Nederlandse hostingbedrijven aanpakken. Vorig jaar startte de Nationale Politie, de Autoriteit Consument en Markt (ACM), het Openbaar Ministerie en de Technische Universiteit Delft het project Nederland Schoon.



Het project heeft als doel om gezamenlijk met hostingbedrijven cybercrime aan te pakken waarbij het gebruik van de infrastructuur van Nederlandse hostingbedrijven een belangrijke rol speelt.

In de brief stelt de politie dat het nu tot "concrete acties" overgaat. In samenwerking met de TU Delft is namelijk in kaart gebracht welke hostingproviders door cybercriminelen worden gebruikt. Volgens de politie zijn veel hostingbedrijven al goed op weg om cybercriminaliteit tegen te gaan. "Sommige hostingproviders spelen een faciliterende rol bij cybercriminaliteit. Het kan zijn dat u zich als hostingbedrijf niet bewust bent van uw faciliterende rol", aldus de brief.

Daarom gaat de politie onder andere in gesprek met hostingproviders die volgens de meting van de TU Delft hoger scoren dan hun branchegeenoten. De door de TU ontwikkelde methodiek is goedgekeurd door de branchevereniging DHPA. Ook zal de politie middels een vragenlijst in kaart brengen welke best practices hosters toepassen op het gebied van het weren van cybercrime. De politie stelt dat de gesprekken binnenkort worden ingepland en hostingproviders geen actie hoeven te ondernemen en zelf voor een gesprek worden uitgenodigd.

Infrastructuur

De aanwezigheid van één van de grootste internetknooppunten ter wereld en een professionele en volwassen hostingbranche zorgen er onder andere voor dat Nederland wereldwijd bekendstaat als belangrijk 'hostingland' van digitale data. Volgens de politie trekt dit niet alleen bonafide partijen aan, maar ook minder bonafide partijen. "Daardoor is Nederland bovengemiddeld vaak een uitvalsbasis voor uiteenlopende vormen van cybercrime", zo laat de politie weten.

Het gaat onder andere om het verspreiden van malware, het onderbrengen van kinderporno, het versturen van phishing- en spamberichten en het stalen van gestolen data. Via Nederland Schoon hoopt de politie samen met hostingproviders



Je autokenteken wordt getagd met een RFID-chip

De kans is groot dat binnen enige jaren het kenteken van je auto is getagd met een RFID-chip, voor de juiste identificatie natuurlijk en als echtheidsmerk. Fraudeurs vallen door de mand.



Om fraude met kentekens tegen te gaan is de toepassing van een [RFID-chip](#) een mogelijkheid die wordt onderzocht. Dat zegt minister Van der Steur van Veiligheid en Justitie tegen de Tweede Kamer. Eerst wordt een test gedaan met nieuwe chips, daarna gaat de minister be- zien of het als kentekentoepassing wordt doorgevoerd.

Een nieuw soort RFID-chip

Drie aanbieders van "een nieuw ontwikkelde passieve RFID-chip" gaan een jaar lang een praktijktest doen met de chip op het Opleidings- en Trainingscentrum van het Ministerie van Defensie in Oirschot. De test start op 1 juni van dit jaar. Het nieuwe aan de chip is blijkbaar dat die alleen kan worden uitgelezen door "daartoe bevoegde personen of instanties die in het bezit zijn van een gecertificeerde reader met een hoog beveiligingsniveau." De praktijktest moet gaan uitwijzen of de chip altijd en overal goed is uit te lezen. Daarnaast wordt er een uitgebreide securitycheck gedaan.

Overigens is er al eerder gesproken over RFID-chips in kentekenplaten. TNO en de Rijksdienst voor het Wegverkeer waren al in 2011 helemaal voor en in 2013 werd er nog op Europees niveau over gesproken.

Het bewaren van vernietigde kentekens

Op dit moment zijn er nog omslachtige methoden om fraude tegen te gaan. Zo is daar de nogal cryptisch door Van der Steur omschreven bewaarplicht. Letterlijk zegt Van der Steur: "Het invoeren van de bewaarplicht leidt ertoe dat bij de export en sloop van voertuigen de vernietigde platen (of delen daarvan) moeten worden be- waard als bewijs van inname. Door een bewaarplicht van vernietigde kentekenplaten in te voeren, kan hier (steekproefsgewijs) op worden gecontroleerd." Hoe ken- tekenplaten na vernietiging nog kunnen worden be- waard, vermeldt de bewindsman niet.



Telecomgegevens Nederlanders 2 miljoen keer opgevraagd

In 2014 is 2 miljoen keer informatie opgevraagd over de eigenaar van een telefoonnummer of ip-adres. Dat is opnieuw iets minder dan een jaar eerder.



Dat blijkt uit de cijfers uit het jaarverslag van het Centraal Informatiepunt Onderzoek Telecommunicatie ([CIOT](#)), dat donderdag is gepubliceerd.

De instantie geeft opsporingsdiensten toegang tot persoonsgegevens die staan opgeslagen bij telecom- en internetproviders. Als een ip-adres kinderporno heeft verspreid, kan de politie zo bijvoorbeeld de bijbehorende internetgebruiker vinden.

In 2013 werd 2,08 miljoen keer de gegevens van de eigenaar van een telefoonnummer of ip-adres opgevraagd. In 88 procent van de gevallen leverde het verzoek ook daadwerkelijk gegevens op.

In totaal zijn er 3,36 miljoen antwoorden verstrekt. Het is mogelijk dat er meerdere antwoorden aan een vraag te koppelen zijn. Hierdoor zijn er meestal meer antwoorden dan opvragingen.

Oost-Nederland

De politie Oost-Nederland heeft de meeste gegevens opgevraagd. In totaal vroeg de eenheid 412.679 keer om gegevens over de eigenaar van een telefoonnummer of ip-adres.

Op de tweede en derde plek staan de politie-eenheden van Den Haag en Amsterdam met respectievelijk 314.442 en 253.694 opvragingen.

2013 en 2012

In 2013 werd er 2,3 miljoen keer informatie opgevraagd over de eigenaar van een telefoonnummer of ip-adres. In 2012 was dit aantal nog 2,7 miljoen.



Nederlands Foxt-IT detecteert NSA hack

Het Nederlandse beveiligingsbedrijf Fox-IT heeft een manier ontdekt om de geavanceerde Quantum Insert-hack van de Amerikaanse geheime dienst NSA te detecteren.

Dat meldt Fox-IT op zijn blog. De NSA gebruikt Quantum Insert om internetverkeer te injecteren met kwaadaardige software tijdens het surfen. De hackmethode kwam eind 2013 aan het licht door klokkenluider Edward Snowden.

Quantum Insert werd door de NSA gebruikt om doelwitten in het Midden-Oosten te bespioneren, maar uit gelekte Snowden-documenten blijkt dat de Amerikaanse geheime dienst de hackmethode ook heeft ingezet om medewerkers van de Belgische telecomdienst Belgacom te hacken. Daarmee kon de NSA het Europese telefoonverkeer af luisteren.

Fox-IT, die Belgacom hielp bij het ontdekken en ruimen van de NSA-malware, heeft nu een manier ontdekt om de Quantum Insert-hack te detecteren. De hack werkt middels speciale servers die dichtbij de computer van een doelwit staan en een malafide website tonen, net voordat de legitieme website wordt geladen.

Hoe Quantum Insert werkt

Zo toonde de NSA bijvoorbeeld een malafide LinkedIn-pagina van een Belgacom-medewerker als degene naar zijn eigen LinkedIn-pagina wilde surfen. Daarvoor werden onder andere het ip-adres, Gmail-account, profielen op sociale netwerken en Skype-account van de medewerker geïdentificeerd.

Op het moment dat de NSA-servers een zogeheten get-

request ontvangen, waarmee de computer van het doelwit een specifieke website opvraagt, worden de servers direct geactiveerd om een malafide website van het origineel te tonen - net iets sneller dan de server van de legitieme website.

Vervolgens installeert de NSA-server onopgemerkt malware op de computer van het doelwit.

