Secure Computing Magazine

INDEX

Blijf ook tijdens Uw vakantie op de hoogte van het laatste cybernieuws. Bezoek de Secure Computing Magazine website en Facebookpagina

www.securecomputing.jouwweb.nl

www.facebook.com/SecureComputingMag

Rubrieken:

INDEX

Hoe word je cyber crimineel?

Cyber Crime as a Service. Ofwel Cyber Crimineel worden zonder technische kennis. Tegenwoordig mogelijk door het groeiende aanbod op het darkweb van malware-pakketten. Deze trends zorgen voor een steeds verder toenemende dreiging voor Nederlandse bedrijven.

Cyber criminaliteit kende lange tijd twee belemmeringen. In de eerste plaats het te gelde maken of liquideren van de gestolen middelen, daarnaast het ontbreken van de technische kennis. Dit maakte het voor (potentiële) cyber criminelen complex om op grote schaal acties uit te voeren.

Goedkoop en anoniem
Maar de opkomst van de bitcoin heeft geleid tot een anoniem verkeer van middelen. En het darkweb verzorgt de oplossing voor het gebrek aan technische kennis. Ransomware aanvallen, exploit kits, bitcoin stealers, sets vers gestolen credit cards of identiteitsbewijzen; allemaal te koop voor een kleine vergoeding. Anoniem via bitcoin of een andere cryptocurrency afgerekend. Surelock noemt dit 'Cyber Crime as a Service'.

Risico op digitale aanval breidt zich uit
Al met is er een tweedeling in de wereld van de cyber criminaliteit ontstaan. Een bende mèt technische kennis stelt middelen beschikbaar aan andere criminelen. Gevolg is dat het uitvoeren van een digitale aanval voor een steeds grotere kring van personen mogelijk wordt.

Aanbod gijzelingssoftware met reviews
Surelock heeft onderzoek uitgevoerd op meer dan 50 darkweb marketplaces. Anonieme markten waar vraag en aanbod naar o.a. wapens, drugs & hack-services samenkomen. De grootste en bekendste 'marktplaatsen' zijn AlphaBay, Silkroad & Wall Street. Hier worden voor bedragen tussen $9,99 en $9.999,- pakketten met gijzelingssoftware aangeboden. De marktplaatsen hebben zelfs een review functie waar de cyber criminelen onderling hun ervaringen delen.

Promotie-video's
De producten worden met clickbait strategieën (misleidende, sensationele titels) aan het publiek aangeboden. Zelfs worden promo-video's (http://bit.ly/2qitG1l) ingezet om het product aan de man te brengen. De advertentie waarin Philedelphia Ransomware wordt aangeboden beschikt over een Clikbait titel, de lage prijs en de enorme flexibiliteit van het pakket maken het een populair product op AlphaBay. Het product is dan ook meer dan 25.000 keer verkocht sinds begin september 2016 beschikbaar kwam.

Groeiend maatschappelijk probleem vraagt om aandacht media.
Gezien de steeds verdergaande kennis en vaardigheden van de cyber criminelen is het niet verbazingwekkend dat media het als hun plicht zien aandacht te besteden aan dit groeiende maatschappelijke probleem.

INDEX

Youtube onderneemt stappen tegen extremisme

Youtube gaat stappen ondernemen tegen extremistische boodschappen op zijn platform. Dat schrijft de videowebsite in een stuk dat verscheen in de Amerikaanse 'Financial Times'. Het gaat om vier concrete stappen die de verspreiding van haatboodschappen en wervingspropaganda moeten tegengaan.

Vier stappen
De website werkt blijkbaar al enige tijd samen met verschillende regeringen en politie-organisaties. Samen trachten ze deze boodschappen te identificeren en te verwijderen. Kent Walker, senior vice-president bij Google en degene die het stuk schreef, geeft evenwel toe dat er nog meer kan en moet worden gedaan.

De eerste stap is om machine learning in te zetten om haatboodschappen efficiënter op te sporen. Ten tweede breidt het zijn 'Trusted Flaggers uit': experts die speciale privileges krijgen op het platform om filmpjes te verwijderen die de gebruiksvoorwaarden schenden. Momenteel zijn er in deze groep al 63 NGO's actief voor het volbrengen van deze taak; er komen er nu nog eens 50 bij.

Net wel, net niet
De derde stap is een verstrenging van wat aanvaardbaar is. Video's die de gebruiksvoorwaarden van Youtube niet echt schenden, maar flirten met het onaanvaardbare, zullen sneller bestraft worden. Ze worden niet meteen verwijderd, maar komen achter een waarschuwing te staan, en de auteur van het filmpje kan niet langer advertentiegeld ontvangen.
Ten slotte zal Youtube zijn slimme advertentiealgoritmes inzetten om mogelijk rekruten voor IS om te leiden van de extremistische filmpjes naar andere video's die dienen voor ontradicalisering. Op die manier wordt een mogelijk doelwit van IS weggehaald bij wervingspropaganda en krijgt die persoon het tegenbeeld te zien.

Propaganda
Het kalifaat van IS staat zwaar onder druk. Het geeft elke dag meer terrein prijs aan een alliantie van naties die de terroristische organisatie probeert uit te roeien. Dat houdt de propagandamachine evenwel niet tegen. Met de regelmaat van de klok verschijnen nog steeds extremistische boodschappen op verschillende media als Twitter en Youtube. Met het nieuwe stappenplan van die laatste zal IS de almaar groter worden druk ook online gaan voelen. Zonder digitale propaganda wordt het immers zeer moeilijk om nieuwe strijders aan te werven.

Bron: YouTube

INDEX

Hackers kunnen data stelen via LED-lampjes op router

Malware kan de LED-lampjes van een router of switch misbruiken om gegevens vanuit je netwerk naar kwaadwilligen door te spelen.
Onderzoekers aan de Israëlische Ben Gurion-universiteit ontwikkelden software die data subtiel kan omzetten in lichtsignalen. Ze doopten hun creatie xLED. Een hack via de lampjes van netwerkapparatuur is omslachtig maar dat hoeft geen bezwaar te zijn voor criminelen. Wie zijn toevlucht zoekt tot gespecialiseerde malware zoals deze, heeft als doel gevoelige netwerkinfrastructuur aan te vallen. Denk daarbij aan bedrijven of overheden met geheime informatie.

Netwerken die dergelijke informatie bezitten, zijn vaak voorzien van een 'airgap'. Ze zijn met andere woorden afgesloten van het publieke internet zodat een aanval van buitenaf nauwelijks mogelijk is. Normaliter maakt monitoringsoftware het bovendien onmogelijk om zomaar gegevens via een usb-stick te stelen. De LED-methode in combinatie met een camera laat hackers toe om gegevens uit een beveiligde omgeving te halen zonder dat iemand door heeft dat er iets mis is. De klassieke firewall is immers waardeloos, net als de logboeken.

Om van het LED-hack gebruik te maken, moet een aanvaller er wel in slagen routers of switches te besmetten met xLED. Vervolgens zet de software gegevens die door de router passeren om in LED-flitsen die ééntjes en nulletjes weergeven.
Het is niet de eerste keer dat de Israëliërs met de hulp van lampjes data doorseinen. Eerder ontwikkelden ze al een gelijkaardig stuk malware waarmee ze gegevens van een harde schijf konden halen, opnieuw met de hulp van het statuslampje.

INDEX

Het hoe, wat en waarom van ’s werelds krachtigste computers

High-performance computing en de bijhorende supercomputers zijn meer dan dure stukjes speelgoed voor theoretische natuurkundigen. HPC is niet meer weg te denken uit de maatschappij, al weten weinig mensen wat er precies achter de term schuilt en nog minder hoe breed het toepassingsgebied wel is. We onderzoeken in dit dossier hoe HPC in onze contreien gebruikt wordt. Daartoe gaan we op bezoek bij één van de krachtigste supercomputers in de Benelux: de BrENIAC van het Vlaamse Supercomputer Centrum in Leuven. We bekijken wat er praktisch komt kijken bij de ontwikkeling, het onderhoud en het gebruik van de indrukwekkende Tier-2-machine en onderzoeken hoe minder bekende, maar daarom niet minder belangrijke Tier-2-computers hun steentje bijdragen. HPC is een onmisbaar onderdeel geworden in het dagelijkse leven, al besef je dat misschien nog niet.

De bouw van een supercomputer

BrENIAC is de krachtigste supercomputer van België en één van de krachtigste systemen van de Benelux. In het ICTS-datacenter van de KU Leuven ontdekken we wat zo’n systeem precies allemaal om het lijf heeft.

“Vergelijk een supercomputer niet met Superman.” Ingrid Barcena, Tier 1-projectlead bij het Vlaamse Supercomputercentrum, wil meteen duidelijk maken wat een supercomputer wél is, maar ook wat zo’n ding niet is. “Een supercomputer is één van de vele tools in de wereld van de high-performance computing (HPC),” klinkt het. Voor HPC heeft ze meteen een definitie klaar: “High-performance computing is het gebruik van parallel rekenwerk om geavanceerde toepassingen op een snelle en betrouwbare manier te draaien.”

Veel hardware

Parallel is hier het sleutelwoord. Een supercomputer als BrENIAC is niet opgebouwd uit unieke en mysterieuze krachtige hardware die fabrikanten reserveren voor de bouw van dergelijke systemen, maar uit heel veel herkenbare componenten. Zowat alle huidige supercomputers zijn gebaseerd op dezelfde x86-architectuur die je in je laptop terugvindt. Zo heeft je laptop waarschijnlijk één dual-coreprocessor van Intel aan boord en is hij in elkaar gevezen door een OEM zoals Dell of HP.

BrENIAC heeft geen Core-CPU’s maar Xeon-processors aan boord. Concreet gaat het om Intel Xeon E5 2680v4-processors met een kloksnelheid van 2,4 GHz. Het systeem heeft 580 rekennodes die telkens twee Xeons bevatten, goed voor 16.240 rekenkernen. Naast de CPU’s bevat iedere Node nog 64 GB aan RAM. BrENIAC is na een aanbesteding gebouwd door NEC. De Xeon-chip is uitermate geschikt voor gebruik in HPC-systemen dankzij de bredere bandbreedte en de enorme hoeveelheid cache: 35 MB L3. De 14 core-processor is door Intel gebakken met de 14 nm-Broadwell-architectuur en heeft de klassieke Intel-paradepaardjes aan boord. Multithreading tekent present, net als een turbo die de kloksnelheid van 2,4 GHz naar 3,3 GHz kan stuwen.

Weg met turbo

Dat klinkt impressionant maar Herman Moons, hoofd van de Dienst Centrale ICTS-infrastructuur aan de KU Leuven waar BrENIAC staat, is niet onder de indruk. “Zowel de turbo als multithreading zijn gedeactiveerd in de BrENIAC,” vertelt hij. “Als onderzoekers hun algoritmes goed hebben geoptimaliseerd voor de supercomputer, biedt hyperthreading geen meerwaarde. De turboboost maakt de snelheid waarmee een cluster opdrachten uitvoert dan weer variabel, wat evenmin wenselijk is.

De hardware levert BrENIAC meer dan 600 teraflops aan rekenkracht op. Daarmee veroverde de computer eind 2016 plaats 196 in de top 500 van ’s werelds krachtigste supercomputers. BrENIAC is de krachtigste computer van België maar niet van de Benelux. In Nederland heeft de Cartesius-supercomputer sinds een upgrade naar Broadwell-processors in 2016 een rekencapaciteit van 1,8 petaflops.

Leger

Een supercomputer haalt zijn kracht uit het samenwerken van alle verschillende kernen. Barcena vergelijkt BrENIAC daarom liever met een leger soldaten dan één onwaarschijnlijke krachtpatser als Clark Kents alter ego. Om zoveel mogelijk uit de beschikbare kracht van een HPC-systeem te halen, moeten onderzoekers leren om code en simulaties uit te werken die dat ganse leger zo efficiënt mogelijk aanspreken. Iedere soldaat moet te allen tijde aan het werk zijn. De kernen moeten natuurlijk ook vlot samen kunnen werken. Een supercomputer is meer dan een vrachtwagenlading Xeon-processors recht uit het Intel-magazijn.

Infiniband

“De interconnects zijn extreem belangrijk,” weet Barcena. “Alle rekennodes zijn met elkaar verbonden via een razendsnelle Infiniband-interconnect.” Die doet nog het meest denken aan een soort ethernetverbinding op steroïden. Infiniband is dezer dagen de populairste technologie om de nodes van supercomputers met elkaar te verbinden. De interconnect zorgt voor een enorme bandbreedte (6,5 gigabyte per seconde bij BrENIAC) gecombineerd met een erg lage latency. Je zal Infiniband terugvinden in BrENIAC, Cartesius maar ook vele andere krachtige(re) supercomputers wereldwijd.

