

Secure Computing Magazine

Met de CTRL toets + het scrolwieltje van uw muis , kunt u de pagina vergroten en verkleinen. U kunt dus zelf uw leesbaar formaat kiezen.

INDEX

Geef nooit een kopie van je ID op Marktplaats
Vier manieren waarop cybercriminelen je bitcoin proberen te stelen
Wraakporno op Facebook te lijf met fotoherkenning
EU overweegt 'achterdeurtje' geëncrypteerde data voor autoriteiten
Google gaat nepnieuws wereldwijd als vals aanduiden in zoekresultaten
Blockchains - niet alleen voor Bitcoin
Engeland: "Aanslag moet ogen Facebook, Twitter en Google openen"
Eisen aan poltieonderzoek smartphone
Politie loopt in onderzoek steeds vaker vast op IP-adres
EU komt in juni met regels voor versleutelde chat-apps
Jonge cybercrimineel verschilt van andere jonge criminelen
Een derde van online kinderporno staat op Nederlandse servers
Bekeerde hacker voorspelt cyberwereldoorlog
Cybercriminelen verruilen macro voor lnk-bestand in Word -documenten
Dreiging blijft met IS 2.0 en Al Qaeda
Jihadverdachten horen via Facebook dat hun zaak begint
Google: aantal gehackte sites in 2016 met eenderde gegroeid
Kabinet bekijkt boete discriminatie internet
Hoe DNSSEC het internet veiliger maakt
NSA kan meekijken bij betalingsverkeer tientallen banken
Swift lanceert tool tegen frauduleuze banktransacties
Takedown notice; informatie van social media verwijderen
WhatsApp Status : Helder uitgelegd & privacy instellingen
Internetscamming in Ghana
Europol en China gaan samen cybercrime bestrijden
Ssd-tips: Bestanden verwijderen of herstellen

AKTUEEL

50-plussers bezorgd over veiligheid persoonsgegevens op het internet

Ondanks dat veel 50-plussers al maatregelen nemen om zichzelf online te beschermen, is meer dan de helft van hen bezorgd over de veiligheid van persoonsgegevens op het internet. Dat blijkt uit een onderzoek onder ruim duizend 50-plussers van het Nationale 50plus Panel.

Phishing

,,Phishing is nog altijd de meest voorkomende vorm van internetfraude", meent Dekker. Bij phishing proberen fraudeurs via e-mail achter bankgegevens te komen, bijvoorbeeld door mensen naar een valse (bank)website te lokken waar een inlognaam en wachtwoord moeten worden ingevuld. 55 procent van de deelnemers denkt te weten hoe je een veilige website kunt herkennen.

Volgens Dekker zijn 50-plussers de afgelopen jaren steeds meer intensief gebruik gaan maken van het internet. Ze zoeken niet langer alleen informatie op, maar e-mailen steeds vaker, lezen nieuwswebsites en doen aan internetbankieren. Bovendien maakt de groep steeds vaker gebruik van sociale media als Facebook en Pinterest.

Aankopen doen

Ook doen 50-plussers steeds vaker aan internet-shoppen. ,,Eerst deden 50-plussers vooral aankopen bij betrouwbare websites door bijvoorbeeld direct bij een vliegtuigmaatschappij een ticket kopen", vertelt Dekker vanuit zijn eigen ervaring met Startpagina. ,,Nu kopen ze steeds vaker producten bij kleinere, minder betrouwbare websites, bijvoorbeeld via websites die worden aangeboden via AliExpress", aldus Dekker.

————————————————————————

Rubrieken:

- Verder op Facebook / de website
- Cops in Cyberspace
- Rechtspraak
- Verschijningsvorm cybercrime
- Wetsartikel
- Video
- Handig

Geef nooit een kopie van je ID op Marktplaats

Een nieuwe trend van identiteitsfraude is fraude via bijvoorbeeld Marktplaats verkregen kopieën van identiteitsbewijzen. Identificatie hoeft steeds minder vaak in persoon aan de balie. Het gebeurt steeds vaker online met een kopie van een identiteitsbewijs. Bijvoorbeeld bij het afsluiten van een telefoon-abonnement en bankrekening. Een oplichter heeft alleen een kopie van jouw ID nodig.

Met een kopie van je ID kunnen ze telefoonabonnementen en leningen afsluiten of bankrekeningen openen. Ze vragen je dan ook nog om 1 cent over te maken, zogenaamd om zeker te weten dat je niet rood staat. In werkelijkheid activeer je hiermee een bankrekening op jouw naam die met de kopie van je ID is aangevraagd.

Je komt erachter dat jouw identiteit is misbruikt wanneer er ineens geld van je rekening is afgeschreven, of als er ineens een incassobureau voor de deur staat omdat er nog allerlei rekeningen open staan van spullen die op jouw naam zijn gekocht of omdat er leningen zijn afgesloten die nooit zijn afbetaald. Het kan ook gebeuren dat mensen op Facebook je beschuldigen van oplichting, omdat die kopieën een eigen leven zijn gaan leiden. De criminelen gebruiken jouw identiteit vaak weer om anderen op te lichten. De oplichters verkopen dan uit jouw naam (en hebben een kopie van je ID om dat te bewijzen!) en blijven zelf buiten schot. Voor misbruik zijn soms trouwens alleen al een geboortedatum en een naam voldoende. Daarmee kunnen oplichters toegang krijgen tot allerlei instanties waar je staat ingeschreven. Dus zet je geboortedatum niet openbaar op Facebook.



Voorbeelden:
Eén truc is dat ze niet-bestaande vacatures plaatsen op vacaturesites, waar ze dan om een kopie van je identiteitsdocument of een loonstrookje vragen. Een andere truc is dat ze zogenaamd een kamer te huur hebben. Ze zeggen dan: 'stuur vast een kopie op, ik maak dan het contract in orde'.
Wat ook gebeurt is identiteitsfraude via verkoopsites als Marktplaats. Oplichters bieden spullen aan die gewild zijn, zoals populaire telefoons en tickets voor concerten en festivals. Ook hier vragen ze om je identiteitsdocument, zogenaamd om zeker te weten met wie ze te maken hebben.

Tips om identiteitsfraude te voorkomen

- Stuur bij handel op **verkoopsites** nooit kopieen van je ID-document of andere documenten
- met identiteitsgegevens.
- Als toch een kopie van het ID nodig is , **maak dan de kopie onbruikbaar:** schrijf datum en doel erop en streep door wat niet nodig is (vaak het BSN-nummer). De overheid heeft hiervoor de **KopieID-app** .
- Zet op **social media** nooit foto's van je paspoort, identiteitskaart of rijbewijs. Zet ook niet je geboortedatum openbaar op Facebook.
- Beveilig je **DigiD** extra met een sms-code. Dit kun je instellen op digid.nl. Vul op die site ook je
- e-mailadres in, zodat je geïnformeerd wordt bij onregelmatigheden.
- Controleer geregeld je **bankafschriften.**
- Bij **Marktplaats:** kijk of iemand al langer actief is

Vier manieren waarop cybercriminelen je bitcoin proberen te stelen

Cybercriminelen passen uiteenlopende technieken toe om geld te ontvreemden van hun slachtoffers. Een laatste trend in de illegale online wereld is dat hackers op sociale media op zoek gaan naar goedgelovige mensen die bitcoins willen kopen. Deze digitale valuta wordt door veel mensen aangekocht in de hoop dat ze hun munten voor een grote winst weer kunnen verkopen. Op sociale media bevinden zich een hoop mensen die bitcoins voor het eerst willen kopen en bijgevolg weinig kennis hebben over de digitale munteenheid. Zij vormen de ideale slachtoffers voor cybercriminelen die snel geld willen verdienen.

Uit onderzoek van ZeroFOX blijkt dat er momenteel 126.276.549 valse bitcoinlinks te vinden zijn op onder andere Facebook, Twitter en Instagram. Deze grote groep bestaat uit 3.618 unieke oplichtingstechnieken. ZeroFox vermoedt dat botnets er mee voor zorgen dat er zoveel kwaadaardige links verspreid worden.

ZeroFox heeft vier categorieën gevonden waarin alle oplichtingstechnieken die op sociale media worden gebruikt vallen. Bij elke van deze technieken worden andere manieren gebruikt om geld te ontfutselen van goedgelovige slachtoffers.

1. Valse bitcoinwallets

Vaak klikken we zonder na te denken op links in sociale media die er interessant uitzien. Met name wanneer je wordt belooft om op een erg eenvoudige manier aan bitcoins te geraken, trappen veel mensen in de val. Cybercriminelen verspreiden daarom links die zogenaamd naar bitcoinwallets leiden, maar die eigenlijk malware verspreiden.

De kwaadaardige software kan privégegevens over je verzamelen, of je computer kan tot een botnet worden ingelijfd. Verder kunnen cybercriminelen eveneens geld verdienen wanneer je op de verkeerde link klikt.

Een belangrijke les die ook voor phishing geldt, is dat wanneer iets te goed lijkt om waar te zijn, dit waarschijnlijk ook het geval is. Zeker wanneer de berichten komen van een anonieme of standaard account zou je op je hoede moeten zijn.

2. Bitcoin phishing

Sommige cybercriminelen doen zich voor als legitieme bitcoindiensten, waarbij ze zelfs zo ver gaan om bepaalde merken over te nemen. Eenmaal ze het vertrouwen hebben gewonnen van hun slachtoffer, kunnen ze hun slag slaan. Op phishing websites proberen ze mensen zo ver te krijgen om hun bitcoinsleutels te delen. Eenmaal ze de sleutel in handen hebben, kunnen de hackers je bitcoinwallet plunderen.



3. Bitcoin flipping

Zoals eerder aangehaald kopen veel mensen bitcoins aan in de hoop dat ze winst kunnen maken door het verkopen van hun digitale munten. Dit proces wordt in de economische wereld flipping genoemd: je koopt een goed tegen een lage prijs, om deze later voor een hogere prijs te kunnen verkopen.

Cybercriminelen maken misbruik van investeerders die ongeduldig worden wanneer hun bitcoins niet snel in waarde stijgen. Op sociale media vindt je daardoor een hoop links terug van mensen die beloven zij ervoor kunnen zorgen dat je snel geld kan verdienen, uiteraard tegen een betaling. De hackers beloven je bitcoins te flippen, maar lopen weg met je geld.

4. Piramide

De laatste oplichtingstechniek die wordt toegepast door cybercriminelen is de klassieke piramidetruc. Hackers moedigen mensen aan om deel te nemen aan een investering die weinig geld kost en die je een hoop geld kan opbrengen wanneer je andere mensen laat deelnemen in de investering. Op deze manier krijgen cybercriminelen op korte tijd veel investeerders bij elkaar, waarna ze het geld verzamelen zonder aan de deelnemers ook maar iets terug te betalen.

Wraakporno op Facebook te lijf met fotoherkenning

Het komt veelvuldig voor: het telkens opnieuw plaatsen van intieme foto's op sociale netwerken tegen de zin van de geportretteerde. Facebook gaat dit soort wraakporno aanpakken.

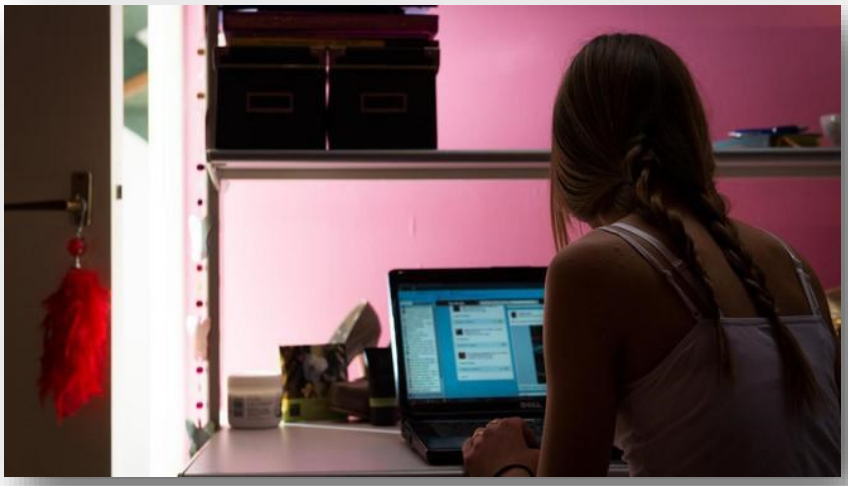
Om de verspreiding tegen te gaan, zet het social mediabedrijf een aantal wapens in. Allereerst kunnen gebruikers die stuiten op een naaktfoto waarvan ze vermoeden dat de persoon die daarop staat daar geen toestemming voor heeft gegeven, Facebook waarschuwen. Dit gebeurt via de knop 'Foto rapporteren'. Een getraind team beoordeelt de foto vervolgens en komt in actie.