Detectie Fox-IT

Als de NSA-server een malafide website voorschotelt, ontvangt de browser van het doelwit na de get-request twee antwoorden: één van de NSA-server en daarna één van de originele website. De browser negeert normaliter het tweede antwoord.

Beide antwoorden van de servers lijken veel op elkaar, maar verschillen toch een beetje. Als beide antwoorden van dezelfde legitieme website komen, zijn de datapakketten echter precies hetzelfde. Door het kleine verschil tussen de antwoorden van de servers kan Fox-IT een dergelijke Quantum Insert-hack detecteren.

Op de codewebsite Github heeft Fox-IT een toevoeging voor het gratis opensource-beveiligingssoftwarepakket Snort gepubliceerd. De software kan worden geüpdatet met de code van Fox-IT om Quantum Insert-hacks te detecteren.

Malafide Dixon-websites massaal op Marktplaats

Criminelen hebben allerlei domeinnamen met de naam van Dixons geregistreerd en via zo'n 25.000 advertenties op Marktplaats.nl en Zehands.be gebruikt om internetgebruikers op te lichten.



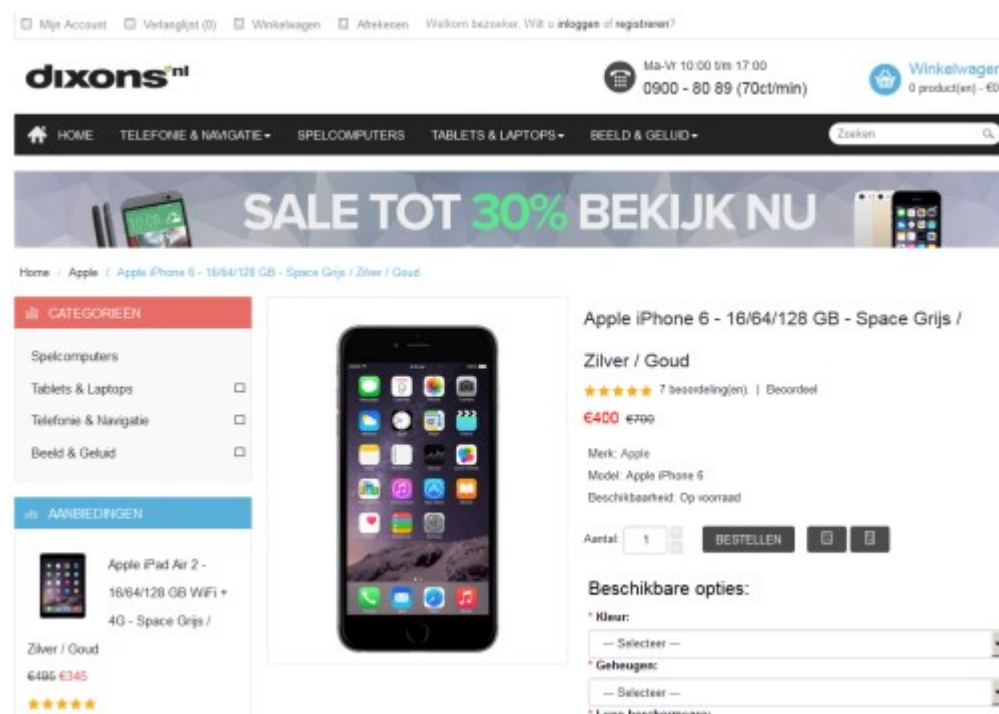
Het gaat onder andere om dixons-aanbieding.com en dixons-discounter.com, aldus gebruikers van de website. Via Marktplaats werden tienduizenden spectaculaire aanbiedingen voor onder andere de Apple iPhone 6 verspreid.

"Naast haar scherp geprijsde assortiment trakteert Dixons haar bezoekers ook op een dagaanbieding: Dixons Today. Door de combinatie van grote aantallen en de juiste inkoopkanalen kan Dixons producten voor zeer scherpe prijzen aanbieden. Om deze reden kan Dixons via Dixons Today iedere dag weer een verrassend product voor een waanzinnig lage prijs ten toon stellen", aldus de oplichters in de advertenties. De advertenties werden geplaatst met Marktplaats-accounts die soms al jaren actief waren. Volgens een moderator van Opgelet op Internet gebruiken de oplichters hiervoor gehackte Marktplaats-accounts.

"Ik ben helaas zo dom geweest om op deze website een ibook air te bestellen (van 609,- euro) Via een marktplaats account (8 jaar actief) leek de site betrouwbaar",

aldus een gedupeerde gebruiker. "Toen de bestelling raar liep (er was iets fout gegaan in het systeem) en mij werd gevraagd nogmaals het bedrag over te maken werd mij duidelijk dat het om een oplichter ging." De gebruiker deed aangifte en kreeg vandaag bericht dat het account van Marktplaats is verwijderd.

Andere slachtoffers melden hoe ze een GoPro (279 euro), PlayStation 4 (275 euro), Philips Hue starterskit (100 euro) en een iPhone 6 (400 euro) via de website kochten. Een andere gebruiker had meer geluk. Hij wilde gisteravond via de malafide website een iMac Mini bestellen, maar zijn bank, de Rabobank, hield de betaling tegen omdat er geen geldig rekeningnummer zou zijn opgegeven. De politie liet eind vorig jaar nog weten dat het regelmatig malafide webwinkels offline haalt, onder andere van Dixons.



Cybercrimineel laat Apple's OS X en iOS links liggen

Ook in de tweede helft van 2014 is er nauwelijks malware voor de platformen van Apple verschenen, zo blijkt uit cijfers (pdf) van het Finse anti-virusbedrijf F-Secure. Voor Mac OS X werden in de laatste zes maanden van 2014 slechts 17 unieke malware-exemplaren ontdekt.



Het ging om zestien backdoors en één "rogue". Vijf van de malware-exemplaren waren afkomstig van drie nieuwe families, waaronder "Wirelurker", die zich op Chinese softwarepiraten richtte en waarvan de vermoedelijke auteur eind vorig jaar door de Chinese autoriteiten werd opgepakt. Verder was de Ventir-backdoor nieuw vorig jaar, alsmede de XLSCmd-familie die bij gerichte aanvallen werd ingezet. Deze laatste malware kan toetsaanslagen opslaan en screenshots maken.

Voor iOS ontdekte F-Secure maar drie aanvallen, namelijk een PDF-exploit die vorig jaar september bekend werd gemaakt, de eerder genoemde Wirelurker-malware en XSSER. De XSSER-malware werkte alleen op gejaillbreakte toestellen, terwijl de PDF-exploit een lek in oudere iOS-versies gebruikte. Een aanvaller die via deze exploit ook willekeurige code op het toestel wil uitvoeren moet ook over een tweede kwetsbaarheid beschikken. Of er aanvallen via de PDF-exploit hebben plaatsgevonden is onbekend.

De hoeveelheid malware voor iOS en Mac OS X steekt schril af tegen de hoeveelheid malware voor Android en Windows. Voor Android verschenen er in de laatste helft van vorig jaar 61 nieuwe malware-families en honderden unieke exemplaren. F-Secure geeft voor het Windowsplatform geen overzicht van nieuwe malware-families en exemplaren, maar uit andere rapporten blijkt dat het hier om miljoenen gaat. Wel laat de Finse virusbestrijder zien dat de 7 jaar oude Confickerworm nog steeds de actiefste malwaredreiging voor Windows is.



Gratis virusscanners overtuigen op Mac OS X

Mac OS X heeft met veel minder malware te maken dan Windows, zoals onlangs nog uit een rapport van het Finse anti-virusbedrijf F-Secure bleek. Toch zijn er ook dreigingen voor Apple's besturingssysteem, die zich voornamelijk via illegale software en het downloaden van software uit verkeerde bron weten te verspreiden.



Aanleiding voor het Duitse testorgaan AV-Test om tien gratis en betaalde virusscanners voor OS X te testen.

