



Oktober 2014

JAARGANG 3

Secure

Computing

In dit nummer oa:

Europol waarschuwt voor online moorden

Terughacken cybercriminelen praktisch onmogelijk

Hackvrije browser

Doe sporenonderzoek op je PC

Print een sleutel voor elk slot

Veel lees(r)plezier

(NB: met Ctrl+ scrolwielje 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 index klikt u onderaan de pagina op Index

Bronnen:

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

[Europol waarschuwt voor online moorden](#)

[Terughacken cybercriminelen praktisch onmogelijk](#)

[Zeroday attack](#)

[Groen licht voor de administrator](#)

[Overal veilig toegang tot je wachtwoorden](#)

[Hackvrije browser](#)

[Doe sporenonderzoek op je PC](#)

[Print een sleutel voor elk slot](#)

[FBI adviseert een fabrieksreset bij mobiele spyware](#)

[APPLE kan versleutelde iPhone niet ontsleutelen](#)

[Malware wist SD geheugenkaart van Android toestellen](#)

[Hacker hebben vrij spel in PC winkels](#)

[Crypto oorlog](#)

[Facelock: raadt het plaatje als antwoord](#)

[Google hoeft veroordeelde niet te vergeten](#)

[Wissel bestanden uit tussen Windows, MAC, iOS en Android](#)

[Belastingdienst verzamelt gegevens van Marktplaats-adverteerders](#)

[Software schatkist](#)

[Snapshots](#)

[Cops in Cyberspace](#)

[Handig](#)

[Wetsartikelen](#)

Europol waarschuwt voor online moorden

Europol waarschuwt in een rapport voor het dreigende gevaar van moord via internet. Overheden zouden slecht zijn voorbereid. De in 2013 overleden Nieuw-Zeelandse hacker en beveiligingsexpert Jack Barnaby liet een aantal jaren geleden al zien hoe hij een pacemaker, of een insulinepomp, online kon beïnvloeden en zodoende iemand kon ombrengen. Het klinkt als science fiction, maar lijkt realiteit.



De Amerikaanse voedsel- en warenautoriteit (FDA) adviseerde de gezondheidsindustrie onlangs om medische apparaten, die verbonden zijn met internet, te controleren op mogelijke 'zwakke plekken' en deze indien nodig aan te passen. Met de huidige waarschuwing onderschrijft Europol die oproep. Meer en meer elektrische en elektronische apparaten zijn tegen verbonden met het web.

In het rapport [The Internet Organised Threat Assessment \(iOCTA\)](#) beschrijft de Europese politiedienst welke gevaren en risico's die deze koppeling met zich meebrengt. Het vermeldt daarbij een nieuwe vorm van afpersing, zoals losgeld voor gehackte slimme wagens en woningen, maar ook fysiek letsels en 'mogelijke dood'. Daarbij moet bijvoorbeeld worden gedacht aan het ontregelen van pacemakers.

Pacemaker [Dick Cheney](#)

In oktober 2013 liet de voormalig Amerikaanse vice-president Dick Cheney zicht in het televisieprogramma 60 Minutes ontvallen dat zijn cardioloog hem had aangeraden [de draadloze functie van zijn pacemaker uit te schakelen](#), om zo te voorkomen dat het apparaatje gehackt kon worden. Beveiligingsbedrijf IID voorspelde vervolgens dat in 2014 de eerste moord via een met internet verbonden apparaat gepleegd zou worden.

Wil van Gemert, adjunct directeur van Europol, zegt tegen nieuwsblad De Morgen: 'We worden erg afhankelijk van een heleboel apparaten, die soms essentiële levensfuncties regelen. Vandaag zijn er 10 miljard apparaten verbonden met het internet, rond 2020 worden dat er 20 à 50 miljard. Dat verhoogt het risico behoorlijk.' Hackers met criminele bedoelingen liggen op de loer.

'Het lijkt me sensatiezucht'

Joost Bijl van cyberbeveiligingsbedrijf [Fox-IT](#) ziet het gevaar, maar is nuchterder: 'Het lijkt me sensatiezucht. Je kunt niet gericht iemand uitkiezen en die via het net doden, zover is het nog lang niet. De trend is wel om steeds meer apparaten op het internet aan te sluiten, en sommige zijn daar qua veiligheid niet op voorzien.'

Bijl denkt dat Europol vooral wil waarschuwen voor de toekomst. 'Terecht', zegt hij en wijst op een site als [ShodanHQ.com](#) dat gericht zoekt naar online controlesystemen voor onder meer windturbines en energiecentrales. 'Er zijn mensen die via het net op zoek gaan naar open klimaatsystemen in woningen, om de verwarming heel laag of heel hoog te zetten. Als je dat doet in de kamer van iemand die ziek of bejaard is, kan dat verregaande gevolgen hebben.'

Terughacken cybercriminelen praktisch onmogelijk

De wetsvoorstellen die terughacken door de politie mogelijk moeten maken, zijn volgens beveiligingsdeskundigen vooral bedoeld om de opsporingsdiensten op papier meer handvatten te geven. Maar praktische haken en ogen maken het terughacken van geduchte cybercriminelen bepaald geen sine-



[Minister Opstelten](#) wil dat de politie meer bevoegdheden krijgt om terug te hacken. Een van de belangrijkste is de bevoegdheid om computersystemen heimelijk binnen te dringen, het zogenoemde terughacken. Daarbij wordt een trojan bij een cybercrimineel geïnstalleerd, net zoals cybercriminelen [malware](#) plaatsen bij gebruikers.

Een van de methoden die minister Opstelten voorstelt, is om bijvoorbeeld een [keylogger](#) te installeren bij een verdachte. Deze trojan verzamelt informatie die als bewijs kan worden opgevoerd in een rechtszaak. “Door middel van het vastleggen van bepaalde gegevens is het mogelijk om toegang te verkrijgen tot versleutelde gegevens. Hiermee kan worden voorkomen dat de officier van justitie zijn toevlucht moet nemen tot [een de-cryptiebevel](#) aan de verdachte”, schrijft minister Opstelten.

Politietrojan wordt gedetecteerd

Maar zo’n [keylogger](#) wordt simpelweg gedetecteerd, denken antivirusleveranciers en het heimelijk installeren van deze software gaat dan ook lastig worden bij een geduchte cybercrimineel die zijn of haar software op orde heeft. Volgens beveiligingsexpert Eddy Willems van G Data is het zeker niet zo dat leveranciers van deze beveiligingssoftware zullen meewerken aan het doorlaten van een politietrojan.

“Antivirusapplicaties zijn niet verplicht om bijvoorbeeld overheidsmalware niet te detecteren en we waarschuwen dus zeker óók voor deze applicaties”, aldus Willems. “Alle programma’s die niet gewenst zijn op de

computer van de gebruiker zijn per definitie malware, dus ook als het van een overheid afkomt.”

Ook beveiligingsonderzoeker Mikko Hypponen van F-Secure denkt dat standaardbeveiliging voldoende moet zijn. Goede software zorgt er volgens hem voor dat malafide toegang sowieso wordt verijdeld. “Het maakt voor beveiligingssoftware niet uit of je te maken hebt met een Russische cybercrimineel, hacktivist of de politie. Malware wordt tegengehouden.”

Slordige cybercrimineel

“Het doel is om malafide software te detecteren. Als het gaat om nieuwe, nog onbekende malware, dan zorgt de beveiligingssoftware ervoor dat er een waarschuwing komt dat er software wordt gedraaid die zeldzaam is en nauwelijks wordt gebruikt”, vertelt Hypponen aan Webwereld. Een politietrojan wordt dan bij een gebruiker aangemerkt als verdacht, die vervolgens informatie erover kan doorsturen naar de leverancier van de antivirussoftware.

[Trojans](#) krijg je sneller binnen bij mensen die hun systeem niet goed op orde hebben. “Er zijn vaak wel mogelijkheden om in te breken, vooral als mensen minder goede maatregelen gebruiken”, stelt Willems. “Maar het is erg moeilijk om malware te plaatsen bij mensen die security-minded zijn. De Nederlandse High Tech Crime Unit is goed uitgerust om cybercriminaliteit aan te pakken, zeker in vergelijking met andere landen. Maar zo maar meekijken? Zo makkelijk is dat niet.”

De slimme cybercrimineel zal volgens beveiligingsdeskundigen daarom niet snel geraakt worden door overheidsmalware. Dat geldt misschien in mindere mate voor de kruimelcyberdief. “Voor een groot deel is opsporing afhankelijk van de fouten die criminelen zelf maken”, vertelt Willems. “De politie kan pc’s alleen ‘hacken’ als de gebruikers zelf slordig zijn.”