In de praktijk neemt een supercomputer daarom de vorm aan van een rij serverkasten. Vooraan zitten de computernodes met daarin de twee Xeon-processors. Een handvol nodes is telkens verbonden met een Infiniband-switch. Die switches zijn op hun beurt verbonden met andere switches tot het hele systeem op een slimme en vooral snelle manier gelinkt is. Barcena: “Het op een snelle manier verbinden van alle rekennodes is de grootste uitdaging bij de bouw van een moderne supercomputer.”

Het resultaat is een lange kast die tot de nok gevuld is met rekenkracht en dag in dag uit op volle toeren draait. Moons: “Het systeem is ontwikkeld om vrijwel non-stop aan hoge capaciteit rekenwerk uit te voeren.” Jan Ooghe, verantwoordelijke van de faciliteiten voor onderzoek aan de KU Leuven verduidelijkt wat dat wil zeggen. “100 procent belasting van het systeem is niet ideaal. Idealiter draait een supercomputer non-stop aan 60 procent tot 70 procent van zijn capaciteit.”

INDEX

EU akkoord met sancties tegen hackers

De Europese Unie kan nu sancties opleggen aan iedereen die computernetwerken in EU-landen heeft aangevallen. Het is de nieuwste poging om hackers af te schrikken, na eerdere aanvallen in Groot-Brittannië en Frankrijk.

De Europese ministers van Buitenlandse Zaken gingen maandag akkoord met een pakket maatregelen zoals reisverboden en het bevriezen van banktegoeden. Voor het eerst kan ook de zogenoemde blanket ban worden ingezet. Dit is een algehele ban op het doen van zaken met een persoon, een bedrijf of een overheid.

Gezamenlijkheid
“Een gezamenlijke reactie op de kwaadaardige cyberactiviteiten is gewenst gezien de strekking, de grootte, de duur, intensiteit, complexiteit en de impact hiervan”, aldus de ministers in een gezamenlijke verklaring.

Na de beschuldigingen van Russische betrokkenheid bij de verkiezingen in de Verenigde Staten en Frankrijk, zijn er zorgen over het eerlijke verloop van de aankomende Duitse verkiezingen in september. Amerikaanse veiligheidsdiensten hebben geconcludeerd dat Rusland e-mails van de Democratische Partij heeft gehacked en gelekt, in een poging de uitkomst in het voordeel van Donald Trump te sturen. Rusland ontkent dit.

De Fransen lieten eerder het plan vallen om in het buitenland wonende stemgerechtigden digitaal te laten stemmen door het risico op cyberaanvallen. De Britse veiligheidsdiensten hebben politieke partijen opgedragen zichzelf beschermen tegen cyberaanvallen.

Bron: Europese Unie

INDEX

Delftse wetenschappers werken aan niet af te luisteren internet

Wetenschappers zijn wereldwijd aan het werk om een niet af te luisteren internet te bouwen gebaseerd op verstrengeling – de onzichtbare quantum-fysische band tussen deeltjes.
Een grote uitdaging is dat deze verstrengeling bij elk nieuw knooppunt zwakker wordt. Wetenschappers uit Delft en Oxford zijn er nu in geslaagd om een sterke verstrengelingsverbinding te distilleren uit meerdere zwakkere verbindingen. Deze doorbraak maakt het op korte termijn mogelijk om voor het eerst rudimentaire quantumnetwerken te bouwen, en levert meteen een essentieel element voor een toekomstig quantuminternet. De wetenschappers publiceren dit werk vandaag in het tijdschrift Science.

Spookachtig internet
Veilige communicatie is een van de grootste uitdagingen in dit digitale tijdperk. Over de hele wereld werken wetenschappers aan nieuwe methoden om écht veilige netwerken te realiseren: gebaseerd op de wetten van de quantummechanica. In zulke netwerken is het fundamenteel onmogelijk om ongemerkt afgeluisterd te worden, maar het maken van sterke verbindingen in deze netwerken, gebaseerd op het krachtige maar kwetsbare principe van quantum verstrengeling, is een grote uitdaging.

De onderzoeksgroep van Ronald Hanson bij QuTech is beroemd door het realiseren van verbindingen gebaseerd op quantumverstrengeling. Met behulp van lichtdeeltjes zijn de wetenschappers in staat om de quantuminformatie te verbinden over grotere afstanden: tot ruim een kilometer. Met een belangrijke test lieten de wetenschappers eerder de kracht van zo'n verbinding zien: verstrengeling is onzichtbaar voor een tussenpersoon: de informatie kan niet worden afgeluisterd.

Gedeelde informatie
"Verstrengelde elektronen gedragen zich als het ware als één, ongeacht de afstand. Op welke manier je ook naar de elektronen kijkt, ze hebben altijd gedeelde informatie", vertelt professor Ronald Hanson. Een meting op het ene deeltje, beïnvloedt direct een meting op het andere deeltje, zelfs wanneer ze lichtjaren van elkaar gescheiden worden.
Wetenschappers zijn nu bezig om verstrengeling in te zetten voor radicaal nieuwe technologie. "De informatie bevindt zich als het ware op beide plekken tegelijkertijd en gevoelige informatie hoeft daardoor geen weg af te leggen", licht Hanson toe. "We voorzien in de toekomst veilige netwerkverbindingen gebaseerd op verstrengeling: een quantuminternet."
"Waar we eerst verstrengde informatie realiseerden tussen twee elektronen in twee diamanten, gebruiken we nu ook één van de aanwezige kernspins in iedere diamant om de verstrengelde informatie tijdelijk op te slaan." Terwijl de informatie veilig is opgeslagen, verstrengelen de wetenschappers de elektronen opnieuw. Hanson: "Nu zijn er twee verbindingen. Door deze op een slimme manier met elkaar te combineren, kunnen we uit die zwakkere verbindingen één sterkere verstrengelde verbinding halen, een beetje zoals whisky wordt gedistilleerd uit lager-alcoholische basisingrediënten." Deze distillatie van verstrengeling kan in principe steeds vaker herhaald worden totdat de verbinding de gewenste kracht heeft.

Verreikende mogelijkheden
Deze methode opent belangrijke deuren voor het quantum internet. Promovendus Norbert Kalb: "Om zo'n netwerk te realiseren hebben we alles nodig dat het huidige internet ook gebruikt: een geheugen, een processor en verbindingen. Nu laten we zien dat we de kernspins als geheugen kunnen gebruiken, zonder dat deze verstoord worden door nieuwe verbindingen tussen de elektronen, de processor."
Hanson: "Op deze manier kunnen we verder gaan dan twee verbindingen en het eerste echte quantumnetwerk gaan opzetten. We gaan dan ook qua wetenschap echt onbekend gebied in." Deze distillatie van verstrengeling is essentieel voor de toekomst van het quantuminternet: waarin vele quantumverbindingen bestaan, die ook nog eens van hoge kwaliteit moeten zijn. Volgens Hanson is die toekomst niet ver weg: "binnen vijf jaar willen we vier grote steden in Nederland verbinden in een rudimentair quantumnetwerk."

INDEX

1Password wachtwoord-app komt met speciale reismodus

Wachtwoorden-app 1Password heeft een nieuwe functie waarmee gebruikers op reis ontraceerbaar een deel van hun wachtwoorden van hun apparaat kunnen verwijderen.

De functie is vooral bedoeld voor de steeds strengere grenscontroles waarbij reizigers toegang tot hun telefoon moeten verlenen, schrijft 1Password-ontwikkelaar AgileBits.

Gebruikers moeten op de site van 1Password voorafgaand aan een reis een aparte verzameling wachtwoorden, logins, notities en codes maken die zij ook onderweg willen gebruiken. Die verzameling kan dan worden aangeduid als 'Safe for Travel'.

Ontraceerbaar
Op diezelfde site kan vlak voor de reis dan de reismodus aangezet worden. Dan worden alle wachtwoordkluizen die niet als 'Safe for Travel' staan aangeduid van alle gekoppelde apparaten verwijderd. Eenmaal ingeschakeld is niet te detecteren dat de reismodus is ingeschakeld. Volgens de ontwikkelaar blijft er geen enkel spoort van de verwijderde informatie achter.

Als de gebruiker op zijn bestemming is aangekomen, kan via de site de reismodus weer worden uitgeschakeld. Wanneer de 1Password-apps dan worden geopend, worden alle verwijderde wachtwoorden automatisch weer gedownload.

De functie werkt voor alle betalende gebruikers van 1Password. De dienst is er voor Windows, Mac, iOS en Android.

INDEX

Jongeren meest onvoorzichtig op onbeveiligd wifi-netwerk

Jongeren maken het meest gebruik van openbare, onbeveiligde wifi-netwerken en houden het minste rekening met mogelijke risico's als privacyschending.

De helft van de internetgebruikers geeft aan wel eens gebruik te maken van een openbaar, niet beveiligd wifi-netwerk. Maar jongeren doen dat een stuk vaker dan ouderen. Zeven op de tien internettende 18- tot 25-jarigen maken gebruik van zulke netwerken tegen één op de tien internettende 75-plussers. Dat meldt het CBS op basis van nieuwe cijfers.

Meekijkers
Gebruikers van openbare wifi-netwerken die niet zijn beveiligd met een gebruikersnaam en wachtwoord, riskeren dat hun gegevens worden bekeken door anderen.
Van de mensen die wel eens verbinding maken met onbeveiligde, openbare wifi-netwerken, zegt 34 procent het gebruik te beperken vanwege zorgen om de veiligheid. Dat doen ze door ofwel af te zien van wifi-gebruik ofwel door in te loggen op een beveiligd netwerk, als dat mogelijk is. Een kwart van de jongeren en iets meer dan de helft van de 65-plussers beperkt het gebruik vanwege veiligheidszorgen.

Vier op de tien gebruikers van zulke onbeveiligde wifi-netwerken zeggen altijd bewust bepaalde activiteiten op het web wel of niet uit te voeren als zij op zo'n netwerk zitten. Bijna twee op de tien gebruikers gaat hier meestal bewust mee om. Oudere en hoogopgeleide gebruikers gaan vaker dan gemiddeld bewust om met internet op onbeveiligde netwerken.

De meest genoemde reden – ruim de helft - om niet actief zijn op niet-beveiligde wifi-netwerken, is dat ze daar geen behoefte aan hebben. 43 procent geeft aan dat twijfels over de veiligheid een rol spelen.

INDEX

Tweede Kamer: 'Doe iets aan onveilige internet of things-apparaten'

De Tweede Kamer heeft met een overgrote meerderheid een motie aangenomen waarin de regering wordt opgeroepen iets te doen aan onveilige internet of things-apparaten.
De motie werd dinsdag met een een meerderheid van 148 stemmen aangenomen. Alleen de tweemans-fractie van FvD stemde tegen.

SP-Kamerlid Maarten Hijink en D66-Kamerlid Kees Verhoeven dienden de motie vorige week in, tijdens een debat over ransomware WannaCry. De snelle verspreiding van de ransomware zette het belang van een sterke digitale beveiliging weer hoger op de politieke agenda.

Gehackte koelkast
Hijink en Verhoeven roepen het kabinet in de motie op om te onderzoeken welke minimale veiligheidseisen aan internet of things-apparten kunnen worden ge-steld, hoe die eisen kunnen worden afgedwongen en welke overige maatregelen nodig zijn om consumenten te beschermen tegen slecht beveiligde apparatuur. "Niemand zit te wachten op een massale cyberaanval via gehackte waterkokers of koelkasten", aldus de motie. Verhoeven van D66 pleitte eind 2016 al voor officiële veiligheidsstandaarden voor internet of things-apparaten.

Standaardwachtwoord
Veel apparaten hebben tegenwoordig een internetver-binding, maar zijn niet goed beveiligd of gebruiken rechtstreeks uit de verpakking bijvoorbeeld een stan-daardwachtwoord. Daarmee vormen zulke apparaten een zwakke schakel in de internetbeveiliging van con-sumenten, waar hackers misbruik van kunnen maken. Hoewel de Europese Commissie onderzoek doet naar een eventuele standaard voor dergelijke apparten, is daar vooralsnog niets uitgekomen. Verhoeven stelde vorig jaar voor om als Nederland alvast stappen te nemen, Hijink gaat daarin mee.

INDEX

Slimmer op vakantie met je smartphone en tablet

Met de drie apps die in dit artikel worden besproken kan je vakantie nog leuker worden. Lekker gratis lezen, overal je favoriete films en series bekijken en zonder internetkosten altijd je weg vinden.

