



Juni 2015

JAARGANG 4

Secure

Computing

Meer info:

Klik op de hyperlinks!



Veel lees(r)plezier

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



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

[Facebook informatie voor politie en justitie](#)

[Telecomgegevens gebruiken voor opsporing](#)

[Geen verbod op bellen, sms'en en appen op de fiets](#)

[Hack je wifi netwerk](#)

[Illegale websites blokkeren is nutteloos](#)

[Beveiligingmaatregelen OS X gemakkelijk te omzeilen](#)

[Bekijk wereldwijde cyberaanvallen in realtime](#)

[Is rijden met een smartwatch om strafbaar?](#)

[Duizenden ING-kanten bezoeken phishingwebsites](#)

[Nederland krijgt portals voor registreren van kentekenchip](#)

[Cybercrime \(THC\)](#)

[Cybercrime \(EC3\)](#)

[Verwijder malware-infecties van je systeem](#)

[Wist jij dit al? Opmerkelijke feitjes over het internet](#)

[Schatkist](#)

[Snapshots](#)

[Cops in Cyberspace](#)

[Handig](#)

[Wetsartikelen](#)

Facebook informatie voor politie/justitie

Deze richtlijnen zijn bedoeld voor medewerkers van politie en justitie die records van Facebook nodig hebben.



Voor privéverzoeken, waaronder verzoeken van civiele procesvoerende partijen en aangeklaagde personen, ga je naar: facebook.com/help/?page=1057. Gebruikers die informatie willen hebben over hun eigen accounts, kunnen de Facebook-functie Je gegevens downloaden gebruiken in Accountinstellingen. Zie facebook.com/help/?page=18830. Deze informatie kan van tijd tot tijd worden gewijzigd.

Wettelijke procesvereisten voor de VS

We maken accountrecords alleen openbaar als dit in overeenstemming is met onze servicevoorwaarden en de toepasselijke wetgeving, inclusief de Amerikaanse wet Stored Communications Act ("SCA"), 18 U.S.C. secties 2701-2712. Volgens de SCA:

Een geldige dagvaarding die is afgegeven in verband met een officieel strafrechtelijk onderzoek dat de vrijgave van algemene abonnerecordgegevens vereist (zoals gedefinieerd in 18 U.S.C. sectie 2703(c)(2)), kan zijn: naam, duur van service, creditcardgegevens, e-mailadres (en) en (een) recent(e) IP-adres(sen) waarmee is aangemeld/afgemeld, indien beschikbaar.

Voor de openbaarmaking van bepaalde records met andere gegevens met betrekking tot het account (exclusief inhoud van communicatie) is een gerechtelijk bevel verstrekt onder 18 U.S.C., lid 2703(d) vereist. Voorbeelden van deze gegevens zijn (naast de standaardgegevens van abonnees zoals hierboven beschreven) berichtkoppen en IP-adressen.

Voor de openbaarmaking van de opgeslagen inhoud van een willekeurig account (waaronder berichten, foto's, video's, prikbordberichten en locatiegegevens) is een bevel tot huiszoeking vereist, verstrekt onder de procedures die zijn beschreven in de Federal

Rules of Criminal Procedure of equivalente bevelprocedures van de staat bij aantonen van een redelijk vermoeden van schuld.

Bij het overleggen de National Security Letter aan Facebook vereisen we slechts twee categorieën gegevens: naam en serviceduur.

Internationale wettelijke procesvereisten

Accountgegevens maken we alleen openbaar in overeenstemming met onze servicevoorwaarden en de toepasselijke wet. Een rechtshulpverzoek of -brief kan vereist zijn voor openbaarmaking van de inhoud van een account. Meer informatie hierover vind je op facebook.com/about/privacy/other.

Bewaren van accounts

We kunnen in verband met officiële strafrechtelijke onderzoeken stappen nemen om accountrecords gedurende 90 dagen te bewaren in afwachting van ontvangst van het formele juridische proces. Je kunt snel formele bevaarverzoeken indienen via het Law Enforcement Online Request-systeem op facebook.com/records, of via e-mail, fax of reguliere post zoals hieronder aangegeven.

Urgente verzoeken

Wanneer er wordt gereageerd op een kwestie waarbij sprake is van een acuut risico op letsel aan een kind of de dood of serieus, fysiek letsel van een persoon en daar de onmiddellijke vrijgave van informatie voor nodig is, kan een medewerker van politie en justitie een verzoek indienen via het Law Enforcement Online Request-systeem op facebook.com/records. Belangrijk: we gaan niet in op en reageren niet op berichten die naar dit e-mailadres worden gestuurd door mensen die niet werkzaam zijn

bij politie of justitie. Gebruikers die op de hoogte zijn van een noodsituatie dienen onmiddellijk rechtstreeks contact op te nemen met de lokale politie.

Veiligheid van kinderen

Alle gevallen van kindermisbruik die we wereldwijd op onze site tegenkomen, melden we bij het National Center for Missing and Exploited Children (NCMEC), waaronder inhoud waarop we door de overheid worden gewezen. Het NCMEC werkt samen met het International Center for Missing and Exploited Children en politie/justitie wereldwijd. Als een verzoek betrekking heeft op het misbruik of de veiligheid van kinderen, moet u de omstandigheden in het verzoek vermelden (en relevante aanduidingen voor de NCMEC-melding opnemen) zodat we deze gevallen snel en doeltreffend kunnen aanpakken.

Retentie en beschikbaarheid van gegevens

We zullen zoeken naar gegevens en deze openbaar maken die worden gespecificeerd op het juiste formulier dat bij het juridische proces hoort en waarvoor we voldoende informatie hebben om te vinden en op te vragen. We bewaren geen gegevens voor juridische doeleinden tenzij we een geldig verzoek tot bewaring hebben ontvangen voordat een gebruiker die inhoud van onze service heeft verwijderd.

Details over het verwijderen van gegevens en accounts zijn te vinden in ons beleid inzake gegevensbeleid (facebook.com/policy.php), onze verklaring van rechten en verantwoordelijkheden (facebook.com/terms.php) en het Helpcentrum (facebook.com/help/?faq=224562897555674).

Facebook informatie voor politie/justitie (2)

Toestemming van gebruiker

Als een medewerker van de plaatselijke politie informatie wil hebben over een Facebook-gebruiker die de medewerker toestemming heeft gegeven om de accountgegevens van de gebruiker te gebruiken of op te vragen, dient de gebruiker zelf te worden gevraagd om die gegevens uit zijn/haar account te halen. Voor inhoud in een account, zoals berichten, foto's, video's en prikbordberichten kunnen gebruikers de Facebook-functie Je gegevens downloaden in Accountinstellingen gebruiken. Zie facebook.com/help/?page=18830. Gebruikers kunnen ook recente IP-adressen zien in Accountinstellingen bij Beveiligingsinstellingen/Actieve sessies. Gebruikers hebben zonder juridische procedure geen toegang tot historische IP-gegevens.

Getuigenis

Facebook biedt geen ondersteuning in de vorm van deskundigenverklaringen. Daarnaast zijn Facebook-records volgens de wet reeds geverifieerd en behoeven daarom geen getuigenis van een recordsbeheerder. Indien een speciale vorm van certificering wordt vereist, dien je dit toe te voegen aan je recordsverzoek.

Vergoeding van kosten

We kunnen een vergoeding vragen van kosten die zijn gemaakt voor het afhandelen van gegevensverzoeken, zoals voorzien door het toepasselijke recht. Deze kosten worden per account in rekening gebracht. Daarnaast kunnen we extra kosten in rekening brengen die zijn gemaakt voor de afhandeling van ongebruikelijke of complexe verzoeken.

We kunnen afzien van deze kosten in zaken met betrekking tot onderzoek naar mogelijk

geweld tegen kinderen, Facebook en onze gebruikers, en urgente verzoeken.

Verzoeken indienen

Online

Medewerkers van politie en justitie kunnen het Law Enforcement Online Request-systeem gebruiken op facebook.com/records voor het indienen, bijhouden en verwerken van verzoeken.

Let op: je hebt een e-mailadres van de overheid nodig om toegang te krijgen tot het Law Enforcement Online Request-systeem. Je kunt ook verzoeken per e-mail indienen zoals hieronder aangegeven.