Als een foto of video inderdaad tegen de huisregels ingaat, krijgt deze een unieke code mee, een zogenoemde hash. Deze foto-DNA maakt het mogelijk om ook het herplaatsen van wraakporno op Facebook, Messenger of Instagram tegen te gaan. De fotoherkenningssoftware van Facebook herkent dan immers gelijk of het om beelden gaat die al eerder zijn gerapporteerd. Deze techniek wordt ook gebruikt om ander ongewenst materiaal op te sporen, zoals kindermisbruik of terroristische propaganda.

Samenwerking

Als iemand zo'n foto toch weer probeert te verspreiden binnen de verschillende netwerken van Facebook, dan krijgt degene een waarschuwing. Facebook heeft naar eigen zeggen samengewerkt met 150 verschillende organisaties die zich met deze problematiek bezighouden. In Nederland is dat het meldpunt voor online misbruik Helpwanted.nl.

Helpwanted.nl zegt regelmatig meldingen van jongeren te ontvangen wier naaktfoto telkens opnieuw onder verschillende accounts online wordt gezet. 'Doorgaans melden ze het bij Facebook of Instagram en worden de foto's snel verwijderd. Maar met een paar simpele handelingen staat de foto opnieuw online onder een ander account', stelt het meldpunt. Helpwanted.nl is 'bijzonder blij' met de nieuwe maatregelen, waar het lang voor heeft gelobbyd.



Bron: Facebook

EU overweegt ‘achterdeurtje’ geëncrypteerde data voor autoriteiten

De Europese Unie overweegt maatregelen die de autoriteiten de mogelijkheid moet bieden om versleutelde gegevens op te vragen in leesbare vorm.

Europees Commissaris Věra Jourová doet in juni enkele voorstellen om een wetgeving op te stellen die bedrijven verplicht om geëncrypteerde data toegankelijk te maken voor bevoegde instanties. Jourová zal “drie tot vier opties” voorleggen, waaronder een wettelijk kader en een vrijwillige toezegging van bedrijven die moet dienen tot de wetgeving wordt goedgekeurd, rapporteert Euractiv.



Encryptie

Bepaalde online diensten versleutelen de gegevens van hun gebruikers om ze te beschermen tegen aanvallen van buitenaf. Zo encrypteert chatapplicatie Whatsapp de gesprekken die de gebruikers houden via het platform: zelfs wanneer de gegevens worden gestolen, is de data onleesbaar. De vorm van beveiliging kon echter al op kritiek rekenen, omdat de gegevens zo ook ontoegankelijk zijn voor veiligheidsdiensten.

“Vrijwillige toegang”

“Op dit moment zijn aanklagers, rechters en ook politie en gezaghebbende autoriteiten afhankelijk van de vraag of providers vrijwillig toegang verlenen en het bewijs voorleggen,” legt Jourová uit. “Dat is niet de manier waarop we de veiligheid van Europeanen kunnen faciliteren en verzekeren, door afhankelijk te zijn van een vrijwillige medewerking.” Een wetgeving zou bevoegde instanties een ‘achterdeurtje’ kunnen bieden waarmee ze niet meer moeten rekenen op de vrijwillige medewerking, maar de bedrijven achter de online diensten dwingen om de data vrij te geven.

Onder andere landen als het Verenigd Koninkrijk, Frankrijk en Duitsland lobbyen al langer om veiligheidsdiensten toegang te verlenen tot geëncrypteerde informatie. In december werd nog een vernieuwd wetsvoorstel aangenomen dat OTT-diensten, waaronder Skype en Whatsapp, aan strengere regels houdt.

Google gaat nepnieuws wereldwijd als vals aanduiden in zoekresultaten

Google gaat wereldwijd informatie die factcheckers als vals hebben bestempeld, voorzien van een label in zijn zoekresultaten. De stap moet voorkomen dat gebruikers valse informatie voor waarheid aannemen. Het is de jongste stap in de strijd tegen nepnieuws.

De functie zal ook beschikbaar zijn in Nederland, in de algemene zoekmachine en in Google Nieuws, zegt de zoekgigant. Op dit moment heeft het Amerikaanse bedrijf nog geen Nederlandse organisaties en bedrijven die als factcheckers dienen, maar als zij aan bepaalde eisen voldoen, is dat wel mogelijk, zo zegt het zoekbedrijf.

Onder het zoekresultaat staat een regel met daarin de bron van de factcheck en de bevinding daarvan. Als het nieuws nep is, staat er 'FALSE' achter. De factcheck zal wereldwijd werken in de zoekmachine en in Google Nieuws.

De stap is de nieuwste in de strijd tegen zogenoemd nepnieuws, artikelen van sites die via bewust foute en misleidende informatie bezoekers proberen te trekken en zo geld willen verdienen aan reclames. Google en Facebook sloten dergelijke sites al eerder af van hun advertentieplatforms en Facebook begon vorige maand maatregelen te nemen tegen nepnieuws in Nederland.

Bron: ZDnet / Google

Blockchains - niet alleen voor Bitcoin

Een tijdlang was de blockchain een ondergeschoven kindje in de hype die ontstond rond de Bitcoin. Aandacht voor de achterliggende datastructuur van deze cryptocurrency was behoorlijk beperkt. Maar nu dromen we over meer toepassingen.

Hoe werkt een blockchain?

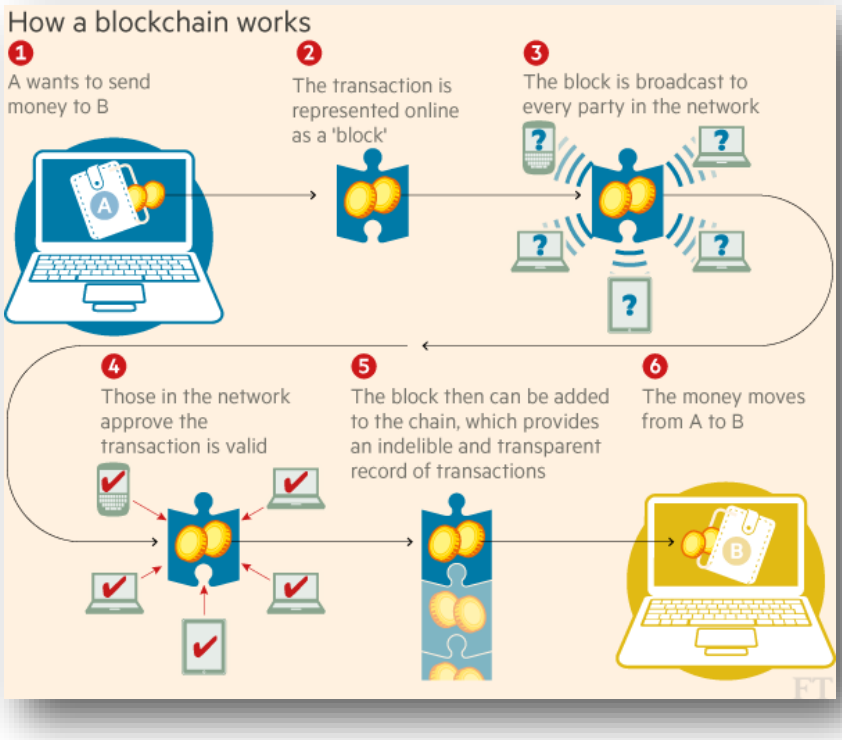
Het basisidee van een blockchain is dat het een database is van transacties, te vergelijken met een grootboek, kasboek of register. Op zichzelf niets bijzonders: in het dagelijks leven hebben we direct en indirect te maken met tal van databases waarin transacties worden opgeslagen. Banken houden in grootboeken bij wie naar wie geld overmaakt. Verenigingen noteren in kasboeken wie er al contributie heeft betaald en waaraan die bijdragen worden besteed. In het Kadaster wordt geregistreerd wie de eigenaar van een pand is en of er wellicht een hypotheek op een huis rust.

Het revolutionaire van de blockchain is dat dergelijke transacties en eigendomsgegevens decentraal in een database worden opgeslagen. Dat maakt een blockchain-grootboek transparant en toegankelijk. Omdat de blockchain, net zoals internet, van iedereen en niemand is, hoef je niet meer aan te kloppen bij een centrale instantie om vast te stellen dat degene die jou iets wil verkopen ook daadwerkelijk de eigenaar van dat bezit is. Iedereen die meedoet aan een blockchain krijgt hetzelfde overzicht met informatie, waarmee op elk moment valt te verifiëren wie de zeggenschap heeft over een bepaald bezit.

Vanwege het grote aantal kopieën van de blockchain is het extreem moeilijk om de informatie in het grootboek te vervalsen. In het geval van de Bitcoin heeft bijvoorbeeld elke full node (dit zijn centrale punten binnen het blockchain-netwerk die voortdurend met elkaar in contact staan) een kopie van de blockchain (op dit moment ongeveer 75.000 MB groot). Een full node heeft daarmee een overzicht van elke transactie die ooit heeft plaatsgevonden en alle nieuwe transacties. Elke full node controleert bovendien of een transactie wel aan alle voorwaarden voldoet. Wordt een Bitcoin bijvoorbeeld niet twee keer uitgegeven?

In het kort werkt het zo:

1. A wil geld overmaken naar B.
2. De informatie over de transactie (een block) wordt gedeeld met alle full nodes in het netwerk.
3. De nodes controleren de transactie. Is degene die het geld wil overmaken daadwerkelijk de eigenaar?
4. De nodes keuren de transactie goed of af.
5. Als de transactie wordt goedgekeurd, kan het block worden toegevoegd aan het register (de chain) waarin alle transacties staan vermeld.
6. Het geld wordt overgemaakt van A naar B.



Bron: Reshift Digital

Blockchains - niet alleen voor Bitcoin (vervolg)

Interessant voor banken

Dankzij het decentrale karakter en de ingebouwde beveiliging is de blockchain een concept dat bij veel mensen tot de verbeelding spreekt. In navolging van de blockchain voor de Bitcoin zijn er daarom nu tal van blockchains voor andere toepassingen. De blockchain wordt vanzelfsprekend gebruikt bij alle andere cryptocurrencies die in navolging van de Bitcoin het levenslicht hebben gezien.

Maar dat je op elk moment kunt vaststellen wie de eigenaar van iets is, biedt ook buiten de wereld van virtuele munten eindeloos veel mogelijkheden. Het grootste enthousiasme voor dergelijke toepassingen lijkt er vooralsnog te bestaan in de wereld van de haute finance. Van ING tot Deutsche Bank en van Goldman Sachs tot BNP Paribas: iedere zichzelf respecterende bank toont belangstelling voor de technologie.

Eerder dit jaar bootsten grote spelers als JPMorgan Chase, Citigroup en Credit Suisse een maandlang de handel in zogeheten credit default swaps na via de blockchain. De handel in dergelijke faillissementsverzekeringen is nu nog een bureaucratische rompslomp. Transacties in dergelijke financiële producten moeten aan tal van partijen worden doorgegeven. De koper, de verkoper, de betrokken banken en de centrale boekhouder van Wall Street moeten allemaal in kennis worden gesteld.

Door gebruik te maken van een blockchain is het mogelijk deze bureaucratie geheel of op zijn minst gedeeltelijk te elimineren. Dankzij de blockchain heeft iedereen immers hetzelfde overzicht van welke transacties er hebben plaatsgevonden. Het is niet langer nodig om verschillende grootboeken op gezette tijden naast elkaar te leggen.

De decentrale verificatie van eigendom via een blockchain kan allerhande andere grootboeken overbodig maken. De economische voordelen daarvan voor de financiële sector kunnen groot zijn. Analisten van Autonomous Research becijferden dat gebruik van blockchains voor het bijhouden van transacties een jaarlijkse besparing van zestien miljard dollar kan opleveren. Desondanks gaat het vermoedelijk nog jaren duren voordat financiële instellingen de blockchain daadwerkelijk op grote schaal gaan inzetten voor het registreren van transacties.

Kritiek

Sommige deskundigen vragen zich af of de combinatie blockchain en banken überhaupt wel mogelijk is. De Bitcoin en de blockchain zijn immers in het leven geroepen als een vorm van protest tegen de gevestigde financiële orde: de mysterieuze Bitcoin-bedenker Natoshi Sakamoto wilde in de eerste plaats een alternatief bieden voor de centrale banken, die naar eigen goeddunken de geldpers kunnen aanzetten, en als alternatief voor de gewone banken, die allerlei transactiekosten rekenen.