Gratis lezen in je vakantie

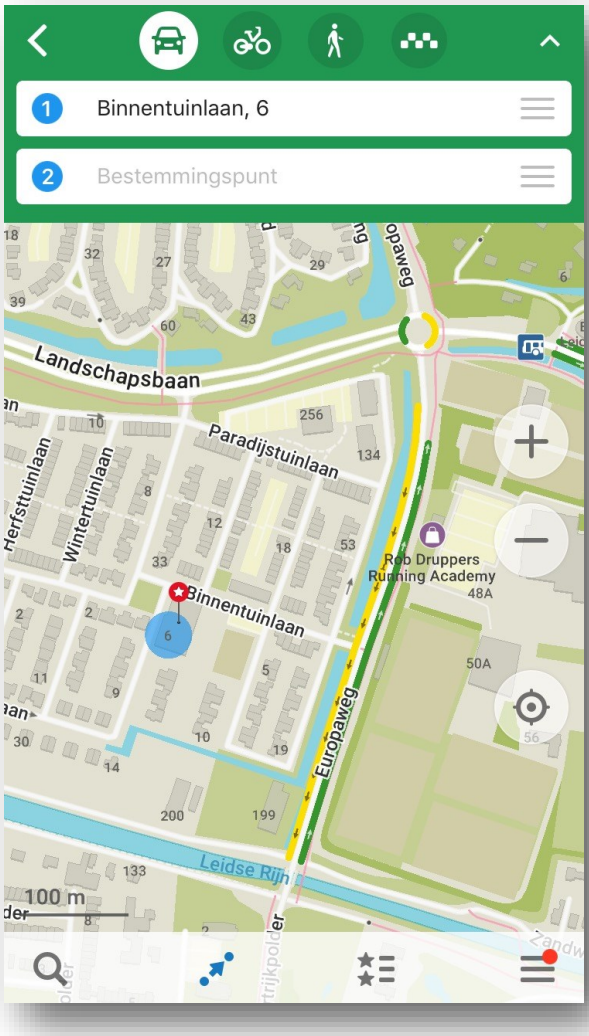
Met de Vakantiebieb-app kan iedereen meer dan 60 gratis e-books lezen in de vakantie. Geen gesleep meer met boeken op je vakantie. Vanaf 1 juni zijn er al 35 leuke kinderboeken en in juli en augustus komen er ook recente boeken voor volwassenen beschikbaar. Je moet de boeken wel voor 31 augustus uitlezen want daarna verdwijnen ze uit de app. Zie ook https://vakantiebieb.nl/ of ga direct naar de appstore voor jouw besturingssysteem en download de app. NB Had je de app al? Zorg er dan voor dat je hem update om toegang te krijgen tot die nieuwste boeken.

Films en series kijken op vakantie

Met de Netflix-app (ook voor Android) kun je nu heel gemakkelijk films en series vooraf downloaden op je smartphone en tablet om ze later zonder internetverbinding overal te bekijken. Handig voor in het vliegtuig en overal waar je internetverbinding langzaam of duur is. En als je nog gebruik kunt maken van hun gratis proefmaand kan het zelfs helemaal gratis. Download de programma's niet te lang voor je vakantie want na 1 maand wordt de ruimte op je toestel automatisch weer vrijgemaakt. Handig is dat NetFlix bij de Android-versie nu ook toestaat om de films en series op te slaan op een SD-kaartje. Om naar het Nederlandse aanbod te kijken kan een VPN-verbinding in het buitenland nodig zijn of je zet eenvoudig de internetverbinding uit. Een gratis VPN app voor iOS die erg gemakkelijk werkt en prima presteert is Turbo VPN.

Altijd je weg vinden

Voor het fietsen en wandelen en om offline uitgebreid te zoeken, adviseren we je om ook eens te kijken naar de gratis app maps.me (ook voor Android). Na het downloaden van de gedetailleerde en actuele kaarten zul je, waar je ook heen gaat op vakantie, niet meer verdwalen. Via de zoekfunctie linksonder vind je alles gemakkelijk zonder dat je een internetverbinding nodig hebt.



INDEX

Zo kun je op een veilige manier je Android-telefoon uitlenen

Veel mensen vinden het niet prettig om hun telefoon aan anderen uit te lenen. Gelukkig kun je ervoor zorgen dat al je persoonlijke informatie voor andere gebruikers onzichtbaar is. Zo kun je veilig je Android-telefoon uitlenen aan anderen.

Soms wil iemand even snel je telefoon lenen als de batterij van zijn of haar eigen apparaat leeg is. Maar misschien geef je je telefoon liever niet zomaar uit handen omdat die persoon dan kan zien welke apps er allemaal open staan, je e-mails kan lezen en op je social media-accounts kan rondsnuffelen. Op je Android -telefoon kun je ervoor zorgen dat vrienden, kennissen en vreemden aan wie je je telefoon uitleent niet bij je persoonlijke gegevens kunnen.

Permanent account

Als een bepaald iemand regelmatig van jouw telefoon gebruik wil maken, zoals bijvoorbeeld een gezinslid of je beste vriend(in), dan kun je voor hem of haar op je telefoon een gebruikersaccount aanmaken. Op die manier heeft deze persoon altijd toegang tot zijn of haar favoriete apps, e-mails, instellingen en andere persoonlijke informatie.

Open de Instellingen app, ga naar Apparaat > Gebruikers en kies Gebruiker toevoegen. Staat deze optie er niet? Druk dan op Gebruiker of profiel toevoegen en vervolgens op Gebruiker. Bevestig je keuze door op OK te drukken.

Als de nieuwe gebruiker naast je staat, kun je hem of haar meteen het account laten instellen door op Nu instellen te drukken. Je zult eerste je apparaat moeten ontgrendelen als beveiligingsmaatregel. Daarna kan de andere gebruiker het account gaan instellen.

Je kunt van gebruiker wisselen door onder de snelle instellingen op Gebruiker wijzigente drukken. Vervolgens kan de andere gebruiker op het apparaat inloggen om bij zijn of haar account te komen.

Wil je iemands account van je apparaat verwijderen? Ga dan naar Instellingen > Apparaat > Gebruikers. Druk naast de gebruikersnaam op Instellingen > Gebruiker verwijderen. De gebruiker wordt dan uit de lijst gewist.

Wil je je eigen account van het apparaat van iemand anders verwijderen? Ga naar Instellingen > Apparaat > Gebruikers en druk op Meer. Kies [Gebruikersnaam] verwijderen van dit apparaat. Je kunt deze stap niet ongedaan maken, dus zorg dat je goed oplet. Vervolgens wordt je account verwijderd en wordt het account van de beheerder actief.

Gastsessie

Wil je de mogelijkheid hebben om je apparaat aan verschillende mensen uit te lenen zonder dat ze toegang hebben tot jouw persoonlijke gegevens? Dan is het een goed idee om een gastsessie te starten. Een gast kan namelijk na gebruik snel en eenvoudig verwijderd worden.

Om een gastsessie te starten moet je naar de snelle instellingen gaan, op Gebruikerdrukken en Gast toevoegen of Gast kiezen.

Wil je een nieuwe gast aan je apparaat toevoegen of wil je de gegevens van de vorige gast verwijderen? Druk dan op Opnieuw beginnen. Wil je de gegevens van de vorige gastsessie blijven gebruiken? Druk dan op Doorgaan.

INDEX

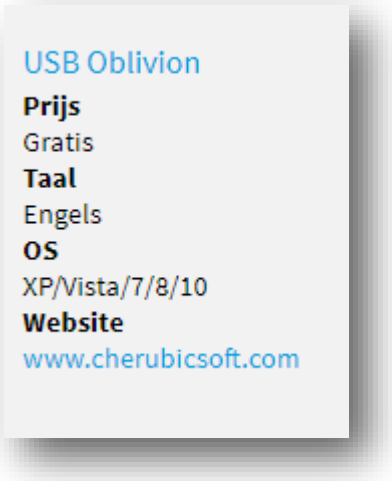
USB Oblivion - Wis al je usb-sporen

Dat je je op internet allerlei sporen achterlaat wanneer je je browser gebruikt, dat hoeven we je niet meer te vertellen. Maar wat je misschien niet wist, is dat Windows je zelfs precies kan vertellen welke usb -apparaten er allemaal aangesloten zijn geweest op je computer! Die sporen kun je laten verdwijnen, bijvoorbeeld met USB Oblivion.

Je kunt je natuurlijk afvragen waarom je de behoefte zou hebben om je usb-sporen uit te wissen. Dat kan natuurlijk allerlei redenen hebben, van op je werk verbergen dat je een privé-usb-stick hebt aangesloten (foei) tot aan simpelweg het feit dat het niemand (op een andere pc dan je eigen pc) iets aangaat wat jij op die computer hebt gedaan. Met het blote oog is het overigens lastig om dit soort informatie uit het register van Windows te halen, maar met de juiste software (zoals USBDeview) is dat een fluitje van een cent. Gelukkig is het verwijderen van die informatie dat ook.

USB Oblivion
Het enige dat je hiervoor hoeft te doen is een klein programma te downloaden, genaamd USB Oblivion. Het goede nieuws is dat je de software niet eens hoeft te installeren, je kunt het dus bij je dragen op – hoe ironisch – een usb-stick. Al is het wel belangrijk dat je de software naar de computer kopieert waarop je het wilt gebruiken. Anders wordt de usb-stick waarop het programma draait, alsnog geregistreerd zodra je deze stick uit Windows verwijdert. Dubbelklik op het 32- of 64bit-exe-bestand om te beginnen.
Usb-geschiedenis wissen
De interface die je te zien krijgt is heerlijk minimalistisch. Sterker nog, er is eigenlijk maar één knop waarop je hoeft te drukken en dat is Clean. Je kunt hier zonder enige aarzeling op klikken, want het programma werkt standaard in testmodus, zodat je kunt zien welke informatie er wordt gevonden en verwijderd. Ben je vervolgens klaar voor het echte werk, vink dan Do real clean aan, en klik nogmaals op Clean. In principe heb je overigens niets te vrezen, er wordt geen cruciale informatie verwijderd. Voor de zekerheid maakt de software wel een reservekopie van het registerbestand aan, die je later kunt terugzetten via het register, helaas niet via USB Oblivion.

Conclusie
USB Oblivion doet precies wat het belooft: het verwijdert de lijst met in het verleden aangesloten usb-apparaten. Voor de zekerheid wordt een reservekopie van het register gemaakt.



INDEX

Verberg data in een plaatje of breng een digitaal watermerk aan

Wil je privacygevoelige gegevens bewaren op zo'n manier dat niemand er ook maar aan denkt dat er zulke data worden bewaard dan kun je een steganografische methode gebruiken, zoals je die in de open-brontool OpenStego terugvindt. Deze tool dubbelt trouwens als een digitale watermerktool, waarmee je bijvoorbeeld ongemerkt een merkteken in afbeeldingen kunt aanbrengen. Dat kan je helpen bij het detecteren van illegale kopieën.

Vermomming

Om data te verbergen moet je al zeker over twee bestanden beschikken: een 'message file', die de eigenlijke gegevens bevat, en een 'cover file' (ook wel carrier file genoemd: het draagbestand waarin de privacygevoelige data onmerkbaar worden opgenomen). OpenStego laat je overigens toe meerdere draagbestanden tegelijk te selecteren. Het eerste bestand is typisch een tekstbestand of een document. Het draagbestand is (althans bij OpenStego) een afbeeldingsbestand, met de extensie (w)bmp, gif, jp(e)g of png. Uiteraard moet dit laatste bestand groot genoeg zijn om alle gegevens uit het eerste bestand vlotjes – en onzichtbaar voor wie het gemodificeerde beeldbestand bekijkt – te kunnen opnemen. Het resulterende bestand is bij OpenStego standaard een png-bestand.

Voor je het steganografische proces laat uitvoeren kun je eventueel nog het gewenste encryptie-algoritme instellen: standaard is dat AES128, maar je kunt ook DES of AES 256 selecteren. Deze versleuteling kun je dan nog met een stevig wachtwoord afschermen.
Uiteraard moet dit proces omkeerbaar zijn. Anders gezegd: jijzelf of de bedoelde ontvanger moet de data ook weer uit het gemodificeerde beeldbestand kunnen lichten. Dat is eveneens mogelijk vanuit OpenStego: je hoeft slechts naar het bronbestand te verwijzen, de doelmap voor het verstopte bestand in te vullen en desgevallend ook het bijhorende wachtwoord in te tikken.

Watermerk

Zoals gezegd laat OpenStego je ook toe onmerkbaar een digitale 'handtekening' in een afbeelding te stoppen. Deze module bevindt zich weliswaar nog in een bètastadium maar is in principe al bruikbaar. Eerst vult je de tekst voor je handtekening in – een of ander copyright-statement wellicht – waarna OpenStego die boodschap naar een sig-bestand zal omzetten. Vervolgens geef je aan welk bestand je van deze handtekening wilt voorzien en waar het resulterende bestand hoort terecht te komen. Uiteraard voorziet OpenStego ook in een functie om na te gaan of een afbeeldingsbestand effectief zo'n handtekening bevat.