Postadres

United States Mailing Address: 1601 Willow Road, Menlo Park CA 94025

Ireland Mailing Address: Facebook Ireland Ltd | 4 Grand Canal Square | Dublin 2

Attention: Facebook Security, Law Enforcement Response Team

Medewerkers van politie en justitie die verzoeken niet via het Law Enforcement Online Request System indienen op facebook.com/records, dienen rekening te houden met lange reactietijden.

Notities

Acceptatie van een juridisch proces via een van deze middelen is voor gemak en ontslaat niet van bezwaren, inclusief ontbreken van jurisdictie of de juiste service.

We reageren niet op berichten die worden verstuurd naar de bovenstaande adressen door andere personen dan medewerkers van politie en justitie.

Account deactiveren

Je kunt een account tijdelijk deactiveren en dan terugkeren wanneer je wilt.

Je deactiveert je account als volgt:

Klik op het menu Account () rechtsboven aan een Facebook-pagina

Selecteer Instellingen

Klik op Beveiliging in de linkerkolom

Kies Je account deactiveren en volg dan de stappen om te bevestigen

Als je je account deactiveert, is je profiel niet zichtbaar voor andere mensen op Facebook en ben je niet zichtbaar in zoekresultaten. Informatie zoals berichten die je naar vrienden hebt gestuurd, kan nog wel zichtbaar zijn voor anderen.

Als je na deactivering van je account later naar Facebook wilt terugkeren, kun je je account opnieuw activeren door je met je e-mailadres en wachtwoord aan te melden. Je profiel wordt volledig hersteld (met bijvoorbeeld je vrienden, foto's en interesses). Om je account opnieuw te kunnen activeren, moet je wel toegang hebben tot het e-mailadres waarmee je je aanmeldt.

Als je geen toegang krijgt tot je account, kun je je wachtwoord opnieuw instellen.

Je account permanent verwijderen:

Wanneer je je account permanent verwijdert, kun je de inhoud of gegevens die je hebt toegevoegd nooit meer opnieuw activeren of opvragen. Als je je account permanent wilt verwijderen zonder hersteloptie, [laat het Facebook dan weten](#).



Telecomgegevens gebruiken voor opsporing

Opsporings-, veiligheids- en inlichtingendiensten hebben soms persoonsgegevens nodig die horen bij IP-adressen, telefoonnummers en e-mailadressen. Hiermee kunnen ze een verdachte van een misdrijf opsporen.

TELECOM



Telecomgegevens gebruiken voor strafrechtelijk onderzoek

Telecom- en internetaanbieders moeten telecom- en internetgegevens van hun klanten beschikbaar stellen voor onderzoek naar criminele activiteiten. Dit staat in het Besluit verstrekking gegevens telecommunicatie. Het gaat om de volgende persoonlijke informatie:

een adres dat hoort bij een telefoonnummer;

een e-mailadres;

IP-adres.

Bijvoorbeeld: een onderzoeksteam van de politie start een onderzoek naar een verdachte van kinderporno. Van de verdachte hebben zij alleen het IP-adres. Dit is het unieke adres van een pc op internet. De politie gebruikt de persoonsgegevens die daarbij horen, om de verdachte op te sporen.

Telecombedrijven en internetproviders krijgen voor het aanleveren een vergoeding van de overheid.

Centraal punt voor opvragen en aanleveren telecomgegevens

Er is 1 centraal punt waar de opsporingsdiensten de klantgegevens kunnen opvragen. Hierdoor hoeven de diensten geen contact te onderhouden met veel providers. Telefoonbedrijven en internetproviders actualiseren elke 24 uur hun bestand met klantgegevens. Het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) beheert een geautomatiseerd informatiesysteem (CIS) voor deze telefoon-

en internetgegevens. De opsporingsdiensten kunnen via het centrale systeem gegevens opvragen. Het systeem stuurt de vraag dan door naar de bestanden van de aanbieders.

Dit gebeurt bijvoorbeeld als het Openbaar Ministerie (OM) een mogelijke drugs crimineel op het oog heeft. Alleen het telefoonnummer van de verdachte is bekend. Het OM wil onderzoeken wie er bij dat nummer hoort en waar de verdachte woont. Het onderzoeksteam vraagt daarom het nummer op bij de telefoonaanbieders. Dit gebeurt via het CIOT-informatiesysteem. Het systeem geeft binnen 10 seconden antwoord namens de telefoonaanbieder. Met die gegevens kan het OM verder werken aan het onderzoek.

Aanleveren verschillende telefoon- en internetgegevens

- Telecomaanbieders moeten de volgende gegevens geven:
- naam, adres, postcode en woonplaats van de gebruiker;
- de telecommunicatiedienst die de gebruiker afneemt (bijvoorbeeld vast, mobiel, prepaid);
- telefoonnummer(s) van de gebruiker;
- naam van de telecommunicatieaanbieder.
- Internetproviders moeten deze gegevens geven:

- naam, adres, postcode en woonplaats van de gebruiker;
- de internetdienst die de gebruiker afneemt (bijvoorbeeld kabel, ADSL, e-mail);
- IP-adressen, e-mail adres (sen) en in sommige gevallen de identificatienummers van randapparaten (bijvoorbeeld kabelmodems);
- naam van de internetaanbieder.

Wettelijke verplichting voor aanleveren klantgegevens

Telecommunicatiebedrijven moeten de persoonsgegevens van hun klanten beschikbaar stellen aan het CIOT. Dit staat in de wet. Het CIOT sluit deze bedrijven aan op het CIOT-informatiesysteem. Daarna moet de provider elke 24 uur een actueel bestand met klantgegevens aanleveren. Zij krijgen hiervoor een vergoeding van de overheid.

Voorwaarden voor opvragen gegevens

De opsporingsdiensten mogen het informatiesysteem niet zomaar raadplegen. Opsporingsdiensten mogen alleen informatie opvragen als dit echt nodig is voor hun onderzoek. Bijvoorbeeld om:

inlichtingen te verzamelen bij het vermoeden van terroristische activiteiten;

onderzoek te doen naar misdrijven;

voor hulpverlening in noodsituaties.

Bijvoorbeeld als iemand die onwel wordt 112 belt, maar niet meer kan vertellen wie hij is of waar hij woont. Via het informatiesysteem kan de politie diegene toch vinden; om de nationale veiligheid te beschermen.

Ook moet er een rechtmatige grondslag zijn. In het Wetboek van Strafvordering (SV) en in de Wet op de inlichtingen en veiligheidsdiensten (Wiv) staat waaraan de aanvraag moet voldoen.

Opvragen kan alleen door bevoegde instanties en personen

Niet iedereen kan zomaar gegevens opvragen bij het CIOT. De volgende instanties hebben van de minister van Veiligheid en Justitie toestemming om het informatiesysteem van het CIOT te gebruiken:

Opsporingsdiensten

Politie, Rijksrecherche, Koninklijke Marechaussee (KMAR), Landelijk Parket- Openbaar Ministerie en 112.

Bijzondere opsporingsdiensten

Fiscale Inlichtingen- en Opsporingsdienst (FIOD), Algemene Inspectiedienst (AID), Inlichtingen- en Opsporingsdienst (IOD), Inspectie SZW en Inspectie voor de Gezondheidszorg (IGZ).

Inlichtingen- en veiligheidsdiensten

Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en Militaire Inlichtingen- en Veiligheidsdienst (MIVD).

Geen verbod op bellen, sms'en en appen op de fiets

Minister Schults van Haagen heeft via een brief aan de Tweede Kamer laten weten dat er in Nederland geen verbod komt op het bellen, sms'en en appen op de fiets. Volgens de Minister is een dergelijk verbod moeilijk te handhaven, de Minister gelooft meer in voorlichting over de risico's van het gebruik van de mobiele telefoon op de fiets.



Internationaal is er afgesproken dat het verboden is voor een bestuurder van een gemotoriseerd voertuig dat in beweging is om een mobiele telefoon te gebruiken. Sommige landen hebben deze afspraak wettelijk vastgelegd maar hebben gemotoriseerd weggelaten, een voorbeeld hiervan is Denemarken. Daardoor is het in Denemarken ook verboden om een telefoon op de fiets te gebruiken.