Gebruik [zerodays](#) beperkt

Voor de cybercrimineel die security-minded is, moeten de terughackers dus met zwaarder geschut komen. Dan denk je al gauw aan de nog onontdekte kwetsbaarheden die gebruikt kunnen worden. Hypponen denkt dat het wel mee zal vallen met het gebruik van zerodays om in de computers van burgers in te breken. “Daar bescherm je jezelf inderdaad slecht tegen, maar de politie zal zo’n kwetsbaarheid alleen gebruiken als ze vrij zeker weten dat ze met een zware crimineel te maken hebben”, vertelt hij.

“[Zerodays](#) zijn erg waardevol en daarom ook behoorlijk duur. Als je deze inzet, verspeel je meteen deze optie omdat het gat vervolgens openbaar wordt. Als je als overheid op zo’n dure exploit zit, zal je dat dus niet snel inzetten tegen een doelwit van ondergeschikt belang”, aldus Hypponen die daarom zegt dat de gemiddelde burger niet bang hoeft te zijn voor politiegesnuffel via onbekende gaten in het systeem.

Zeroday attack

Een zerodayattack (of nuluren- of nuldagenaanval, -aanslag of -dreiging) is een computerdreiging die probeert misbruik te maken van zwakke delen in software welke onbekend zijn voor anderen of de softwareontwikkelaar. Zero-day-exploits is software die gebruikmaakt van een daadwerkelijk gat in de beveiliging voor het uitvoeren van een aanval. Deze worden gebruikt of gedeeld door aanvallers voordat de ontwikkelaars van de doelsoftware iets afweten van deze kwetsbaarheid.



Malwareschrijvers zijn in staat 'zero-day-kwetsbaarheden' uit te buiten door middel van een aantal verschillende aanvalsvectoren. Webrowsers zijn een bijzonder doelwit vanwege hun grote verspreiding en gebruik. Aanvallers kunnen ook e-mailbijlagen versturen, die bij het openen van de bijlage actief worden en de kwetsbare software aanvallen.[Exploits die gebruik maken van vaak gebruikte bestandstypen worden opgenomen in databanken zoals US-CERT (United States Computer Emergency Readiness Team). Malware kan worden gemanipuleerd om te profiteren van deze bestandstypes om zo aangevallen systemen te compromitteren of vertrouwelijke gegevens te stelen, zoals bankwachtwoorden en persoonlijke identiteitsgegevens.

Zero-day-aanvallen treden op tijdens het kwetsbare moment dat bestaat uit de tijd tussen het moment dat er een eerste uitbuiting is van het beveiligingslek en wanneer de softwareontwikkelaars komen met een oplossing om de bedreiging tegen te gaan. Bij virussen, Trojaanse paarden en andere zero-day-aanvallen bestaat meestal al deze tijdslijn:

De ontwikkelaar maakt software met een (onbekend) beveiligingslek.

De aanvaller vindt het lek vóór de ontwikkelaar.

De aanvaller schrijft en distribueert een exploit, terwijl het lek nog niet bekend is bij de ontwikkelaar.

De ontwikkelaar is bewust van het beveiligingslek en start met de ontwikkeling van een softwarefix.

Het meten van de lengte van dit kwetsbare moment kan moeilijk zijn. Aanvallers konden niet aan wanneer ze een lek voor het eerst ontdekken. Het is ook mogelijk dat de ontwikkelaars de gegevens niet willen verspreiden voor commerciële- of veiligheidsredenen. Soms weten de ontwikkelaars niet dat het lek al wordt misbruikt na de fix van de software, en dus weten ze niet dat er een zero-day-aanval was. Het kan wel gemakkelijk worden aangetoond dat het lek over langere tijd, bijvoorbeeld verschillende jaren, actief was. Een voorbeeld van in 2008 toen Microsoft bekendmaakte dat er een beveiligingslek in Internet Explorer was, waardoor sommige versies, uitgebracht in 2001, getroffen waren. De datum van de ontdekking van het lek is niet bekend, maar het kwetsbare moment zou in dit geval tot 7 jaar geweest zijn.

Een speciaal type van procesmanagement bij softwareontwikkelaars is gericht op het vinden en het elimineren van zero-day-beveiligingslekken. Het is een proces om de veiligheid en kwaliteit te waarborgen

dat gericht is op het garanderen van de veiligheid en sterkte van zowel in-house-software als software van derden door het vinden en de vaststelling van onbekende (zero-day-)kwetsbaarheden. Deze onbekende manier van procesmanagement bestaat uit vier fasen: Analyseren, testen, rapporteren en het inperken van.

Analyseren: deze fase richt zich op de oppervlakteanalyse van de aanval.

Test: de test fase richt zich op het testen van de geïdentificeerde aanvalsvectoren.

Rapport: deze fase is gericht op de reproductie van de gevonden problemen voor ontwikkelaars.

Beperken: in deze fase kijkt men naar beschermende maatregelen.

[Whitelisting](#) beschermt effectief tegen zero-day-bedreigingen. Whitelisting laat alleen goede en gekende toepassingen toegang tot het systeem en dus elke nieuwe of onbekende exploits hebben geen toegang. Hoewel whitelisting zeer effectief is tegen zero-day-aanvallen, kan een toepassing, bekend om zijn "goedheid", kwetsbaarheden hebben die niet ontdekt zijn tijdens het testen op beveiligingslekken.

Groen licht voor de administrator

Sommige programma's vereisen administrator-rechten om (volledig) te kunnen functioneren. Vervelend is wel dat het gebruikersaccountbeheer van Windows dan telkens weer om je toelating vraagt. Tenzij je die al (eenmalig) aan UAC Pass hebt gegeven...



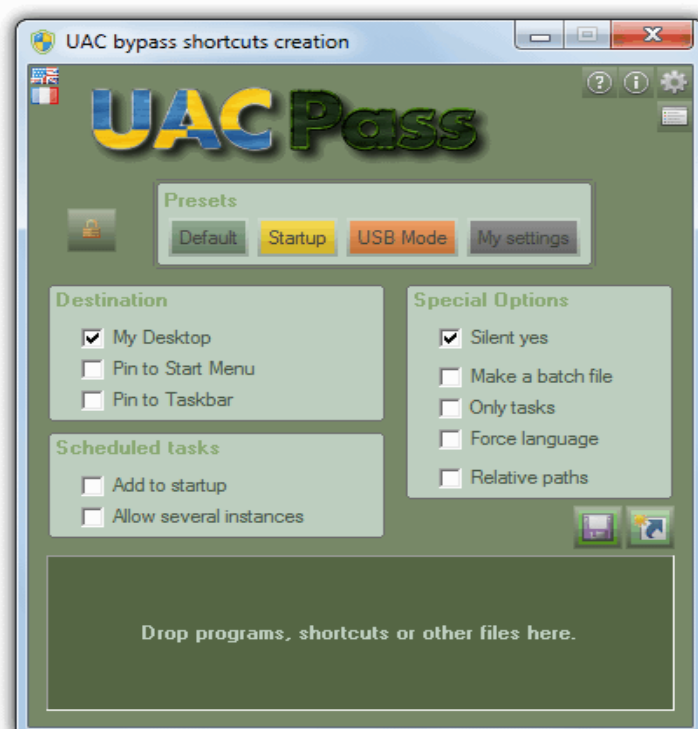
[UAC Pass](#) maakt het gebruikers accountbeheer wat permissiever.

Voor alle duidelijkheid: je kunt vanuit Windows zelf ook wel het UAC op betere gedachten brengen door het beveiligingsniveau (via het Configuratiescherm) op een lager pitje te zetten, maar erg veilig en dus verstandig is dat niet. Je doet er daarom beter aan een tool als UAC Pass in te zetten. Die maakt het namelijk mogelijk dat de beveiliging je niet langer om de oren zal slaan voor specifieke programma's, althans niet voor toepassingen die je zelf hebt geselecteerd.

Moeilijk is het in elk geval niet! Je start het programma op (dat trouwens niet eens een installatie behoeft) en je versleept de snelkop-

peling van de beoogde toepassing naar het venster van UAC Pass. Verder geef je aan waar de nieuwe snelkoppeling moet terechtkomen: op je bureaublad, vastgepind aan het startmenu of op de Windows taakbalk. Dat is het ongeveer.

Wanneer je vervolgens de nieuw gecreëerde snelkoppeling opstart, zal het Windows gebruikers accountbeheer je niet langer lastig vallen met de vraag of je het programma wel degelijk met administratorrechten wilt uitvoeren. Een kleine tool dus, maar best wel handig wanneer je vaak 'elevatie van gebruikersmachtigingen' nodig hebt voor deze of gene toepassing.