INDEX

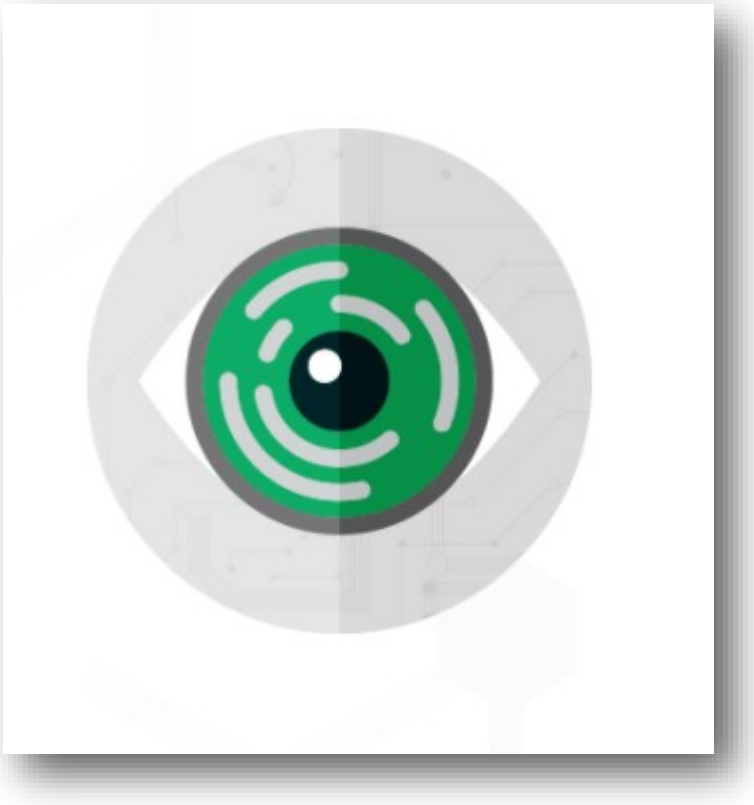
Houd ransomware buiten!

De laatste paar jaar maakt ransomware heel wat furore en… slachtoffers! Denk maar aan de wereldwijde aanval door WannaCry. Heel wat ransomware ontsnapt aan detectie door reguliere anti-virustools omdat ze van zero-day exploits gebruik maken.

Zoals de naam al doet vermoeden richt AppCheck AntiRansomware zich specifiek op ransomware en de tool maakt zich sterk dat die probleemloos naast je al bestaande antivirustool laat installeren. AntiRansomware maakt geen gebruik van een handtekeningendatabase maar bedient zich van heuristische methodes: wanneer ransomware typisch gedrag vertoont – zoals het aanpassen van documentbestanden – grijpt de tool in. Het programma opereert geheel los van de cloud en kan dus ook zijn werk doen wanneer je offline bent.

De gratis versie voorziet in twee beveiligingslagen: Ransom shelter (die een realtime back-up van bestanden maakt) en Ransom Guard. Deze laatste blokkeert ransomware en hoort vervolgens je originele bestanden vanuit de 'shelter' te herstellen. We kunnen echter niet zeggen hoe goed AntiRansomware in de praktijk opereert bij gebrek aan geschikt testmateriaal (lees: we beschikten niet over ransomware).

Er is tevens een betaalde Pro-variant beschikbaar die onder meer voorziet in een ingeplande back-up van zelf aan te duiden data (met versiebeheer). Deze back-up wordt afgeschermd van mogelijke ransomware-infecties.



INDEX

Creëer versleutelde bestandsarchieven

Wil je vermijden dat derden privacygevoelige data kunnen inkijken, dan blijft de meest aangewezen methode nog altijd stevige encryptie. Dat is precies waar CrocoCryptFile kan voor zorgen, waarbij je zelf de gebruikte encryptiemethode kiest.

Kies je code
CrocoCryptFile laat zich erg eenvoudig bedienen. Na installatie start je de tool op waarna je in een verkenner-achtig venster een of meer bestanden of mappen aanduidt die je wil laten versleutelen. Of je klikt die in de Verkenner met de rechtermuisknop aan en je kiest Encrypt with CrocoFile.

In beide gevallen verschijnt nu een nieuw dialoogvenster waarin je enerzijds de doelmap voor het versleutelde archief aanduidt en anderzijds een van de acht beschikbare versleutelingsalgoritmes selecteert.

Dit archief blijkt een propriëtair formaat te zijn (met de extensie croco). De encryptie-algoritmes zijn grotendeels 'wachtwoord-gebaseerd', waarbij je de keuze hebt tussen AES, TwoFish, Serpent en Camellia (telkens 256-bits). Verder zijn er nog: Windows KeyStore, GPG/OpenPGP Key (beide telkens 256-bits) en twee 'cloaked' (aka headerless) algoritmes: AES-TwoFish-256 en 'output padding'.

Afhankelijk van het gekozen algoritme wordt je dan eerst nog om een stevig wachtwoord gevraagd van minimaal 8 tekens, waarna het versleutelde archief wordt aangemaakt.

Ontsluiten
Het decrypteren gaat nog iets eenvoudiger. Het volstaat te dubbelklikken op zo'n croco-bestand, waarna je aangeeft waar de uitgepakte bestanden moeten terechtkomen en je desgevraagd ook het bijhorende wachtwoord invult.

CrocoCryptFile is dus een eenvoudige tool, maar veel meer hoeft dat niet te zijn: de achterliggende encryptie-algoritmes zijn best wel stevig. Zorg er wel voor dat je je wachtwoord niet vergeet, want dat wordt nergens (automatisch) opgeslagen.

INDEX

Bestanden delen zonder veel moeite

Er bestaan onderhand al heel wat services waarmee je ook grote bestanden kunt versturen. In de meeste gevallen houdt dat wel in dat je die bestanden eerst naar een externe server uploadt, vanwaar ze dan door de beoogde ontvanger kunnen worden opgehaald. O&O FileDirect werkt net dat ietsje anders – veiliger ook, zijn we geneigd te denken.

Wanneer je O&O FileDirect installeert kun je kiezen tussen een volledige en een aangepaste installatie. Niet dat daar zoveel verschil in zit: bij deze laatste kun je eventueel wel de automatische updateservice uitschakelen.

O&O FileDirect laat zich erg makkelijk bedienen. Je versleept een of meer bestanden of mappen naar het kleine programmavenster waarna meteen de bijhorende download-url verschijnt (https://file.direct/f/…). Met een druk op de knop stuur je die meteen ook richting Windows klembord. Je hoeft die url nu maar aan de bedoelde ontvangers te bezorgen waarna die de bestanden van je eigen pc – via de service van O&O – kunnen ophalen. Die hoeven dus zelf niet eens O&O FileDirect op hun toestel te hebben geïnstalleerd; een browser met internetconnectie volstaat.

Je pc moet dus wel zijn ingeschakeld, met het internet zijn verbonden en de bestanden moeten op dezelfde locatie beschikbaar zijn. Geef je zo'n bestand bijvoorbeeld een andere naam dan lukt het dus niet meer. Wanneer je meerdere bestanden naar het venster versleept dan creëert O&O FileDirect daar zelf een zip-bestand van – dat belandt dan standaard in de map C:\Users\<naam>\AppData\Roaming\oofd\shared.

Het is bovendien mogelijk aan te geven hoeveel dagen de download ter beschikking moet blijven of hoeveel downloads er maximaal mogen plaatsvinden. Verder kun je ook een wachtwoord aan de download (s) koppelen.

Handig is ook dat je op een apart tabblad een overzicht krijgt van de bestanden die je op deze manier 'gedeeld' hebt. Je verneemt dan de namen van de bestanden, evenals het aantal keren dat ze al zijn gedownload evenals de eventuele vervaldatum.

INDEX

Maak geheime schijfpartities

Ondanks de populariteit van laptops en computers worden er in veel huishoudens nog toestellen gedeeld door verschillende gebruikers. Nochtans is niet alles wat je als ouder doet op een computer even geschikt voor kinderogen. Bovendien kunnen gezinsleden (onbedoeld) je documenten verwijderen of veranderen. Om problemen te vermijden, kan je een geheime partitie aanmaken. Deze partitie is alleen te zien wanneer je het juiste wachtwoord hebt opgegeven en kan al je belangrijke bestanden bevatten.

Stap 1: Installatie

Hidden Disk is een gratis tool die je kan gebruiken om geheime partities aan te maken. De software wordt via de website van Cyrobo aangeboden. Klik op de startpagina op Hidden Disk en druk op de rode Download-knop. Wanneer je ten slotte op Download Setup File hebt geklikt, zal het installatiebestand naar je computer worden gehaald. Dubbelklik op het bestand om de installatie te starten. Het installatieproces van de software vergt enkele klikken, waarna je op Finish moet drukken. Indien je de standaardinstellingen hebt behouden, zal Hidden Disk automatisch starten nadat de installatie is voltooid.

Stap 2: Partitie aanmaken

Eenmaal Hidden Disk is gestart, krijg je een eenvoudige gebruikersinterface te zien. In de eerste plaats moet je de driverletter kiezen voor de nieuwe partitie die je zal aanmaken. Om de partitie aan te maken, klik je onderaan op Create disk X. Indien je een letter hebt gekozen die al wordt gebruikt door een andere partitie, zal je een waarschuwing krijgen en moet je een andere letter kiezen. Je kan de nieuwe partitie terugvinden door Windows Verkenner te openen en naar Deze pc te gaan. Onder Apparaten en stations zie je je nieuwe partitie staan.

Stap 3: Partitie beveiligen

Om je partitie te beschermen tegen pottenkijkers moet je een paswoord creëren. Klik hiervoor op Create/update password. Geef in de twee bovenste velden een paswoord in en voeg eventueel je e-mailadres toe. Dit adres zal worden gebruikt wanneer je je wachtwoord bent vergeten en zal daarom wel eens goed van pas kunnen komen. Het zou immers jammer zijn dat je je belangrijke documenten niet langer kan raadplegen doordat je ze te goed hebt beschermd. Nadat je de nodige bestanden aan je geheime partitie hebt toegevoegd, wordt het tijd om de drive te verbergen. Klik hiervoor op Disable disk X en sluit Hidden Disk af. Je zal merken dat je geheime partitie niet langer terug te vinden is in Windows Verkenner.

Stap 4: Partitie openen

Wanneer je de bestanden die je hebt verstopt in je geheime partitie opnieuw wilt raadplegen, open je Hidden Disk. De applicatie zal in de eerste plaats naar je wachtwoord vragen. Geef dit in en klik op Unlock om verder te gaan. Om je documenten wederom te kunnen raadplegen, klik je hierna op Create disk X. De partitie en alle bestanden die je erin hebt opgeslagen, zullen wederom beschikbaar zijn. Indien je je wachtwoord bent vergeten, heb je twee opties. De beste mogelijkheid die je hebt, is op Recover password by email te klikken. Hierdoor zal je een nieuw wachtwoord ontvangen via mail dat je kan gebruiken om aan te melden. Je doet er goed aan hierna een nieuw wachtwoord in te stellen via Create/update password. Indien je in de voorgaande stap geen e-mailadres hebt opgegeven, zit er niks anders op dan op Reset disk and password te klikken. Hidden Disk geeft je meermaals de waarschuwing dat alle bestanden in de geheime partitie verwijderd zullen worden. Negeer deze waarschuwingen om de applicatie weer bruikbaar te maken.

INDEX

Verander je computer in een Chromecast

Door je computer Chromecastfunctionaliteit te geven, kan je er vanop een afstand beeldmateriaal naartoe sturen. Net als bij een echte Chromecast kan je via een andere computer 'casten'. Denk daarbij aan Netflix of Google Foto's, maar ook aan tabbladen uit de browser van een andere computer. De functionaliteit is vooral handig in scholen of op het werk, al kan je er natuurlijk ook thuis van genieten.

Stap 1 / Installatie
Om je computer te veranderen in een Chromecast heb je software nodig. Google Cast For Education is de tool van dienst. De naam verraadt al dat de functionaliteit niet echt bedoeld is voor thuis, maar laat je daardoor niet afschrikken. Cast For Education is beschikbaar als extensie voor Google Chrome. Zoek in de webstore van Chrome naar de app of surf naar http://bit.ly/2i5VKvY. Klik op toevoegen om de kleine applicatie te installeren.

Stap 2 / Openen
Omdat Google Cast For Education geen echt programma maar een extensie is, moet je de applicatie openen via de Chrome-browser. Zoek links bovenaan in de browser de knop Apps om naar een tabblad met al je geïnstalleerde Chrome-applicaties te gaan. Hier vind je ook snelkoppelingen naar andere Google-diensten zoals Play Music, Keep, Inbox of de agenda. Als laatste toevoeging vind je de nieuwe app. Klik erop om het Cast For Education-venster te openen. Hoewel het om een extensie gaat, verschijnt de app, eens geopend, wel onderaan in de taakbalk van Windows.