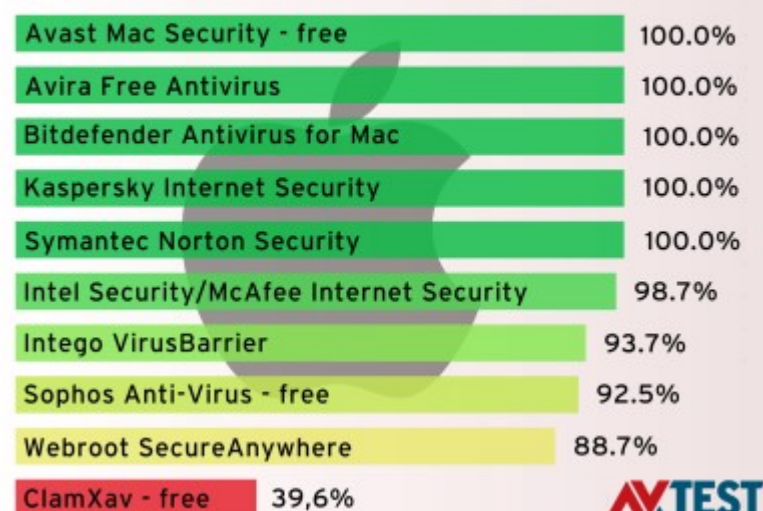
"Criminelen zoeken altijd naar groepen die het waard zijn om van te stelen. De inmiddels groot geworden groep Mac-gebruikers is nu een goed doelwit", zegt Maik Morgenstern van AV-Test. Voor de test werd er naar verschillende onderdelen gekeken, zoals de detectie van malware, false positives, systeembelasting en features. Voor de detectietest werd gewerkt met een "on-demand" scan en een "on-access" scan. Voor deze twee tests werden in totaal 244 malware-exemplaren gebruikt.

Gemiddeld weten de scanners 91% van de malware te detecteren. Dit percentage wordt vooral door ClamXav naar beneden gehaald, dat respectievelijk 36,6% en 54,7% scoort. De overige virusscanners zitten boven de

88%, waarbij Avira en Symantec voor beide tests zelfs 100% scoren. Avira is echter een gratis product. Ook de gratis virusscanner van Avast weet met een score van 100% en 98,8% te overtuigen.

Als het gaat om systeembelasting zet Symantec de beste score neer. Het kopiëren van 26,6GB aan bestanden duurde zonder scanner 66,1 seconden. De virusscanners deden er gemiddeld 75,4 seconden over. Symantec zit daar met 66,2 seconden ruim onder, terwijl Intego met 97,9 seconden de grootste belasting voor het systeem vormt. Wat betreft "false positives", het onterecht beschouwen van schone bestanden als malware, ging geen enkele scanner in de fout. Op ClamXav na werden alle virusscanners door AV-Test gecertificeerd. Hieronder de uitslag van de on-demand scan.

Test: 10 Security Suites for Mac OS X (On-Demand Test):



AVTEST

[Index](#)

6 nieuwe gevaarlijke hacktechnieken

Experts hebben tijdens de RSA conferentie nieuwe aanvalstechnieken op een rijtje gezet, en dus een belangrijke trend waar we de komende jaren mee van doen krijgen.



Nieuwe trends, nieuwe aanvallen, nieuwe modus operandi van de slechteriken. Tijdens de RSA-conferentie besprak een panel van experts de verwachte problemen voor het komende jaar en daaruit kwamen de volgende 6 gevaarlijke trends die door Information-Week op een rijtje zijn gezet..

1. Het afvangen van Kerberos-tickets

Kerberos is een netwerkauthenticatieprotocol dat standaard gebruikt wordt door Windows-servers, waarbij de client zich aanmeldt in het Windows-domein. Het is ook mogelijk het Kerberos-protocol te gebruiken voor UNIX-gebaseerde systemen, zoals OS X, Solaris, AIX en grote Linux-distro's. De hacktruc zit hem erin dat je de ticket die uitgewisseld wordt door client en server (dat het versleutelde wachtwoord van de gebruiker bevat) afvangt.

Volgens Ed Skoudis van SANS Institute maakt het niet uit of je als hacker toegang hebt tot een client of een server, zolang je maar in het domein zit. Vervolgens steel je alle Kerberos-tickets van de client die door de server van een authenticatiestempel zijn voorzien. Die zijn tien uur geldig, waarin de aanvaller vrij spel heeft.

2. Doelgerichte aanvallen op ICS en SCADA

De industriële systemen die aan het internet hangen zijn maar magertjes beveiligd tegen indringers en daar wordt steeds meer gebruik van gemaakt. Aanvallers zoeken nu naar specifieke systemen waarvoor zij op maat gesneden exploits maken en kopen. Daarbij wordt rekening gehouden met specifieke taken die de systemen kunnen uitvoeren.

Ook nieuw is het aanvalsvertrekpunt. Gezocht wordt naar een systeem dat met de ICS communiceert en waarvan de netwerkrelatie door het ICS wordt vertrouwd. Door het andere systeem over te nemen kan daardoor makkelijker worden binnengedrongen in het ICS-doelsysteem.

Dat houdt in dat aanvallers phishingaanvallen uitvoeren op technici die met hun eigen systeem toegang hebben tot de doel-ICS.

Ook worden zogeheten drinkplaatsen gecreëerd, watering holes, op sites waar veel technici komen. Verder zoeken aanvallers naar manieren om ICS-bestanden te infecteren met trojans die bedoeld zijn om mee te gaan met bijvoorbeeld een systeemupdate, zodat die infecties makkelijker door een firewall heenkomen.

3. Encryptie wordt een aanvalsmethode

Nu al wordt versleuteling gebruikt in aanvallen, zie de toename aan ransomware. Maar die methode wordt steeds verfijnder, zegt Johannes Ullrich van SANS Institute. Tot voor kort was een aanval via ransomware nog een probleem voor de consument, maar er valt veel meer geld te halen in het bedrijfsleven. Zo wordt er onder meer gekeken naar het versleutelen van backups bij grote bedrijven, die nu nog versleutelde gegijzelde data kunnen vervangen via de backup. De eerste aanvallen op NAS-systemen hebben zich al voorgedaan.

4. Meer aanvallen op het Internet of Things

Steeds meer apparaten hangen aan het bedrijfsnetwerk, waaronder de eigen smartphones, tablets en notebooks van het personeel. Voeg daarbij printers en WiFi-routers en het

hackparadijs is compleet. Doordat ieder apparaat ook nog eens een verschillende versie van software met zich meedraagt en door het ontbreken van een patchbeleid ook nog eens kwetsbaar zijn voor aanvallen op oudere kwetsbaarheden, is het voor de aanvaller steeds makkelijker om tot een bepaald niveau van het netwerk door te dringen.

5. Aanvallers gebruiken gestolen data slimmer

Aanvallers die in het bezit komen van (bedrijfs)data gaan daar steeds slimmer mee om. Zo kozen de aanvallers van Sony voor een periodieke publicatie van informatie die ze van de servers van Sony hebben gestolen en kiezen ze daarvoor per keer een publicatiekanaal. Daardoor weet het getroffen bedrijf nooit wanneer er welke informatie naar buiten komt en is er qua public relations geen enkele verdediging tegen. Publieke vernedering is Sony's deel geworden, niet 1 keer, maar herhaaldelijk.

6. DDoS-aanvallen worden heftiger en slimmer

DDoS-aanvallen op het netwerk? De meeste bedrijven en organisaties weten er alles van. Maar de aanvallers gaan nu een stapje verder en pakken specifieke applicaties aan. Dat kan met veel minder data, op wat Ullrich noemt een layer-7-niveau van een denial-of-service. De data die op een applicatie wordt afgevuurd is veel minder dan bij een DDoS, en blijft vaak onder de radar, maar de applicatie krijgt te veel informatie om nog goed te kunnen reageren. Daardoor wordt de applicatie feitelijk onbruikbaar gemaakt.

Is een gemiste zelfscan bij Albert Heijn diefstal?