Overall veilig toegang tot je wachtwoorden

We hoeven het je vast niet meer te vertellen: altijd en overall hetzelfde wachtwoord kiezen is niet veilig. Maar telkens een ander, complex wachtwoord instellen is erg lastig. Tenzij je al je login-ID's veilig versleuteld in een digitale kluis stopt, die je op zijn beurt vergrendelt met een stevig hoofdwachtwoord. Dat is precies het idee van Safe in Cloud.



Safe in Cloud is er in verschillende vormen: een gratis desktopapplicatie voor Windows, een gratis browserextensie voor Firefox en Chrome (die weliswaar ook de installatie van de desktopapplicatie vereisen gezien die tool op de achtergrond actief moet zijn) en twee mobiele betaalapps, voor Android en iOS.

En er is uiteraard nog de cloud. Als je dat zo instelt, synchroniseert Safe in Cloud je wachtwoorden automatisch en veilig versleuteld met AES 256-bits naar je [Dropbox](#), Google Drive of OneDrive.

Installeren

We houden het hier even bij het Windowsverhaal.

Installeer je eerst de browserextensie en druk je de Safe in Cloud-knop in de

browserbalk in, dan klaagt die erover dat Safe in Cloud niet is gestart. Bedoeld wordt de desktopapplicatie dus. Je moet die dus eerst (ook) installeren.

Tijdens de installatie krijg je de vraag of je een nieuwe database wil creëren dan wel je database wil herstellen vanuit de cloud. Dat laatste is zeker zinvol mocht de lokale database van een eerder geïnstalleerde Safe in Cloud corrupt zijn geworden. Uiteraard scherm je je database vervolgens af met een stevig wachtwoord.

Vervolgens beland je in het hoofdvenster van Safe in Cloud. De interface ziet er fris en overzichtelijk uit en bevat een drietal panelen: links de rubrieken (waarin je de diverse login-ID's en aanverwanten kunt onderbrengen), in het midden een lijst met ID's van de geselecteerde rubriek en rechts de inhoud van de geselecteerde ID. Allemaal vrij logisch dus.

Zo'n ID (oftewel: ingang in de database) noemt Safe in Cloud een 'kaart'. Je kunt een onbeperkt aantal van die kaarten aanmaken. Overigens is het ook mogelijk notities te creëren – je weet nooit waar zo'n infoblaadje nuttig voor kan zijn. Bij het creëren van zo'n kaart kun je uit diverse sjablonen kiezen, met telkens een aantal specifieke velden. Kies je bijvoorbeeld

voor Creditcard, dan verschijnen velden als naam, nummer, vervalt, cvv, pin enzovoort. Kies je Webaccount, dan duiken de velden inloggen, wachtwoord en URL op, enzovoort.

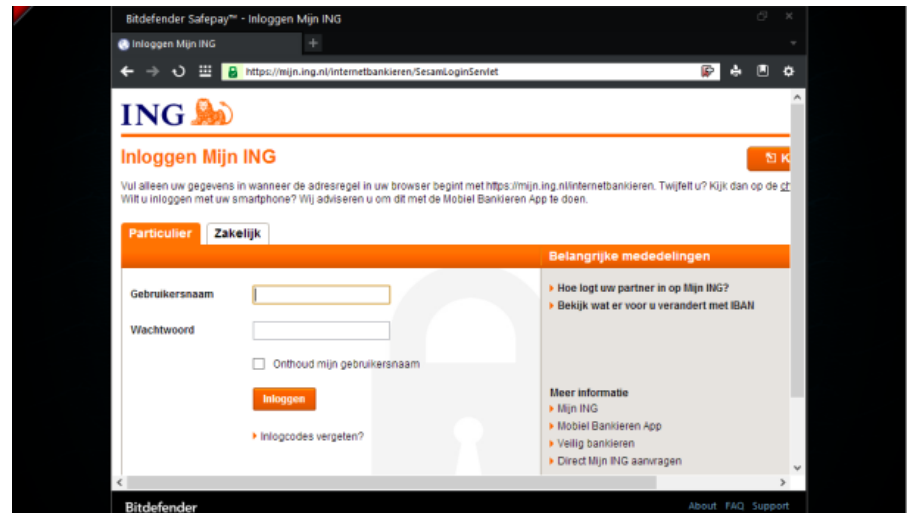
Dankzij de webintegratie – met behulp van plug-ins voor Firefox en Chrome – kan je naderhand zonder veel moeite de juiste 'kaart trekken'. Als het goed is, haalt Safe in Cloud automatisch de juiste kaart op op basis van de URL van de site. Maar je kunt altijd nog (manueel) voor een andere kaart kiezen, vanuit het contextmenu.

[DOWNLOAD](#)

[Index](#)

'Hackvrije' browser

Hoewel banken en overheid steeds meer maatregelen nemen om diefstal in je online bankrekening te voorkomen, lukt het cybercriminelen nog altijd om een uitstekende boterham te verdienen.



De installatie van [Bitdefender Safepay](#) op zich vergt slechts enkele muisklikken. Je moet echter direct erna een account aanmaken bij Bitdefender en op de link in de bevestigingsmail klikken. Pas hierna kun je verder met Bitdefender Safepay.

Allereerst voert het programma een malwarescan op je systeem uit om het risico op infecties te verkleinen. Wanneer het programma is opgestart, is het wel even schrikken: van je bureaublad is geen spoor meer te zien. Er wordt namelijk een gevirtualiseerde omgeving ([sandbox](#)) gecreëerd waarbinnen Bitdefender Safepay opereert, geheel gescheiden dus van (de andere applicaties op) je systeem.

Op zich stelt het programma niet zo veel voor: het blijkt om een sterk uitgekleden browser te gaan, gebaseerd op Chromium. Dit is ook de bedoeling: je zult hier geen overtollige plug-ins vinden die het risico op infecties alleen maar kunnen vergroten.

Kale browser

Veel instellingen zijn er dan ook niet. Zo maak je duidelijk of je Java en/of Flash wil activeren, stel je desgewenst een proxy in en geef je aan of Bitdefender Safepay bij elke start de malwarescan moet uitvoeren. Je bepaalt ook zelf tegen welke soort sites het programma je moet beschermen: fraude, phishing, malware, spam enzovoort.

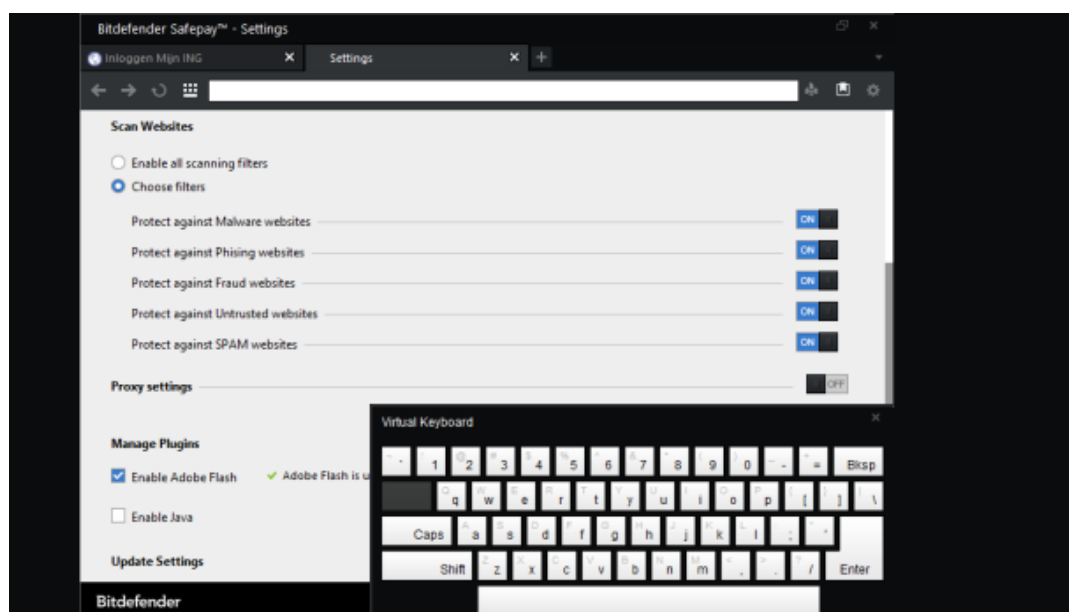
Veiligheidshalve laat je uiteraard alle filters geactiveerd. Verder biedt de browser je nog de mogelijkheid om veel bezochte pagina's te bookmarken en om pagina's naar je standaardprinter te sturen. Om [keyloggers](#) de pas af te snijden, kun je in de browser een virtueel toetsenbord oproepen. Jammer genoeg bleek deze functie op onze testtoestellen niet goed te functioneren.