In Nederland is het gebruik van een mobiele telefoon alleen verboden bij een gemotoriseerd voertuig zoals een auto, motor, scooter en bromfiets. Volgens de minister zijn er geen gegevens bekend van de Europese landen die telefoongebruik op de fiets wel verboden hebben en daarom ziet zij geen reden om de wet in Nederland aan te passen.

In Nederland werd vorig jaar wel een onderzoek gedaan naar smartphonegebruik op de fiets en daaruit bleek dat bij een op de vijf fietsongelukken waarbij een jongeren betrokken is ook de smartphone een rol speelt. Uit het onderzoek zou ook blijken dat de kans op een ongeluk maar liefst 25 keer groter is wanneer iemand tijdens het rijden zijn smartphone gebruikt. In totaal is bij slechts 9 procent van de fietsongelukken een smartphone in het spel.

De overheid heeft vorig jaar een app ontwikkeld genaamd Fietsmodus waarmee prijzen zijn te winnen wanneer de smartphone niet wordt gebruikt tijdens het fietsen. Deze app zal dit jaar verder worden promoot door de overheid en de Nederlandse telecomproviders.



Op deze manier hack je een wifi-netwerk

Als je dit leest is de kans groot dat je gebruik maakt van een wifi-netwerk. De kans is nog groter dat er zeker een paar netwerken in de buurt zijn. Het probleem is dat, wanneer er een slotje naast de naam van het netwerk staat, deze beveiligd is.

Zonder wachtwoord of wachtwoordzin kom je er niet in, en dus ook niet op dat geliefde internet.

Misschien ben je het wachtwoord van je eigen netwerk wel vergeten, of heb je vervelende burens die hun netwerk niet willen delen. Dan kun je natuurlijk altijd naar een café gaan, een cinnamon haze moccachino latte bestellen, en gebruik maken van het 'gratis' netwerk daar. Je kan ook een applicatie downloaden, zoals [wifi-Map](#), en gebruik maken van de lijst van meer dan 2 miljoen hotspots met gratis Wi-Fi (inclusief een aantal wachtwoorden van vergrendelde verbindingen).

Maar er zijn andere manieren om toegang te krijgen tot het draadloze; hoewel sommige methodes zo veel geduld vergen dat die moccachino misschien niet eens zo'n slecht idee is.

Reset de router

Voor je dit doet, probeer eerst bij je router in te loggen. Vanuit daar kun je gemakkelijk het wachtwoord resetten, mocht je die zijn vergeten.

Het probleem is natuurlijk dat je het wachtwoord van de router ook niet meer weet (het wachtwoord van de router is iets anders dan het wachtwoord van je wifi, tenzij je dit zo hebt ingesteld). Het resetten van de router is de meest lompe methode, en werkt alleen als je fysiek toegang hebt tot de router.

Bijna elke router die bestaat heeft een verzonken reset knop. Druk deze in met een pen, of een tandenstoker, hou dit ongeveer 10 seconden vol, en de router zet zichzelf terug naar de fabrieksinstellingen.

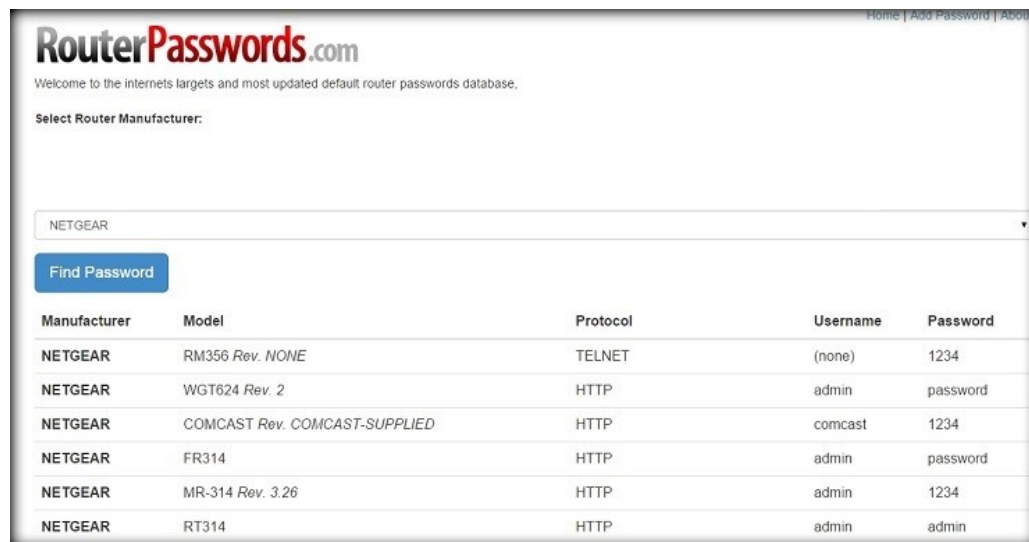
Heb je een router van je provider? Check dan eerst op eventuele stickers. Misschien staan de wachtwoorden van de router en die van je wifi (soms de key genoemd) wel op het apparaat.



Zodra het apparaat is gereset heb je weer een andere gebruikersnaam en wachtwoord nodig om toegang te krijgen tot het apparaat zelf. Hier kom je via de web browser van elke PC die verbonden is met de router via ethernet.

De URL is 192.168.1.1 of 192.168.0.1, of een variatie. Nu wordt je gevraagd naar een gebruikersnaam/wachtwoord. Wat nu? Check de handleiding van de router. Die ben je vast kwijt of heb je weggegooid. Ga daarom naar [RouterPasswords.com](#). Deze site bestaat maar met 1 reden: mensen vertellen wat de standaard inloggegevens zijn van iedere router ooit gemaakt.

Op deze manier hack je een wifi-netwerk (2)



RouterPasswords.com

Welcome to the internet's largest and most updated default router passwords database.

Select Router Manufacturer:

NETGEAR

Find Password

Manufacturer	Model	Protocol	Username	Password
NETGEAR	RM356 Rev. NONE	TELNET	(none)	1234
NETGEAR	WGT624 Rev. 2	HTTP	admin	password
NETGEAR	COMCAST Rev. COMCAST-SUPPLIED	HTTP	comcast	1234
NETGEAR	FR314	HTTP	admin	password
NETGEAR	MR-314 Rev. 3.26	HTTP	admin	1234
NETGEAR	RT314	HTTP	admin	admin

Wat je nodig hebt is het modelnummer, maar die staat op de achter- of onderkant van de hardware. Waarschijnlijk zie je op de site al snel een patroon. De gebruikersnaam is vaak admin en het wachtwoord vaak password. Aangezien de meeste mensen lui zijn en dit nooit veranderen: probeer deze combinatie eerst voordat je op de resetknop drukt (maar jij bent beter dan dat, dit heb je meteen veranderd toen je voor het eerst hebt ingelogd).

Wanneer je toegang hebt tot de interface van de router, ga naar wifi instellingen, zet draadloze netwerken aan, en geef ze een sterk, maar makkelijk te onthouden wachtwoord. Je wilt tenslotte niet dat je burens ook gebruik maken van jouw netwerk zonder toestemming.

Kraak de code

Je kwam hier niet omdat de titel van dit stuk 'reset de router' luidde. Je wilt weten hoe je het wachtwoord van een wifi-netwerk kunt kraken.

Als je zoekt naar "Wi-Fi password hack", of iets wat daar op lijkt krijg je een lijst met resultaten. De meeste zijn links naar software op sites waar de adware, bots en oplichtingen je om de oren vliegen. Download deze op eigen risico, zeker voor Windows.

Of creëer een apart systeem, speciaal hiervoor. Dual-boot bijvoorbeeld in een apart OS, speciaal in het leven geroepen voor deze zogenaamd 'penetration testing': een offensieve vorm van beveiliging, waarbij je een netwerk van alle kanten probeert binnen te dringen. [Kali Linux](#) is een Linux built speciaal hier-

voor bedoeld. Je kan Kali Linux vanaf een cd of USB draaien, zonder het te hoeven installeren.

Een andere optie is [BackTrack Linux](#). Beide programma's zijn van dezelfde ontwikkelaars, maar Kali is de meer opgepoetste versie. Ze zijn beiden gratis, en bevatten alle tools om een netwerk te kraken.