Via een blockchain-achtig systeem zou bijvoorbeeld kunnen worden bijgehouden wie welke aandelen bezit. Wie in aandelen wil handelen, hoeft dan niet meer een beleggingsrekening te openen, maar kan direct aandelen kopen van en verkopen aan andere aandelenhandelaars. Dankzij de decentrale blockchain kan immers iedereen direct vaststellen dat een andere persoon de gewenste aandelen bezit. Een derde partij die je vertrouwt – lees: een financiële instelling als een bank – is dankzij de blockchain niet meer nodig.

De econoom Saifedean Ammous oordeelde in een column voor de site American Banker in februari van dit jaar dan ook spijkerhard over alle banken die de blockchain nu omarmen. “Je kunt net zo goed een paard uitrusten met een motor en dat dan technologische innovatie noemen,” schreef hij. “Maar die benadering zorgt er alleen maar voor dat het paard trager wordt. Er wordt geen enkel probleem mee opgelost.”



Bron: Reshift Digital

Engeland: “Aanslag moet ogen Facebook, Twitter en Google openen”

Hoewel nog nauwelijks is aangetoond dat Khalid Masood, de man achter de aanslag op Westmister Bridge, veel gebruik maakte van, dan wel heel actief was op sociale media, leggen autoriteiten een deel van de schuld bij bedrijven als Facebook, Twitter en Google.

Korpschef Craig Mackey van Scotland Yard vindt de aanslag ‘een wake-up call’ voor die bedrijven. ‘Put your own house in order’, adviseert hij ze streng. Mackey stelt dat de bedrijven niet allerlei ethische normen en waarden over bijvoorbeeld blootfoto’s kunnen uitdragen terwijl aan de andere kant veel jihadistiche en/of terroristische content ongemoeid blijft.

Minister Boris Johnson (Buitenlandse Zaken) sprak van een ‘disgusting failure to remove extremist material’. Zijn collega Amber Rudd (Binnenlandse Zaken) heeft inmiddels bij Whatsapp toegang geëist tot Whatapp-berichten. Masood was aan het Whatsappen vlak voordat hij op de brug op mensen inreed. Die berichten zijn in principe niet te lezen, want ‘end-to-end’ versleuteld. Volgens Rudd is dat ‘volstrekt onacceptabel’ en mag er ‘geen enkele plaats zijn waar terroristen zich kunnen verbergen’.

Critici noemen Rudds actie opmerkelijk: kennelijk beschikt de politie over Masoods telefoon en dan kun je die berichten toch gewoon lezen? En was het niet juist de politie die vond dat Masood geen bedreiging (meer) vormde en hem niet meer in de gaten hield? En is het bovendien ook niet zo, vraagt Huib Modderkolk in De Volkskrant, dat diezelfde overheden encryptie juist heel belangrijk vinden? Ook Rudd zei al eens dat ze end-to-end-encryptie ondersteunt vanwege het belang voor de economie en cybersecurity.

Het ‘selectief kraken van Whatsapp bestaat niet’: het toegankelijk maken van versleutelde berichten voor geheime diensten én het waarborgen van sterke encryptie gaan niet samen.



Eisen aan poltieonderzoek smartphone

Een smartphone mag voortaan alleen nog door de politie onderzocht worden als de inbreuk op de privacy van de eigenaar van die smartphone ‘beperkt’ is. De Hoge Raad bepaalde dat de politie niet zo maar alle gegevens mag uitlezen. Het arrest komt in een zaak uit 2014 waarbij de politie een smartphone onderzocht van een man die werd verdacht van drugssmokkel.

De Hoge Raad heeft deze zaak terugverwezen naar het gerechtshof dat opnieuw moet beijken of er met het achterhalen van álle contacten, alle oproepen, alle berichten en alle (privé)foto’s op de smartphone niet een te grote inbreuk is gemaakt op de privacy van de verdachte. Zo’n uitgebreid onderzoek is alleen nog mogelijk met toestemming van officier of rechter-commissaris.

De Hoge Raad wijst in het arrest ook op het ontbreken van wettelijke regels. Volgens het ministerie van VenJ wordt er aan zo’n regeling gewerkt.

Bron: Scotland Yard / Overheid.nl

Politie loopt in onderzoek steeds vaker vast op IP-adres

Een IP-adres is niet langer het 'gouden spoor' naar de verdachte van een misdrijf. Dat blijkt uit de beantwoording van Kamervragen door demissionair staatssecretaris Sander Dekker van Onderwijs. Dekker informeerde de Tweede Kamer vandaag over de zelfmoord van de 14-jarige scholier Onur uit Enschede, van wie een naaktfoto op Instagram circuleerde. ,,Het blijkt dat een IP-adres steeds minder geschikt is voor identificatie-doeleinden", schrijft Dekker in antwoord op de vraag of opsporingsdiensten beschikken over IP-adressen die voor pesten en sexting worden gebruikt.

Openbare netwerken
Iedere computer, smartphone of tablet die verbinding maakt met internet krijgt een IP-adres, waarmee de gebruiker te herkennen is. De politie kan zo - met hulp van een internetprovider - achterhalen wie bepaalde handelingen op internet heeft verricht.

Maar door de brede beschikbaarheid van openbare wifi-hotspots, openbare netwerken, versleutelde dataverbindingen en de toename van zogenaamde 'mobile pools' is het steeds moeilijker om een IP-adres te herleiden tot een verdachte, schrijft Dekker.



De demissionair staatssecretaris meldt ook dat burgers steeds vaker gebruik maken van effectieve afschermingsmethoden. Ook zijn er de laatste jaren meer mogelijkheden bij gekomen om online te communiceren zonder sporen na te laten.

Andere informatie
Volgens Rejo Zenger, ict- en privacyexpert bij Bits of Freedom, is het niet verbazingwekkend dat de politie meer moeite heeft om daders te vinden via een IP-adres. ,,Tegenwoordig gaan steeds meer mensen bij bijvoorbeeld een koffiezaak op het wifi-netwerk. Het IP-adres is dan niet direct te herleiden naar de gebruiker van een telefoon of computer. De politie kan alleen achterhalen in welke koffiezaak de gebruiker zat."

Toch is de politie nu niet kansloos, zegt Zenger. ,,Je kunt tegenwoordig niet meer het internet opgaan zonder op een bepaalde manier gevolgd of geregistreerd te worden. Denk bijvoorbeeld aan een foto die je maakt met je mobieltje. In die foto wordt vaak de locatie vastgelegd. Van dat soort informatie kan de politie gebruik maken."

EU komt in juni met regels voor versleutelde chat-apps

Vanwege ‘de veiligheid van Europeanen’ komt de Europese Commissie rond juni met nieuwe regels voor versleutelde chat-apps, zoals Whatsapp, Signal en Telegram.

Rond deze apps is continu veel gedoe als weer eens blijkt dat criminelen ze gebruiken. De nieuwe regels komen vooral na oproepen daartoe van Duitsland, Frankrijk en Groot-Brittannië, niet toevallig landen waar recent aanslagen plaatsvonden.

Volgens Europees Commissaris Vera Jourová (Justitie) zijn politie, opsporingsdiensten, aanklagers én rechters nog te afhankelijk van de bereidheid van providers om mee te werken. ‘Maar zo kunnen we de veiligheid van Europeanen niet verzekeren’.

Bron: Overheid.nl / EU

Jonge cybercrimineel verschilt van andere jonge criminelen

Jongeren die zich aan cybercrime schuldig maken hebben een ander profiel dan jeugdige daders van traditionele, offline misdrijven. Dat blijkt uit onderzoek van het Wetenschappelijke Onderzoek- en Documentatie Centrum (WODC) van het ministerie van Veiligheid en Justitie.

Jeugdige cyberdaders keuren bijvoorbeeld offline misdrijven af, hebben minder criminele vrienden (ook online) en zijn vaker van Nederlandse herkomst. Volgens de onderzoekers is het dan ook de vraag of bestaande interventies bij deze groep jeugdige daders bruikbaar zijn. Daarnaast is er volgens de onderzoekers een groep online jeugdige daders die zowel cyber als gedigitaliseerde delicten pleegt.

Deze groep jeugdige daders kent een groot aantal - ook bekende - risicofactoren. Zo keuren ze offline criminaliteit goed, zijn ze minder open richting hun ouders en hebben ze vaker vrienden die online misdrijven plegen. De onderzoekers denken dat bij deze groep een deel van de bestaande interventies wel bruikbaar is. Verder laat het onderzoek zien dat er mogelijk een verplaatsing onder jongeren is van offline naar online misdrijven.

Op dit moment kijken de onderzoekers welke interventies bij jonge cybercriminelen mogelijk zijn en hoe de aard en omvang van deze nieuwe vormen van jeugdcriminaliteit op andere manieren in kaart kunnen worden gebracht. Uit eerder onderzoek van de Monitor Jeugdcriminaliteit bleek dat 28 procent van de jongeren claimde een online delict te hebben gepleegd.



Een derde van online kinderporno staat op Nederlandse servers

Volgens een onderzoek van de Internet Watch Foundation staat maar liefst een derde van alle kinderporno die online te vinden is, op Nederlandse servers.

De IWF vond in totaal 2416 websites met daarop 57.335 url's die verwezen naar illegale afbeeldingen. 92% daarvan stond gehost in vijf landen: Nederland (37%), VS (22%), Canada (15%), Frankrijk (11%) en Rusland (7%).

De plaatjes stonden vooral op image hosting sites (72%), in 'cyberlockers' (11%) en eigenlijk nauwelijks op sociale media (1%). Meer dan 80% van alle kinderpornowebsites heeft een domeinnaam die eindigt met .com, .net, .se, io of .cc.

Bron: WODC / Internet Watch Foundation

Bekeerde hacker voorspelt cyberwereldoorlog

In 2000 kostte MafiaBoy de Amerikaanse economie 1,5 miljard dollar en bezorgde hij het machtige Yahoo een paniekaanval. Vandaag werkt hij als beveiligingsexpert: een gesprek met een notoir hacker.

Michael 'MafiaBoy' Calce is een bijzondere figuur. In 2000, op vijftienjarige leeftijd, legde hij Yahoo, eBay, Amazon, Dell en CNN een uur lang plat. De aanvallen kwamen er nadat enkele hackers hem vertelden dat het onmogelijk was om websites van zulke grote en machtige bedrijven neer te halen. Woorden die de jonge MafiaBoy niet graag hoorde: "vroeger draaide het voor een hacker immers niet om geld, maar om prestige en erkenning," herinnert Calce zich.

Paniek

"Iedereen, hacker of niet, heeft ooit in zijn leven wel eens het gevoel 'fuck, wat heb ik gedaan?' Voor mij kwam dat moment er in 2002, toen president Bill Clinton op televisie verkondigde dat een speciale taskforce werd opgericht om mij te vinden. Slik." Calce had naar eigen zeggen geen idee dat zijn acties zo'n grote gevolgen zouden hebben. Naast een paniekaanval bij de getroffen bedrijven hield de gebeurtenis het volledige internet nog een tijdlang in zijn greep. Ook wij (ZDNet) hielden het voorval in 2000 nauwlettend in de gaten.

De acties van Calce kostten de Amerikaanse economie ongeveer anderhalf miljard dollar; een massa geld voor wat toen nog steeds een opkomende industrie was. De dotcomcrisis zat er bovendien aan te komen, wat de zenuwachtigheid van de Amerikaanse president geen goed deed.

Canadese strafmaat

Uiteindelijk zou het nog vier maanden duren vooraleer de Canadese politie de jonge hacker wist op te sporen. In de zoektocht naar erkenning en beruchtheid was hij beginnen opscheppen over zijn daden in de chatroom van een Californische universiteit. De rechtszaak zou ruim een jaar aanslepen en al die tijd werd in de media gewag gemaakt van een zware straf, om een voorbeeld te stellen. Die kwam er niet: "het werden acht maanden in een open opvangcentrum, een boete van 250 dollar en vijf jaar internetverbod. God zegene Canada," lacht Calce, en de zaal met hem.

Ik bevind mij op de HP Innovation Summit in Londen en Calce heeft de zaal op zijn hand. De hele middag door luistert iedereen beleefd, en bij momenten geboeid, naar de vele sprekers. Wanneer Calce het podium op komt, wordt evenwel duidelijk naar wiens presentatie iedereen echt uitkeek. MafiaBoy heeft nog geen minuut nodig om met enkele mopjes en een straf verhaal de journalisten en HP-medewerkers te boeien.