Heen en weer

Wil je tijdelijk terug naar je vertrouwde bureaubladomgeving, dan hoeft je niet noodzakelijk de browser geheel af te sluiten. Linksboven tref je namelijk een knop aan waarmee je meteen je bureaublad te zien krijgt. Op het bureaublad vind je rechtsboven eenzelfde knop terug die je direct terugbrengt naar de afgeschermdede omgeving van Bitdefender Safepay.

Er is ook een betaalde variant van het programma beschikbaar, deze biedt je onder andere bescherming bij het gebruik van (mogelijk onveilige) wifi hotspots.

Wie het maar eng vindt om via zijn browser online bankbetalingen uit te voeren, is een goede kandidaat voor BitDefender Safepay, een veilige 'hackvrije' browser, die grotendeels gratis is.



Doe sporenonderzoek op je pc (of die van een ander....)

OSForensics is, zoals de naam al doet vermoeden, een forensische tool. Je kan er dus allerlei – vaak diep verborgen - data mee uit opvissen uit een systeem.



Ga er voor persoonlijke lering en vermaak gerust mee aan de slag op je eigen toestel, maar let er wel voor op die, zonder expliciete toestemming, in te zetten op een systeem van derden.

In tegenstelling tot veel andere forensische tools oogt de interface van [OSForensics](#) erg overzichtelijk, uitnodigend haast. Het hoofdvenster is opgesplitst in een 7-tal rubrieken, met telkens een aantal bijhorende tools. De rubrieknamen laten weinig aan de verbeelding over: File Searching & Indexing, Hashing & File Identification, Viewer, System Artifacts & Passwords, ...

Naast de klassieke zoekfuncties, waarmee je zowel naar bestaande als naar verwijderde bestanden kunt zoeken, bevat OSForensics ook geavanceerde zoekopties die je bijvoorbeeld toelaten om snel alle sporen van recente computer- en internetactiviteit te verzamelen. Of je spoort naar 'mismatched file types', waarbij iemand bijvoorbeeld een documentbestand de extensie .jpg heeft meegegeven (of omgekeerd) om bepaalde sporen te maskeren.

Het is eveneens mogelijk eigen indexen te creëren van bepaalde bestandstypes en locaties. Die

kan je vervolgens inzetten om zeer snel naar een of ander trefwoord te zoeken.

Verder heeft de tool nog een reeks 'viewers' aan boord, waarmee je ook op hex-niveau de inhoud van bestanden en van fysieke schijven kan bekijken. Dat maakt het bijvoorbeeld mogelijk headers van bepaalde bestanden te analyseren of een kijkje te nemen in de sectoren buiten de Windows-partities (waarin zich onder meer de MBR bevindt). Ook een module voor het opsporen van allerlei wachtwoorden ontbreekt niet. Het duurde bijvoorbeeld maar enkele seconden om de wachtwoorden op te diepen die onze drie browsers "veilig" hadden opgeslagen. En wie aast op wachtwoorden van Windows-accounts: je kan gebruik maken van [Rainbow-tables](#) om ook lastige wachtwoorden aan te pakken.

OSForensics

[Index](#)

Print een sleutel voor elk slot

Met een 3D-printer, een foto van het sleutelgat en een handig stukje software maken deze inbrekers je deur moeiteloos open - geen gestolen sleutel



Twee beveiligingsconsultants en competitie-slotenkrakers hebben een techniek ontwikkeld waarmee inbreken plots wel erg eenvoudig wordt.

Ze ontwikkelden een specifiek stuk software, Photobump genaamd, waarmee ze een slagsleutel of bump key kunnen produceren met een 3D-printer. En in tegenstelling tot de meeste methodes die inbrekers vandaag gebruiken, hebben ze er geen bestaande sleutel voor nodig - een foto van je slot volstaat.

Slagsleutels op zich zijn niets nieuws. Het concept is relatief eenvoudig. Traditioneel wordt een sleutel afgevijld, met uitzondering van een aantal tanden die tegen de pinnetjes in een standaardslot rusten. Door de sleutel in het slot te schuiven en er op de juiste manier en met de correcte torsie tegen te tikken met een hamer, kan een goede slotenkraker de pinnen verplaatsen tot het slot opent.

Zo'n sleutels waren echter altijd moeilijk te maken voor complexe sloten. Fabrikanten van sloten van hoge kwaliteit gaan ook erg voorzichtig om met de ontwerpen voor hun sleutels, waardoor het voor inbrekers moeilijker wordt om een voorbeeld te pakken te krijgen.

Met de software die Jos Weyers en Christian Holler ontwikkelden heb je echter helemaal geen voorbeeldsleutel no-

dig. "Als ik weet hoe je slot eruit ziet en hoe diep het is, kan de software een bump key produceren," zei Weyers.

Er is echter nog niet meteen reden voor paniek. Het slotenbrekende duo is niet van plan om hun techniek en software door te verkopen aan de hoogste criminele bidder - het zijn uiteindelijk security-specialisten. Wel willen ze de aandacht van slotenproducenten trekken.

Op dit moment vertrouwen veel slotenmakers erop dat de geheimgehouden vorm van hun sleutels hun sloten beveiligd tegen [bumping](#). "Dat is een vals gevoel van veiligheid," zegt Holler. "Als je alleen vertrouwt op een geheim sleutelprofiel, dan moet je je ervan bewust zijn dat dit niet langer volstaat."

Holler en Weyers stellen dat de techniek alleen maar goedkoper en eenvoudiger zal worden als 3D-printers meer ingeburgerd raken. "De wereld verandert, en mensen kunnen nu makkelijker dan ooit objecten maken," zegt Weyers. "Slotenfabrikanten weten hoe ze een slot moeten maken dat bump-bestendig is. Ze kunnen er maar beter werk van maken."

Klik [hier](#) voor de video !



FBI adviseert fabrieksreset bij mobiele spyware

Eigenaren van een smartphone die vermoeden dat ze zelf of iemand anders spyware op het apparaat hebben geïnstalleerd krijgen het advies van de FBI om een fabrieksreset uit te voeren.



Het advies volgt op de arrestatie van de aanbieder van het programma StealthGenie.

Dit is een vorm van spyware om onopgemerkt gesprekken, sms-berichten, e-mail, video's en andere communicatie op mobiele telefoons te monitoren. In het geval van StealthGenie is het nodig om fysiek toegang tot het toestel te krijgen. "Als een gebruiker zich zorgen maakt over de mogelijke aanwezigheid van spyware op hun telefoon, is de enige manier om er zeker van te zijn dat de app permanent van de telefoon wordt verwijderd het uitvoeren van een fabrieksreset", aldus de FBI.

Bij het resetten van de instellingen wordt de telefoon in de oorspronkelijke staat hersteld. De FBI waarschuwt wel dat hierbij alle gegevens en apps die sindsdien geïnstalleerd zijn zullen worden verwijderd. Daarom is het belangrijk om eerst een back-up te maken. Verder merkt de Amerikaanse opsporingsdienst op dat een fabrieksreset er niet voor zorgt dat eerder verzamelde informatie door de spyware kan worden verwijderd.



Apple kan versleutelde iPhone niet ontsleutelen

Met de lancering van iOS 8 heeft Apple een belangrijke beveiligingsmaatregel toegevoegd waardoor bestanden op iOS-toestellen automatisch worden versleuteld als gebruikers een passcode instellen en een bekende professor op het gebied van encryptie heeft nu in technisch detail uitgelegd waarom Apple versleutelde iPhones niet kan ontsleutelen.

iOS 8
Great OS. Great design.
Now in color.



Hoewel [encryptie](#) ook al in iOS 7 aanwezig was, worden via de nieuwe maatregel nu veel meer gegevens versleuteld en kan Apple de versleutelde gegevens niet ontsleutelen, tot onvrede van de FBI en Europol. De sleutel voor de encryptie wordt afgeleid van de passcode van de gebruiker gecombineerd met een unieke geheime 256-bit sleutel genaamd UID, die in de hardware van de telefoon wordt opgeslagen, waar die lastig te achterhalen is. Apple stelt dat het deze sleutels niet opslaat of kan benaderen.

Secure Enclave

Bij nieuwere iOS-apparaten, die over een A7 of nieuwere A-processor beschikken, wordt de sleutel en het "mixproces" nog eens extra beveiligd middels een cryptografische co-processor genaamd Secure Enclave. De Secure Enclave is ontworpen om het uitlezen van de UID-sleutel te voorkomen. Op oudere Apple-apparaten bevond deze sleutel zich in de applicatieprocessor zelf.