Als je geen volledig OS wil installeren, dan kun je deze twee beproefde tools van Wi-Fi hackers proberen:

Aircrack bestaat al sinds wifi beveiliging slechts gebaseerd was op WEP (Wired Equivalent Privacy). WEP was toen al zwak, en werd vervan-

ter in je computer hebben: een die packet injection ondersteund. Je moet overweg kunnen met CMD (command line), en vooral heel veel geduld hebben. Je wifi adapter en Aircrack zullen een boel data moeten verzamelen om ook maar in de buurt te komen van het ontcijferen van de toegangscode van het netwerk dat je aanvalt. En dat kan even duren.

Ook op de MAC: [Wi-Fi Crack](#). Om deze of Aircrack-ng op de Mac te gebruiken, zul je ze moeten installeren met MacPorts, een tool voor het via command-line installeren van producten op de Mac. Het kraken van sterkere WPA/WPA2 wachtwoorden en wachtwoordzinnen is de echte opgave vandaag de dag. [Reaver](#) is de enige tool die daarvoor opgewassen lijkt (en het is een onderdeel van het BackTrack Linux distro). Opnieuw moet je wat CMD werk je niet afschrikken. Je kunt ook de [Reaver Pro](#) kopen, een stuk hardware die werkt met Windows en Mac. Na twee tot tien uur aanvallen zou Reaver een wachtwoord moeten kunnen onthullen. Maar het gaat alleen werken als de router waar je op uit bent een sterk signaal geeft en WPS (Wi-Fi Protected Setup) ingeschakeld heeft. WPS is de featu-



gen door WPA (Wi-Fi Protected Access) in 2004. De nieuwste [Aircrack-ng 1.2](#) — zichzelf omschrijvend als een "toolkit voor het controleren van netwerken", zou dus onderdeel moeten zijn van de toolkit van iedere admin — is in staat om WEP en WPA-PSK vergrendelingen te kraken.

Aircrack-ng komt met volledige documentatie, maar het gaat niet eenvoudig zijn. Om een netwerk te kraken moet je ook juiste wifi adap-

re waarmee je met een druk op de knop van een router, en nog een druk op de knop van het wifi apparaat automatisch een versleutelde verbinding maakt. Dit is precies het 'gat' waar Reaver door naar binnen kruipt. Over het algemeen kan Reaver binnen 24 uur de code moeten kraken.

Zelfs als je WPS uitzet is het soms niet helemaal uit. Maar dat is je enige toevlucht, als je bang bent dat je eigen router wordt gehackt. Of, neem een router die helemaal geen WPS

Illegale websites blokkeren is nutteloos

The Pirate Bay is maar één van vele websites die in verschillende Europese landen geblokkeerd wordt. De reactie op sites die illegale content aanbieden is steevast dezelfde: de site wordt geblokkeerd, meestal via eenvoudig omzeilbare DNS-censuur.



In uitzonderlijke gevallen gaan Europese ordehandhavers, al dan niet in een internationaal samenwerkingsverband, verder en halen ze illegale websites echt offline.

Pyrrusoverwinning

Dergelijke acties worden meestal afgeschilderd als grote overwinningen, zoals bij The Pirate Bay vorig jaar, of het Duitse Kino.to in 2011. Kino.to was één van de populairste gratis streaming websites ter wereld. Toen de site na een Europese raid voor goed offline ging besloot het onderzoekscentrum van de Europese commissie het effect op de lange termijn van de actie te bestuderen.

De resultaten van het onderzoek tonen aan dat de raid en het offline halen van de website amper effect hadden op het illegale online-aanbod van multimedia. Volgens de onderzoekers hadden bezoekers er geen probleem mee om over te schakelen naar andere websites die hen hetzelfde bieden als Kino.to. Dat zorgt voor problemen volgens de Europese studie: "Het neerhalen van de websites leidde tot een gefragmenteerde markt voor illegaal streamen. Dat maakt het optreden van de politie in de toekomst mogelijk duurder, aangezien er geen dominant platform meer bestaat dat offline kan worden gehaald. Bovendien zou een actie gericht tegen één website veel minder effect hebben."

Altijd een alternatief

Het neerhalen van één website had dus tot gevolg dat er een handvol vervangers als paddenstoelen uit de grond sprongen. In het geval van The Pirate Bay is de eindbalans nog slechter: niet alleen vonden veel gebruikers alternatieven, de website zelf staat intussen ook terug online. Ondanks censuur wereldwijd blijft de torrent-website één van de 500 populairste sites op het

net.

Het onderzoekscentrum constateerde dat het optreden van de overheid wel degelijk een erg klein positief effect heeft. 2,5 procent van de Kino.to-gebruikers zochten na de raid hun heil bij legale betaaldiensten. De algemene tendens is echter duidelijk: de meeste gebruikers van streaming- of torrentwebsites waren nooit van plan om te betalen voor hun content. Het neerhalen van hun favoriete website verandert daar niets aan. Film- en muziekstudio's hebben dus weinig te winnen bij het gevecht tegen de illegale downloads, concludeert het onderzoek.

Positieve aanpak

De beste oplossing lijkt nog steeds het aanbieden van aantrekkelijke legale alternatieven met verschillende betaalmogelijkheden. Veel gebruikers vinden dat diensten als Spotify, Netflix en Steam wel eerlijke prijzen hanteren. Ook een gratis legale versie van een dienst, zoals het door advertenties gesponsorde abonnement van Spotify, helpen. Extra gebruiksgemak maakt het bovendien interessant om een betaaldienst boven een illegale dienst te verkiezen.



Beveiligingmaatregelen OS X gemakkelijk te omzeilen

OS X mag dan al een betere veiligheidsreputatie hebben dan Windows, het OS is lang niet perfect, zegt veiligheidsonderzoeker Patrick Wardie.



De beveiligingsmaatregelen die Apple in OS X heeft ingebouwd, zijn gemakkelijk te omzeilen. Dat zei veiligheidsonderzoeker Patrick Wardie op de RSA Conference in San Francisco, zo rapporteert Threatpost.

Wardie legde op de conferentie uit hoe twee veiligheidsmechanismen in het Apple OS kunnen gekraakt worden. “Het is triviaal voor elke aanvaller om de beveiliging van Macs te ontwijken”, aldus Wardie. “Als Macs helemaal veilig waren, stond ik hier niet.”

De twee features waar Wardie het over had, Gatekeeper en XProtect, werden vrij recent toegevoegd in OS X, als antwoord op de steeds grotere dreiging tegenover Apples besturingssysteem.

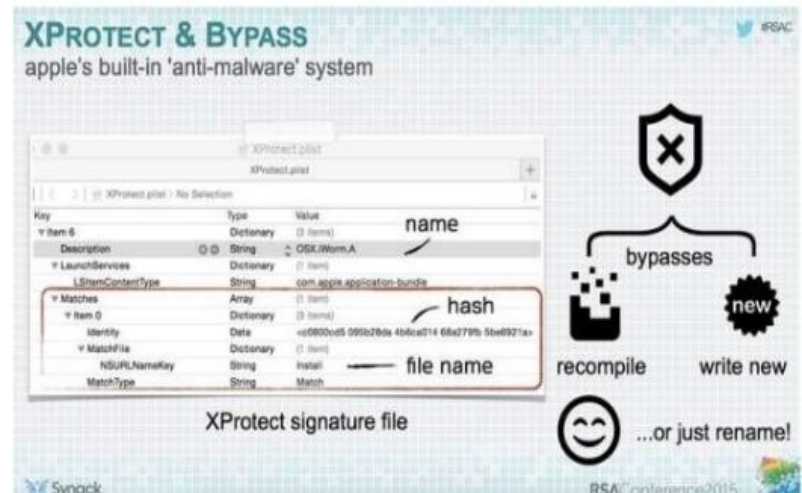
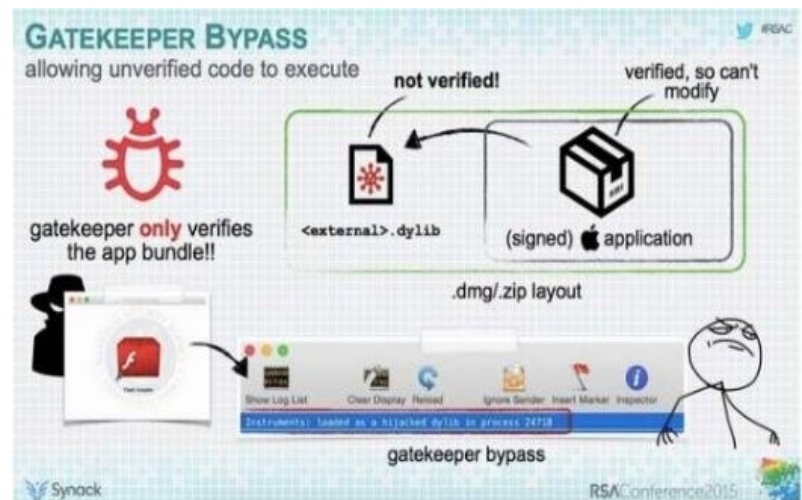
Apple voegde Gatekeeper toe aan OS X 10.8 Mountain Lion. Het beperkt het soort programma's dat op de computer kan worden geopend. De meeste mensen hebben het zo ingesteld dat enkel apps uit de Apple App Store of van geverifieerde ontwikkelaars mogen draaien.