Onlangs zijn de voorwaarden van het zelfscannen van Albert Heijn gewijzigd. Er staat nu in dat je diefstal pleegt als achteraf blijkt dat niet alles gescand is. Maar mag AH wel zo kort door de bocht aannemen dat hun systeem onfeilbaar is? Het zou immers zomaar kunnen dat een gebruiker tegen een bug aanloopt, waarbij het systeem 'bleep' doet als indicatie dat het product gescand is, maar het product niet op de virtuele kassabon terecht is gekomen.



In de voorwaarden van de app staat nu:

Blijkt bij controle dat niet alle producten zijn gescand nadat u uw (mobiele) Bonuskaart bij de betaalpaal hebt gescand, dan beschouwen wij dit als diefstal en kunnen wij aangifte doen.

Dat klinkt nogal streng, want er wordt inderdaad geen ruimte gelaten voor de situatie dat er wél is gescand maar dat niet is geregistreerd. Ook niet voor situaties waarin je oprecht vergeten was iets te scannen, hoewel dat natuurlijk geen sterk argument is als je bij de uitgang van een supermarkt staat.

Echter, het is niet zo dat je een strafbaar feit begaat enkel omdat iemands algemene voorwaarden zeggen dat dat zo is. Natuurlijk mag men aangifte doen als men meent dat je iets strafbaars hebt gedaan, maar de inhoud van je contract met het bedrijf is daarbij niet relevant.

Je steelt als je iets wegneemt met de bedoeling je dat toe te eigenen zonder te betalen. En die bedoeling moet bewezen worden. Enkel dat je met een product in je handen buiten staat, is daarvoor niet genoeg. Je kunt

iets vergeten zijn te scannen, of de software werkte niet goed. Die opties moeten worden uitgesloten voordat men kan bewijzen dat je het product stiekem wilde meenemen.

Een aanvullend punt is nog hoe het zit met de broncode. Zonder de broncode van de zelfscan-app kun je niet bewijzen hoe deze werkt, dus dan sta je zwak als je wilt aantonen dat er een bug in de software zit. Dat is een lastige. Er is geen recht om broncode van bewijsmiddelen op te eisen. De enige manier is een kennis nogmaals eenzelfde set aankopen te laten doen en dat filmen om zo vast te leggen dat hij vaker die fout maakt. Maar als het een eenmalige bug was (of afhankelijk van de stand van de maan in combinatie met het aantal mobiele telefoons in de buurt én het feit dat de rozijnen in de bonus waren) dan wordt dit wel heel moeilijk inderdaad.



Zijn ouders aansprakelijk voor downloads van kinderen?

Kinderen blijken stiekem films te downloaden via Popcorn Time. Nu weet je dat je hiermee uit illegale bron downloadt, dus is het verboden maar stel dat Brein hierachter komt, ben je dan aansprakelijk voor hun downloadgedrag?



Downloaden uit illegale bron is juridisch gezien een onrechtmatige daad, niet anders dan iemands auto bekrassen of een bal door de ruit schoppen. En voor die laatste daden heeft de wet voor kinderen een bijzondere regeling.

Kinderen tot 14 jaar zijn zelf niet aansprakelijk voor schade die zij anderen toebrengen (art. 6:164 BW). Daar heeft een benadeelde rechthebbende dus niets te halen. Bij een kind van 14 tot 18 jaar mag dus gewoon een claim worden ingediend, hoewel natuurlijk de vraag is of er wat te halen valt.

Ouders van minderjarige kinderen tot zestien jaar zijn meestal aansprakelijk voor wat die kinderen doen. De wet onderscheidt twee situaties (art. 6:169 BW):

1. Het kind is nog geen veertien jaar. Dan zijn de ouders aansprakelijk als sprake is van 'doen', oftewel een actieve handeling. Downloaden is een doen, en hiervoor zijn dus de ouders van de veertienminner aansprakelijk. (Bij een nalaten, zoals niet waarschuwen dat er een gevaarlijke situatie is, is kind noch ouder aansprakelijk.)

2. Het kind is veertien maar nog geen zestien. De ouders zijn nu aansprakelijk (voor doen én nalaten) tenzij het hen niet kan worden verweten dat zij niet ingegrepen hebben om dit te beletten.

Bij kinderen onder de veertien is het dus eenvoudig: de ouders zijn aansprakelijk, net zoals ze zijn als ze zelf had-

den zitten downloaden. Bij kinderen vanaf zestien jaar zijn de ouders niet aansprakelijk.

Bij de tussencategorie krijg je dus de vraag: had je als ouder moeten voorkomen dat je kinderen gaan downloaden of torrenten? Of is dit iets dat kinderen van die leeftijd gewoon doen, en dus voor hun eigen rekening moet komen?

We hadden ooit een zaak waarin auteursrechtsschending door een kind aan de ouders werd verweten. De rechter vond dat niet gepast: bij een vijftienjarige is het normaal dat hij een website heeft en daar foto's op zet, dus valt het de ouders niet te verwijten dat ze de auteursrechtinbreuk door foto-overname hebben laten gebeuren.

Als een website bouwen op je vijftiende al normaal is, dan is downloaden dat al helemaal. Het staat zelfs in de Donald Duck, en als het daarin staat dan is het volledig aanvaard in de maatschappij. Dus in die leeftijdscategorie ben je niet aansprakelijk voor downloadgedrag van je kind.



Google onthult Password Alert tegen phishingaanvallen

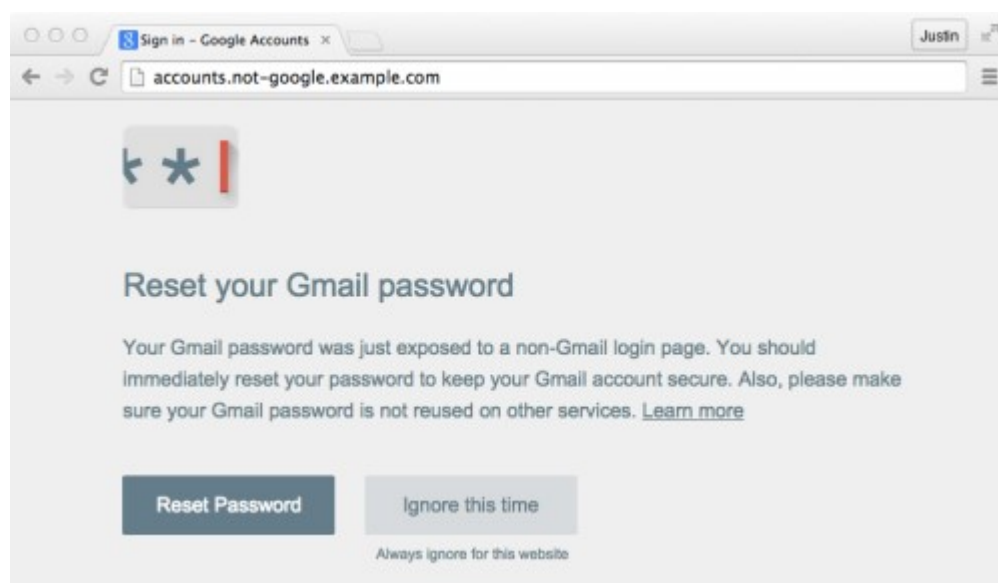
Om te voorkomen dat internetgebruikers het wachtwoord van hun Google-account op phishingsites invoeren heeft Google recentelijk een nieuwe beveiligingsmaatregel onthuld.



["Password Alert"](#) is een Chrome-extensie die gebruikers waarschuwt als ze hun Google-wachtwoord op een phishingsite invullen.

De extensie, die open source is, moet gebruikers zowel tegen phishingaanvallen beschermen als het gebruik van verschillende wachtwoorden voor verschillende websites aanmoedigen. Zodra de extensie in Chrome is geïnstalleerd zal die een gecodeerde versie van het wachtwoord opslaan. Google omschrijft dit als een "salted reduced-bit thumbnail". De extensie bewaart deze informatie alleen voor veiligheidsdoeleinden en zal die niet met anderen delen. Google merkt op dat Password Alert geen keylogger is en geen toetsaanslagen opslaat of die doorstuurt.