Secure Enclave biedt een extra beveiligingslaag die zelf blijft werken als de applicatieprocessor is gecompromitteerd, bijvoorbeeld via een jailbreak. Dat stelt Mathew Green, cryptograaf en onderzoeksprofessor aan de John Hopkins Universiteit. Aangezien alleen het apparaat het UID kent, en het UID niet uit de Secure Enclave kan worden gehaald, houdt dit in dat alle pogingen om het wachtwoord te kraken op het apparaat zelf moeten worden gedaan.

Apple stelt dat het kraken van een willekeurig wachtwoord van zes karakters bestaande uit kleine letters en cijfers 5,5 jaar in beslag neemt. Een pincode kan echter al binnen een half uur worden gekraakt, aldus Green. Hij merkt op dat het dus belangrijk voor iOS-gebruikers is om een sterke passphrase te kiezen.



Malware wist SD-geheugenkaart van Android-toestellen

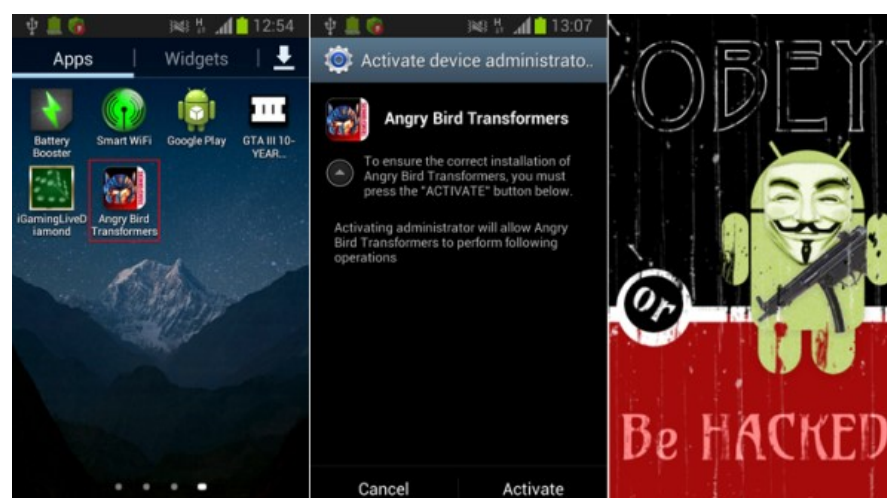
Onderzoekers hebben een Trojaans paard ontdekt dat van Android-toestellen de SD-geheugenkaart wist en de vensters van populaire chat-applicaties als WhatsApp, Hangouts, Facebook en de standaard sms-applicatie blokkeert.



Daarnaast stuurt de 'Elite Trojan', zoals de malware wordt genoemd, om de vijf seconden naar alle contacten in het adresboek een sms met de tekst "Elite has hacked you. Obey or be hacked."

Het bericht wordt ook als antwoord op ontvangen sms-berichten verstuurd, zo meldt het Russische anti-virusbedrijf Doctor Web. De Elite Trojan doet zich voor als het spel Angry Bird Transformers. Zodra de malware actief is vraagt het gebruikers om beheerdersrechten, zogenaamd om de installatie af te ronden. In werkelijkheid gebruikt het Trojaanse paard deze rechten om de SD-geheugenkaart te formatteren en alle aanwezige data te wissen.

Hierna wacht de Trojan totdat de gebruiker populaire chat-applicaties start en blokkeert vervolgens het actieve venster hiervan en laat een afbeelding met de tekst "OBEY or Be HACKED" zien. Verder verbergt de malware de waarschuwing dat er een sms-bericht is ontvangen en stuurt vervolgens om de vijf seconden een bericht naar alle contacten in het adresboek. Doctor Web adviseert gebruikers om geen apps van onbetrouwbare bronnen te downloaden, wat suggereert dat de Elite Trojan op onofficiële marktplaatsen en websites wordt aangeboden.



Hackers hebben vrij spel in pc-winkels

Het is bij Media Markt, MyCom, Paradigit en Computerland mogelijk malware te activeren op laptops in de winkel. Dat blijkt uit onderzoek van Computerworld. Getroffen winkels ondernemen actie.



Computerworld verkende de situatie in de locaties na een tip van een informati-castudent, die zegt maandenlang showmodellen van Saturn (nu omgedoopt tot Media Markt) misbruikt te hebben voor het minen, ofwel het aanmaken, van [Bitcoins](#). In één maand zegt hij vorig jaar met behulp van 105 showmodellen €500 verdiend te hebben. In een vestiging van MyCom claimt hij via een webcam van een van de aanwezige laptops bezoekers bespioneerd te hebben.

Het gesignaleerde gebrek aan beveiliging maakt duidelijk dat elke kwaadwillende de voorbije jaren persoonsgegevens van bezoekers heeft kunnen stelen. Wie op een van de showmodellen Facebook of zijn e-mail opent, loopt risico persoonlijke data te delen. Op een deel van de demonstratiemodellen bij de computerwinkels draait tevens geen antivirusprogramma, zodat malware niet wordt gedetecteerd of geblokkeerd.

'Vooral zaak van locaties en leveranciers'

Media-Saturn Netherlands, eigenaar van Media Markt, zegt in een reactie dat 'het niet mogelijk zou moeten zijn op showmodellen malware te draaien'. De keten is van mening dat 'een showmodel voldoende beveiligd moet zijn met het wachtwoord van een beheerder'. Dat zegt Rob Okhuijsen, pr- en crisismanager bij Media-Saturn Netherlands, in een emailreactie.

Nu het toch mogelijk blijkt malware te implementeren, legt de Nederlandse moedermaatschappij de verantwoorde-

lijkheid neer bij de leidingen van de afzonderlijke locaties. Media-Saturn is van elk van zijn locaties 90% eigenaar, 10% is eigendom van een franchisenemer.

Okhuijsen: "Aanlevering en installatie van de showmodellen gebeurt vooral in overleg tussen leveranciers en winkels. Als de beveiliging niet goed geregeld is, dan moet dáár iets aan veranderen."

"Dank daarom voor de tip. We gaan in overleg met de locaties en leveranciers en gaan samen met hen de feiten na. Daar waar nodig komen we met nieuwe, dan wel aangescherpte protocollen."

Beveiliging optimaliseren

Opmerkelijk is dat ketens niet of maar gedeeltelijk oplossingen benutten zoals de kioskmodus, waarmee de keuzevrijheid op een showmodel beperkt kan worden tot gebruik van één of enkele applicaties. Verder zijn er een reeks andere opties waarmee protocollen aan te scherpen zijn.

"Je kunt malware simpel weren op showmodellen", weet ook de anonieme tipgever, die gestopt is met hacken in winkels omdat hij naar eigen zeggen inzag dat zijn activiteiten 'niet door de beugel konden'. "Verleen in ieder geval geen internettoegang, blokkeer de automatische uitvoer van bestanden via de USB-uitgang en zorg er dat de harde schijven van alle pc's automatisch 's nachts worden gewist."

'Computerwinkel verkapt internetcafé'

Lub ten Napel, de CIO van MyCom-eigenaar [BAS Group](#), spreekt van 'een delicate situatie'. "Enerzijds erken ik dat we alleen optimale beveiliging kunnen bieden als showmodellen geen toegang tot het internet bieden, anderzijds is de optie altijd online te gaan essentieel voor de klantbeleving die we bieden. Zo niet het allerbelangrijkste. Je kunt de BAS Group niet alleen typeren als winkel, maar ook als internetcafé."

De BAS Group, die maandelijks in 200 winkels ruim 160.000 bezoekers ontvangt, zegt al een tijd met het probleem te 'worstelen'. Ten Napel: "De worsteling zit in wat je wel en niet kan voorkomen en wat je wel of niet afschermt om niet af te doen aan de beleving van het opgestelde apparaat. We hebben wel eens webcams afgeplakt, maar klanten willen alles testen en dus gaat het plakband er weer af. Ook hebben we memo's geplaatst die bezoekers op de gevaren wijzen, maar dat soort waarschuwingen schrikken de consument ook af."

Desalniettemin intensiveert Ten Napel nu de zoektocht naar een waterdichte beveiliging. "We spreken ons personeel erop aan dat het scherper let op verdacht gedrag van bezoekers. Ook installeren we over twee maanden, samen met Microsoft en Intel, een kioskmodus op onze showmodellen. Daarmee kunnen mensen niet zomaar van alle programma's en functionaliteiten gebruik maken. Waar mogelijk volgen er nog meer maatregelen."

Facelock: raad het plaatje als wachtwoord

Wachtwoorden hebben hun beste tijd gehad. Deze techniek vraagt je om het gezicht van een persoon die jij kent aan te wijzen.