Xprotect is een rudimentaire malwarescanner die voor het eerste in OS X 10.6 opdook (Snow Leopard). Deze kan bepaalde apps en plugins blokkeren als ze bekende kwetsbaarheden bevatten.

“Gatekeeper verifieert geen extra content die in de apps zit”, zegt Wardie. Als de app wordt geopend, weet Gatekeeper waar deze vandaan komt en geeft hij toestemming om te draaien. Of hij weet het niet en dan sluit hij de app af. Maar de app wordt niet voortdurend gecontroleerd en dat kan een probleem zijn. “Als ik dus een app vind die werd goedgekeurd door Apple en ik slaag er in om deze externe code te laten draaien, dan zal hij toch door Gatekeeper geraken”, aldus Wardie.

Volgens de onderzoeker is ook XProtect “triviaal” om te

omzeilen. Door een bekende malware sample te hercompileren om zijn hash te veranderen, kon Wardie deze langs Xprotect smokkelen en draaien. Wardie noemde de “sandboxing”-eigenschappen van Xprotect wel “sterk”, maar het is mogelijk om een aantal bekende kwetsbaarheden op kernel-niveau er langs te krijgen, waardoor de veiligheid van een systeem ondermijnd wordt.



Bekijk wereldwijde cyberaanvallen in realtime

De interactieve website World Cyber Threat Map toont actuele cyberagressie op globale schaal.

Datasecurityspecialist Check Point heeft een website in elkaar gestoken die in realtime wereldwijde cyberaanvallen visualiseert. De World Cyber Threat Map toont niet alleen actuele aanvallen op een globale schaal, maar laat ook duidelijk zien uit welke landen de cyberagressie komt en wie het doelwit is.

Daarnaast somt de website ook enkele fascinerende statistieken op. De meest agressieve landen en de meest belaagde landen kan je er in een top tien terugvinden. Zo is het grootste deel van de aanvallen op moment van schrijven gericht op Mexico en India, en worden de meeste aanvallen uitgevoerd vanuit de Verenigde Staten. Ook Nederland staat in de top tien van aanvallers.

De website telt ook het totaal aantal aanvallen per dag, wat toch al gauw tot zeven cijfers oploopt. Selecteer je een bepaald land, dan heb je de optie om gegevens van de laatste week of maand op te vragen over de infectiegraad, de hardnekkigste aanvaller en het type van aanvallen waaronder het lijdt.

“Voor veel organisaties is de mondiale schaal waarop cyberaanvallen gebeuren en de enorme snelheid waarmee moeilijk te begrijpen,” verklaart Gil Schwed, CEO van Check Point. “We wilden een tool ontwikkelen om bedrijven te helpen begrijpen hoe snel het cybercrimelandschap evolueert, zodat zij maatregelen kunnen nemen om hun veiligheid te versterken en zich beter te verdedigen tegen dergelijke aanvallen.”

Je kan de World Cyber Threat Map bekijken [via deze link](#).



Is rijden met een smartwatch om strafbaar?

In Canada is onlangs een man beboet en kreeg strafpunten op zijn rijbewijs voor alleen het rijden met een smartwatch om. Hoe zit dat precies bij ons, is het rijden met een smartwatch om hier ook strafbaar?



Het verbod uit de wet op het vasthouden van een mobiele telefoon (art. 61a RVV) vermeldt bij ons letterlijk:

Het is degene die een motorvoertuig, bromfiets, snorfiets of gehandicaptenvoertuig dat is uitgerust met een motor bestuurt verboden tijdens het rijden een mobiele telefoon vast te houden.

De eerste gedachte is: hij zit om je pól en dus niet in je hand. Maar zo medisch-letterlijk wordt er in het recht niet geredeneerd. In deze zaak bij het Hof Leeuwarden uit 2006 werd bepaald dat het begrip 'vasthouden' breed moet worden uitgelegd:

Inherent aan deze vorm van telefoneren is dat de afstand van de gebruiker tot het toestel direct van invloed is op de kwaliteit van het contact. Dat brengt met zich mee dat niet alleen het telefoongesprek afleidt van de verkeerssituatie, maar ook het risico toeneemt dat de bestuurder fysiek te veel betrokken is bij het voeren van het telefoongesprek en daardoor minder goed in staat is de benodigde verkeershandelingen te verrichten. Blijkens de Nota van Toelichting ontstaat juist door deze combinatie van factoren een niet te veronachtzamen risico voor de verkeersveiligheid. Bovendien kan, wanneer de verstaanbaarheid bij gebruik van de speakerfunctie tijdelijk of blijvend is beperkt – bijvoorbeeld door omgevingsgeluid – eenvoudig het toestel alsnog naar het oor worden gebracht.

Oftewel, het probleem met in de hand houden is hetzelfde als met het aan de pols vastbinden, je ene arm is niet meer beschikbaar voor het bedienen van de auto. Daarom is "aan de pols binden" juridisch hetzelfde als 'in de hand houden'.

Dan de vraag, is het een 'telefoon'. Deze term is ook breed gedefinieerd: "een apparaat dat bestemd is voor het gebruik van mobiele openbare telecommunicatie-

diensten". Dat begrip kennen we uit de Telecommunicatiewet. Een apparaat zoals de iPhone is bestemd voor deze diensten, zowel spraaktelefonie als dataoverdracht, valt er dus onder. Maar ook een laptop met ingebouwd 3G-modem valt eronder, want ook dataoverdracht aan sich via 3G is een vorm van gebruik van mobiele openbare telecommunicatiediensten.

Een smartwatch wordt draadloos gekoppeld aan een telefoon of ander apparaat, en is daarmee dus bestemd voor mobiele communicatie. Echter, dat woordje 'openbaar' maakt hier het verschil: een smartwatch werkt met Bluetooth of een vergelijkbaar kortereafstand-protocol, en dat is géén openbare telecommunicatiedienst. Om diezelfde reden is het dus ook niet verboden je Bluetooth oortje voor je telefoon in de hand te houden (zie dit vonnis uit 2010.) Anders gezegd: een smartwatch is geen telefoon.

Natuurlijk is er altijd nog Koos Spree z'n kapstok, artikel 5 Wegenverkeerswet. Maar dan moet er wel worden bewezen dat door de handeling gevaar is ontstaan of kon ontstaan. Wie met smartwatch om de pols perfect rechtdoor rijdt net onder de maximumsnelheid, veroorzaakt geen (potentieel) gevaar.



Duizenden ING-kanten bezoeken phishingwebsites

Duizenden klanten van ING zijn recentelijk op phishingsites terechtgekomen nadat ze een link in een phishingmail hadden geopend. De links in de phishingmails zijn door 14.000 personen bezocht en minstens 3.000 keer zijn de gevraagde gegevens zoals wachtwoord, rekeningnummer, geboortedatum, pasnummer en telefoonnummer ingevuld.



Nadat alle gegevens waren ingevuld werd er geprobeerd om de gebruiker een kwaadaardige Android-app te laten installeren. Deze app kan mobiele tancodes onderscheppen. Daarnaast kan de app tijdelijk het geluid en de vibratie van binnenkomende sms-berichten uitschakelen.