Chrome beschikt al over "Safe Browsing" om gebruikers voor phishingaanvallen te waarschuwen, maar het kan zijn dat er phishingsites worden gemist. Password Alert zal elke keer dat een gebruiker zijn Google-wachtwoord op een website invult die niet accounts.google.com is alarm slaan en vertellen dat de gebruiker zijn wachtwoord moet wijzigen. Iets wat direct via de waarschuwing kan worden gedaan. Op dit moment is Password Alert alleen voor Chrome-gebruikers beschikbaar.



Nieuwe Tor Browser verbetert veiligheid en gebruiksgemak

Er is een geheel vernieuwde versie van de Tor Browser verschenen die veel gebruiksvriendelijker is dan voorgaande versies en daardoor meer internetgebruikers moet aanspreken.



Tor Browser bestaat uit een aangepaste versie van Firefox en software om verbinding met het Tor-netwerk te maken.

Via het Tor-netwerk kunnen gebruikers hun werkelijke IP-adres afschermen en wordt het webverkeer versleuteld zodat internetproviders niet kunnen zien welke websites er worden bezocht. Hoewel veel mensen zeggen privacy belangrijk te vinden maken gemiddeld 2,5 miljoen mensen gebruik van het Tor-netwerk. Om dit aantal te vergroten zijn in Tor Browser 4.5 allerlei grote veranderingen doorgevoerd.

Zo zal de Windowsversie van Tor Browser nu automatisch aan het Start Menu/Applicaties worden toegevoegd, zodat de browser eenvoudiger is te vinden en te starten. Het gaat hier trouwens alleen om een snelkoppeling, de installatie zelf is nog steeds een "portable app". Verder is ook het Tor-menu en de bijbehorende configuratievensters vereenvoudigd. Zo geeft het menu nu informatie over het gebruikte Tor Circuit en biedt de optie om een nieuw Tor Circuit aan te vragen.

Security Slider

Op het gebied van security is de "Security Slider" toegevoegd. Door de slider te verschuiven kunnen gebruikers de veiligheid aanpassen. Hoe hoger de slider, hoe kleiner het aanvalsoppervlak en worden er features uitgeschakeld waar in het verleden allerlei kwetsbaarheden zijn gevonden. Ook is de Windowsversie nu gesigineerd. Daardoor krijgen Windowsgebruikers geen waarschuwing meer dat Tor Browser van een onbekende bron afkomstig is.

[Tor Browser 4.5](#) bevat een lange lijst van allerlei aanpassingen, bugfixes en andere verbeteringen. De browser is via deze pagina te downloaden. Sinds versie 4.0 beschikt Tor Browser ook over een automatische updatefunctie. Vanwege de grote veranderingen in versie 4.5 zal deze versie pas over een week onder gebruikers van versie 4.0 via de automatische updatefunctie worden verspreid.



Rond het Android-ecosysteem hangen heel wat onfrisse verhalen over te lakse veiligheid en een overaanbod aan malware. Maar klopt dat wel? Neen, zeggen Google-ingenieurs.



De reputatie van Android op het vlak van cyberveiligheid is niet de allerbeste. Maar is er een groot verschil tussen reputatie en werkelijkheid? Op de RSA-conferentie in San Francisco zei Adrian Ludwig, hoofd van Android Security bij Google, alvast dat dat verschil er zeker is. Volgens Ludwig zijn er heel wat mythes over veiligheid in Android en malware in het algemeen: de verspreiding van kwaadaardige software neemt almaar toe, veel mobiele toestellen zijn niet beschermd en alle malware kan de toestellen binnendringen. Die stellingen kloppen niet, argumenteert Ludwig. Bijna alle gebruikers zijn standaard beschermd zodra ze hun toestel aanzetten, mobiele malware kan geclassificeerd en geïsoleerd worden en het aantal stukken mobiele malware neemt ook niet toe.

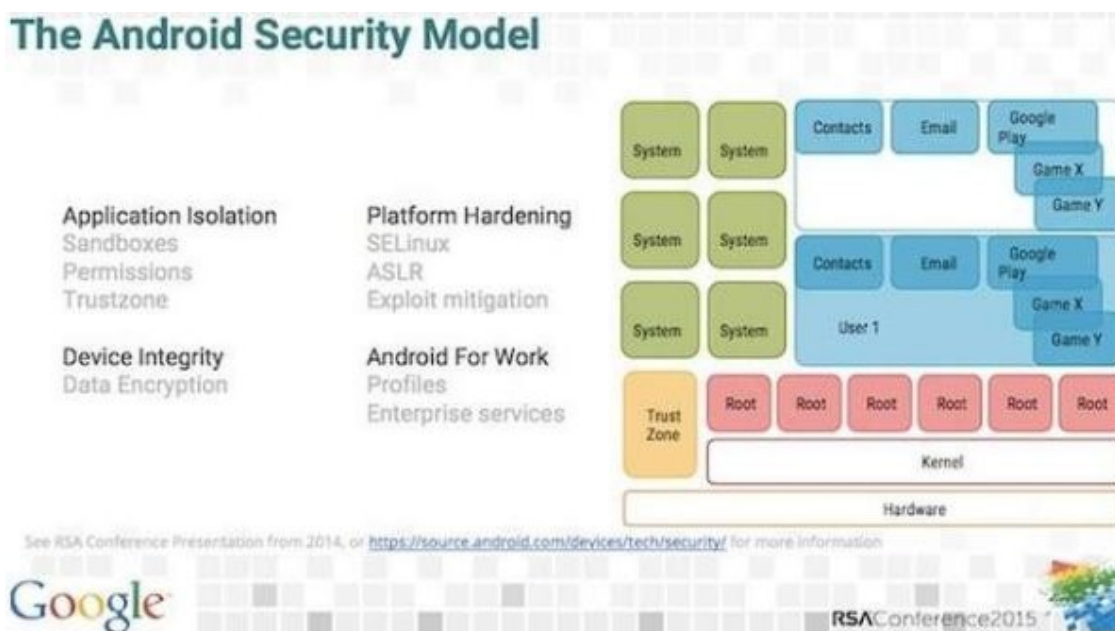
De aanpak van Google om zijn platform veilig te houden, is simpel, aldus de securityspecialist: neem de beste veiligheidstools die er zijn (wat ze ook kosten) en maak die diensten dan gratis zodat andere er verder kunnen op bouwen.

Om zijn stelling kracht bij te zetten, bracht Ludwig een slide mee met daarop een schematische voorstelling van hoe Google een en ander concreet aanpakt: het Android Security Model. Op het eerste zicht lijkt het op de typi-

sche verzameling diagrammen van elk ander security-model: versterking van het platform, applicaties die geïsoleerd worden, de integriteit van het apparaat dat wordt onderzocht en bedrijfstoepassingen (in dit geval: Android for Work).

Bij de initiële manieren om gebruikers veilig te houden, zitten onder meer het verifiëren van apps in de Play Store en het Android Safety Net, dat vorig jaar meer dan een miljard apparaten heeft gescand en gecontroleerd. Op minder dan één procent van de onderzochte apparaten werd een Potential Harmful App (PHA) gevonden, aldus Google. Het aantal geïnstalleerde PHA's daalde in 2014 met meer dan 50 procent, voert Ludwig aan. Specifieke spyware daalde met meer dan 90 procent.

Al zijn er ook wel enkele uitzonderingen. In wat Ludwig “regionale variaties” noemde, blijken China en Rusland twee landen te zijn waar het aantal PHA’s een stuk hoger ligt. Er valt ook geen echte lijn te trekken in het soort kwaadaardige software dat wordt aangetroffen, het verschilt van dag tot dag en van regio tot regio. Soms is het één slechte app die voor moeilijkheden zorgt, soms is het een hele familie van apps die een bepaald doelwit in het vizier nemen, zoals een bank.