"Mijn drijfveer in alles wat ik doe, is niet het oplossen van een puzzel," zegt Calce. "Het boeit mij daarentegen mateloos om verschillende manieren te bedenken om één puzzel op te lossen." Toen zijn vader in 1990 thuiskwam met een computer om zijn bescheiden zaak te moderniseren, mocht Calce het uitvogelen. "Maar het zou oneerbiedig zijn om te zeggen dat hij de kat bij de melk heeft gezet."

Gratis internet

Calce's fascinatie voor het internet begon in 1993, hij was dan 9 jaar. Hij kwam in het bezit van een cd die de gebruiker een maand lang gratis internettoegang bezorgde. Al snel kreeg hij ruzie met een oudere internaut die het internet geen plaats vond voor jonge nieuwsgierigen. "Hij sneed mijn toegang tot het internet af, in een vingerknip. Ik was kwaad, maar ook gefascineerd." De vonk sloeg over en al snel kwam hij erachter welk programma hem het onrecht had aangedaan.

"Uiteraard begon ik dat programma zelf te gebruiken op zeer regelmatige basis," zegt Calce. Met het juiste gereedschap op zijn computer slaagde hij erin om als negenjarige tientallen volwassenen te beduvelen met 'social engineering': hij stuurde e-mails naar mensen met internettoegang en vertelde hen dat ze hun inloggegevens moesten doorsturen omdat het systeem werd geüpdatet.



Een truc die vandaag nog steeds in omloop is.

"Ik kon gratis op internet, zo veel en zo vaak ik wou," vertelt Calce, duidelijk nog steeds trots op de prestaties van zijn jonge jaren. "Niet dat ik er veel te zoeken had, maar ik was in het bezit van zoveel macht dat ik er niet weg kon blijven. En die truc waarbij je iemand van het internet afsneed? Die gebruikte ik vaak," zegt hij, opnieuw met een grijns op het gezicht. De zaal lacht mee, want de man heeft berouw getoond, hij was toen nog jong en het was allemaal toch onschuldig, niet?

(Lees verder ....)

Bekeerde hacker voorspelt cyberwereldoorlog (2)

Piraterij

De onschuldige kwajongensstreken escaleerden snel tot meer. Op elfjarige leeftijd zoekt hij nieuwe manieren om games te kunnen downloaden. Toen gebeurde dat met behulp van bots die elke downloader een bepaalde bandbreedte toewijzen. Op het forum van de downloadsite komt hij in contact met hackers die manieren kennen om sneller te downloaden. Hij leert zichzelf programmeren om die bots te kunnen omzeilen en om indruk te maken op het forum.

Calce blijft nieuwe trucs toevoegen aan zijn arsenaal en in 1997, hij is dan dertien jaar, wordt hij gerekruteerd door een van de meest beruchte hackersgroepen van dat moment: het Russische TNT. Zowat de helft van alle malware uit die periode is afkomstig van een lid van deze notoire club. Calce laat zich meer en meer in met kleine hackersoorlogjes die moeten uitwijzen wie de beste is. In 1997 worden al bescheiden sommen verdient met malware, maar de meesten is het nog steeds te doen om de erkenning van medehackers.

De bedenkers

Altijd op zoek naar meer erkenning, meer puzzels, meer oplossingen en steeds grotere uitdagingen staat Calce mee aan de wieg van DDoS-aanvallen. Samen met zijn vriendenhackers maken ze hun aanvallen grootser en gerichter. Het culmineert in 2000 in Project Rivolta, een gecoördineerde aanval op enkele van de belangrijkste websites van hun tijd. Een aanval die leidde tot de totstandkoming van verschillende wetten die de exploten van Calce moesten definiëren buiten de aanvaardbare grenzen van de wet. Hoeveel wetten zijn er al geschreven ter uwer ere?

Na zijn digitale huisarrest ging Calce niet opnieuw aan de slag als hacker. “In mijn dagen als hacker hield ik mezelf voor dat ik bezig was met een goede zaak: ik zorgde voor de bewustmaking rond internetveiligheid,” zegt Calce. “Ik deed het ook nooit voor het geld, puur om mezelf berucht te maken. Het was bovendien moeilijk om berouw te voelen voor mij daden terwijl ik ze uitvoerde; je hebt namelijk niet het idee dat wat je doet illegaal is, of dat je er een economie zoveel geld mee kan kosten. Het enige dat mij bezighield, was dat andere hackers zeiden dat het onmogelijk was en dat ik, een vijftienjarige, ze wel even op hun plaats zou zetten.”

Calce noemt zichzelf een goed persoon, met dank aan een goede opvoeding: “Ik deed het nooit om mensen geld af te luizen, ik wilde gewoon kunnen opscheppen. En natuurlijk was ik dol op de macht die ik bezat.”

Reputatieschade

Maar de tijden veranderen. Vroeger werd een hacker door onzuivere figuren aangeworven op basis van reputatie. Een hacker nam ook niet zomaar elke klus aan, uit schrik dat het zorgvuldig opgebouwde imago besmeurd werd. “Vandaag is het evenwel de hoogste bieder die iets gedaan krijgt. En dat mag je heel letterlijk nemen: een hacker zal zijn malware verkopen aan de hoogste bieder, wie dat ook moge zijn,” legt Calce uit.

Het draait meer dan ooit om geld: hacken is een industrie op zichzelf geworden. “Het is nooit zo makkelijk geweest voor vijftienjarigen om te beginnen hacken. Je downloadt Kali Linux, installeert enkele plug-ins en je bent vertrokken. Ransomware koop je aan als een suite en je krijgt er een helpdesk bij. Je hebt slechts een halfuur voorbereiding nodig om je te mengen in verkiezingen – ik ga geen voorbeelden noemen.”

Bovendien speelt normvervaging eveneens een grote rol volgens Calce: “de huidige generatie vijftienjarigen weet niet meer waar de grens ligt. Grofgebektheid wordt op het internet als normaal gezien, en presidenten doen er vaak zelfs nog een schepje bovenop. En het wordt steeds makkelijker om economische schade aan te richten als je malware vrij goedkoop kan aanschaffen.”

Ethish hacken

Calce verkoopt zijn diensten vandaag aan ‘de goeien’. Hij voert met zijn bedrijf penetratietests uit die onderzoeken hoe sterk de beveiliging van een bedrijf of organisatie is, en daarnaast werkt hij samen met HP om betere beveiligingsmethodes te bedenken. Waar ziet hij vandaag de grootste tekortkomingen? “Werknemers zijn nog steeds de zwakste schakel. Bedrijven kunnen zo goed beveiligd zijn als ze willen, het is nog altijd een eitje om via een nietsvermoedend



personeelslid binnen te geraken.”

“Een tijdje geleden deed ik een penetratietest voor een groot bedrijf. Ik dacht mezelf nog eens uit te dagen en de conventionele methodes, social engineering en phishing, links te laten liggen. Ik onderzocht de routines van enkele werknemers en kwam uit bij een man, niet oud, niet jong, iemand die even goed met een computer kan werken als de volgende in de rij.”

“Hij werkte elke dag op de trein op weg naar zijn werk. Hij volgde braaf de voorschriften van zijn IT-departement: bescherm de ‘line of sight’, de kijkhoek, zet bluetooth uit enzovoort. Hij gebruikte wel het internet van de trein, omdat dat nodig was voor zijn werk. Ik kraakte de router van de trein, legde hem plat en presenteerde mijn computer als nieuwe treinnetwerk, enkel en alleen door het een gelijkende naam te geven. De man logde in en van zodra hij aankwam op zijn kantoor en zijn computer verbinding maakte met het bedrijfsnetwerk, had ik het hele bedrijf in handen.”

Bekeerde hacker voorspelt cyberwereldoorlog (3)

Riolering

Het klinkt als een Ian Fleming-verhaal, maar het gebeurt echt. We lezen en zien zoveel spionageverhalen dat we vergeten dat vele van die verzinsels geënt zijn op praktijkvoorbeelden. Bovendien helpt het niet dat onderwijzing in de gevaren van het internet nog steeds geen prioriteit is in onze bedrijfswereld. Wij Belgen moeten nochtans beter weten: een tijd geleden stonden we nog bovenaan in de lijst van meest gedupeerde landen.

“Bedrijven zijn te veel gericht op de voor- en achterdeur. Ze denken dat als ze die beveiligen, ze veilig zijn. Hackers denken echter meer als inbrekers: als de deur van de kluis te zwaar beveiligd is, dan gaan ze wel via de riolering. Ze vinden altijd wel een zwakke plek,” zegt Calce.

Naar de wuppe

Calce had het eerder al over verkiezingen die beïnvloed werden. Het kost ieder weldenkend mens exact twee seconden om door te hebben waar hij op alludeert: Donald Trump. Met de nakende verkiezingen in Frankrijk en Duitsland kan dat wel eens een gevaarlijk precedent worden: “als je iets doet zonder resultaat, kan het even duren vooraleer iemand anders het opnieuw probeert, maar als iets succesvol is, is het logisch dat anderen zullen volgen,” zegt Calce.

Hij is er dan ook van overtuigd dat deze situatie vroeg of laat zal escaleren: “achter de schermen woedt al langer een hevige strijd, met een grote impact op verschillende landen. De volgende grote oorlog wordt sowieso een cyberoorlog waarbij de grote infrastructuur een doelwit zal zijn: kerncentrales, ziekenhuizen, internetproviders,… Voorlopig is er nog niets ontploft, maar wat als dat wel gebeurt?” vraagt Calce zich af.



“Je hebt immers maar één getalenteerde hacker nodig om de vlam in de pan te doen slaan. De V.S. hebben goede hackers, China ook, maar in Roemenië vind je eveneens genoeg individuen die een oorlog kunnen starten. Maar de echte heersers van het internet vind je nog steeds in Rusland: de hackersgemeenschap daar is nog steeds de beste ter wereld. Met de stijgende spanningen met de V.S. en Syrië kan morgen de hel losreken.”

Cybercriminelen verruilen macro voor lnk-bestand in Word-documenten

Een beruchte groepering cybercriminelen genaamd Carbanak, die eerder al miljoenen euro's bij banken wist te stelen, gebruikt een nieuwe tactiek om haar doelwitten te infecteren. Eerder werden spearphishingmails met een kwaadaardig Word-document als bijlage gebruikt. Het document bevatte een macro die na inschakeling malware op het systeem installeerde. De groepering is nu met het gebruik van macro's gestopt, zo stelt het Amerikaanse beveiligingsbedrijf FireEye.

Momenteel worden er Word-documenten verstuurd die een embedded lnk-bestand bevatten. Dit is de bestandsextensie voor snelkoppelingen. Via lnk-bestanden is het mogelijk om kwaadaardige scriptcode uit te voeren en uiteindelijk ook malware te installeren. Als gebruikers op het embedded lnk-bestand klikken krijgen ze de vraag of ze het bestand willen uitvoeren. In de melding wordt weergegeven dat het uitvoeren van het bestand schade aan de computer kan aanrichten.

De nu waargenomen aanvallen richten zich op restaurantketens, horeca-bedrijven en financiële instellingen. De e-mails en bijlagen hebben als onderwerp klachten, cateringbestellingen en c.v.'s. In het geval de aanval succesvol is wordt er een backdoor genaamd "Halfbaked" op de computer geïnstalleerd.

Bron: TechPulse / Security.nl

Dreiging blijft met IS 2.0 en Al Qaeda

Ook al wordt IS verdreven uit Raqqa en Mosul, ook al stort het kalifaat in, dan nog is er een forse terreurdreiging.

Volgens EU-terreurcoördinator Gilles de Kerchove zou 'IS 2.0' nog wel eens gevaarlijker kunnen zijn dan de huidige groep. De Kerchove ziet minder jihadisten richting het slagveld vertrekken, er komen er ook minder terug maar volgens hem vermindert de dreiging desondanks niet.

Ook al verdwijnt het kalifaat, dat is het cyberkalifaat er nog altijd wél. 'IS vraagt niet langer naar het kalifaat te komen om te strijden, maar om in de eigen omgeving geïsoleerde aanslagen te plegen. De daders worden gemanipuleerd via het internet of zijn gefrustreerd omdat ze niet konden vertrekken. IS kan zich transformeren tot een IS 2.0', zegt hij tegen De Tijd. Hét gevaar van IS 2.0? Cybercriminaliteit!

De Kerchove vreest dat de groepen op een dag het internet gaan gebruiken voor aanslagen. 'Nu doen ze dat enkel om hun ideologie te propageren, jongeren te rekruteren en zich te financieren, maar wat als ze gaan inbreken in de computersystemen van luchtverkeersleiding, stuwdam of kerncentrale'?