Stap 3 / Instellen
Na het openen word je getrakteerd op een scherm waar je de naam van je virtuele Chromecast moet kiezen. Indien je wenst, kan je onderaan een afbeelding van het web kiezen die als achtergrond moet dienen wanneer er niets gecast wordt, maar eigenlijk hoef je je van de instellingen niets aan te trekken. Kies een naam, klik op Save en wacht even. Het initialiseren van de gesimuleerde Chromecast heeft tijd nodig. Je kan achteraf altijd terug naar het scherm gaan om de instellingen of de naam aan te passen.

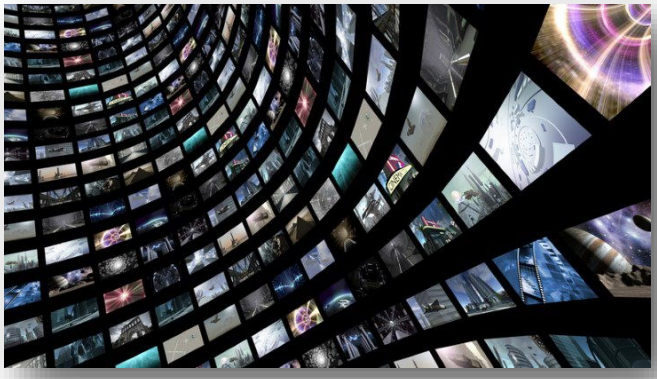
Stap 4 / Account
Google linkt de virtuele Chromecast automatisch aan het account waarmee je bent ingelogd in de Chrome-browser. Eigenlijk is het de bedoeling dat je een Google Education-account hebt, maar de cast-app werkt ook zonder. Dat brengt helaas enkele beperkingen met zich mee. In de praktijk is je virtuele cast enkel zichtbaar voor jou. Dat wil zeggen dat je ernaar kan casten via andere toestellen waarmee je zelf bent ingelogd, maar dat bezoekers met een eigen Google-account het virtuele toestel niet zullen zien. Dat is een jammere beperking die het sociale aspect van de Chromecast, waarbij je bijvoorbeeld samen Youtubefilmpjes kiest en bekijkt, teniet doet. De zet van Google is wel begrijpelijk: de virtuele Chromecast is gratis terwijl een echt exemplaar Google wel centjes oplevert.

Het 'tv-scherm' van dienst voor de virtuele cast-app kan je met een sneltoets het volledige display laten innemen.
Stap 5 / Volledig scherm
Het cast-venster doet dienst als virtuele tv. Hier zal je de gecaste inhoud te zien krijgen. Je kan het venster uiteraard maximaliseren en het geheel nog meer cast-functionaliteit geven door je pc aan te sluiten op een tv-toestel via bijvoorbeeld HDMI. Om echt het volledige scherm te benutten, moet je de F11-toets op het toetsenbord gebruiken. Zo verdwijnen ook de startbalk en de vensterbalk bovenaan. Met je virtuele Chromecast in positie is het tijd om te casten.

Stap 6 / Cast-extensie
De virtuele Chromecast werkt het best met andere pc's. Zo kan je een oude computer of een kleine computerstick van bijvoorbeeld Intel of Lenovo aan je tv hangen en instellen, waarna je snel films of foto's van je laptop naar de tv kan sturen. Om te casten vanop een computer heb je een andere Chrome-extensie nodig. Die heet gewoon Google Cast en vind je opnieuw in de Chrome Web Store. Je kan ook rechtstreeks de url intypen: http://bit.ly/MoM7JH. Klik opnieuw op Toevoegen aan Chrome. Als het goed is, vind je nu links bovenaan je browservenster een cast-icoon. De functie werkt niet alleen met de virtuele Chromecast maar ook met gewone Chromecast-toestellen.

Stap 7 / Casten
Casten doe je door op het icoon in je browser te klikken. Als het goed is, verschijnt je virtuele Chromecast nu in de lijst met beschikbare toestellen. Kik op de naam om de browsertab naar de Chromecast te sturen. De acties op het tabblad op je pc worden gespiegeld in het Chromecastvenster. Let wel: er zit een kleine vertraging op de gecaste tab. Je kan dus geen spellen spelen op je tv op deze manier.

Stap 8 / Bureaublad delen
Je kan niet alleen een tab casten, maar ook je hele bureaublad. Klik daartoe op het pijltje naast Casten naar. Je kan nu kiezen op welke manier je je scherm wilt delen. Selecteer Bureaublad casten om de schermoutput van je hele systeem te casten. Indien je meerdere schermen ter beschikking hebt, verschijnt er eerst nog een dialoogvenster waarop je moet kiezen welk display je precies wilt delen. Je kan ook kiezen om geluid wel of niet te casten. In de plaats van een mooie tab zie je nu je hele computerscherm gedupliceerd via de Cast-app. Dat is bijvoorbeeld handig bij vergaderingen of presentaties op het werk. Zo kan je immers snel een Powerpoint tonen op een andere pc zonder dat je die hoeft door te sturen. Opnieuw gaat het hier om een functie die niet exclusief is aan de Google Cast For Education-app: ook op een gewone Chromecast heb je deze functies ter beschikking. Klik om te stoppen met casten op de broncomputer op het blauwe Cast-logo links bovenaan en selecteer Stop.



INDEX

Facebook lekte privégegevens moderatoren

Een werknemer van Facebook zit al maanden ondergedoken nadat zijn persoonlijke gegevens waren uitgelekt en bekeken door vermeende terroristen. Het incident draait om een lek in de databases waarin gegevens zijn opgeslagen van alle moderatoren; de medewerkers die dagelijks alle content screenen op kinderporno, ander naakt en terroristische content.

Van meer dan duizend van hen is de identiteit nu bekend; techneuten spreken tegenover The Guardian van een bug waardoor onder geweigerde content niet alleen de standaardmelding kwam te staan maar ook de naam en foto van de desbetreffende moderator.
Het gaat om werknemers van 22 afdelingen, waarvan een stuk of veertig van de contra-terrorisme unit in het Europese hoofdkantoor in Dublin, Ierland. Zes van hen zijn door het bedrijf nu als 'high priority target' benoemd. Toen bleek dat hun profielen bekeken waren door aanhangers van IS en andere groeperingen, kregen ze bescherming.

Eén werknemer woont daarom zelfs al maandenlang in een ander land, uit vrees voor vergeldingsacties. 'It was getting too dangerous to stay in Dublin', zei de man, een geboren Irakees die met zijn ouders juist naar Ierland verhuisde om aan zulke acties te ontsnappen. 'When you have people like that knowing your family name you know that people get butchered for that. The punishment from Isis for working in counter-terrorism is beheading. All they'd need to do is tell someone who is radical here'.

De moderators merkten dat er wat mis was toen ze opeens vriendenverzoeken kregen van mensen uit radicale en extremistische hoek, soms zelfs van de mensen van wie ze wel eens postings, foto's en filmpjes hadden verwijderd. Onderzoek door de technici van Facebook bracht toen het lek naar boven. Zoals zo vaak probeerde het bedrijf dat eerst te bagatelliseren. 'Jouw naam valt vast niet op in die enorme lijst met gebruikers', schreef een ceo aan een van de moderatoren.

Aan me hoela, schreef die terug. 'I'm not waiting for a pipe bomb to be mailed to my address until Facebook does something about it'.

INDEX

Europees Parlement wil geen backdoors in encryptie

Regeringen en geheime diensten wereldwijd strijden tegen encryptie. Ze zijn van mening dat verregaande encryptiemethoden de bescherming van de burger tegen bijvoorbeeld terroristische aanslagen bemoeilijkt. Tegelijk zijn er bedrijven die juist vinden dat encryptie de privacy van de burger beschermt. Het Europees Parlement lijkt die laatste lijn te volgen.

De LIBE-commissie van het Europees Parlement diende vorige week een proefversie van een rapport over databescherming binnen de Europese Unie in. In het rapport valt te lezen dat de EU achterop is geraakt als het aankomt op bestrijding van bedreigingen en dat dataprotectie gemoderniseerd moet worden.

In het voorstel valt te lezen dat sinds in 2002 de regulering van privacy en elektronische communicatie werd vastgelegd er te weinig is gebeurd om de wetgeving de realiteit bij te laten benen. Zo is er geen wetgeving met betrekking tot machine-to-machine verkeer en het internet-of-things.

Leidend bij het vernieuwen van de wetgeving zou de bescherming van de burger moeten zijn, blijkt uit een van de amendementen. Zo staat in amendement 116 het volgende:
“De verleners van elektronische communicatiediensten moeten ervoor zorgen dat er voldoende bescherming is tegen ongewenste toegang of veranderingen aan de elektronische communicatiegegevens, en dat de vertrouwelijkheid en veiligheid van de verzending ook gegarandeerd worden binnen de aard van de transmissie gebruikt, of door de nieuwste end-to-end encryptie van de elektronische communicatiedata.”

Een backdoor mag niet ingebouwd worden, wat de commissie betreft. “Decryptie, reverse engineering of het monitoren van zulke communicatie moet verboden worden,”lezen we namelijk ook. De EU-lidstaten zouden dan ook niet mogen eisen van communicatieproviders dat er een achterdeur ingebouwd wordt.

Dat gaat direct in tegen beleid binnen lidstaten. Zo heeft de Duitse regering een wet in de maak, waarmee de overheid het recht krijgt om boodschappen te ontcijferen. Ook andere landen – waaronder het Verenigd Koninkrijk, de Verenigde Staten en Australië – volgen zo’n lijn en zijn van mening dat er veilige achterdeuren ingebouwd kunnen worden.

Bron: techZine

INDEX

Rijk worden met virtueel geld: is ethereum het nieuwe bitcoin?

De snelle waardestijging van het cryptogeld ethereum is opvallend. Ethereum is het jongere broertje van het bekendere bitcoin, het zogenoemde cryptogeld. Wie een paar jaar geleden nog voor weinig geld bitcoins kocht, kan nu rijk zijn. Geldt datzelfde straks voor ethereum? We spraken specialist Rutger van Zuidam.

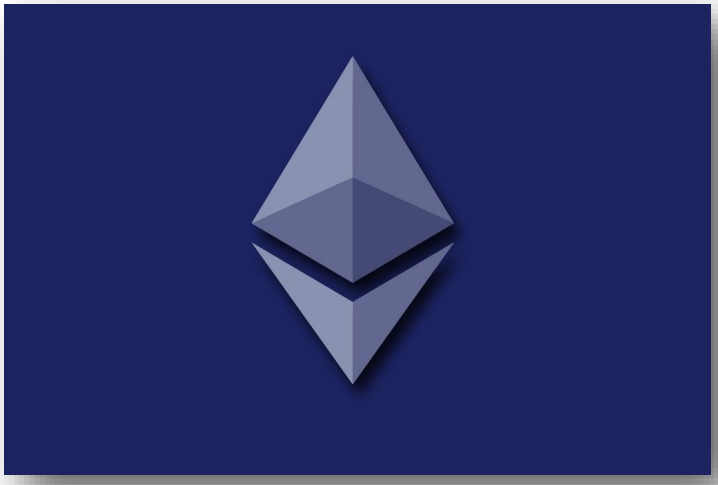
1. Ik kende alleen bitcoin, maar nu hoor ik ineens veel mensen over ethereum. Wat is dat nou weer?
,,Bitcoin was de allereerste, en ethereum is van het zogeheten 'tweede generatie' cryptogeld. Ze werken beiden op basis van blockchain, wat een soort beveiligde database is waarop je je digitale geld kunt opslaan en verkopen. Verder zijn ze eigenlijk niet te vergelijken, want elk cryptogeld heeft zijn eigen technologie."
,,Het hele systeem van cryptogeld, of cryptovaluta, is eigenlijk vergelijkbaar met het internet van rond het jaar 1992. Veel mensen experimenteerden er mee, er waren nog geen browsers en mensen waren blij met elke e-mail die ze kregen. Niemand wist nog hoe het zich precies verder zou ontwikkelen. Maar je ziet wel dat steeds meer mensen geïnteresseerd raken, en er iets mee willen doen."

2. Hoe komt het dat ethereum zo in prijs is gestegen?
,,Tot nu toe is deze cryptocurrency na elke tegenslag steeds sterker teruggekomen, en dus gegroeid. Het kwam in 2016 op de markt, en is qua technologie wat complexer, maar in het gebruik gemakkelijker. Er zijn nu veel bedrijven en mensen die in ethereum geloven, en dat is belangrijk. Doordat er steeds meer bedrijven geld in stoppen, doet ethereum het zo goed. Net zoals op de beurs. Het draait allemaal om vertrouwen."

3. Iedereen om me heen koopt massaal ethereum, omdat de prijs daarvan zo is gestegen. Is dat verstandig?
,,Ik zou zelf nooit geld dat ik écht nodig heb in cryptocurrency stoppen, omdat het een zeer groot risicogehalte heeft. Uitproberen met een kleiner bedrag is een beter idee, en door te experimenteren begrijp je deze vorm van cryptogeld ook iets beter. Maar je spaargeld erin stoppen, zou ik niet zo snel doen."