10 tips om je online privacy te beschermen

Je kan vandaag niet meer online gaan zonder dat je surfgedrag door tientallen bedrijven en organisaties in kaart wordt gebracht. Tien privacytips.



1. Pas je privacy-instellingen aan. Stel je browserinstellingen zo in dat cookies na afsluiten van de browser automatisch verwijderd worden. Wis ook regelmatig je browsergeschiedenis.
2. Gebruik de privémodus. Wil je geen sporen achterlaten van je surfgedrag, maak dan gebruik van de incognito- of privémodus in je browser. De browser houdt dan niet bij waar je overal online geweest bent. Lees ook ons artikel "Acht andere redenen om incognitomodus te gebruiken".
3. Installeer een browserextensie. Een browserextensie als Ghostery houdt bij welke bedrijven je allemaal online proberen te volgen, en blokkeert hun toegang tot je informatie. Lees ook ons artikel "Drie tools om je surfgedrag geheim te houden" voor meer suggesties.
4. Gebruik een privacyvriendelijke zoekmachine. Google haalt heel wat informatie uit uw zoekgedrag, en geeft dat door aan adverteerders. Bent u daar niet mee opgezet, gebruik dan een privacyvriendelijke zoekmachine zoals [DuckDuckGo](#).
5. Gooi je Facebookprofiel toe. Neem je privacy-instellingen op Facebook onder de loep, zodat je weet wie er allemaal toegang heeft tot de informatie die je deelt op het sociale netwerk. Schroef ze wat strakker aan indien nodig.
6. Pas op met cadeaus en aanbiedingen. Online komen we heel wat kortingen en andere aanbiedingen tegen, vaak in ruil voor ons e-mailadres en andere informatie. Pas op met wat je deelt met dergelijke kortingsites, en ga eerst na of je ze wel vertrouwt.
7. Schakel locatiediensten uit. Deze tip geldt in de eerste plaats voor smartphones of tablets. Schakel de locatiediensten uit als je niet wilt dat Google en Facebook via de gps in je toestel kunnen nagaan waar u overal bent geweest.
8. Vermijd publieke wifinetwerken. Gratis wifi is fijn, maar niet altijd even veilig. Je weet nooit wie er allemaal kan meekijken via een onbeveiligd wifinetwerk. Probeer publieke netwerken daarom te vermijden.
9. Denk twee keer na voor je iets online plaatst. Als je iets online plaatst op Facebook, maak dan eerst even de volgende analogie: "Zou ik deze informatie tijdens een avondje uit ook luidop voor alle klanten in het café verkondigen?"
10. Blijf offline. Misschien een beetje drastisch, maar als je niets over jezelf prijs wilt geven online, dan is er maar één oplossing: trek de internetkabel uit je computer, verwijder je Facebookprofiel en leef een anoniem offline bestaan.



Bendeoorlog tussen cybercriminelen

De topcriminelen op het internet hebben elkaar de oorlog verklaard. Twee bendes proberen elkaar in de luren te leggen met onder meer phishingmails. Het gaat om Naikon en Hellsing, waarbij de eerste de aanval opende op de tweede, maar die had dat op tijd door en slaat nu terug.



De oorlog tussen de rivaliserende criminele bendes werd ontdekt door Kaspersky. Het beveiligingsbedrijf kreeg een phishingmail onder ogen die gestuurd bleek te zijn door Hellsing en kreeg interesse erin toen bleek dat het doel van de phishingcampagne een andere bende betrof, namelijk Naikon. Verder onderzoek wees uit dat Hellsing slechts reageerde op een eerdere aanval van Naikon.

The Empire Strikes Back

Kaspersky noemt de reactie van Hellsing "The Empire Strikes Back" en volgde de oorlog tussen de beide rivalen terug naar februari 2014. Volgens Kaspersky is het in het verleden wel eens vaker voorgekomen dat rivaliserende bendes elkaar troffen in APT-aanvallen, maar dat was eerder toeval in een grotere campagne. Maar nu wordt gericht op elkaar geschoten.

Dat Hellsing zich laat verleiden tot een dergelijke aanval op Naikon is opmerkelijk, zegt Kaspersky. Hellsing is zeer selectief in het uitkiezen van zijn doelen en is waar-

schijnlijk slechts bij 20 organisaties binnengedrongen.

De organisatie is extreem goed in het onzichtbaar opereren, in tegenstelling tot Naikon. Die Aziatische bende werd bekend van het versturen van phishingmails na het verdwijnen van het vliegtuig MH370, toen werd getracht informatie binnen te hengelen over de vordering van het onderzoek naar het vliegtuig.

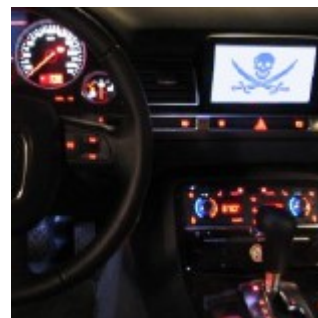
Hellsing geeft zich bloot door bendeoorlog

Juist doordat Hellsing heeft gereageerd op de aanval van Naikon konden onderzoekers van Kaspersky de bende in kaart brengen. "Zonder die aanval was Hellsing waarschijnlijk nog een onbekend en duistere organisatie gebleven", zegt Kaspersky. Onbekend is of het Hellsing is gelukt binnen te dringen in de Naikon-organisatie.

[Klik hier](#) voor de film en ontdek wat het met het verdwenen toestel van Maylesian Airlines te maken heeft.....

Leg je elektronische autosleutel in de koelkast

Autodieven gebruiken een goedkope en simpele manier om dure auto's te stelen: door het signaal van het slot te versterken, leggen ze contact met de sleutel die binnen ligt.



Een man zag hoe een dief zijn Prius opende met een zwart kastje en ging op onderzoek uit. Hij kreeg nul op het rekest van de plaatselijke politie, Toyota wist van niets en een beveiliging vermoedde dat het kastje een brute force-aanval uitvoerde. Maar het gaat mogelijk om een verrassend simpele aanval: via een signaalversterker.

Door het signaal te versterken, legt het slot contact met de sleutel die in dit geval op het aanrecht van het slachtoffer lag, legt Zwitserse beveiligingsexpert Boris Darné uit. Zo'n versterker kost een paar tientjes, waardoor de ROI voor een autodief erg hoog ligt. In de regel kun je ervan uitgaan dat de eigenaar van een geparkeerde auto zich in een van de huizen in de buurt bevindt.

Faraday biedt uitkomst

De methode om je te beschermen tegen de methode is dan ook om sleutels te bewaren in een kooi van Faraday. In het geval van dit slachtoffer: zijn koelkast. De politie van Toronto waarschuwt al jaren na een reeks diefstallen van auto's waarbij het slot onbeschadigd bleef om extra voorzichtig te zijn met slimme sloten. De Canadese autoriteiten adviseren om de auto bij voorkeur niet op straat, maar in een garage te zetten.



De 9 beste alternatieven voor WhatsApp

[WhatsApp](#) staat op bijna iedere smartphone. Ook na de overname van Facebook bleef de messaging-app razend populair. Wil je toch iets anders, dan zijn hier 9 alternatieven.



[Telegram](#)

Telegram hamert op snelheid, veiligheid en privacy. Vooral die laatste twee zijn voor veel WhatsApp-gebruikers een reden geweest om de app even te proberen nadat Facebook WhatsApp heeft overgenomen. Ondanks de goede beoordelingen van de app is het nog lang geen bedreiging voor WhatsApp.

[Line](#)

De van oorsprong Japanse app [Line](#) heeft honderden miljoenen gebruikers en is populair in Azië. Vooral het gebruik van stickers en de groepsgesprekken vallen in positieve zin op. Er zijn ook versies voor de iPad, Mac en pc.

[Facebook Messenger](#)

In potentie heeft [Facebook Messenger](#) het grootste bereik omdat alle Facebook-gebruikers er meteen gebruik van kunnen maken. Met de aparte chat-app kun je zelfs niet-Facebook-leden uitnodigen. Maakt ook gebruik van stickers en laat je makkelijk spraakberichten verzenden.