Jihadverdachten horen via Facebook dat hun zaak begint



Chatten met het OM over je dagvaarding – ook het OM gaat met de tijd mee. In de rechtszaak tegen tien jihadverdachten die vermoedelijk nog steeds in het strijdgebied verblijven, heeft het OM de dagvaardigingen via sociale media verstuurd. Van de tien waren immers geen betrouwbare adressen voorhanden.

Officier Ferry van Veghel zegt dat het OM alle mogelijke moeite heeft gedaan de verdachten te informeren. Zo is een facebook advertentie uitgezet, gericht op 18- tot 30-jarigen die verblijven in het gebied rond Mosul. Met succes: de oproep werd 1,1 miljoen keer getoond, achtduizend keer geliked en één verdachte reageerde binnen een uur. Deze verdachte stuurde het OM vervolgens een foto van hemzelf en een medeverdachte terwijl ze een pizza aten in Syrië. Andere verdachten zijn, aldus De Volkskrant, door 'achterblijvers' via sociale media of Skype op de hoogte gesteld van de dagvaarding.

Bron: EU / OM

Google: aantal gehackte sites in 2016 met eenderde gegroeid

Google zegt dat in 2016 een derde websites meer gehackt zijn dan het jaar daarvoor. Daarnaast stelt de zoekgigant dat de meeste eigenaren van die sites hierover geen bericht kregen. Het bedrijf waarschuwt ervoor dat deze trend vermoedelijk voort zal duren.

“We verwachten niet dat deze trend af zal remmen,” schrijft Google in zijn rapportage. “Nu hackers agressiever worden en steeds meer websites verouderd raken, zullen hackers hier gebruik van maken en nog meer sites te infecteren.”



Google gebruikt de Safe Browsing technologie om gebruikers van Google Chrome en Google Search te waarschuwen voor het bezoeken van een site. Dat doet het als er het vermoeden is dat die gehackt is, of doorverwijst naar pornosites of dubieuze webadressen. Die waarschuwingen worden steevast getoond, tot een site vrij van infectie lijkt te zijn.

Een van de belangrijkste manieren waarmee Google de eigenaren van die websites waarschuwt, is de Google Search Console. Volgens Google weet 84 procent van de site-eigenaren die hier gebruik van maken, hun site ook succesvol vrij te maken van hackers. Dat is een mooi percentage, maar minder mooi is het aantal eigenaren dat er nooit achter komt dat zijn site gehackt is: 61 procent.

Google definieert een site als gehackt, op het moment dat de Search Console een aantal problemen detecteert op het betreffende adres. Zo gaat het om spam, dubieuze weblinks, doorverwijzingen, verborgen tekst en te veel sleutelwoorden.

Kabinet bekijkt boete discriminatie internet

Net zoals in Duitsland. Het (demissionaire) kabinet bekijkt de invoering van forse boetes voor sociale netwerkbedrijven die discriminerende uitlatingen niet of te laat weghalen.

Minister Stef Blok (VenJ) antwoordde op kamervragen van de CU die het Duitse model ook in Nederland wil invoeren. In het Duitse voorstel krijgen bedrijven als Facebook en Twitter enorme boetes, oplopend tot vijftig miljoen euro, als ze te weinig doen om strafbare uitingen of gedragingen, zoals discriminatie, bedreigingen, haat en nepnieuws, niet binnen 24 uur weghalen.

In Duitsland kreeg het voorstel forse kritiek; het zou de vrijheid van meningsuiting beperken. Minister Blok wijst daar ook op. Volgens hem brengt zo’n wet ‘een heel aantal intrigerende vragen en spanningen’ met zich mee en raakt het ‘heel wezenlijke grondrechten’.

Bron: Google / Overheid.nl

Hoe DNSSEC het internet veiliger maakt

In februari luidde SIDN, de stichting die het .nl-domein beheert, de noodklok over de slechte DNSSEC-beveiliging van Nederlandse domeinnamen. Meer dan de helft van de Nederlandse domeinnamen blijkt geen DNSSEC te gebruiken. Met name banken hebben DNSSEC als extra beveiling nog niet omarmd. Dat klinkt allemaal zorgwekkend. Maar wat is DNSSEC eigenlijk en hoe maakt DNSSEC het internet veiliger?

Wat is DNS?
Iedere computer die met het internet verbonden is, heeft een uniek IP-adres. Aan de hand van deze IP-adressen weten computers elkaar te vinden. Als je dus verbinding met een andere computer wilt maken, moet je het IP-adres van die computer weten. Omdat het lastig is om al die IP-adressen te onthouden, zijn domeinnamen bedacht. Omdat een domeinnaam aan een IP-adres is gekoppeld, hoef je alleen nog maar die domeinnaam te onthouden. Zo is de domeinnaam bof.nl gekoppeld aan het IP-adres 82.94.213.237. Als je dus de website van Bits of Freedom wilt bezoeken, hoef je niet dat IP-adres te onthouden, maar kun je gewoon bof.nl intypen.

De koppeling tussen domeinnamen en IP-adressen wordt mogelijk gemaakt door een systeem dat het Domain Name System (DNS) heet. Vanwege deze koppeling wordt het DNS vaak vergeleken met het ouderwetse telefoonboek: als jij (of je computer of je smartphone) wil weten welk IP-adres er bij een bepaalde domeinnaam hoort, zoek je dat op in het DNS. Het 'DNS-telefoonboek' wordt beschikbaar gemaakt door een groot aantal servers verspreid over de hele wereld: de DNS-servers. Iedere DNS-server neemt een klein stukje van dat telefoonboek voor zijn rekening. Als je computer wil weten welk IP-adres aan een bepaalde domeinnaam is gekoppeld, dan vraagt hij dat aan één van die DNS-servers.

De kwetsbaarheid van DNS
Het DNS speelt dus een belangrijke rol voor de werking van het internet en is daarom één van de fundamentele technologieën die het internet mogelijk maken. Het DNS is ook één van de oudste onderdelen van het internet. In de begintijd van het internet, enkele decennia geleden, speelde beveiliging niet zo'n grote rol. Het internet in die dagen was vooral een wetenschappelijk onderzoeksproject. Dus toen het DNS in die periode ontworpen werd, kreeg het geen beveiligingsmechanismen. Hierdoor is het DNS nu kwetsbaar voor een aantal vormen van misbruik.

Een DNS-server vertelt je welk IP-adres er aan een domeinnaam is gekoppeld. Het probleem is dat je niet zeker kunt weten dat het antwoord van een DNS-server juist is. Want omdat het DNS geen beveiliging heeft, is het mogelijk om het antwoord van zo'n DNS-server te vervalsen of te manipuleren. Een internetcrimineel (of iemand anders met slechte bedoelingen) kan je op deze manier naar een verkeerde website sturen – zonder dat je dat doorhebt.

Stel, je wilt naar de website van je bank om een betaling te doen. Je opent je browser en typt www.jouwbank.nl in. Je computer maakt verbinding met een DNS-server om te vragen welk IP-adres er aan www.jouwbank.nl is gekoppeld. Maar deze DNS-server is in handen van een internetcrimineel. Het IP-adres dat je computer van deze DNS-server krijgt, is niet van de bank, maar van de internetcrimineel. Het gevolg is dat je niet op de website van je bank terechtkomt, maar op een vervalste website van de internetcrimineel.

Je computer maakt meestal gebruik van een DNS-server die beschikbaar wordt gesteld door het netwerk waar je op dat moment mee verbonden bent. Als je thuis aan het internetten bent, is dat meestal de DNS-server van je internetprovider. Maar als je verbonden bent met een openbaar wifi-netwerk, dan ben je afhankelijk van de DNS-server die dat wifi-netwerk je voorschotelt. Als dat wifi-netwerk slecht beveiligd is – of helemaal niet beveiligd – dan is het redelijk eenvoudig om de informatie in het DNS-telefoonboek te vervalsen. Dit is één van de redenen waarom je extra voorzichtig moet zijn als je een openbaar wifi-netwerk gebruikt.

Maar de onveiligheid van DNS heeft meer gevolgen. Voor je mail bijvoorbeeld. E-mail wordt verstuurd en ontvangen door mailservers. Zo'n mailserver heeft natuurlijk ook een IP-adres. Als iemand dus in het DNS een vals IP-adres aan een mailserver koppelt, kan hij de mail voor die mailserver omleiden en onderscheppen.

DNSSEC: het laagje beveiliging bovenop DNS
Het probleem van het DNS is dus dat je niet weet of de antwoorden van DNS-servers betrouwbaar zijn. De informatie die afkomstig is van DNS-servers kan daarom door internetcriminelen vervalst zijn. Om hier iets aan te doen, is DNSSEC verzonnen.

DNSSEC staat voor DNS Security Extensions en is eigenlijk een laagje beveiliging bovenop het oorspronkelijke DNS. Met DNSSEC worden antwoorden van DNS-servers voorzien van een digitale handtekening. Met behulp van deze handtekeningen kun je verifiëren dat het oorspronkelijke DNS-antwoord niet vervalst is.

DNSSEC kan niet in één keer voor het hele DNS-telefoonboek ingeschakeld worden. Voor iedere domeinnaam moet namelijk zo'n digitale handtekening worden gemaakt. En dat is iets wat alleen de beheerder van de domeinnaam kan doen. Helaas zijn er veel beheerders die dat (nog) niet gedaan hebben. Dit is de reden waarom SIDN de noodklok luidde.

Naast de domeinnaambeheerders is er een tweede partij die actie moet ondernemen om DNSSEC tot een groter succes te maken. Dat zijn de internetproviders. Zoals gezegd, maakt je computer of je smartphone meestal gebruik van een DNS-server die door je internetprovider beschikbaar wordt gesteld. Voor de werking van DNS is het vereist dat deze DNS-servers ook DNSSEC ondersteunen. Deze DNS-servers moeten namelijk de digitale handtekeningen van domeinnamen controleren. Helaas zijn er nog niet veel internetproviders die DNSSEC op hun DNS-servers hebben aangezet. Op dit moment is XS4ALL in Nederland de enige landelijke internetprovider die deze stap heeft gezet.

Helaas kun je zelf vrij weinig aan deze situatie doen. DNSSEC is niet iets wat je zelf aan kunt zetten. Je bent afhankelijk van de domeinnaambeheerders en van de interproviders: zij zijn de enigen die DNSSEC kunnen 'aanzetten'. Je kunt natuurlijk wel contact opnemen met je internetprovider en aangeven dat je het voor je internetveiligheid belangrijk vindt dat ze DNSSEC gaan ondersteunen.

Bron: Bits of Freedom

NSA kan meekijken bij betalingsverkeer tientallen banken

De Amerikaanse NSA is diep geïnfiltreerd in het internationale betalingssysteem en kan bij tientallen banken zien wie naar wie geld overmaakt. De hackers van de geheime dienst hebben via EastNets, een bedrijf dat wereldwijd zogeheten Swift-betalingen regelt, toegang gekregen tot in theorie meer dan 1000 financiële instellingen in 120 landen. Dat blijkt uit documenten die het hackerscollectief Shadow Brokers online heeft gezet.

Het betalingssysteem Swift zelf is niet gehackt. Uit eerder uitgelekte NSA-documenten van klokkenluider Edward Snowden bleek al dat de NSA in staat was om Swift-betalingen te volgen. Tot nu was het onduidelijk hoe de NSA dat kon doen. Als iemand geld overmaakt naar het buitenland, dan gaat dat via Swift. Grote banken communiceren rechtstreeks met Swift, maar kleinere banken laten dat vaak via een servicebureau lopen. Zo'n bedrijf is EastNets, een grote speler wereldwijd. Ook ING en ABN Amro maken in bepaalde landen gebruik van de diensten van EastNets, zoals in Zuid-Korea. De NSA heeft dit servicebureau, en een gelieerd bedrijf BCG, vanaf zeker augustus 2013 gehackt. Daarmee krijgt de dienst in één klap toegang tot alle aangesloten banken.

Shadow Brokers publiceert al sinds de zomer van 2016 informatie van een geheime dienst. Experts twijfelen er niet aan dat dit de NSA moet zijn. De documenten geven een indruk van het wapenarsenaal van de dienst: met name gebruikte kwetsbaarheden in software. Het is niet helemaal duidelijk wie erachter het hackerscollectief zit. Een voormalig medewerker van de NSA, Harold T. Martin III, is eerder aangehouden op verdenking van het stelen van liefst 50 terabyte aan informatie. Hij had toegang tot systemen van de hackeenheid van de NSA. Maar sommigen, zoals Edward Snowden, vermoedden juist dat Rusland achter het lek zat.