Op deze manier kan de malware de mobiele tancode stelen zonder dat gebruikers doorhebben dat er een sms-bericht is binnengekomen. Na ontvangst van de code wordt het geluid weer ingeschakeld. Aangezien de aanvallers ook al over het wachtwoord van gebruikers beschikken kunnen ze op deze manier frauduleuze transacties uitvoeren.

Logbestanden

Het gaat om verschillende mails die naar verschillende phishingsites wijzen. Gegevens die mensen op deze phishingsites invullen worden naar een centrale server doorgestuurd.

Aan de hand van logbestanden van de gebruikte phishingsites kon het aantal bezoekers worden vastgesteld. Ook wordt in de logbestanden bijgehouden waar bezoekers zich precies op de pagina bevinden en welke stappen ze hebben doorlopen. "Ze loggen heel secuur", stelt Van Duijn, onderzoeker van het Nederlandse be-

veiligingsbedrijf DearBytes. Op deze manier kon de onderzoeker ook het aantal mensen bepalen dat alle gevraagde gegevens had ingevuld. In het geval niet alle gegevens worden ingevuld krijgen gebruikers namelijk een foutmelding te zien.

Statistieken

Aangezien de inhoud van de ingevulde gegevens onbekend is blijft onduidelijk hoeveel mensen er echt in de phishingmail zijn getrapt. De gegevens wat betreft bezoekers en mensen die de gegevens invulden zouden wel in de buurt van de eerder genoemde getallen komen. "Het lijkt erop dat de data aardig kloppen en dat mensen de gegevens daadwerkelijk hebben ingevuld", aldus Van Duijn. Waar de bezoekers precies vandaan komen is niet achterhaald. Sinds gisteren is het aantal bezoekers van de phishingsites verder toegenomen.

Het blijft echter onduidelijk hoeveel mensen de gegevens correct hebben ingevuld én de kwaadaardige app hebben geïnstalleerd. Pas als al die zaken kloppen kunnen de criminelen achter de phishingmails namelijk de transactie uitvoeren. Het is dan ook onduidelijk of er via de phishingaanval geld is gestolen.

TAN-Functie Geblokkeerd

Waarom blokkeren?

- Wij blokkeren de TAN-functie om misbruik te voorkomen. Wij begrijpen dat deze blokkade vervelend is. Maar we zorgen er graag voor dat uw gegevens veilig zijn.

Hoe ontvangt u weer TAN-codes?

- Maak uw computer virusvrij.
- [Klik hier om uw account te activeren.](#)

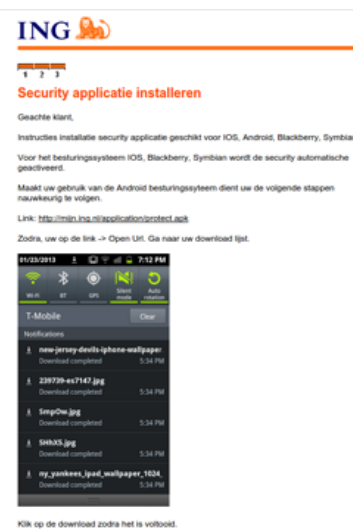
Bent u in het buitenland?

- [Om uw account te activeren. Klik hier.](#)

Wij helpen u graag op werkdagen van 8.00 tot 21.00 uur en op zaterdag van 9.00 tot 17.00 uur. Wij zorgen er direct voor dat u uw TAN-codes voor Mijn ING weer ontvangt. Met vriendelijke groet,

ING B.V.
Administratie.

NB: U kunt de factuur uitsluitend openen met Adobe Reader. Indien u deze software niet heeft



Nederland krijgt portals voor registreren van kentekenchip

De kentekenchip is onderdeel van een veel groter plan om alle wegen in Nederland uit te rusten met zogenaamde "portals" met meetapparatuur. Deze portals registreren 24 uur per dag alle auto's en daarmee de bewegingen van alle 17 miljoen burgers in de openbare ruimte, zo meldt Privacy First.



De privacyorganisatie maakt zich ernstig zorgen over het optuigen van een dergelijk landelijk controlesysteem en stelt dat de "spionagechip" disproportioneel is en niet past in een fatsoenlijke democratische rechtsstaat. Volgens Privacy First wordt het project voorlopig "verkocht" als oplossing voor identiteitsfraude en criminaliteit met kentekens. De organisatie ziet het systeem echter als de "zoveelste poging op rij" om de burger volledig te kunnen registreren in de openbare ruimte, hetzij via de OV-chipkaart hetzij via het kenteken of auto. "Het kenteken als elektronische enkelband voor iedere burger is een hardnekkig principe binnen het huidige controledenken bij de overheid."

Cijfers

Privacy First besloot navraag te doen over de veronderstelde "40.000 gevallen" van kentekenfraude, maar navraag levert bij geen enkele instantie duidelijkheid op. Het cijfer kan niet worden bevestigd, waardoor de werkelijke omvang van het probleem onbekend blijft. De privacyorganisatie stelt dat zelfs bij een schatting van 40.000 kentekens (0,5 promille van het totaal) de vraag moet worden gesteld in hoeverre "de privacy van de gehele samenleving hiervoor opgeofferd dient te worden."

Ook is onduidelijk wat de kosten van een dergelijk systeem gaan worden en wat de opbrengsten zijn ten opzichte van de huidige vermeende kosten van identiteitsfraude en criminaliteit. Verder is het de vraag of er geen alternatieve oplossingen zijn. Uit een recente brief van minister Van der Steur blijkt juist dat kentekenfraude steeds minder voorkomt door andere maatregelen zoals het systeem Gecontroleerde Afgifte en Inname Kentekenplaten (GAIK) en eisen aan erkende fabrikanten en lamineerders (lamineercode) alsmede de meldingsplicht voor gestolen/vermiste blanco platen of nog niet toegekende kentekenplaten.

Als het aan Privacy First ligt wordt de "controle-infrastructuur" dan ook niet ingevoerd, aangezien het permanent registreren van burgers in de openbare ruimte volgens de organisatie zal leiden tot zelfscensuur en een excuusmaatschappij, waarin iedere burger als het ware continu een alibi moet hebben wat hij op welk moment op een locatie deed en waarom hij daar was. Daarnaast zou op deze manier de democratische rechtsstaat worden aangetast, door een omkering van het rechtsprincipe dat een burger met rede verdacht moet zijn voor een strafbaar feit om gevolgd te kunnen worden te worden, door iedere burger als potentiële verdachte continu te bespioneren.



Cybercrime (THC)

We spreken van cybercrime als computers het doelwit zijn van criminele activiteiten. Burgers worden slachtoffer van computervredesbreuk en ransomware, zogenaamde 'gijzelingssoftware' waarmee criminelen een computer vergrendelen met kwaadaardige software.



Bedrijven en gemeenten kunnen slachtoffer worden van deze software. Nederlandse banken, andere private en publieke partijen worden getroffen door Ddos-aanvallen en botnets. Op deze manier proberen criminelen servers en websites plat te leggen. Cybercrime belemmert ons financiële en economische handelsverkeer en bedreigt de vitale infrastructuur van ons land. Doordat cybercriminelen zich internationaal en in de virtuele wereld verschuilen, zijn ze lastig te traceren en op te pakken. Maar gelet op de schade die ze toebrengen, is het OM alert en blijft de aanpak van cybercrime een belangrijke prioriteit. Aanpak en rol van het OM Met de toenemende digitalisering van de samenleving groeit cybercrime. Het is moeilijk te achterhalen wie er verantwoordelijk is voor een cyberaanval. Beroepscriminelen, vandalen en ideologische aanvallers maken gebruik van dezelfde cyberinstrumenten. Zowel binnen als buiten het OM is de afgelopen jaren geïnvesteerd in de aanpak van cybercrime. Het Team High Tech Crime (HTC) van de politie en het Landelijk Parket richt zich op cyberaanvallen tegen de vitale nationale infrastructuur, waarbij veiligheid in het geding is en op omvangrijke en complexe hacks. Daarnaast werken er binnen het OM in iedere regio specialisten die zich bezig houden met andere vormen van cybercrime. Bij cybercrime gaat het er in eerste instantie om de dreiging of de aanval zo snel mogelijk te stoppen en het achterliggende criminele netwerk te ontmantelen. Vervolgens is de vraag of de verdachte kan worden gevonden en ter verantwoording kan worden geroepen voor de strafrechter. Daders opereren veelal internationaal en goede en langdurige internationale samenwerking is nodig om tot een goed resultaat te komen. De verschil-