Bij het creëren van wachtwoorden draait het niet noodzakelijkerwijs om de moeilijkheidsgraad die we bedenken. Een letterreeks blijft eenvoudig te kraken en het wachtwoordsysteem is daarom allang achterhaald. Er worden heel nieuwe dingen geprobeerd en een van deze technieken is [Facelock](#), waar een aantal wetenschappers onlangs over publiceerde in wetenschappelijk tijdschrift PeerJ.

We kijken vaak naar hightech toepassingen als irisscans als een manier om authenticatie uit te voeren, maar Facelock gebruikt geen gezichtsherkenning. De techniek is gebaseerd op psychologisch onderzoek om te bepalen hoe en wanneer je een gezicht herkent als deze op een scherm is te zien. De software herkent jou dus niet, maar jij moet juist gezichten identificeren.

In de praktijk zou het zo ongeveer gaan:

Je kiest een set gezichten die jij kent, maar die een andere gebruiker mogelijk niet kent.

Je krijgt een raster met gezichten te zien en je moet bijvoorbeeld "persoon A" aantikken.

Volgens het gekoppelde onderzoek is het haast onmogelijk om een bekend gezicht kwijt te raken, dus als je weet hoe iemand eruit ziet, kun je een specifiek gezicht snel herkennen in een raster met gezichten. Andersom kan iemand die jou of de gezichten niet kent niet snel een correcte keuze maken. Zelfs als je een

keuze maakt uit gezichten van bekende mensen, is het voor een ander moeilijk om de juiste keuze te maken. Ze herkennen dan de rij beroemdheden, maar weten bijvoorbeeld niet wie daarvan je hebt uitgekozen voor je account.

Op dit moment is er maar één app beschikbaar die deze functionaliteit benadert. Bedrijven kunnen Passfaces integreren in hun authenticatiesysteem en met deze software kiezen gebruikers een gezicht uit een groep mensen om toegang te krijgen. Bij Facelock zou je dan zelf de gezichten uit kunnen kiezen en daarmee mensen die je kent kunnen gebruiken. Daarmee wordt het nog makkelijker om je 'wachtwoord' te onthouden, terwijl het nog steeds lastig is voor anderen om de juiste keuze(s) te maken.

Het is een goede zaak dat er zoveel stappen genomen worden om authenticatie te verbeteren. Facelock heeft niet dezelfde aantrekkingskracht als een James Bond-gadget, maar het is niettemin interessant. Het lijkt misschien nu nog vreemd, maar een techniek als deze is over een paar jaar gemeengoed. En daar kunnen we dankbaar voor zijn, want zo zijn we straks verlost van die ellendige wachtwoorden en wordt informatiebeveiliging tegelijkertijd sterker. Laten we daarom hopen dat Facelock een vlucht neemt.



Google hoeft veroordeelde niet te 'vergeten'

Google hoeft de naam van escortbaas Arthur van M, veroordeeld voor het plannen van een huurmoord, niet uit de zoekresultaten te wissen.



Het eerste vonnis in Nederland over het recht om vergeten te worden is duidelijk: Google hoeft zoekresultaten die voor een veroordeelde onwelgevallig zijn niet te verwijderen.

De zaak is aangespannen door Arthur van M. die in 2012 is veroordeeld voor het opdracht geven van een moord op een concurrerende escortbaas. De moord ging overigens niet door.

Hij eiste dat Google een lijstje met links moest wissen als je zocht op zijn volledige naam, maar ook op afgekorte versies daarvan. Bovendien moest Google de [autocomplete](#) wijzigen, omdat die zijn naam meteen koppelde aan Peter R. De Vries, die een uitzending aan de zaak wijdde, die leidde tot zijn veroordeling. Die associatie is "irrelevant en onlogisch" aldus de klager.

Crimineel verleden blijft relevant

Maar de rechtbank Amsterdam geeft nul op het rekest. Opmerkelijk aan de zaak is dat Google na het vergeetverzoek al zelf enkele links had verwijderd, maar Van M. wilde zijn naam en criminele daad verregaand wegpoetsen. Zelfs een link naar een boek over de zaak moest weg.

Maar dit verleden is zonder twijfel relevant, oordeelt de rechtbank, dus de criteria uit het historische Costeja-arrest gaan niet op: "Bij de beoordeling van de verzoeken tot verwijdering van eiser onwelgevallige zoekresultaten dient voorop te worden gesteld dat in dit kort geding ervan dient te worden uitgegaan dat eiser in 2012 is veroordeeld voor poging tot uitlokking van een huurmoord. Dat eiser tegen dat vonnis hoger beroep heeft ingesteld, doet daaraan niet af."

Koppeling Peter R. blijft

Ook de pijnlijke autocomplete-associatie met Peter R. De Vries hoeft niet weg, die is immers automatische genereerd op basis van eerder ingevoerde zoektermen, en dus wel degelijk relevant.

"De veroordeling voor een ernstig misdrijf zoals het onderhavige en de negatieve publiciteit als gevolg daarvan zijn in het algemeen blijvend relevante informatie over een persoon", concludeert de Amsterdamse rechtbank in het donderdag uitgesproken vonnis.

Google Nederland laat weten: "Deze Nederlandse uitspraak geeft nuttige richtlijnen voor wat betreft de vraag hoe aan de

uitspraak van het Europese Hof van Justitie voldaan kan worden, en verduidelijkt hoe om te gaan met verwijderingsverzoeken die gaan over criminele veroordelingen."

Recht op een update

De advocaat van de klager hekelt het vonnis en overweegt hoger beroep. Volgens haar gaat wel degelijk om informatie die niet (meer) klopt, alsmede links naar een "apert lasterlijk" boek dat uit de handel is gehaald.

"Het ging in deze procedure niet zozeer om 'het recht om vergeten te worden', als wel om 'het recht op een update'. Deze geautomatiseerde update in de zoekmachines van Google is cliënt helaas door de rechter niet vergund", aldus Dieuwke Levinson-Arps.

Wel is ze te spreken over het feit een kort geding 'achter gesloten deuren' werd toegelaten. "Ook andere klagers kunnen deze snelle, directe en tot aan de uitspraak vertrouwelijke procedure voor de rechter dus inzetten."

Wissel bestanden uit tussen Windows, Mac, iOS en Android

Er zijn veel oplossingen en diensten om bestanden te versturen via internet. Send Anywhere maakt het eenvoudig om bestanden uit te wisselen tussen Windows, Mac, iOS en Android. Het enige dat je nodig hebt is een internetverbinding en webbrowser. Voor smartphones en tablets is een app be-



Stap 1: Send Anywhere

Met [Send Anywhere](http://www.send-anywhere.com) kun je bestanden versturen en ontvangen. Hierbij wordt geen gebruik gemaakt van een 'tussenserver' waarbij je bestand tijdelijk wordt opgeslagen. Send Anywhere werkt volgens het p2p-principe. Dit houdt in dat de verzendende partij online moet zijn als de ontvangende partij het bestand wil binnenhalen. Registratie en mailadressen achterlaten is overbodig, je kunt Send Anywhere direct gebruiken op elk apparaat en elk besturingssysteem.

Stap 2: Verzenden

De website van Send Anywhere werkt met twee type bezoekers: een zender en een ontvanger. Surf op de computer vanwaar je bestanden wilt versturen naar www.send-anywhere.com. Klik op Add files en kies de bestanden die je wilt sturen. Je kunt meerdere bestanden gelijktijdig selecteren of steeds de knop Add files gebruiken om meer bestanden klaar te zetten om te versturen. Bevestig met de knop Send files. De website toont onder andere een korte cijfercode en QR-code.