Het is hoe dan ook bijzonder pijnlijk voor de Amerikaanse overheid. Na de hele Snowden-affaire zijn er al diverse lekken geweest. Onlangs publiceerde WikiLeaks nog duizenden bestanden van de hackeenheid van de CIA. Deze documenten maken wederom duidelijk hoe grootschalig de Amerikanen wereldwijd te werk gaan. Daarbij kiezen ze de makkelijkste methode om met één infiltratie bij een heleboel bedrijven te komen. Eerder bleek bijvoorbeeld dat de Amerikanen samen met het Britse GCHQ een specifieke tak van de Belgische telecomprovider Belgacom hadden gehackt. Dit onderdeel, BICS, regelde wereldwijd mobiel telefoonverkeer en is met name groot in het Midden-Oosten en Afrika.



Swift lanceert tool tegen frauduleuze banktransacties

De internationale bankorganisatie Swift heeft een nieuwe tool gelanceerd waarmee banken frauduleuze transacties kunnen opmerken. De maatregel volgt op verschillende bankovervallen waarbij aanvallers via frauduleuze transacties miljoenen euro's wisten te stelen die vanuit de banken werden verzonden.

De Society for Worldwide Interbank Financial Telecommunication (Swift) is een internationale coöperatieve organisatie voor internationale banktransacties. Banken kunnen via het Swift-systeem transacties uitvoeren. Digitale overvallers wisten via het Swift-systeem 81 miljoen dollar bij de Centrale Bank van Bangladesh te stelen. Dezelfde aanvallers zouden ook een bank in Vietnam en de Filipijnen hebben aangevallen. Het Swift-systeem zelf was niet gehackt, maar de lokale bankomgeving, waardoor de aanvallers transacties via het Swift-systeem konden uitvoeren.

De nu gelanceerde tool biedt banken de mogelijkheid om betalingsopdrachten aan de hand van zelf opgegeven parameters te controleren en is direct binnen de Swift-berichtenstroom te gebruiken. Met de tool, die transactiepatronen van banken kan leren, richt Swift zich op kleinere banken. Het wordt als een gehoste oplossing aangeboden. Volgens Swift gaat het om een belangrijke mijlpaal in het beveiligingsprogramma dat vanwege de bankovervallen werd aangekondigd.

Bron: SWIFT

Takedown notice; informatie van social media verwijderen

Neem zo snel mogelijk actie

Het verwijderen van berichten waarin jij bent vermeld of foto's en video's waar jij op staat van social media kanalen zoals Facebook, LinkedIn, Twitter of Google+ kan lastig zijn. Het virale karakter van social media kan er voor zorgen dat informatie snel wordt verspreid. Het is daarom belangrijk om zo snel mogelijk actie te ondernemen. Hoe sneller je bij de bron bent, hoe minder schade een bericht kan aanrichten.

Berichten van jezelf verwijderen

Een eigen bericht van jouw tijdlijn verwijderen is op zich altijd mogelijk. Het is daarom altijd goed uit te zoeken waar de "delete-knop" zich bevindt. Maar wanneer een van je volgers het bericht al heeft gedeeld, getagd, geliked of een +1 heeft gegeven, blijft het bericht zichtbaar op de tijdlijn van jouw volgers. Je zult in dit soort gevallen aan de betreffende personen, een voor een moeten vragen of ze het bericht willen verwijderen van hun tijdlijn. Indien het bericht op de foto goed gedeeld is, kan dat aantal flink oplopen.

Berichten van anderen verwijderen

Het kan ook voorkomen dat een bericht tegenkomt waar in je op negatieve wijze wordt genoemd. Het beste kan je de betreffende persoon op vriendelijke wijze te verzoeken om het bericht te verwijderen of aan te passen. Doe dit bij voorkeur via e-mail of een privébericht. Ook hier geldt weer dat wanneer het bericht eenmaal is gedeeld door anderen, je ook deze personen individueel zal moeten verzoeken om het bericht te verwijderen.

Wat is een Takedown notice?

Nu kan het gebeuren dat de plaatser van het bericht niet wil meewerken. Gaat het om onrechtmatige, strafbare inhoud of om informatie die in strijd is met het beleid van het desbetreffende socal media kanaal, dan kun je een zogeheten Takedown notice verzoek indienen.

Een Takedown notice (ook wel een Notice of Claimed Infringement genoemd) is een procedure die start op het moment dat iemand een melding bij een service provider doet over vermeende onrechtmatige of strafbare inhoud op internet. De procedure kan eindigen met het verwijderen van specifieke informatie op een webpagina of zelfs het uit de lucht halen van de betreffende website. Er is van te voren echter geen garantie te geven of het verzoek wordt ingewilligd.

Voor welke informatie kun je een Takedown notice indienen?

Je kunt een Takedown notice indienen wanneer je informatie tegenkomt waarvan je denkt dat deze onrechtmatig of strafbaar is. Soms kan een verzoek worden ingediend wanneer de informatie op een social media kanaal niet overeenkomt met het beleid van dit kanaal. Veel social media kanalen zullen in hun voorwaarden iets hebben staan over bijvoorbeeld het verspreiden van kwetsende informatie. Je hoeft van tevoren niet compleet zeker te weten of de informatie daadwerkelijk onrechtmatig of strafbaar is. Maar je moet wel goed onderbouwen waarom je van mening bent dat de informatie onrechtmatig of strafbaar is.

Welk soort informatie kan leiden tot een succesvolle verwijdering?

Informatie niet in overeenstemming met het beleid van het social media kanaal

Publicatie van iemands persoonsgegevens

Inbreuk op auteurs- en/of merkenrecht

Haat zaaiende en racistische uitlatingen

Smaad en lasterlijke teksten

Cyberstalking

Hoe kan ik een verzoek indienen?

De meeste social media kanalen hebben een eigen procedure op hun website gepubliceerd waarin staat uitgelegd hoe je een Notice of Claimed Infringement kunt indienen. Vaak vind je hier ook een standaardformulier waarmee je een verzoek kunt indienen om bepaalde informatie te laten verwijderen. Door dit formulier te gebruiken komt het verzoek vaak meteen op de juiste plek terecht en wordt vaak binnen enkele dagen geantwoord.

Welke gegevens worden vaak gevraagd bij een Takedown notice?

Voor een Notice of Claimed Infringement moet je vaak een aantal gegevens invullen. Probeer zo volledig mogelijk te zijn zodat het social media kanaal jouw verzoek goed kan beoordelen. Dit zijn onder andere:

De eigen contactgegevens.

De informatie die volgens jou onrechtmatig is, voeg bij voorkeur een print screen van de ongewenste informatie toe ter verduidelijking.

De URL's (een link) waarop de ongewenste informatie is gepubliceerd.

Een beschrijving waarin je uitlegt waarom de inhoud volgens jou onrechtmatig of strafbaar is.

Indien mogelijk voeg je documenten toe waarmee je bewijst dat jij de rechtmatige eigenaar bent van de gegevens, bijvoorbeeld in geval van plagiaat van copyright, stuur dan deze documenten voor de volledigheid mee.

Hoe lang duurt de procedure van een Takedown notice voor social media?

De termijn voor het afhandelen van een verzoek hangt af van verschillende factoren en verschilt per social media kanaal. De mate van aantoonbaarheid van de onrechtmatige of strafbare inhoud, de aard en omvang van de schade naast de betrouwbaarheid van de bron kunnen allemaal van invloed zijn. Houd er rekening mee dat goed aantoonbare onrechtmatigheid of strafbaarheid sneller zal worden afgehandeld.



WhatsApp Status | Helder uitgelegd & privacy instellingen

Wat is de WhatsApp Status functie?

Het was al even bekend dat WhatsApp met deze nieuwe feature in de weer was, maar sinds 20 februari 2017 is WhatsApp Status officieel gelanceerd, vrijwel gelijktijdig met het 8-jarig bestaan van de chatdienst. Iedereen die WhatsApp gebruikt kan nu zijn status delen doormiddel van een onbeperkt aantal filmpjes en foto's, eventueel voorzien van tekeningen, grappige gifjes of tekst. Daarmee vervangt het de oude status-functie die slechts door een tekstbericht werd weergegeven.

De feature is eigenlijk niet nieuw; Instagram en Snapchat gebruiken een soortgelijke 'story-functie' al langer. Dat deze populaire social media diensten elkaars functies kopiëren laat goed zien hoe stevig ze de strijd met elkaar aangaan.

Wat houdt "Mijn Status" in?

Heb je al WhatsApp dan krijg je een automatisch update waarbij het menu-item 'Status' is toegevoegd. Zo kom je op "Mijn Status" en kan je met de camera direct je eigen beeldverhaal vastleggen. Of je gebruikt gifs uit je fotoalbum. Ook alle statusupdates van je contactpersonen zie je in dit menu.

Hoe werkt de WhatsApp Status functie?

Een nieuwe WhatsApp Status maken doe je zo:

Kies 'Status'.

Klik op de cirkel met plusje.

De camera is direct actief; klik eenmaal op de ronde knop voor een foto, houd je deze ingedrukt dan maak je een filmpje.

Geef het een titel en bewerk de video of foto eventueel nog met tekst, tekeningen en emoji's.

Je kunt nog meer foto's toevoegen via de grijze cameraknop.

Klaar? Klik linksboven op het kruisje en daarna op de blauwe verzendknop.

Je kunt nu aangeven met wie je deze status wilt delen; aan al je contacten of slechts een selecte groep.

Na 24 uur word deze status automatisch bij jou en je contacten verwijderd. Doe je dat liever eerder, open dan je status en klik op delete (Android), of swipe het weg (iOS). Zien wie jouw statusupdates heeft bekeken? Klik dan op de drie puntjes achter je status.

De privacy instellingen WhatsApp Status

Net als de gewone WhatsApp-berichten zijn de WhatsApp Status updates versleuteld. Ze worden gecodeerd doorgestuurd en kunnen alleen worden bekeken op de telefoon van de ontvanger. Via de instellingen onder de tab 'Privacy' geef je aan wie jouw status wel of niet mag zien. Je hebt de keuze uit:

Mijn contacten (allemaal)

Mijn contacten behalve (sluit hier een aantal personen uit)

Alleen delen met (selecteer stuk voor stuk de ontvangers)

Je kunt de privacy instellingen steeds veranderen, maar de wijzigingen gelden dan niet voor de statusupdates die je al hebt verstuurd.

De WhatsApp status functie wordt komende weken wereldwijd uitgerold. En hoewel de nieuwe feature door velen enthousiast wordt ontvangen zijn er ook kritische geluiden; veel fervente WhatsApp gebruikers zien graag de eenvoudige tekst -status weer terug. De ontwikkelaars achter WhatsApp hebben beloofd dit in overweging te nemen.



Bron: WhatsApp

Internetscamming in Ghana

Uitzending gemist? Kijk dan (nogmaals) naar de prachtige aflevering van De Westerlingen over internetscammers in Ghana.

Over jonge mannen die fulltime chatten met hun slachtoffers. 'I am really missing you so much baby' en zo. Voor jongeren zonder scholing biedt internet in steden als Accra een enorme kans. Niet meer vanuit een internetcafé maar gewoon thuis, op laptop en smartphone.

Scamming is big business hier en 'een manier van overleven'. De scammers zien zichzelf als zakenman. 'Jullie zoeken liefde. Ik verkoop liefde. Ik zie het niet als iets crimineels, zoals jullie'. Moeilijk is het niet: 'Vrouwen willen lieve woordjes, maar mannen, die vallen gewoon voor wat ze zien. Zo simpel is het'.

Als je de chats meeleest kan je bijna niet geloven dat er mensen zijn die erin trappen. Maar romance-scammers - jonge oplichters uit West-Afrika die zich op datingsites voordoen als westerling - verdienen een aardig centje met teksten als 'I'm really missing you so much baby.'

Maandenlang chatten de scammers met westerse singles. Als ze een band hebben vragen ze om geld. Omdat hun oom ziek is, hun verre dochter in problemen is geraakt, of omdat ze geld nodig hebben voor een ticket om hun geliefde te bezoeken. Klik hier om de uitzending te bekijken….



Europol en China gaan samen cybercrime bestrijden

Europol en China hebben vandaag een strategische samenwerkingsovereenkomst getekend om onder andere samen cybercrime te bestrijden. Onder de overeenkomst mogen er algemene strategische inlichtingen alsmede strategische, technische en operationele data worden uitgewisseld.

Het uitwisselen van persoonlijke gegevens is onder deze overeenkomst niet toegestaan. Dit mag alleen bij een operationele overeenkomst. Volgens Europol is de nu gesloten overeenkomst belangrijk om misdrijven aan te pakken waar zowel de Europese Unie als China mee te maken heeft.