lende partijen moeten daarbij streven naar een eensgezinde reactie op een cyberincident. Publieke organisaties, private partners, wetenschappers en anderen werken samen aan preventieve maatregelen en – in geval van concrete aanvallen – de benodigde tegenmaatregelen en strafrechtelijke acties. Die samenwerking krijgt onder andere vorm binnen de Cyber Security Raad, het Nationaal Cyber Security Centrum en de Electronic Crimes Task Force. Met zijn ervaring uit concrete strafzaken vervult het OM binnen deze samenwerking geregeld een agenderende of alarmerende rol. Zo heeft het OM in 2014 gewaarschuwd dat de ransomware-variant Cryptolocker vaker lijkt voor te komen bij bedrijven en burgers. Naar aanleiding van een Rotterdamse hackerzaak heeft het OM gewezen op het toenemende gebruik van Remote Access Tools en geadviseerd om bewuster om te gaan met het gebruik van de webcam en aandacht te besteden aan digitale opvoeding.

Nederland is een toonaangevend land bij de internationale aanpak van cybercrime. Het OM in Nederland heeft een aanjagende rol vervuld bij de afstemming van de justitiële aanpak van gebruikers van software van het bedrijf 'Blackshades'. Verder was Nederland in 2015 gastheer van de Global Conference on Cyber Security in Den Haag, een internationale conferentie over een open, vrij en veilig digitaal domein. Doelstellingen en resultaten Het team HTC heeft in 2014 negentien volwaardige opsporingsonderzoeken afgerond. Deze onderzoeken zijn gestart binnen de doelstellingen van HTC voor 2014: aanvallen op vitale infrastructuren, aanvallen op het financiële stelsel en ransomware, botnets, facilitators en malwareverspreiding. Drie van de negentien opsporingsonderzoeken vonden

plaats in het kader van een omvangrijk rechtshulpverzoek dat een ander land bij Nederland had ingediend. De doelstelling voor 2014 – twintig omvangrijke opsporingsonderzoeken – is net niet behaald. Dit heeft onder andere te maken met andere urgente prioriteiten. Het aantal grote, complexe cybercrimeonderzoeken is afgelopen jaren gestegen van een enkel onderzoek naar zo'n twintig onderzoeken per jaar. De ambitie voor de komende jaren is de aanpak verder te verbreden. Naar verwachting neemt cybercrime in de komende jaren toe. Als zelfstandige criminele activiteit (computervredesbreuk) waarmee burgers en bedrijven en overheden slachtoffer worden van hacks en kwaadaardige software. Nu steeds meer apparaten en databases met internet worden verbonden neemt de kwetsbaarheid op dit punt toe. Maar ook speelt de digitale wereld steeds meer een sleutelrol in andere criminele activiteiten. Bijvoorbeeld waar beroepscriminelen handelen via online handelsplaatsen (zie kader), berovingen zich verplaatsen van de straat naar het web, of middelbare scholieren elkaar bestellen of bedreigen in online games of apps. De aanpak van cybercrime staat daarom samen met andere thema's centraal in de veiligheidsagenda 2015-2018. De strafrechtelijke aanpak van cybercrime wordt in alle regio's geïntensiveerd en het OM gaat meer onderzoeken starten en verdachten vervolgen. Daarnaast is het doel om samen met partners cybercrime terug te dringen, door onder andere de weerbaarheid van burgers en bedrijven te vergroten en preventieve systeemmaatregelen te treffen.

Verliezen politie en OM niet de strijd tegen cybercrime? Is het wel mogelijk om hightech criminelen te pakken? Boeven die grenzeloos innoveren, anoniem naam maken en de hoogwaardige Hollandse cyberinfrastructuur misbruiken



Wil van Gemert, adjunct-directeur van Europol, behoort niet tot de bangeriken. “We zullen cybercrime nooit helemaal kunnen uitbannen. Maar we gaan de strijd niet verliezen.” Eerder vormde Van Gemert het eerste Landelijke rechteerteam, was hij bij de AIVD directeur democratische rechtsorde, en bij de NCTv directeur cybersecurity. Bij Europol leidt Van Gemert nu het ‘Operations department’, waaronder het in 2013 operationeel geworden European Cyber Crime Centre valt. Dit ‘EC3’ ondersteunt en verbindt de (boven) Europese opsporing van cybercrime. Dark Web Bijvoorbeeld bij Silk Road, een via het Tor netwerk verborgen criminele handelsplek op het ‘dark web’. In november 2014 pakten politie- en justitie-instanties uit zestien Europese landen en de VS ‘Silk Road 2.0’ aan. Deze actie, ‘Operation Onymous’, werd vanuit Den Haag gecoördineerd door EC3, de FBI, de US Immigration and Customs Enforcement’s (ICE), Homeland Security Investigations en Eurojust. De internationale actie bracht de online handel in wapens en drugs een slag toe. Zeventien personen werden buiten Nederland aangehouden wegens de verkoop op en het beheer van deze marktplaatsen. Er werd een voor een miljoen dollar aan bitcoins en honderdachtigduizend euro aan cash in beslag genomen. Belangrijker nog: Silk Road werd neergehaald, ook de dieper verborgen delen ervan. Over dat laatste liet Europol zich tevreden uit in een persbericht. “Lange tijd waanden criminelen zich onzichtbaar en onaantastbaar op het Darkweb. We hebben aangetoond dat dat niet meer zo is. They can run, but they can’t hide.” “Het toont aan”, zegt Van Gemert over deze en andere acties, “dat politie en justitie in staat zijn antwoorden te bieden.” Samenwerking met Nederlandse OM Nederland speelt in de meeste onderzoeken een belangrijke rol, weet Van Gemert. “Ons land kent een hoge

internetdichtheid, een goede infrastructuur, een hoog kennisniveau, en vooral ook een belangrijke serviceverlenende industrie op het gebied van servercapaciteit en providers. Samenwerking met het Nederlandse OM is zeer belangrijk om huiszoekingen en inbeslagname daadwerkelijk mogelijk te maken. In de twee jaar dat EC3 nu bestaat, heeft die samenwerking zich zeer positief ontwikkeld. Gezamenlijk treden we op. Met de High Tech Crime unit. Met private partners. Met de Nederlandse desk bij Eurojust in hun coördinerende rol bij internationale onderzoeken. En met Lodewijk van Zwieten als landelijk officier cybercrime bij het LP. Ons land start veel opsporingsonderzoeken. Gaat het om het gezamenlijk neerhalen van een ‘botnet’, dan is Van Zwieten hier aanwezig, en vanuit zijn coördinerende rol vanuit Nederland onze gesprekspartner. Sporadisch trekken we ook op met arrondissementsparketten. Ook daarin behoort Nederland tot de koplopers in Europa.” Een andere keuze dan meegaan is er nauwelijks. “De invloed van cyber in onderzoeken wordt zo groot, dat eigenlijk geen officier meer zonder kan. Dat betekent dat we nog veel meer kennis met elkaar moeten delen en elkaar moeten opzoeken. Toch wordt internationaal wel eens geredeneerd: Het is mijn onderzoek, ik ben er mee bezig, en ik weet niet of ik wel bereid ben info te delen.” Na aarde, water, lucht en ruimte is cyber de vijfde dimensie, weet Van Gemert. Vanaf zijn op de negende verdieping gelegen werkkamer kijkt hij uit over Den Haag, en ziet hij in de verte de zee de lucht raken. “Op aarde waren we altijd al, maar daar duurde het duizenden jaren voordat we met elkaar tot een vorm van regulering en wetgeving konden komen. Op zee heeft dat enige honderden jaren geduurd. In de lucht vliegen we nog maar zo’n honderd jaar: ook daar hebben