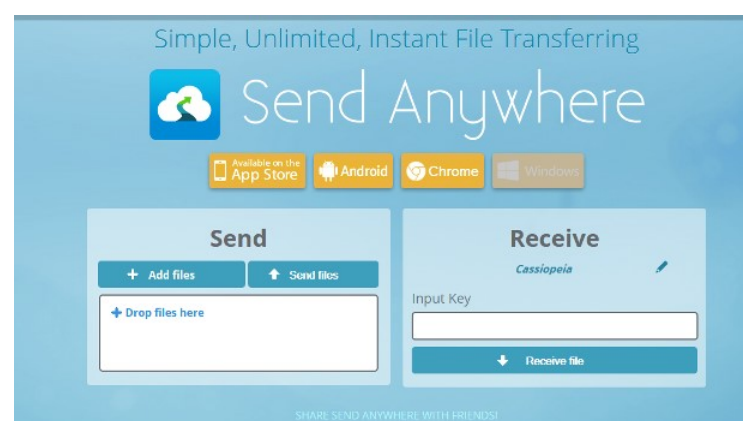
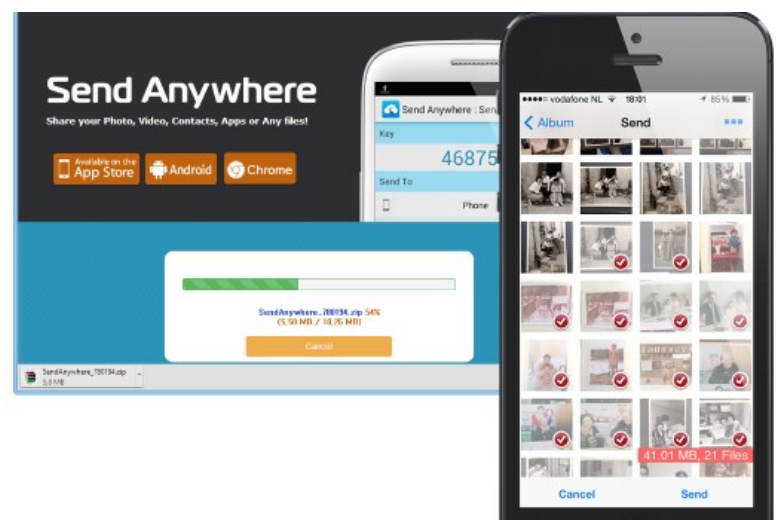
Iemand (jij of een ander) die de bestanden die zojuist zijn klaargezet wil ophalen, surft naar www.send-anywhere.com. Geef de korte cijfercode op bij Input key en haal de bestanden binnen met de knop Receive file.

Stap 3: Van- en naar mobiel

Voor iOS- en Android-gebruikers is er een Send Anywhere-app. Hiermee kun je bestanden eenvoudig versturen vanaf je smartphone/tablet naar je eigen computer of andere smartphone/tablet. De werking is nagenoeg hetzelfde als de website: tik op Send, geef aan wat je wilt versturen en de app toont een korte cijfercode en QR-code. Als je bestanden wilt ontvangen, kun je een korte cijfercode opgeven bij Receive. De optie Scan QR code maakt het intikken van de cijfercode zelfs overbodig en is handig om bestanden te ontvangen van je eigen computer.

Send Anywhere kan overal en altijd gebruikt worden: thuis, onderweg en met elk type apparaat.

Send Anywhere is niet alleen handig om bestanden met anderen uit te wisselen, je kunt de dienst ook gebruiken in je thuisnetwerk om iets van een pc naar je laptop te kopiëren. Ingewikkelde netwerkinstellingen en prutsen met gedeelde mappen is niet nodig, Send Anywhere werkt direct!



Belastingdienst verzamelt gegevens Marktplaats-adverteerders

De Belastingdienst ontvangt regelmatig gegevens van Marktplaats-gebruikers. Onder andere persoonsgegevens (zoals adressen, telefoonnummers en IP-adressen) en geplaatste advertenties worden opgevraagd door de fiscus.



Dat blijkt uit berichten van RTL Nieuws. Daar zou een memo van de Belastingdienst zijn uitgelekt, waarin het protocol voor het opvragen van gebruikersdata is vastgelegd.

Oude advertenties

[De Belastingdienst](#) kan naast persoonsgegevens ook advertenties opvragen van maximaal 4 jaar oud. Dat kan handig zijn voor de fiscus om onderzoek te doen naar oude transacties en inkomsten van mensen.

Rekeningnummers

De Belastingdienst kan geen gegevens als wachtwoorden achterhalen, maar wel bankrekeningnummers in bepaalde gevallen. Dat mag echter alleen als de fiscus de identiteit van de adverteerder niet kan achterhalen, of als er vermoedens zijn dat iemand heeft lopen frauderen bij zijn belastingaangifte.

Fraude

De gegevens zijn volgens de Belastingdienst nodig "om fraude te voorkomen", en merkt op dat overheidsinstellingen een wettelijk mandaat hebben dergelijke informatie te verzamelen. Marktplaats zegt tegen RTL de informatie "niet pro-actief aan te leveren", maar

alleen als de fiscus daar om vraagt.

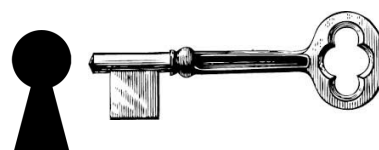
Profielen van onschuldige burgers

De Belastingdienst is groot fan van het verzamelen van grote hoeveelheden persoonlijke informatie - zo werd onlangs al bekend dat de fiscus op grote schaal profielen aanmaakt van alle Nederlandse burgers, uiteraard "om fraude tegen te gaan".





Software schatkist



Browser Hijack Recover

Trusteer Rapport

Blackberry Desktop Software

PC Transfer

DVD Flick

EaseUs Partition Master

EmsiSoft Emergency Kit

Any Burn

Freemake Video Converter



Marechaussees die deel uitmaken van de VN-missie in Mali zijn door de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) gewaarschuwd voor verdachte USB-sticks die door Chinese VN-collega's als cadeau waren uitgedeeld. Eén van de marechaussees vertrouwde het niet en ging naar de MIVD.

De inlichtingendienst gaf het advies om de USB-stick niet te gebruiken. Of er ook daadwerkelijk malware op de USB-sticks is aangetroffen is onbekend. Een woordvoerder van de MIVD laat tegenover de Telegraaf weten niet op het specifieke voorval in Mali in te kunnen gaan, maar stelt dat de overheid al langer waarschuwt voor de digitale spionageactiviteiten vanuit diverse landen, waaronder China.

"De hele overheid, en dus ook Defensie, waarschuwt haar personeel altijd al voor de risico's die het in ontvangst nemen en gebruiken van USB-sticks met zich meebrengt. Er kan malware staan op USB-sticks waarvan je het fijne niet weet, en dus ook op sticks die je in ontvangst neemt van buitenlandse relaties. Voor het veilig opslaan van informatie verstrekt Defensie aan haar personeel beveiligde USB-sticks", aldus de MIVD-woordvoerder.

De Belastingdienst waarschuwt internetgebruikers via de eigen website voor valse e-mails die op dit moment rondgaan en van ASN DigiD en de Belastingdienst afkomstig lijken. In de e-mails worden ontvangers gevraagd om een digitaal aangifteformulier in te vullen of een verkeersboete te betalen.

De e-mails hebben als onderwerp "Betreft: Digitale Aangifte Inkomstenbelasting!!" en "AANMANING BETALEN". Ontvangers krijgen het advies om de e-mails niet te openen maar deze direct te verwijderen. "De Belastingdienst gebruikt in bepaalde gevallen e-mail. Maar in een e-mail vragen wij u nooit om persoonlijke gegevens. Krijgt u een e-mail waarin dat toch gebeurt, dan is er sprake van phishing", aldus de waarschuwing.

Autobedrijven in met name Nederland, Duitsland en Italië zijn het doelwit van een malware-aanval geworden waarbij wordt geprobeerd om via e-mail computersystemen met een Trojaans paard te infecteren dat allerlei gevoelige gegevens steelt, zoals gebruikersnamen en

wachtwoorden.

Dat meldt anti-virusbedrijf Symantec vandaag. De aanvalscampagne, die de naam "Carbon Grabber" heeft gekregen, werd begin augustus ontdekt. De aangevallen bedrijven ontvingen een e-mail van een Duits bedrijf genaamd Technik Automobile GmbH, dat niet lijkt te bestaan. De afzender van het bericht zegt gebruikte auto's te willen kopen en verwijst naar de meegestuurde bijlage voor een lijst van gewenste modellen.

Malware

De bijlage, TechnikAutomobileGMBH.pdf.zip, is in werkelijkheid malware en installeert de Carbon Grabber Trojan op het systeem. Dit Trojaanse paard injecteert zich in de processen van Microsoft Outlook, Internet Explorer, Google Chrome en Mozilla Firefox. Ook kaapt de malware de browser API's waardoor het informatie kan stelen voordat het versleuteld wordt. Gestolen gegevens zijn inloggegevens voor Outlook en informatie die gebruikers invoeren bij het inloggen op websites en interne webapplicaties. De gegevens worden vervolgens naar de Command & Control-server van de aanvalster teruggestuurd.

De e-mails zouden voornamelijk naar de klantenafdelingen van de getroffen bedrijven zijn verstuurd, waarbij de meeste bedrijven in de auto-industrie actief zijn, zoals verhuurbedrijven, verzekeringsmaatschappijen en commerciële transportbedrijven. Hoeveel systemen er door de malware besmet zijn geraakt laat Symantec niet weten, maar 31% van de infecties zou zich in Nederland bevinden.