[WeChat](#)

Net als Line heeft [WeChat](#) honderden miljoenen actieve gebruikers en is het vooral populair in Azië. Het zit propvol functionaliteit zoals je mag verwachten zoals videochats, groepsgesprekken, stickers en het verzenden van spraakberichten. Door je iPhone te schudden kun je contact leggen met onbekenden.

[Viber](#)

Volgens de makers heeft [Viber](#) meer dan een half miljard gebruikers, maar we weten zeker dat Nederland niet tot de grootge-

bruikers behoort. Toch kan de app er prima mee door, met veel games, openbare chats met bijvoorbeeld beroemdheden, stickers en videobellen.

[Kik](#)

De messagingapp [Kik](#) doet voor veel concurrenten onder qua hoeveelheid mogelijkheden, maar biedt wel een degelijke chat-omgeving voor één-op-ééngesprekken of groepsgesprekken. Erg handig aan Kik is dat je geen telefoonnummer hoeft in te voeren, maar het volstaat om een gebruikersnaam aan te maken.

[Skype](#)

Het grote voordeel van [Skype](#) is dat veel mensen het gebruiken en je de gesprekken die op de Mac en pc voert op je iPhone kunt vervolgen. De dienst heeft wel geregeld moeite met het synchroniseren van berichten en de integratie met bijvoorbeeld Outlook.

[Hangouts](#)

[Hangouts](#) van Google bestaat al weer even en wordt geregeld voorzien van nieuwe functionaliteit, maar blijft het toch vooral goed doen als videochatdienst voor op de Mac of pc. Is natuurlijk wel aan te raden als je Hangouts op de computer al gebruikte en graag veel Google-apps raadpleegt.

[Threema](#)

Als je je grote zorgen maakt over je privacy tijdens chats, is [Threema](#) het overwegen waard. De app moet in tegenstelling tot concurrenten aangeschaft worden, maar gebruikt bijvoorbeeld end-to-end-encryptie om berichten te beveiligen. Na verwerking van een bericht wordt deze van de Threema-server verwijderd.



[Index](#)



Software schatkist

De kist is gevuld met fraaie software. Nieuwsgierig?

Open de kist middels de sleutel en ontdek.....





De Consumentenbond werkt vanaf deze week samen met Opgeletoptinternet.nl, de website die dagelijks speurt naar verdachte online advertenties en domeinnamen. De bond zal 'Nepshops-Alerts' op de site plaatsen, tweets over nep-webshops. Zo'n systeem zou nodig zijn omdat nepshops steeds lastiger te onderscheiden zijn van echte. De bond start tegelijkertijd de campagne Wijzer WebWinkelen, die streeft naar een betere bescherming van consumenten bij onlineshoppingen.

Internetbedrijven als KPN, Ziggo/UPC en Leaseweb hebben harde kritiek op de manier waarop het kabinet online jihadisme wil aanpakken. Onuitvoerbaar, zeggen ze. Zowel strafrechtelijk als qua vrijwillige medewerking van providers. De ministers Asscher en (toen nog) Opstelten beschreven in hun Actieprogramma Integrale Aanpak Jihadisme hoe ze 'radicaliserende, haatzaaiende jihadistische' uitingen op internet wilden aanpakken. Essentieel daarin was dat de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) zou proberen de internetsector 'mee te krijgen'. Dat overleg is totaal mislukt, zegt senior jurist Alex de Joode van Leaseweb. 'Kabinet en NCTV willen ons in de frontlinie plaatsen van de online jihadbestrijding. Die vlieger kan niet opgaan'. Ook KPN en Ziggo 'weigeren de rol als politieagent'. En dus faalt de beoogde online jihadbestrijding, schrijft Computerworld. Vooral omdat providers, eigenlijk al sinds de beginjaren van internet, rond 1995, zich niet geroepen voelen een 'verlengstuk van justitie' te zijn. Bij meldingen over onrechtmatigheid zijn ze voorzichtig: bij twijfel niet offline halen. 'Van criminele sites kunnen wij dat nog wel beoordelen maar bij jihadistische sites niet', zegt De Joode. De taal is een probleem maar ook de uitingen. 'Op zichzelf meestal niet onrechtmatig, maar als onderdeel van rekrutering wellicht wel. Dat kunnen wij onmogelijk beoordelen'. Een tweede probleem ontstaat als het OM de provider tot actie dwingt of wil dwingen – overheids-censuur? Geen officier die daar zijn handen aan brandt.

Lino E., de man die in 2005 zijn vriendin Simone in haar slaap doodstak, daarvoor tot celstraf en tbs werd veroordeeld, probeert in kort geding te bereiken dat zijn naam niet meer vindbaar wordt bij Google. Hij wil niet dat informatie over zijn verleden op internet gevonden kan

worden, het zou hem hinderen bij het vinden van werk. Informatie over de man is onder meer te vinden op de website van de Federatie Nabestaanden Geweldslachtoffers (FNG), maar die weigert de teksten te verwijderen. Volgens FNG-voorzitter Jan van Kleeff – vader van Simone – is E. niet de enige dader die probeert zijn criminele verleden op internet te verhullen, zeker na de uitspraak van april 2014 van het Europese Hof proberen er meer dat. Van Kleeff noemt het echter een principekwestie. 'Wij houden het recht op herinnering levend'. Nog geen maand geleden vonniste het Gerechtshof Amsterdam dat die uitspraak niet geldt voor veroordeelde criminelen.

Je kunt nu [een M-melding](#) ook online doen. Meld Misdaad Anoniem is een proef gestart om melding te doen via smartphone, tablet of computer. Omdat steeds meer mensen (mobiel) online zijn, zegt directeur Titus Visser. 'We spelen in op deze trends in de maatschappij'. Online meldingen gaan via een formulier dat versleuteld wordt verzonden, waardoor de afzender onbekend is. Medewerkers van M. sturen bruikbare informatie vervolgens door naar de politie of andere opsporingsinstanties, het formulier wordt daarna vernietigd. Volgens Visser is die aanpak uniek. 'Anonimiteit gaat verder dan melden via een eenmalig fake-mailadres en een verzonden naam, wat je regelmatig ziet. Onze werkwijze is zo ingericht dat uit de informatie die de politie of andere partners via M. ontvangen niet is af te leiden wie deze informatie heeft doorgegeven en of dat online of telefonisch is gebeurd. Zo blijft de melder anoniem'.

Advertentiesite Marktplaats krijgt gemiddeld twintig keer per maand een verzoek van gemeenten en sociale diensten om informatie te verstrekken over adverteerders. Een jaar terug was dat nog vijftien keer per maand. Volgens het tv-programma De Monitor zijn er steeds meer mensen van wie de uitkering wordt stopgezet of gekort. Want wat voor de een hobby is, is voor sociale diensten soms gewoon handel. Een voorbeeld uit het programma is de vrouw die 850 euro verdiende met de verkoop van enkele jonge raskatjes – niet opgegeven en dus uitkeringsfraude? Marktplaats zegt alleen die verzoeken in te willigen als ze het wettelijk verplicht is. De gegevens betreffen dan de advertentiegeschiede-

nis, niet of iets ook echt verkocht is.

Onderzoekers hebben een nieuwe ransomware-variant ontdekt die opvalt doordat het Amerikaanse computers opzettelijk niet infecteert. [CryptOLocker](#), zoals de ransomware heet, is volgens onderzoekers van Bleeping Computer een variant van de bekende TorrentLocker-ransomware.

Deze ransomware-familie sloeg eind vorig jaar ook in Nederland toe. CryptOLocker blijkt dezelfde communicatiemethodes als TorrentLocker te gebruiken en versleutelt allerlei bestanden, die gebruikers vervolgens voor honderden euro's kunnen laten ontsleutelen. Als slachtoffers niet op tijd betalen wordt het losgeld verdubbeld.