Bron: VPRO / Europol

Ssd-tips: Bestanden verwijderen of herstellen

Je bent van plan een andere computer of ssd aan te schaffen en je wilt je oude systeem of ssd weggeven of doorverkopen. In dat geval wil je wel de absolute zekerheid dat er geen data meer op je ssd te vinden zijn en dat is lastiger dan het lijkt. Hier leggen we uit hoe je bestanden volledig van je ssd kan verwijderen of juist herstellen.

Klassieke shredtechnieken zijn namelijk vaak niet effectief aangezien nieuwe data (zoals overschrijfpatronen) bijna altijd naar andere geheugencellen worden geschreven ten gevolge van zogenoemde wear leveling -technieken. Dat is een technologie die ervoor zorgt dat data evenredig worden verdeeld over alle geheugencellen om zo de levensduur ervan te verlengen. Bovendien kan er data achterblijven in speciaal gereserveerde opslagruimtes ('over-provisioning') die niet voor gewone (wis) programma's bereikbaar zijn.

Om toch de ganse inhoud van een ssd te kunnen wissen moet je een speciaal wis-commando aanroepen: ATA Secure Erase. Dit commando gelast de ssd-controller alle gebieden van de schijf te overschrijven, reservegebieden incluis. Veel ssd's slaan echter data versleuteld op en dat maakt veilig wissen tot een snel en makkelijk proces: het volstaat dat de huidige sleutel wordt verwijderd en door een nieuwe wordt vervangen om je oude data onbereikbaar te maken.

Een shredtool die zich van ATA Secure Erase bedient vind je nagenoeg altijd in de meegeleverde toolkit van de ssd-fabrikant. Doorgaans moet je hiervoor wel van een ander medium booten (zoals een live usb-stick of dvd), aangezien dat niet vanuit Windows zelf kan.

Parted Magic

Een mogelijk alternatief is nog de live Linux -distributie Parted Magic, die overigens ook secure erase kan toepassen op ssd's met het nvm-e-protocol. We tonen even hoe je met deze distro, die trouwens ook dienst kan doen als partitionerings- en kloontool, aan de slag gaat.

Start je systeem met het livemedium; kies de standaardoptie of, als dat niet lukt, opteer voor de Failsafe-modus. Even later verschijnt het bureaublad. Klik hier op Erase Disk. Er verschijnt een dialoogvenster. Laat het tabblad Internal geopend en selecteer het correcte protocol: ATA Secure Erase of nvm-e Secure Erase. We gaan hier van de eerste optie uit. Plaats een vinkje bij de juiste schijf (ssd). Standaard staat de Secure-optie geselecteerd.

Als je ssd dat ondersteunt kun je echter ook Enhanced aanstippen. In dit geval worden alle data met datapatronen overschreven die door de fabrikant zijn bepaald en worden ook sectoren overschreven die niet langer in gebruik zijn door reallocatie. De status moet Not Frozen zijn om te kunnen vernietigen. Is dat niet het geval, klik dan Sleep aan; na het ontwaken (via een herstart) van je systeem is je ssd in principe klaar (Not Frozen). Bevestig met Continue, plaats een vinkje en klik op Start Erase.

Ssd trimmen

Data echt vernietigen op een ssd mag dan extra lastig zijn, dat geldt anderzijds ook voor dataherstel van bestanden die je per ongeluk hebt verwijderd of die zich nog op een defecte ssd zouden bevinden. Dat heeft onder meer te maken met de trim-functie. Hierbij brengt de ssd-controller het besturingssysteem op de hoogte dat de geheugenblokken die daarvoor door de intussen gewiste data nu beschikbaar zijn. De zogenoemde 'garbage collector', actief op de achtergrond, zal dan voor de vrijgekomen ruimte de vlag 'leeggemaakt' instellen en die uiteindelijk ook fysiek leegmaken.

Het probleem met het oog op dataherstel is echter dat de ssd-controller voor deze ruimte alleen maar nullen zal retourneren zodra die vlag is gezet. Dat kan dataherstel met 'klassieke' tools (zoals het voor het overige zeer degelijke en gratis Recuva bemoeilijken. Let wel, installeer deze software nooit op de schijf waar je verdwenen data probeert te herstellen! Vind je met deze en dergelijke tools je data niet meer terug, dan zit er wellicht weinig anders op dan een professionele dataherstelservice aan te spreken.

Om de kansen op dataherstel bij verdwenen bestanden te verhogen zou je kunnen overwegen om de trim-functie uit te schakelen. Dat is echter geen goed idee, omdat dit een nadelige impact heeft op de prestaties van je ssd. We raden je dus absoluut aan trim ingeschakeld te laten. Je kunt de trim-status controleren ga je als administrator naar de Opdrachtprompt en over je het commando fsutil behavior query disabledeletenotify uit.

Krijg je de waarde DisableDeleteNotify = 0 terug, dan is trim geactiveerd. Blijkt de waarde 1 te zijn, dan kun je trim alsnog activeren met het commando fsutil behavior set disabledeletenotify 0 (met 1 schakel je de functie uit). Bij heel wat ssd-toolkits van de fabrikanten kun je trouwens ook de trim-status aflezen en die functie eventueel activeren.



…verder op de website oa ……

GOEDKOPE RANSOMWARE AS A SERVICE ONTDEKT

EEN DERDE VAN DE OUDERS WEET NIET WAT KINDEREN DOEN OP EEN BEELD-SCHERM

PAK RANSOMWARE AAN ZONDER TE BETALEN MET DEZE GRATIS DECRYPTIE-TOOLS

EU KOMT IN JUNI MET REGELS VOOR VERSLEUTELDE CHAT-APPS

CONTROLEER JE SYSTEEM OP VEROUDERDE SOFTWARE

CREATORS UPDATE WINDOWS 10: ALLE NIEUWE FUNCTIES OP EEN RIJ

ULTIEME CURSUS TEGEN VIRUSSEN, MALWARE EN HACKS



…. en meer ……..

…verder op de Facebook pagina oa ……

Deze drie externe tools zijn onmisbaar op je Windows-computer

Herken phishing mails en bescherm jezelf!

Verander je computer in een Chromecast

Zo voorkom je identiteitsfraude en identiteitsdiefstal!

Speelgoed dat met jouw kind meeluistert | Internet of Toys

Geschiedenis verwijderen van het internet; zo doe je dat!

WhatsApp Status | Helder uitgelegd & privacy instellingen

Privacy instellingen; Social media & applicaties

Controleer je systeem op verouderde software

Hoe gevaarlijk is het om 's nachts je smartphone op te laden?

…. en meer ……..



Cops in cyberspace

Ook in Zeeland heeft de politie Facebook Advertising ingezet om getuigen en informatie te vinden. In deze zaak gaat het om de moord op Kees van Schaik uit Rilland. De banner werd uitgezet in een straal van tien kilometer rond Rilland, niet alleen op computers en laptops maar ook op smartphones. Via de banner is in tien uur tijd 786 doorgeklikt naar het opsporingsbericht op Politie.nl.

———————————————————

De politie heeft drie mannen aangehouden op verdenking van grootschalige drugshandel via het dark web. De verdachten (25, 26 en 47, uit Roosendaal en Schijf) zouden onder meer pakketten met mdma-tabletten hebben verzonden, vooral naar de VS. De drugs waren verpakt als visvoer of aquariumzand. De pakketjes werden door de mannen in Duitsland of België op de post gedaan. Bij zoekingen werden verzendbewijzen gevonden. Die adressen worden aan de autoriteiten in de desbetreffende landen verstrekt, zodat de polities daar nader onderzoek kunnen doen. Deze week meldde de Duitse douane nog dat er steeds vaker 'drugsbrieven' in Duitsland worden gepost. Koeriers zouden die pakketjes, waarin vooral amfetamine en xtc zou zitten, vanuit Nederland in Duitse brievenbussen droppen. De douane onderschepte in de laatste vijf maanden van 2016 ruim tweeduizend van die brieven, waarin in totaal 170 kilo drugs verstopt was. Nederlanders zijn relatief oververtegenwoordigd in de online verkoop van drugs, bleek vorig jaar uit onderzoek van het WODC en Rand Europe. Bijna een tiende van alle drugs die op internet verkocht wordt, is afkomstig van Nederlanders.

———————————————————-

De politie heeft in Zaandam vier jongens (16, 17 en 18) opgepakt die in een YouTube-filmpje met wapens liepen te zwaaien. De jochies werden herkend, zowel door agenten als gemeentelijke handhavers. In de filmpjes toonden de vier onder meer een ploertendoder, een stroomstootwapen en enkele vuurwapens, bij zoekingen werden een nepvuurwapen en een bivakmuts (?!) maar ook goederen die van diefstal afkomstig zouden zijn.

Politie en FIOD hebben na een gezamenlijk onderzoek een bende opgerold die via internet anabolen en geneesmiddelen verkochten. Drie mannen zijn aangehouden op verdenking van witwassen en overtreding van de Geneesmiddelenwet. Bij zoekingen in negen woningen, een sportschool en een schoonheidssalon is beslag gelegd op dertig mille in cash, op bitcoins, medicijnen, anabolen, enkele dure auto's, horloges en sieraden, computers en administratie maar ook op de complete inventaris van die sportschool. De gekochte producten werden per post bezorgd maar konden ook worden afgehaald in enkele snackbars. De politie was het onderzoek naar de illegale handel in anabolen gestart op grond van informatie uit een liquidatie-onderzoek

———————————————————

De Blue Whale Challenge, een facebook-'spel' dat in Rusland al tot meerdere zelfdodingen heeft geleid, schijnt nu ook in Engeland populair te zijn. De West Yorkshire Police waarschuwde vorige week in ieder geval voor de gevaren ervan. 'We would urge parents and guardians to remain vigilant and monitor your child's use of the internet'. In het spel krijgen deelnemers vijftig dagen lang elke dag een opdracht, jezelf snijden of zo. Op de laatste dag is de opdracht dan vaak om ergens vanaf te springen. Enkele tientallen Russische kids deden dat naar verluidt al.

———————————————————-

Internetpedo's kunnen kinderen tegenwoordig ook via Tinder-achtige apps vinden en ontmoeten, waarschuwt de politie in Northumbria, Engeland. 'It is very easy for adults to use the app, posing as a young person'. Het gaat specifiek om chat-apps als Yellow die gratis te downloaden zijn in de winkels van Google en Apple, waar ze als 12+ geclassificeerd zijn. Bij een match op Yellow worden de gematchten eenvoudig doorgelinkt naar Snapchat waar ze tekst en beeld kunnen uitwisselen, aldus de politie. Yellow is primair gericht op kinderen tussen 13 en 17 maar niemand let op die leeftijden. De makers van Yellow hebben intussen hun gebruiksvoorwaarden aangepast – profielen zonder foto worden geweerd en wie zijn leeftijd wil aanpassen moet een id-bewijs insturen.

Veertig agenten, honderden dronefilmpjes en uiteindelijk 45 dronebestuurders. Op initiatief van politie, OM en Kmar hebben agenten een hele dag naar dit soort filmpjes zitten kijken. Is er een overtreding gemaakt, kunnen we de 'bestuurder' vinden? De 45 dronebestuurders hebben allemaal een waarschuwing gekregen, vijf van hen worden mogelijk vervolgd. Volgens de politie zijn maar weinig mensen op de hoogte van de regels: drones mogen niet boven mensenmassa's vliegen, ze mogen niet gebruikt worden in de buurt van luchthavens of in het donker. Worden de dronebestuurders nogmaals betrapt, dan krijgen ze een boete.

———————————————————-

Volgens de politie in Kent, Engeland zijn zelfverklaarde pedojagers een gevaar voor hun omgeving. En voor de politie. De groepen – er komen er steeds meer in Engeland – belemmeren het politiewerk, doen aan eigenrichting en wijzen onschuldigen aan als kinderlokker. De waarschuwing komt na een incident in Bluewater waarbij leden van de (facebook)groep The Hunted One een man mishandelden. Een groepslid werd aangehouden. Volgens chief superintendent Thomas Richards van de Kent Police zijn er 'significant concerns about people taking the law into their own hands and the methods they use'. Laat ze vooral de politie bellen als ze iemand verdenken, maar vooral niet zelf aan de slag gaan, zei Richards. 'The police have resources and expertise to protect the vulnerable and people with mental health issues'. De groep zegt zich niks van de waarschuwing aan te trekken en gewoon door te gaan maar dat hun acties niet meer live op YouTube zullen worden gestreamd. Opvallend is dat een Britse rechtbank nog geen maand geleden een andere groep, Dark Justice, toestemming gaf om door te gaan met hun undercoverwerk om kinderlokkers te ontmaskeren.