4. Kan ik beter in ethereum of in bitcoin investeren?
,,Dat is niet te zeggen. Omdat ze zo moeilijk te vergelijken zijn, hangt het echt van je voorkeur af. Lees je in, zoek uit wat erachter zit en kijk waar je het meest in gelooft. Ze zijn beide superinteressant, vind ik als ondernemer."

5. Met bitcoin kun je inmiddels onder andere bij Thuisbezorgd betalen. Wat kunnen we in de toekomst allemaal met ethereum?
,,Bij ethereum is het de vraag of het zich hetzelfde gaat ontwikkelen als bitcoin. Pas als het meer ontwikkeld is, gaan consumenten er iets van merken, hoewel een hoop ook 'onder water' zal gebeuren. Dat wil zeggen: waarschijnlijk helpt ethereum straks om betaalsystemen gemakkelijk en zonder bonnetjes te laten verlopen, maar zal de gemiddelde consument niet doorhebben dat dat door cryptocurrency komt."
,,Het handige is bijvoorbeeld dat de overheid een bedrag in ethereum specifiek aan een bepaalde uitgave kan koppelen. Ze geven dan een soort coupon uit die alleen aan iets heel specifieks kan worden uitgegeven. Je kunt het als geoormerkt geld beschouwen, dat bijvoorbeeld is gereserveerd om aan kinderopvang te worden besteed. Dat scheelt administratieve rompslomp, want er hoeft door de burger geen declaratie gedaan te worden, die weer door een ambtenaar moet worden verwerkt. Dat werkt dus handiger en sneller."



INDEX

Hoe de CIA offline systemen besmet met malware

Air-gapped systemen zijn erg moeilijk te besmetten, aangezien ze niet met het internet verbonden zijn. De CIA heeft echter een manier gevonden om op zo'n sterk beveiligde computer te geraken.
In recent gelekte bestanden op Wikileaks staat beschreven hoe de CIA air-gapped systemen besmet met malware. Via een computer die wel met het internet verbonden is, zoekt de malware van het agentschap zich een weg naar een air-gapped systeem. Hier verzamelt de kwaadaardige software informatie, waarna deze info via de eerste computer naar de CIA wordt verstuurd. Zoals wel vaker rekent de malware op onvoorzichtige mensen om zijn eindbestemming te bereiken.

Air-gapped
Air-gapped systemen worden aanzien als erg veilig, aangezien ze niet verbonden zijn met het internet en de rest van het bedrijfsnetwerk. Hierdoor is het in theorie onmogelijk voor malware om via het netwerk van een firma over te springen op de sterk beveiligde computer. De meest kostbare bestanden van bedrijven worden daarom bewaard op air-gapped computers.
Eerder werden echter al methodes gevonden om de kostbare informatie van air-gapped toestellen toch te ontvreemden. Hierbij wordt gebruik gemaakt van het geluid van een harde schijf, of de warmteoutput van het systeem. De CIA heeft echter een meer geavanceerde methode ontwikkeld om aan de kostbare info van bedrijven te geraken. De methode van het agentschap teert op de onvoorzichtigheid van bedrijfsmedewerkers die fysiek toegang hebben tot de air-gapped computer.

Brutal Kangaroo
De malware, Brutal Kangaroo genaamd, besmet een bedrijfscomputer die wel met het internet verbonden is. Dat toestel wordt de primaire host genoemd en dient als tijdelijke opslagplaats van de malware. Brutal Kangaroo doet niets op de primaire host en wacht tot een externe drive wordt aangesloten. De malware kopieert zichzelf naar de USB-stick en wacht wederom tot het juiste moment om in actie te schieten. Wanneer de externe drive wordt gekoppeld aan een air-gapped systeem kopieert Brutal Kangaroo zichzelf een laatste maal en verzamelt de malware op de achtergrond informatie.
De verzamelde info wordt op de USB-stick opgeslagen, maar kan nog niet onmiddellijk naar de CIA worden doorgestuurd. Hiervoor is immers een internetverbinding nodig. Pas wanneer de drive weer wordt verbonden met de primaire host is de cirkel rond en kan de CIA de kostbare info bemachtigen.

Tot deze informatie behoren niet alleen bestanden van de besmette air-gapped computer, maar eveneens info afkomstig van andere air-gapped toestellen. Brutal Kangaroo richt immers een netwerk op de beveiligde computer op, waardoor andere computers die zich in het air-gapped netwerk bevinden eveneens worden gecompromitteerd.

INDEX

Blok: Toestemming officier vereist voor smartphone-onderzoek

Naar aanleiding van de uitspraak van de Hoge Raad afgelopen april geldt voortaan in strafrechtelijke onderzoeken dat de politie de toestemming van de officier van justitie nodig heeft om in beslag genomen smartphones te onderzoeken. Dat laat demissionair minister Blok van Veiligheid en Justitie weten op Kamervragen van D66.

In april oordeelde de Hoge Raad dat de politie een smartphone mag doorzoeken als dit niet verder gaat dan een beperkte inbreuk op de privacy, maar als alle gegevens op een smartphone worden uitgelezen, waardoor volledig inzicht wordt verkregen in contacten, oproepgeschiedenis, berichten en foto's mag de politie dat niet zo maar doen. D66-Kamerleden Verhoeven en Groothuizen wilden van Blok weten wat de uitspraak betekent voor strafrechtelijk onderzoek naar in beslag genomen smartphones.

"Naar aanleiding van het arrest van de Hoge Raad geldt in strafrechtelijke onderzoeken vanaf 4 april 2017 als hoofdregel dat, indien sprake is van zelfstandig beslag door de opsporingsambtenaar, er voor het doen van onderzoek aan een inbeslaggenomen smartphone of andere elektronische gegevensdrager of geautomatiseerd werk, de toestemming van de officier van justitie voor dat onderzoek vereist is", aldus de minister.

Blok stelt dat alleen als er een niet meer dan beperkte inbreuk wordt gemaakt de opsporingsambtenaar na een zelfstandige inbeslagname het onderzoek zonder toestemming van de officier van justitie mag uitvoeren. Verder laat de minister weten dat alleen in zeer uitzonderlijke gevallen, waarbij er sprake is van een zelfstandige inbeslagname, er sprake zal zijn van betrokkenheid van de rechter-commissaris. Het gaat dan om gevallen waarin op voorhand is te voorzien dat de inbreuk op de persoonlijke levenssfeer zeer ingrijpend zal zijn.

INDEX

Top 10 Veilige e-maildiensten

1. Gmail, Outlook en andere populaire diensten
Je kan relatief anoniem blijven als je een e-mailadres aanmaakt bij een veelgebruikte dienst als Gmail of Outlook, je moet alleen staalhard liegen bij het invullen van je profiel. Deze methode is echter niet 100 procent waterdicht: uiteindelijk zal je iets van informatie moeten geven waarmee de e-mailprovider je identiteit kan verifiëren, zoals een tweede e-mailadres of een telefoonnummer. Bovendien zal iemand je nog altijd kunnen traceren aan de hand van je IP-adres wanneer je een standaarddienst gebruikt en deze beslist om dat openbaar te maken. Om volledig anoniem te gaan heb je een provider nodig die zich in privacy specialiseert.

2. Hushmail
Hushmail kan op de goedkeuring van privacy-waakhond Electronic Frontier Foundation rekenen. Via de dienst kan je je mailverkeer volledig versleuteld laten verlopen. Die beveiliging komt niet gratis: de jaarlijkse kostprijs van een particulier account is 49,98 dollar. Er is ook een gratis versie, maar die omvat maar 25 MB aan opslagruimte. Hushmail is via de browser te gebruiken en heeft ook een iOS-app.

3. Hide My Ass! Anonymous Email
Hide My Ass! Is voornamelijk bekend als gewaardeerde VPN-dienst, maar de ontwikkelaar biedt ook een anonieme mailservice aan. Het speciale aan HMA is dat je op voorhand moet bepalen hoe lang je het adres wil gebruiken, met als maximumtermijn een jaar. De digitale postbus is ook enkel te gebruiken als inbox, je kan er geen berichten mee sturen. Bij het creëren van een account krijg je de vraag om een bestaand e-mailadres op te geven, maar dat is geen vereiste.

4. Guerilla Mail
Guerilla Mail prijst zichzelf aan als “een tijdelijk en wegwerpbaar e-mailadres”. Je kan zonder je in te schrijven een willekeurig e-mailadres bij de provider aanmaken waarop je mails kan versturen en ontvangen. Je kan zelfs bijlagen bijvoegen tot 150 MB. De kwalificatie ‘tijdelijk’ is relatief: het mailadres blijft wel degelijk permanent bestaan, maar ontvangen mails worden na een uur verwijderd.

5. Mailinator
Ook Mailinator biedt wegwerp-mailadressen aan waarvoor je je niet moet inschrijven. Anders dan bij Guerilla Mail krijg je geen willekeurig adres toegewezen; Mailinator laat je je eigen naam verzinnen. De enige voorwaarde is dat deze op “@mailinator.com” moet eindigen. Wanneer je het adres intikt op de startpagina, kan je de inbox bezoeken. Berichten sturen is niet mogelijk, en bovendien kan iedereen de inbox bezoeken zolang ze maar het juiste adres kennen. Mailinator is voornamelijk handig als je je op een online dienst inschrijft maar geen echt mailadres wil opgeven.

6. Hide-Your-Email.com
Heb je liever toch wat meer bescherming voor je mailbox, dan is er Hide-your-email.com. In essentie is dit dezelfde service als Mailinator, maar nog simpeler van opzet én met de gratis mogelijkheid om een bepaald adres te reserveren. Via die optie kan je een wachtwoord instellen voor de inbox. Berichten die je krijgt, duiken meteen op in de inbox, maar ook hier is versturen niet mogelijk.

7. Email On Deck
Je moet twee stappen doorlopen om een adres bij Email On Deck aan te maken, waarvan één stap een CAPTCHA is die moet uitmaken dat je geen robot bent die een e-mail aanvraagt. Stap twee is het ontvangen van je adres. Dat wordt je willekeurig toegewezen en is enkele uren actief is. Niet bruikbaar als permanent anoniem mailadres, maar wel handig om je ergens in te schrijven.

8. TorGuard Email
Net als Hide My Ass! is TorGuard een VPN-dienst die gebruikers ook een anonieme mailservice aanbiedt. Er is een gratis optie met 10 MB aan opslagruimte. Voor 6,95 dollar per maand wordt de geheugenbeperking volledig opgeheven. Ongeacht of je betaalt of niet kan je via TorGuard G/PGP-versleutelde mails sturen en ontvangen en hoef je daarbij ook niet op reclamebanners te kijken.

9. Trashmail.com
Trashmail laat je toe om een tijdelijke e-mail te creëren die je kan koppelen aan je bestaande adres. Trashmail zorgt ervoor dat de mails die je op je anonieme inbox aankrijgt doorgestuurd worden naar je vaste e-mail. Aan die optie is wel een kostprijs verbonden: je kan vijf mails gratis laten forwarden, maar voor een hoger aantal heb je een Trashmail Plus-lidmaatschap nodig dat op 9,99 euro per jaar uitkomt. Trashmail heeft plug-ins voor Google Chrome en Mozilla Firefox beschikbaar, waardoor je de webpagina niet eens moet bezoeken om je mailadres(sen) te beheren.

10. ProtonMail (+Tor)
Protonmail biedt een volledige mailservice met de garantie dat je communicatieverkeer volledig versleuteld verloopt. Een gratis account komt met 500 MB aan opslag en een limiet van 150 berichten per dag. Leg je geld neer voor een Plus- (4 euro/maand) of Visionary-abonnement (24 euro/maand) dan worden die grenzen opgerekt. ProtonMail vraagt geen enkele persoonlijke informatie wanneer je je profiel aanmaakt. Wil je 100 procent anoniem gaan, dan kan je via de Tor-pagina van de maildienst opereren die je vindt op www.protonirockerxow.com.

INDEX

Inloggen DigiD met alleen wachtwoord wordt afgeschaft

Het inloggen met alleen een gebruikersnaam en wachtwoord op sites van de overheid zal op termijn niet meer kunnen. Het beveiligingsniveau van deze manier van inloggen is te laag en de overheid acht het niet veilig om dit zo te blijven doen.

DigiD zal wel blijven werken met naast het wachtwoord een code uit een sms of uit de app van DigiD. Die methoden bieden extra beveiliging, bekend als tweestapsverificatie, ten opzichte van inloggen met alleen een gebruikersnaam en wachtwoord.

DigiD-chip
Ook komen er in 2018 rijbewijzen en id-kaarten met DigiD-chip uit. Het rijbewijs zal beschikbaar zijn in de eerste helft van 2018, de identiteitskaart volgt daarna, aldus demissionair minister Ronald Plasterk van Binnenlandse Zaken in zijn voortgangsrapportage overhet programma eID dat nieuwe manieren van inloggen op overheidswebsites behelst.