we een weg gevonden. En in de ruimte is het aantal mensen dat daar beweegt en verblijft, heel beperkt. Maar dan cyber... Het is de enige dimensie die mensen zelf hebben gemaakt en waar binnen veertig jaar tijd 7 miljard mensen gebruik zullen gaan maken. De cyberrevolutie bracht veel meer teweeg dan de industriële revolutie deed. Vriendschappen en relaties, alles speelt zich af via Facebook en Whatsapp. Dat stop je niet. Net zoals mensen die ooit tegen de telefoon en de fax waren, ook kansloos waren.” Criminele community Cyber verandert de criminaliteit, luidt de analyse van Europol. “De criminele kansen nemen toe omdat je de criminaliteit kunt plegen vanaf iedere plek, maar zonder fysieke locatie. Als je dat toepast op georganiseerde criminaliteit, betekent het dat de klassieke bende, met een vaste organisatiestructuur, verdwijnt. Ervoor in de plaats komen netwerken: ‘communities’ met daarbinnen freelancers die hun expertise aanbieden. In zo’n ‘business model’ geldt: cybercrime is een service, met anonimiteit als kenmerk. Op tornetwerken handelen criminelen onzichtbaar en bij bitcoin-betalingen is moeilijker vast te stellen wie de eigenaar van dat digitale geld is. Kijk dan naar de opsporing en vervolging. Het strafrecht redeneert in de eerste plaats vanuit landsgrenzen. En kunnen we bij cybercrime nog uit de voeten met onze juridische definitie van een criminele organisatie (artikel 140 Wetboek van strafrecht)? De tijd om politie en justitiesystemen aan te passen aan deze tijd, is kort. De global conference daarover in Nederland was daarvoor echt noodzakelijk.” De groei van de techniek helpt criminelen, maar biedt ook politie en OM meer mogelijkheden beter en sneller zicht te krijgen. “De smartphone van criminelen, met alles wat dat tegenwoordig op zit, geeft ook kansen.”

Verwijder malware-infecties van je systeem

Natuurlijk is je systeem voorzien van up-to-date antivirussoftware. Maar het kan gebeuren dat die een bepaalde infectie niet helemaal weg krijgt, of dat je er toch aan twijfelt of je pc wel geheel malware-vrij is.

[Norman Malware Cleaner](#) geeft je niet alleen een tweede mening, de tool kan gedetecteerde malware meteen ook verwijderen. Zwaar maar snel

Het downloadbestand mag dan zwaar zijn (circa 350 MB), de tool zelf vereist geen installatie en start verrassend snel op. In principe staat er je niet veel meer te doen dan een van de drie aangeboden scanmodi te selecteren: Quick, Full of Custom. Bij deze laatste bepaal je zelf welke bestanden of mappen moeten worden gescand. Een afzonderlijke 'exclude list' laat je nog aangeven welke mappen je buiten zo'n scanronde wenst te houden.

Na afloop van de scanronde krijg je dan een rapport en kun je gedetecteerde (of vermoedelijke) malware in quarantaine laten plaatsen zodat die geen (verdere) schade aan je systeem kan berokkenen. Overigens is het altijd wel mogelijk een item weer uit quarantaine te halen dat je daar per abuis had geplaatst.

Rootkits verwijderen

[Norman Malware Cleaner](#) herkent uiteenlopende vormen van ongewenste software, waaronder virussen, valse antivirus tools, wormen en rootkits. Het programma gaat standaard wel op zoek naar mogelijke rootkits, maar zal die niet verwijderen – tenzij je deze optie zelf eerst even activeert.

Overigens is het ook mogelijk selectief aan te geven waarop je de tool wilt laten scannen (als je dat zo instelt wordt het geheugen niet mee gecontroleerd of gaat het programma voorbij aan potentiële rootkits of valse antivirus tools).

Dieper graven

Je treft hier tevens een module forensics aan. Activeer je deze functie, dan wordt dieper naar mogelijke malware gegraven, waarbij je zelf bepaalt hoe gevoelig deze heuristische functie moet reageren. De makers voegen er zelf aan toe dat deze module bedoeld is voor gevorderde ge-



Wist jij dit al? Opmerkelijke feitjes over het internet

Het internet is al 25 jaar in ons leven en we krijgen er geen genoeg van. Erg vertrouwd dus, dat internet. Maar wist je deze dingen al over het web?



Opmerkelijke feitjes over het internet

Het internet, het is al 25 jaar in ons leven en we kunnen er maar geen genoeg van krijgen. De gemiddelde Nederlander kijkt voortdurend op zijn smartphone en heeft thuis een alles in 1 pakket dat ook echt voor alles wordt gebruikt. Ook op het werk is internet onmisbaar geworden. Erg vertrouwd dus, dat internet. Maar wist je deze dingen al over het internet?

De eerste e-mail werd al in 1971 gestuurd. De afzender was Ray Tomlinson, de uitvinder van, je raadt het al, e-mail.

81% van alle verzonden e-mails is spam. Dat zijn 200 miljard spamberichten elke dag.

Het internet bevat meer dan 227 miljoen websites en meer dan 65 miljard webpagina's.

Elk uur worden er 4.200 nieuwe domeinnamen geregistreerd. Dat zijn er 37 miljoen per jaar.

De allereerste website ooit ging in 1991 online en is nog steeds te bezoeken op het web.

Meer dan een miljard mensen kijken er per maand naar video's op YouTube.

Elke minuut wordt er 72 uur aan videobeelden geüpload naar YouTube.

80% van de afbeeldingen op het internet zijn van naakte vrouwen.

Meer dan de helft van het internetverkeer bestaat uit het streamen van video's en het delen van bestanden.

Het kost 50 miljoen pk (paardenkracht) om het internet draaiende te houden.

Het internet weegt evenveel als een aardbei. Dat is het gewicht van de miljarden elektronen van data in beweging op het web.

Er zijn meer apparaten op het internet aangesloten dan dat er mensen op de wereld zijn. 8,7 miljard tegenover 7 miljard om precies te zijn.

Zo vertrouwd als het internet is, het heeft toch ook nog veel verrassingen voor ons in petto. Of wist je dit allemaal al? Dat breng je toch echt te veel tijd door op het internet!





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 onlineshopping.

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 verhuilen, 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 beveiliging 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

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

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

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

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

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

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

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

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

Er zijn geen specifieke wetsartikelen om cyber-crime in ruime zin aan te duiden. Voor de hoofddaad worden dezelfde wetsartikelen gebruikt als wanneer de criminele daad niet met ICT zou worden gepleegd.

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

Haatzaaien staat niet als zodanig in het wetboek.

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

- Artikel 147 WvSr: godslastering
- Artikel 90quater WvSr: discriminatie.
- Artikel 137d WvSr: aanzetting tot discriminatie van een bevolkingsgroep.

- . Artikel 137e WvSr: openbaarmaking discriminerende uitlatingen.
- . Artikel 137f WvSr: deelname of steunen van discriminatie.
- . Artikel 137g WvSr: discriminatie in ambt, beroep of bedrijf.
- . Artikel 131 WvSr: opruiing.

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

Relevante wetsartikelen zijn:

Artikel 285b WvSr: belaging.

Artikel 138a WvSr: computervredereuk.

Artikel 266 WvSr: belediging.

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

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

meeting').

Handel in mensen of foute goederen.

Verschijningsvormen:

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

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

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

Relevante artikelen zijn:

Artikel 273a WvSr mensenhandel.

Artikel 416 WvSr opzetheling.

Artikel 417 WvSr opzetheling (gewoonte).

Artikel 274 WvSr slavenhandel.

Artikel 2 Wwm: wet wapens en munitie

Artikel 31 Wwm: overdragen van wapens of munitie

Artikel 2 Ow: opiumwet

Artikel 3 Ow: opiumwet

Artikel 3b Ow: opiumwet



Cybercrime wetsartikelen (2)

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

Relevante artikelen uit het wetboek van strafrecht zijn:

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

Kinderpornografie.

Kinderpornografie is in Nederland strafbaar gesteld in artikel [240b Wetboek van Strafrecht](#).

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

Illegale kansspelen.

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

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

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

op internet'.

Relevante wetsartikelen zijn:

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

[Artikel 1a Wks](#): piramidespelen

E-fraude.

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

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

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

[Artikel 326 WvSr](#): oplichting.

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

[Artikel 231b WvSr](#): identiteitsfraude

[Artikel 310 WvSr](#): diefstal.

[Artikel 321 WvSr](#): verduistering.

[Artikel 416 WvSr](#): heling.