Rechtspraak

Het OM heeft een vlogger (23, uit Zoetermeer) een boete van 350 euro opgelegd voor het beledigen van de politie. De man filmde, begin januari 2017, agenten toen hij een verkeersboete kreeg. 'Ik ga jullie filmen voor mijn blog', riep hij. Daarna haalde hij zijn 3-jarige zoontje uit de auto, beiden staken hun middelvinger op. 'Fuck you'. Het filmpje ging vervolgens – niet verwonderlijk – viraal. Het OM sprak van kwalijk gedrag, 'nota bene in het bijzijn van een peuter'. De vlogger moet verder de bewuste vlog verwijderen en in een nieuwe vlog excuses aanbieden.

———————————————————

Een primeur: voor het eerst is iemand veroordeeld voor stalking via zijn status-instelling in Whatsapp. De verdachte (36, uit Breda) had zijn ex maandenlang gebeld, gesms't en ge-appt. Ook toen de vrouw zijn telefoonnummer blokkeerde, bleef het stalken doorgaan. Niet meer via berichtjes maar via de status. Omdat de man wist dat zijn ex regelmatig controleerde of hij online was, communiceerde hij op die manier. Hij veranderde zijn status onder meer in 'Ik wil moorden, je bent niet veilig' en 'de dag der waarheid is nabij'. De vrouw maakte screenshots en stapte daarmee naar de politie. Volgens de advocaat van de verdachte waren de statusberichten niet per se aan de ex-vrouw gericht en was dus geen sprake van stalking. De rechtbank oordeelde anders en veroordeelde de man tot 120 uur taakstraf, een contactverbod en het betalen van 750 euro schadevergoeding.

———————————————————-

De rechtbank in Rotterdam heeft een man (38, uit Hoek van Holland) veroordeeld die tien jaar lang een kinderpornoforum op internet beheerde. De verdachte kreeg vier jaar en zeven maanden opgelegd, conform de eis van het OM. Op het forum met veertigduizend foto's en filmpjes voorzag hij andere leden zelfs van adviezen. Hij werd zomer 2016 al schuldig bevonden maar moest nog psychisch onderzocht worden. Omdat hij dat weigerde, is hij nu volledig toerekeningsvatbaar verklaard.

———————————————————-

Ook al bestond het filmpje niet waarmee een man een vriendin probeerde af te persen, hij werd daarvoor toch veroordeeld. De verdachte (28, uit Utrecht) moet veertig uur werkstraf doen. Hij verzon de chantagebeelden toen de vrouw hem uit geldnood een paar keer had gepijpt en daarmee wilde stoppen. 'Ik heb alles gefilmd en als je stopt, zet ik dat op internet', dreigde de man. De vrouw stapte naar de politie. Volgens de rechter was de dreiging ernstig en is de impact 'van dit soort acties groot'.

———————————————————-

De rechtbank in Breda heeft een man (34, uit Dussen) tot drie jaar celstraf (een jaar voorwaardelijk) veroordeeld voor het bezit van een flinke collectie kinderporno. De verdachte S.S. verzamelde in acht jaar tijd meer dan tienduizend afbeeldingen. Rechercheurs stopten na 2700 foto's met het bekijken van de collectie. 'De vaststelling dat de beelden steeds afschuwelijker werden, maakt deze zaak zo ernstig', aldus de officier van justitie. 'Veel walgelijker kan het niet'. De verdachte, die steeds volhield dat hij de beelden bekeek om de verveling te verdrijven, werd sinds 2011 meerdere malen opgepakt voor dezelfde feiten.
Een man (45, uit Apeldoorn) kreeg van de rechtbank Gelderland een veel lagere straf: 26 weken waarvan 25 voorwaardelijk. De verdachte kreeg ook 240 uur werkstraf. Hij bezat tussen 2014 en 2016 een relatief kleine verzameling kinderporno. Volgens de rechter is het positief dat de man direct in therapie ging en zijn computers vrijwillig laat controleren.
En een man (68, uit Berkel-Enschot) kreeg voor het bezit van 22 duizend kinderpornografische plaatjes 90 uur werkstraf opgelegd. Deze verdachte werd eind 2014 al opgepakt.

———————————————————-

Twee jongens (17, uit Waalwijk en Poppel) die verdachten zijn in de 'Tilburgse sexting-zaak' moeten een excuusbrief schrijven aan hun slachtoffer. Ze moeten ook ieder driehonderd euro boete betalen. De zaak zorgde, begin 2016, voor veel commotie, toen bleek dat de scholieren tientallen (bijna)naaktfoto's van minderjarige meisjes verstuurden op sociale media, vooral Instagram. Meerdere slachtoffers deden aangifte, slechts één meisje voegde zich als benadeelde in het proces. Aan dat meisje moeten de jongens nu hun excuusbrief schrijven en de schadevergoeding betalen. Een derde verdachte (16, uit Tilburg) moet nog voorkomen. Hij weigerde de taakstraf die het OM hem aanbood.

———————————————————-

Een man (39, uit Purmerend) moet 250 euro boete betalen omdat hij in tweets de politie uitschold voor nazi's en nazi-moordenaars. Hij richtte zich vooral op een hem bekende wijkagent in Purmer-Noord, die hij 'hoofd SS'er' noemde. De chef van het wijkteam deed vervolgens aangifte wegens smaad maar voor de officier was belediging 'juridisch meer voor hand liggend'. Aanleiding voor de tweets was het feit dat de verdachte in 2015 uit zijn huurwoning was gezet. Volgens de verdachte had de politie daarbij zijn buurman moeten oppakken.

———————————————————-

Ondanks dat tegen haar 49 aangiftes waren gedaan, is een vrouw (44, uit Eindhoven) vrijgesproken van internetoplichting. Het OM kreeg de zaak niet rond. De aangiftes betroffen fraude via Marktplaats: slachtoffers kochten iPhones, iPads etcetera maar kregen die nooit. De verdachte werd opgespoord en opgepakt, op haar laptop stonden veel beschuldigende e-mails maar veel verder kwam de politie niet. Het OM zelf vindt nu dat er te weinig bewijs is en vroeg om vrijspraak.



Bron: Cops in Cyberspace

Verschijningsvorm cybercrime	138ab *lid 1*	138ab *lid 2*	138ab *lid 3*	138b	139c *lid 1*	139d	139e	161 *sexies*	161 *septies*	350a *lid 1*	350a *lid 2*	350a *lid 3*	350b *lid1*	350b *lid2*
● Malware														
Malware maken en/of verspreiden	X					X		X	X	X	X	X	X	X
Malware (Trojaanse paarden) gebruiken	X	X			X			X	X	X	X	X	X	
● Computerinbraak														
Computerinbraak (hacking)	X		X								X			
Computerinbraak vervolg-handelingen		X	X		X	X	X	X	X	X	X	X		
Portscan						X								
Spoofing/cache poisoning	X	X		X	X	X	X	X		X	X			
Sniffing					X	X	X			X				
Draadloze netwerken hacken/ misbruiken	X	X	X	X	X		X	X		X	X			
Password guessing	X			X		X								
● Website aanvallen														
Veroorzaken open relay									X				X	
Wederrechtelijk open relay gebruiken	X							X		X				
Defacing/vernielen website	X							X	X	X			X	
Defacing/doorleiden internet-verkeer	X							X	X	X				
Cross-site scripting	X	X			X	X	X	X		X			X	
SQL-injecties	X	X						X		X				
● Botnets														
Botnet bouwen en beheren	X	X	X		X					X		X		
● Denial of Service														
DDoS-aanval				X				X		X			X	
● Social Engineering														
Phishing		X			X		X							
Vishing/Smishing		X			X									
● E-mail gerelateerd														
Wederrechtelijk open mail relay gebruiken	X							X	X	X				
Spamming (met DoS tot gevolg)				X				X	X				X	

Bron: Overheid.nl

Wetsartikel

Art. 138ab, lid 1 Sr Hacken: opzettelijk en wederrechtelijk binnendringen van een geautomatiseerd werk

Art. 138ab, lid 2 Sr Hacken: overnemen, aftappen of opnemen van gegevens uit een geautomatiseerd werk na binnendringen daarvan

Art. 138ab, lid 3 Sr Hacken door tussenkomst van een openbaar telecommunicatienetwerk

Art. 138b Sr Het belemmeren van toegang tot of gebruik van een geautomatiseerd werk

Art. 139c Sr Het aftappen of opnemen van gegevens (afluisteren)

Art. 139d, lid 1 Sr Plaatsen van opname-, aftap- of afluisterapparatuur; voorbereidingshandelingen

Art. 139d, lid 2 Sr Het ter beschikking stellen of voorhanden hebben van technische hulpmiddelen of toegangscodes bedoeld om het binnendringen van een geautomatiseerd werk, belemmeren van toegang of aftappen te plegen

Art. 139d, lid 3 Sr Zoals in art. 139d, lid 2 Sr, maar met oogmerk gericht op art. 138ab, lid 2 en 3 Sr

Art. 139e Sr Het bezit en verspreiden van gegevens of een voorwerp waarop gegevens staan die door wederrechtelijk aftappen of opnemen zijn verkregen

Art. 161sexies Sr Opzettelijk vernielen etc. van een geautomatiseerd werk of werk voor telecommunicatie; voorbereidingshandelingen

Art. 161septies Sr Vernieling etc. van een geautomatiseerd werk of werk voor telecommunicatie door schuld

Art. 231b Sr Identiteitsfraude

Art. 232 Sr Opzettelijk valselijk opmaken, vervalsen, gebruiken, etc. van betaalpas, waardekaart e.d.

Art. 240b Sr Kinderpornografie

Art. 248e Sr Grooming

Art. 273, lid 2 Sr Bekendmaking bedrijfsgeheimen; heling computergegevens ondernemingen

Art. 273d Sr Schending telecommunicatiegeheim

Art. 317, lid 2 Sr Afpersing door de bedreiging dat gegevens opgeslagen door een geautomatiseerd werk onbruikbaar, ontoegankelijk of gewist worden

Art. 326c Sr Het misbruiken van een publieke telecommunicatiedienst met het oogmerk daarvoor niet volledig te betalen

Art. 350a, lid 1 Sr Opzettelijke vernieling van gegevens die door middel van een geautomatiseerd werk of door telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen

Art. 350a, lid 2 Sr Het feit gepleegd in lid 1 met tussenkomst van een openbaar telecommunicatienetwerk

Art. 350a, lid 3 Sr Opzettelijk gegevens ter beschikking stellen of verspreiden die zijn bestemd om schade aan te richten in een geautomatiseerd werk

Art. 350b, lid 1 Sr Vernieling door schuld van gegevens die door middel van een geautomatiseerd werk of door telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen

Art. 350b, lid 2 Sr Door schuld gegevens ter beschikking stellen of verspreiden die zijn bestemd om schade aan te richten in een geautomatiseerd werk

Video

Tek Tok Late Night:

1. Privacy
2. Internetvrijheid
3. Digitale veiligheid
4. High Tech Crime
5. Data in onderwijs
6. Cybersurveillance
7. Techtrends in onderwijs
8. Veilig internetten
9. MKB cyber secure
10. Cyberellende bij Tek Tok
11. Standaarden en keurmerken
12. Operation Hijg Tech Crime
13. Kraak van de Maand

You Tube:

Doe jij het veilig online
Malware
WiFi ontvangst verbeteren
Internetfraude via de telefoon
Documentaire: Veiligheid en privacy
Herken een nep-hotspot
Gebruik wachtzinnen
Drive-by-downloads voorkomen
Hoe herken je een phishing mail
Beveiligd internetbankieren
Privacy—ik heb toch niets te verbergen
Webinar Computercriminaliteit
Mousejack
Gegijzeld door Ransomware. Wat nu?
Telefonische phishing

Help wanted:

Grooming
Sexting
Webcammisbruik
Bedreigd/gechanteerd
Kinderporno
Nepprofiel

Handig

Phishing- / valse e-mails melden:

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

ING Bank: valse-email@ing.nl

Rabobank: valse-email@rabobank.nl

SNS Bank: valse-email@sns.nl

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

Tips voor veilig handelen op Marktplaats

Internetoplichting: controleer vooraf de (bank)gegevens van de verkoper via

www.mijnpolitie.nl/miocheck

Komt de verkoper voor op de website Opgelet op internet ?

Malware ID website met info omtrent verwijderen van infecties

PCrisk verwijderingsrichtlijnen voor spyware en virussen

Cookie Verwijderen kennisdatabase voor het verwijderen van adware, hijackers, ransomware, toolbars en pop-ups

Computer woordenboek

Secure Computing Naslag

Veel meer handige tips vindt u op de Secure Computing website.