Volgens de huidige versie van de aankomende wet Generieke Digitale Infrastructuur (GDI) die toegang tot digitale dienstverlening bij de overheid regelt, mogen overheidsinstanties tot drie jaar nadat die wet van kracht wordt, laten inloggen met gebruikersnaam en wachtwoord. Hoewel de wet nog niet van kracht is, wil de overheid de minst veilige manier van inloggen sneller afschaffen. Onlangs bleek dat 90 procent van de huidige succesvolle inlogpogingen gebeurt zonder sms-authenticatie.

De overheid is al jaren bezig met eID, een systeem van inloggen met meerdere systemen op websites van de overheid en bedrijven. Naast DigiD moeten er daarom meer systemen komen om in te loggen, die de overheid indeelt in betrouwbaarheidsniveaus. Hoe gevoeliger de gegevens zijn waar het inloggen toegang toe geeft, hoe hoger het betrouwbaarheidsniveau moet zijn. Het inloggen met gebruikersnaam en wachtwoord is van het laagste niveau, de optie met een chip op het rijbewijs is onderdeel van een hoog niveau.

INDEX

Nieuwe Europese privacywet kan bedrijven boetes opleveren

Veel Nederlandse bedrijven en organisaties lopen vanaf volgend jaar kans op hoge boetes, omdat ze nog niet klaar zijn voor een nieuwe Europese privacywet.
Uit onderzoek van consultancybureau PwC onder 350 bedrijven blijkt dat ruim de helft van de bedrijven nog niet serieus begonnen is met de voorbereidingen.
Dat terwijl de nieuwe wet nogal wat om handen heeft. "Als je nu nog moet beginnen, wordt het heel spannend", zegt ict-jurist Arnoud Engelfriet. De boetes bij niet voldoen aan de wet zijn fors: maximaal 4 procent van de jaaromzet of 20 miljoen euro, al is de kans groot dat de boetes in de praktijk lager uitvallen.
Dat veel bedrijven desondanks nog niet klaar zijn, baart Aleid Wolfsen, hoofd van de Autoriteit Persoonsgegevens, grote zorgen. "Het gaat om ingrijpende wetgeving die gevolgen heeft voor onze grondrechten. Bedrijven moeten nu echt aan de slag", zegt hij.
Positief
Voor burgers is de nieuwe wet positief: ze hebben meer controle over hun data. "Je kunt bijvoorbeeld tegen een bedrijf zeggen: ik wil dat deze data over mij worden verwijderd", zegt Wolfsen. "Je kunt de toestemming die je geeft aan een bedrijf om je privégegevens te bewaren straks ook weer intrekken."
Fijn voor onze privacy, maar bedrijven en andere organisaties moeten daar hun computersystemen wel op aanpassen. Ook moeten organisaties veel beter vastleggen wat voor data ze precies bewaren. "Je moet alles wat je opslaat goed documenteren en de beveiliging ervan op orde hebben", aldus Engelfriet. Hoe gevoeliger de gegevens die een bedrijf heeft, hoe strenger de regels.
En lastig daarbij is dat veel bedrijven geen idee hebben van wat ze allemaal opslaan. "Veel bedrijven hebben last van achterstallig onderhoud. Die hebben de afgelopen jaren allemaal nieuwe systemen gebouwd waarin gegevens worden opgeslagen, maar weten niet meer waar alles precies staat en of dat volgens de regels gebeurt", zegt beveiligingsdeskundige Bram van Tiel van PwC.
Bakker en voetbalclub
Dat geldt niet alleen voor de Googles en Facebooks van deze wereld, maar voor alle organisaties die persoonsgegevens opslaan: van de bakker om de hoek met een mailinglijst en de voetbalclub tot middelbare scholen.
"Ik heb er een dagtaak aan", zegt ict'er André Poot van de scholenkoepel CVO-AV. "We moeten al onze privacyreglementen herschrijven en al onze databases in kaart brengen." Dat doet hij niet voor niets: "De privacywaakhond heeft duidelijk gemaakt dat het speelkwartier voor scholen vanaf nu over is en dat we strenger aangepakt gaan worden."
"Je moet continu onder de loep houden wat je precies doet met data", zegt Job Vos van Kennisnet, dat scholen helpt met ict. "Iedere docent moet worden getraind om zorgvuldig met privacy om te gaan." Zo moeten docenten beseffen dat ze gevoelige gegevens niet mogen mailen of uitwisselen op usb-sticks. "Dat mocht al niet, maar straks moet je kunnen aantonen dat je dat ook echt niet doet", zegt Vos.
Datalek
De school van Poot had vorig jaar een datalek waarbij de inhoud van webformulieren via Google te vinden was. Daaronder was gevoelige data, zoals ouders die melden dat ze gingen scheiden.
Voor dat soort dingen kunnen sneller boetes worden opgelegd. Nu geeft de Autoriteit Persoonsgegevens een waarschuwing; als een bedrijf zijn leven niet betert, kan een dwangsom van 800.000 euro worden opgelegd. Dat verandert: straks kan meteen een boete worden opgelegd.
"We krijgen veel meer mogelijkheden om in te grijpen", zegt Wolfsen van de privacywaakhond. "We hebben ook een waarschuwende functie, maar daarnaast kunnen we ook echt boetes gaan opleggen. Dus bedrijven, heb je boel op orde."

Bron: PwC

INDEX

Mobiele ransomware is steeds vaker gericht op ontwikkelde markten

Cybercriminelen achter mobiele ransomware zijn hun aanvallen aan het richten op welvarende landen. Ontwikkelde markten hebben niet alleen een hoger inkomstenniveau, maar ook een meer geavanceerde en op ruimere schaal gebruikte mobiele en e-betalingsinfrastructuur. Dit is aantrekkelijk voor criminelen, aangezien slachtoffers het losgeld met slechts enkele klikken kunnen overboeken.

Dit blijkt uit het Kaspersky Security Network (KSN) rapport van Kaspersky Lab. Het verslag bestrijkt de volledige tweejarige periode die, in het kader van het vergelijkingsmateriaal, is opgedeeld in twee delen van elk 12 maanden: van april 2015 t/m maart 2016 en van april 2016 t/m maart 2017. Deze specifieke periodes zijn gekozen omdat hierin diverse belangrijke veranderingen hebben plaatsgevonden in het dreigingslandschap van ransomware.

Forse stijging in Q1 2017
In het eerste kwartaal van 2017 schoot de activiteit van mobiele ransomware omhoog, met 218.625 mobiele Trojan ransomware-installatiepakketten – 3,5 keer zoveel als in het voorgaande kwartaal. De activiteit daalde vervolgens tot het gemiddeld waargenomen niveau van de tweejarige periode. Ondanks deze verlichting wekt het mobiele dreigingslandschap nog steeds veel onrust op, aangezien criminelen landen aanvallen met ontwikkelde financiële en betalingsinfrastructuren die gemakkelijk zijn te hacken.

Van alle door mobiele ransomware aangevallen gebruikers in de periode 2015-2016, was Duitsland het land met het hoogste percentage slachtoffers (bijna 23%). Dit werd gevolgd door Canada (bijna 20%), het VK en de VS - beide met meer dan 15%. Dit veranderde in 2016-2017, toen de VS van de vierde plaats opschoof naar de eerste positie (bijna 19%). Canada en Duitsland behielden hun top-3 notering met respectievelijk bijna 19 procent en ruim 15%, waardoor het Verenigd Koninkrijk vierde werd met ruim 13%.

Svpeng- en Fusob-malwarefamilies
De opkomst van de Verenigde Staten was grotendeels te wijten aan aanvallen via de Svpeng- en Fusob-malwarefamilies, waarvan de eerste zich voornamelijk richt op Amerika. De malwarefamilie Fusob richtte zich in eerste instantie op Duitsland, maar sinds Q1 van 2017 staat Amerika bovenaan de lijst van doelwitten, met 28% van de aanvallen.

"Deze geografische veranderingen in het mobiele ransomwarelandschap kunnen een indicatie zijn van de trend om aanvallen uit te breiden naar rijke, onvoorbereide, kwetsbare of nog niet eerder bereikte regio's. Dit betekent uiteraard dat gebruikers met name in deze landen uiterst voorzichtig moeten zijn bij het surfen op internet", waarschuwt Roman Unuchek, beveiligingsexpert bij Kaspersky Lab.

Advies
Om het risico op infectie te verkleinen, wordt gebruikers het volgende geadviseerd:
Maak regelmatig een back-up van gegevens;
Gebruik een betrouwbare beveiligingsoplossing en denk eraan om de belangrijkste functies - zoals System Watcher - ingeschakeld te houden;
Houd software altijd bijgewerkt op alle gebruikte apparaten;

Behandel e-mailbijlagen of berichten van onbekenden met de nodige voorzichtigheid. In geval van twijfel, niet openen;

Geef als bedrijf ook voorlichting aan uw medewerkers en IT-teams; houd gevoelige data gescheiden, beperk de toegang en maak altijd overal een back-up van;

Mocht u onverhoopt toch ten prooi vallen aan een encryptor, raak dan niet in paniek. Gebruik een niet-geïnfecteerd systeem om naar de No More Ransom website te gaan; de kans is aanwezig dat u hier een decryptietool vindt die u kan helpen uw bestanden terug te krijgen;

De nieuwste versies van Kaspersky Lab-producten voor kleinere bedrijven zijn uitgebreid met anti-cryptomalware functionaliteit. Bovendien is een gratis anti-ransomware tool beschikbaar gesteld die alle bedrijven kunnen downloaden en gebruiken, ongeacht de beveiligingsoplossing die ze hebben geïnstalleerd;

En niet te vergeten, bedenk dat het verspreiden van ransomware een strafbaar feit is. Meld het bij uw lokale wetshandhavingsinstantie.
Ga voor hulp en advies over het omgaan met ransomware naar No More Ransom. Kijk op No Ransomvoor de nieuwste decryptors, hulpmiddelen om ransomware te verwijderen en informatie over bescherming tegen ransomware.

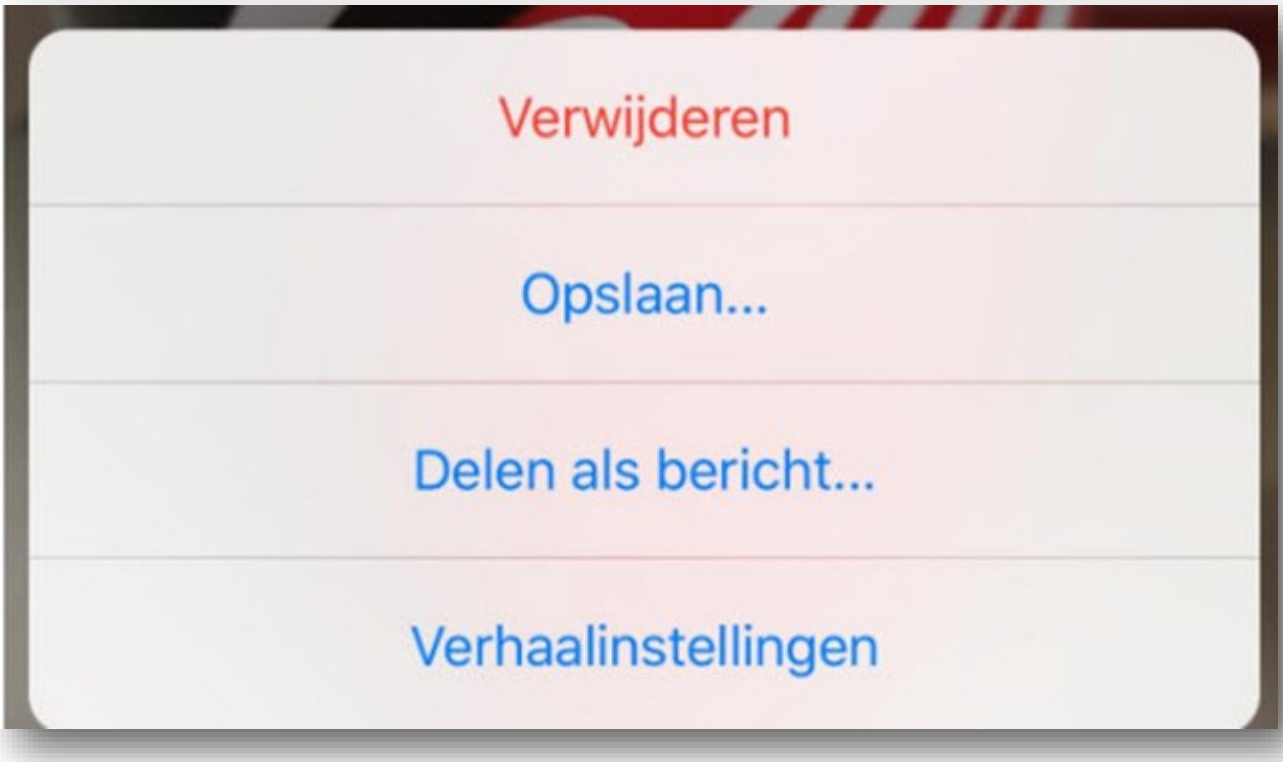
INDEX

Hoe verwijder je een foto uit je Instagram-verhaal?