Waarom CryptOLocker Amerikaanse computers vermijdt is onbekend. In het verleden kwam het voor dat Russische cybercriminelen geen Russische computers infecteerden, om zo niet de aandacht van de Russische autoriteiten te trekken. De nieuwe ransomware is inmiddels in Europa, Azië en Australië opgedoken en verspreidt zich via e-mails die zich voordoen als verkeersovertredingen of overheidsberichten.

Onlangs heeft er een aanval op werkzoekenden plaatsgevonden waarbij er malafide vacaturemails uit naam van het [UWV](#) waren verstuurd, zo laat UWV-topman Bruno Bruins weten. De e-mails waren zowel naar klanten van het UWV als mensen zonder uitkering gestuurd en waren voorzien een vacaturetekst.

Wie reageerde kreeg een e-mail dat er een "assessment" moest worden gedaan, wat online kon. Hiervoor moest er wel eerst een programma worden gedownload, wat 99 euro kostte. In de mail werd gesteld dat het UWV hiermee had ingestemd en deze kosten zou vergoeden. Zowel de vacature als het programma bestonden niet en het geld werd zodoende naar oplichters overgemaakt. Bruins laat in de Telegraaf weten dat de oplichters door snel ingrijpen niet veel hebben kunnen uitrichten.

Zo heeft het UWV de domeinen van waaruit de e-mails werd verstuurd inactief laten maken en zoveel mogelijk benaderde klanten ingelicht en gewaarschuwd. "Betaal nooit voor sollicitaties, hoe aantrekkelijk de functie ook mag zijn. Maak geen geld over voor een assessment, een online test, een tegemoetkoming voor sollicitatiekosten, of wat dan ook", adviseert Bruins.



Hackers, online dieven en andere internetoplichters voelen zich in Nederland 'bijzonder goed op hun gemak', schrijft Metro. Nederland staat vierde op de lijst van landen met cybercrime – zo komt 3% van alle cybercrime en 8% van alle spam wereldwijd van 'polderservers'. Volgens beveiligiger Symantec staat Nederland zo hoog vanwege het grote internetknooppunt AMS-IX in Amsterdam: veel bandbreedte, veel webhosting. Nederland kan wel meer doen om het cybercriminelen moeilijker te maken, zegt Tom Welling van Symantec. Belangrijker nog is bewustwording: 'Menselijk handelen is nog steeds een zwak punt in de defensie tegen cyberaanvallen en criminaliteit'.

Een geheel ander verhaal komt van Mark van Staalduinen (TNO) en Roeland van Zeijst (Nationale Politie) die juist beweren dat cybercriminelen Nederland links laten liggen. Criminelen zouden via het dark net met elkaar communiceren en elkaar waarschuwen om hun criminele activiteiten juist niet in Nederland of op Nederlandse verbindingen uit te voeren. Volgens hun onderzoek omzeilen cybercriminelen Nederland vanwege de goede reputatie en enkele succesvolle acties van het Team High Tech Crime.

Misdaad van de toekomst? De politie heeft bij Paleis Huis ten Bosch een bestuurder van een drone op heterdaad betrapt. De drone vloog in de no-fly zone bij het paleis en is in beslag genomen. De 'bedienaar' van de drone kreeg een proces-verbaal, twitterde de politie.

De politie in Edinburgh, Schotland heeft een nieuw wapen in de strijd tegen de criminaliteit: Lego. Agen-

ten bouwen met Legosteentjes verschillende situaties na, maken daar een foto van en twitteren die. In een poging mensen bewuster te maken van de risico's van woninginbraken en andere delicten. De ene keer is het Lego-figuurtjes is een boef, de andere keer een agent. De campagne is op sociale media al door meer dan 350 duizend mensen gezien, aldus een trotse projectleider. 'Sociale media geven ons de mogelijkheden informatie te geven hoe je crimina

Omdat de jeugd op [Instagram](#) zit, moet de politie daar ook op. Dat zei landelijk projectleider Ed Sabel van het Mobile Media Lab. Volgens Sabel moet de politie zich voortdurend aan nieuwe communicatiemiddelen aanpassen. En omdat jongeren tegenwoordig minder actief zijn op facebook en meer op Instagram, moet de politie mee. Het mobiele lab, een grote witte politietruck, rijdt sinds oktober 2014 door Nederland om burgers op een laagdrempelige manier in contact te laten komen met de politie. Veel burgers weten nog nauwelijks hoe modern de politie tegenwoordig is, met de website, politie-apps, duizenden twitteraccounts en honderden Facebookpagina's. In het lab wordt ook getest hoe online aangifte gaat. 'We ontdekten dat ouderen vaak niet weten wat swipen is. Ze drukten hard op het scherm. In plaats van dat wegvegen hebben we de buttons in pijltjes veranderd'.

Europol waarschuwt dat het opsporen van beveiligingen tegen de nationale en Europese veiligheid steeds moeilijker wordt. De 'gesofisticeerde en versleutelde online communicatie' die terroristen gebruiken, levert grote problemen

op bij het traceren en monitoren van (potentiële) terroristen, helemaal als ze ook nog eens van ondergrondse netwerken gebruikmaken. Versleutelde communicatie is volgens Europol 'de hoeksteen' van terroristische operaties. En dat begint al bij WhatsApp! Het grote publiek vindt dat overigens helemaal niet erg. Niet alleen Edward Snowden toonde aan hoe inlichtingendiensten 'hun voeten vegen' met privacywetten en -regels. Europol werkt in ieder geval aan de komst van een 'European Internet Referral Unit' die terroristische websites moet identificeren en verwijderen.

Amerikaanse ambtenaren en personeel van opsporingsdiensten zijn door het Internet Crime Complaint Center (IC3) van de FBI gewaarschuwd voor cyberaanvallen door [hacktivisten](#). Het gaat dan met name om "doxing", waarbij er allerlei persoonlijke informatie over iemand wordt verzameld en gepubliceerd. Volgens de FBI kunnen "hacking collectieven" publiek beschikbare informatie gebruiken om politieagenten of functionarissen, hun werkgevers en hun familie te identificeren. "Deze groepen moeten dan ook hun online aanwezigheid en blootstelling beschermen", aldus de waarschuwing. Het gaat dan vooral om de informatie die mensen via social media over zichzelf en anderen delen.

Gebruikers van social media krijgen daarom het advies om persoonlijke informatie die ze op dit soort netwerken plaatsen te beperken, te onthouden dat het internet een "openbare bron" is, de privacy instellingen van de betreffende websites te controleren, sterke wachtwoorden te gebruiken en het privacybeleid van social mediasites te lezen.

Phishing- / valse e-mails melden

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

ING Bank: valse-email@ing.nl

Rabobank: valse-email@rabobank.nl

SNS Bank: valse-email@sns.nl

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

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

Websites banken

[ABN AMRO](#)

[LeasePlan Bank](#)

[Argenta](#)

[Rabobank](#)

[Credit Europe Bank](#)

[SNS Bank](#)

[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



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

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 vervalzers, 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 groeiindustriën

op internet'.

Relevante wetsartikelen zijn:

[Artikel 1 Wks](#): wet op de kansspelen

[Artikel 1a Wks](#): piramidespelen

E-fraude.

'De essentie van fraude is steeds dezelfde: mensen eigenen zich middels bedrog geld of vermogensbestanddelen toe waarop ze geen recht hebben en tasten daardoor de rechten van anderen aan. Er zijn verschillende

begrippen in omloop om de cybervorm van fraude te beschrijven, zoals fraude in e-commerce en internetfraude. 'Bij deze vorm van fraude wordt het internet gebruikt om op oneigenlijke wijze gelden, goederen en diensten te verkrijgen zonder daarvoor te betalen of tegenprestaties te leveren'.

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

[Artikel 326 WvSr](#): oplichting.

[Artikel 225 WvSr](#): valsheid in geschrifte.

[Artikel 231b WvSr](#): identiteitsfraude

[Artikel 310 WvSr](#): diefstal.

[Artikel 321 WvSr](#): verduistering.

[Artikel 416 WvSr](#): heling.