1 September jl is er een internationale cybercrime taskforce gelanceerd die vanuit het Europese Cybercrime Centrum (EC3) van Europol in Den Haag zal worden aangestuurd en zich zal gaan bezighouden met de bestrijding van cybercriminelen, waarbij de nadruk op botnets, banking Trojans en het 'darknet' ligt.

De Joint Cybercrime Action Taskforce (J-CAT), een initiatief van het EC3, de EU Cybercrime Taskforce, de FBI en de Britse National Crime Agency (NCA), wordt geleid door Andy Archibald van de NCA en zal cybercrime zowel in de Europese Unie als daarbuiten gaan bestrijden. Inmiddels zijn Oostenrijk, Canada, Duitsland, Frankrijk, Italië, Nederland, Spanje,

Groot-Brittannië en de Verenigde Staten onderdeel van J-CAT.

Pilot

J-CAT is vooralsnog een pilot die zes maanden duurt en door de European Cybercrime Task Force (EUCTF) van de Europese Unie zal worden gemonitord. De taskforce zal voornamelijk onderzoeken naar cybercrime coördineren. De taskforce zal informatie over specifieke cybercrime-onderwerpen uit nationale databases en van relevante overheden en private partners verzamelen en deze "ruwe gegevens" tot bruikbare inlichtingen verwerken, alsmede doelen en netwerken voor onderzoek voorstellen. Ook zal JCAT bijeenkomsten met belangrijke spelers in de private sector en Europese Computer Emergency Response Teams organiseren om hun input te verzamelen over de dreigingen waarmee ze zelf of de samenleving te maken hebben.

Het politiekorps van Dubai zal agenten volgend jaar gaan uitrusten met Google Glass-brillen die van gezichtsherkenningstechnologie zijn voorzien. Op deze manier hoopt de politie "slimme" agenten te creëren, die worden gewaarschuwd als de bril een gezocht persoon herkent.

"De software die we intern ontwikkeld hebben laat Google Glass verbinding met een database van gezochte personen maken", zegt kolonel Khalid Nasser Al Razooqi tegenover 7 Days in Dubai. "Zodra de bril de verdachte aan de hand van een gezichtsafdruk herkent, waarschuwt het de agent." De brillen kosten zo'n 2.000 euro per stuk en zullen naar verwachting begin volgend jaar worden ingezet om criminelen te vangen.

Op dit moment beschikt het politiekorps als onderdeel van een testproject over vier brillen die voor het opsporen van verkeersovertreders en het vinden van gestolen voertuigen worden gebruikt. Hoeveel voertuigen er inmiddels dankzij de technologie zijn teruggevonden of het aantal mensen dat is aangehouden wil de kolonel niet laten weten. Als het aan Razooqi ligt zal Dubai in 2018 over de slimste politiebureaus ter wereld beschikken, waarbij Google Glass ook een rol speelt. "Het zal het werk van de politie helpen, we proberen 'slimme' agenten te maken", zo merkt hij op.



Europol voorspelt dat nog dit jaar de eerste dode valt via een apparaat dat aan internet verbonden is. Een beveiligingsbedrijf waarschuwde daar al eerder voor, maar Europol herhaalt dat nu in het nieuwe 'Internet Organised Crime Threat Assessment'. Deze iOCTA beschrijft alle dreigingen die rondom internet hangen. En daar horen tegenwoordig ook gehackte insulinepompen of pacemakers bij. Veel van die gadgets zijn kwetsbaar, aldus Europol: thuisrousters worden zelden goed gepatcht, er komen meer hackers en meer ransomware en criminelen zullen afpersingstechnieken blijven bedenken.

De Nationale Politie heeft zich aangesloten bij het Virtual Global Taskforce, een internationaal platform dat internet veiliger voor kinderen moet maken. In het platform werken opsporingsdiensten en maatschappelijke organisaties in tien landen samen met Europol en Interpol. November as wordt de tweeverjaarlijkse conferentie van het platform in Nederland gehouden. Deze zal in het teken staan van de aanpak van kinderspektoerisme en live streaming, ofwel misbruik via de webcam. In Nederland stijgt het aantal verdachten van kinderporno weer: van een paar honderd in 2010 naar 568 in 2013 en mogelijk 700 in 2018. De aandacht verschuift daarbij naar zwaardere zaken en 'echte misbruikers en producenten' en niet meer zozeer naar mannen die downloaden.

Ruim 28 duizend mensen deden in 2014 al aangifte van oplichting via internet. Ze werden in totaal voor zo'n 7 miljoen euro benadeeld. Harry Jongkind, projectleider van het Landelijk Meldpunt Internetoplichting, zegt tegen de NOS dat het soms zeer eenvoud-

dig gaat. 'Elektronische tickets worden meerdere keren verkocht. Tablet of smartphones, ook ver onder prijs, zijn tóch voorradig. En webwinkels gebruiken online handelsplaatsen zoals Marktplaats waarop ze advertenties plaatsen met een link naar een nep-site'. De webshopper blijft zo een mooie prooi voor oplichters. Die internetoplichters spelen in op trends en sentimenten in de markt. Jongkind zegt dat er veel fraude is rond spelcomputers, games, tablets en tickets en concertkaartjes. Mensen zijn alerter geworden, controleren vaker of de verkoper betrouwbaar is of dat de website wel deugt, maar fraude uitbannen 'is een utopie', stelt Jongkind. Bij meldingen en aangiftes volgt politieonderzoek, fraudeurs komen op zwarte lijsten en bankrekeningen kunnen (na vijf aangiftes) worden geblokkeerd.

In het eerste halfjaar 2014 is het aantal gevallen van fraude met internetbankieren en skimming van betaalpassen sterk gedaald. Volgens de Nederlandse Vereniging van Banken (NVB) en de Betaalvereniging Nederland (BN) bedraagt de schade over het eerste halfjaar rond de 9,5 miljoen euro, ongeveer eenderde minder dan in de tweede helft van 2013. In 2012 ging het nog om 82 miljoen, in heel 2013 om 33 miljoen. De organisaties melden dat ze fraude steeds beter vooraf kunnen detecteren en dus voorkomen. Ook het blokkeren van buitenlandse overboekingen blijkt effectief. Phishing blijft echter hardnekkig; weliswaar de helft minder dan vorig jaar maar toch altijd nog 1,7 miljoen euro.

Tja. Nu de verkoop van vervalste medicijnen, vooral op internet, zo veel geld

oplevert, stappen steeds meer drugs-handelaren over op namaakgeneesmiddelen. In het radioprogramma Reporter Radio (KRO-NCRV) zegt een Europol-rechercheur dat drugsdealers 'geconverteerd zijn' tot handelaren in nepmedicijnen en dat hij in dossiers over nepmedicijnen steeds vaker criminelen ziet voorkomen die voorheen in drugs handelden. Bijkomend voordeel is dat daarop ook nog eens een lagere straf staat dan op drugshandel. De handel in nepmedicijnen is wijdverspreid, alles is te koop. Maar de beloofde viagra of antibiotica bevat vaak rattengif of boenwas, zegt Ruud Coolen van Brakel van het Instituut voor Verantwoord Medicijngebruik. Hij vindt dat justitie en de politiek het probleem onderschatten.

Twitter, Facebook, Instagram, WhatsApp en al die andere sociale media bestaan al jaren maar ook eind 2014 gaan overheid, politie en brandweer daar bij crises nog altijd 'onwennig' mee om. In het net verschenen boek 'Lessen uit crises en mini-crisis 2013' beschrijven Menno van Duin, lector aan de Politie-academie, en Vina Wijkhuijs, onderzoeker bij het Instituut Fysieke Veiligheid, hoe de hulpdiensten reageerden bij achttien crises uit 2013. In zeker zes van die crises speelden sociale media een belangrijke rol. De politie weet zich nog altijd geen raad met likes, tweets en sharen, schrijft het NRC. Zo liet de politie zich 'verrassen' door de razendsnelle mobilisatie van burgers die gingen zoeken naar Ruben en Julian en door 'heksenjachten' na rellen en vechtpartijen in Eindhoven ('kopschoppers') en Deventer,. In een reactie zegt de nationale politie dat 'sociale media uiteraard onze aandacht hebben'

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

Index

Cybercrime wetsartikelen (2)

Bij **piraterij** gaat het feitelijk om illegale handel van allerhande 'cd's, dvd's, films, software en andere producten waarvoor auteursrechten gelden'. De nadruk ligt volgens het [KLPD](#) veelal bij eindgebruikers, internetpiraten en 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 310 WvSr](#): diefstal.

[Artikel 321 WvSr](#): verduistering.

[Artikel 416 WvSr](#): heling.