In augustus vorig jaar introduceerde Instagram de functie Stories, in het Nederlands netjes vertaald als Instagram-verhaal. Echt nieuw was de functie natuurlijk niet, want Snapchat werkt al tijden met deze verhalenfunctie, maar voor Instagram-gebruikers was het een zeer gewenste uitbreiding. Klein probleempje: het is niet iedereen duidelijk hoe je foto's weer verwijdert uit je verhaal.

De tweesplitsing in Instagram sinds de komst van verhalen is sowieso een beetje verwarrend (waarmee de app in nóg meer opzichten gaat lijken op Snapchat), maar de basis is simpel: een gewone foto upload je via de plusknop onderin, en een Verhaal begin je met behulp van het pictogram van de camera linksboven.
Foto verwijderen uit je Verhaal
Maar als je eenmaal een foto hebt geplaatst, hoe verwijder je deze dan weer uit je verhaal? Het is vrij eenvoudig, maar de optie daarvoor is een klein beetje verscholen. Om een foto uit je verhaal te verwijderen, zul je eerst je eigen verhaal moeten bekijken. Je doet dat door Instagram te starten en te kijken naar de balk met verhalen bovenin. Door hier te drukken op Je verhaal (voorzien van je profielfoto), wordt je Verhaal geopend (als je nog geen foto had geplaatst, dan wordt de camera geopend). Rechtsonderin zie je nu heel klein drie puntjes (afhankelijk van de kleuren van de foto in je verhaal zijn die vrij onzichtbaar). Druk op deze puntjes en vervolgens op Verwijderen. Je dient je keuze nog eenmaal te bevestigen en daarna is je foto voorgoed verdwenen.

Een tweede optie is door in je foto omhoog te vegen. Er verschijnt dan een scherm waarin je niet alleen kunt zien hoeveel mensen je verhaal hebben bekeken, maar ook eventuele reacties daarop kunt zien. Daarnaast zie je een pictogram met een prullenbak. Je raadt het al: druk op dit pictogram en je foto wordt uit je verhaal verwijderd.



INDEX

...verder op de website oa .....

NIEUWE WERELDWIJDE RANSOMWARE-AANVAL KON VERMEDEN WORDEN

ANDROID-MALWARE DOET ZICH VOOR ALS ADOBE FLASH PLAYER

DUITSE OVERHEID WAARSCHUWT VAKANTIEGANGERS VOOR OPEN WIFI

KASPERSKY-GEBRUIKERS KRIJGEN VAKER MET RANSOMWARE TE MAKEN

CYBERSECURITY MONITOT 2017

FRAUDE MET ONLINE HANDEL

MICROSOFT SPOORT SCAMMERS OP MET KUNSTMATIGE INTELLIGENTIE

LIJST FRAUDULEUZE BEVEILINGSSOFTWARE

POLITIE KRIJGT VOORLICHTING OVER AANGIFTE VAN CYBERCRIME

MINISTER: REGIONALE POLITIE MIST KENNIS CYBERCRIME

.... en meer .....

...verder op de Facebook pagina oa .....

Privacy instellingen; Social media & applicaties

Haal uitgebreide informatie over je systeem naar boven

15 beste gratis apps voor een stressloze vakantie

Maak doorzoekbare scans van teksten met je smartphone

Schakel de automatische proxy-configuratie op je pc uit

Zo reset je een vergeten Windows 10-wachtwoord

7 tips om je laptop koel te houden

Gratis firewall om je netwerk te beschermen

Facebook virus; uitgelegd, voorkomen en verwijderen

.... en meer .....

INDEX

Cops in cyberspace

Kort nadat in München een politieagente in haar hoofd geschoten wordt, verschijnt een tweetvan ene DreiBart. Over een ‘wunderschöne Tag’ en champagne die wordt ontkurkt. ‘Weg mit den Bullendreck’. De hashtag #acab is dan eigenlijk al niet meer nodig, want opvallen doet de tweet toch al. Als vervolgens blijkt dat de account toebehoort aan ene Thomas Goede, nummer tien op de lijst van de Piratenpartij voor de Bundestagverkiezing in Brandenburg, besluit de partij niet aan die verkiezingen mee te doen. ‘Es gilt hier ein Zeichen zu setzen, dass wir Piraten uns deutlich von den Äußerungen eines Listenkandidaten distanzieren’, zegt de partijvoorzitter. ‘Menschenverachtende Bemerkungen müssen Konsequenzen haben’. De politie heeft de tweet in onderzoek, mogelijk volgen nog aanhoudingen.

———————————————————

Drie jaar na de aankondiging gaat september as een nieuw politie-team van startmet het actief opsporen van jihadpropaganda op internet. Het team richt zich op content die valt onder de wetsartikelen opruiing en oproep tot deelname aan de gewapende strijd en moet ‘voorkomen dat mensen op slechte ideeën komen’, zegt NP-woordvoerder Ed Kraszewski. De agenten gaan vooral bij techbedrijven als Google, Twitter en Facebook vragen om bepaalde berichten te verwijderen. De komst van het team was in 2014 al aangekondigd, nog in plannen voor toenmalig minister Ivo Opstelten. Volgens Kraszewski heeft het zo lang geduurd omdat er binnen de overheid afspraken over het speciale team gemaakt moesten worden.
De NOS meldde in dit verband dat Nederland ver achterblijft op landen als Frankrijk, Groot-Brittannië, Rusland en Turkije als het gaat om verwijderverzoeken bij de genoemde techbedrijven. In het eerste halfjaar 2016 deed Nederland slechts veertien verzoeken, waar Rusland er bijna duizend indiende, Frankrijk 165 en Groot-Brittannië 155.

———————————————————-

Met een foto van het Amerikaans pornosterretje Kennedy Leigh, geplukt van een Russische pornosite, probeert een onbekende man (?) foto en filmpjes te krijgen van een 15-jarig meisje uit Hengelo. Moeder Laura (niet haar echte naam) vertelt in het AD hoe deze ‘Marlot Daalhuis’ online te werk gaat. Marlot is zogenaamd fotomodel, heeft op facebook zo’n 1200 vrienden. Of beter: vriendinnetjes, jonge meiden uit het hele land, waaronder al een stuk of zeven van dezelfde school als Laura’s dochter. Ze schrijft Laura’s dochter hoe ze snel geld kan verdienen, ‘minimaal 1422 euro’, en vraagt naar cupmaat en ondergoed, blijkt uit de gepubliceerde chats. Marlot zou werken voor een bureau in België maar is daar natuurlijk onbekend. De profielfoto blijkt gekopieerd en de account is, als Laura’s moeder actie onderneemt, snel verdwenen. Bij de politie vond de moeder echter geen gehoor. Er is nog niks strafbaars gebeurd, er zijn geen naaktfoto’s verstuurd, kreeg ze te horen. Maar ‘vragen naar een cupmaat vind ik al drie stappen te ver’. Volgens politiewoordvoerder Simen Klok wordt er wel degelijk onderzoek gedaan, vanwege het grote aantal kinderen waarmee Marlot contact had.

———————————————————-

In Doesburg hebben politieagenten enkele ‘ramptoeristen’ weggestuurd die bij een auto-ongeluk druk aan het filmen en fotograferen waren. Terwijl de brandweer het slachtoffer uit de auto probeerde te halen, werden de beelden al live gestreamd naar facebook. Agenten dreigden één man zelfs aan te houden als hij nog dichterbij de auto zou komen. Ambulancechauffeur Robert Vreugdenhil ziet dat mensen ‘sensatiebeluster’ zijn geworden en dat zelfs kinderen opnames maken. Hij ziet ook ouders met kinderen op hun arm op de eerste rij staan. ‘Wat is het nut daarvan?’. Overigens verleenden andere omstanders, waaronder een verpleegkundige, eerste hulp.

———————————————————-

Het was een aanslag. En geen hypo of lage bloedsuikerspiegel of wat dan ook. Gewoon een aanslag. Op sociale media zegt ‘een opvallend grote groep mensen’ het zeker te weten: de man die acht mensen aanreed móet wel een terrorist zijn, wat de politie ook zegt. De scepsis en het wantrouwen tegenover de ‘officiële’ verklaring van de politie is er vanaf het begin. Als de politie twittert dat de automobilist onwel geworden is, start een enorme geruchtenstroom. Vooral over het feit dat de man eerder door politieagenten was aangesproken en daarna wegreed. Hoe kan dat, eerst aangesproken worden en dan opeens onwel worden, vroegen velen zich hardop af. Waarna het Grote Complot ontstond: waarom zegt de politie niks over de achtergrond van de man, die lage suikerspiegel komt vast door de ramadan dus is het een moslim, waarom zijn er geen camerabeelden van precies dat deel van het plein waar de auto reed, waarom zijn er Israëlische toeristen onder de slachtoffers, etcetera. ‘Is de politie gek geworden, of wil men dat wij dat zijn’, vroeg schrijver Leon de Winter zelfs. Anderen lachten er hardop om: dus én de politie én de brandweer én de ambu én alle trambestuurders zitten allemaal in het complet? Enfin, volgens politiewoordvoerder Marjolein Koek leek het ‘alsof sommige mensen bijna teleurgesteld waren dat het geen aanslag was’.

———————————————————

Na een waarschuwing van de Kansspelautoriteit hebben meerdere goksites ofwel hun casino gesloten ofwel hun beleid aangepast. Goksites mogen (nog steeds) geen .nl adres hebben, geen Nederlandse betaalmiddelen accepteren en geen ‘typisch Nederlandse’ woorden gebruiken, zoals klompenbingo. De toezichthouder kondigde per 1 juni strengere controles aan en dat werkt kennelijk. Zo stopten Poldercasino, Fortuincasino en Klavercasino al en accepteren andere casino’s sinds twee weken geen nieuwe spelers uit Nederland meer. Woordvoerder Marja Appelman van de Kansspelautoriteit verwacht dat meer casino’s zullen stoppen. Gokbedrijven protesteren maar Appelman zegt ‘gewoon de volgende stap in het bestrijden van illegale online aanbieders’ te nemen. ‘Wij krijgen signalen dat consumenten denken dat online gokken wel legaal is. Door deze actie zijn consumenten beter beschermd’.

———————————————————

De politie heeft drie mannen aangehouden in een onderzoek naar sextortion. De verdachten (twee van 21 uit Tilburg en een van 19 uit Bergen op Zoom) kwamen in beeld toen een vrouw in oktober 2016 aangifte deed van afpersing. Via datingsites zouden de verdachten hun slachtoffers hebben verleid naaktfoto’s te sturen. Vervolgens deden ze zich voor als minderjarig meisje en werden de slachtoffers gechanteerd. Bij huiszoekingen zijn meerdere computers en andere digitale goederen in beslag genomen. De politie zoekt nog naar andere slachtoffers.

———————————————————-

De Europol-website met fragmenten van foto’s van kindermisbruik is een groot succes. De foto’s, nu twintig, tonen geen kinderen maar details uit de omgeving. Gehoopt wordt die herkend worden en dat zo slachtoffers en daders kunnen worden opgespoord. De tips, uit geheel Europa, hebben nog niet tot arrestaties geleid.

INDEX

Rechtspraak

Een echtpaar dat op Marktplaats mediaspelers en 'tv-boxen' verkocht waarop al links stonden naar auteursrechtelijk beschermde inhoud, moet daarmee van de rechter stoppen. De zaak was aangespannen door de Stichting Brein. Er is een schikking getroffen: het echtpaar belooft niet meer te adverteren, van alle voorraad is afstand gedaan. Op de tv-boxen, voor 50 euro te koop, was software geïnstalleerd waarmee gebruikers direct films en tv-series konden downloaden. De zaak was een vervolg op een eerdere actie van Brein tegen het bedrijf Filmspeler. Het Europese Hof bepaalde toen dat de verkoop van zo'n speler ook een 'mededeling aan het publiek' was en dus verboden. Inmiddels zijn er nauwelijks nog verkopers van deze kastjes actief.

———————————————————

De rechtbank Oost-Brabant heeft een man (67, uit Vinkel) veroordeeld tot 21 weken celstraf (waarvan 20 voorwaardelijk), 120 uur taakstraf en verplichte behandeling bij de Forensisch Psychiatrische Polikliniek. Bij de verdachte opa werd 'een flinke hoeveelheid' kinder- en dierenporno gevonden. Met de therapie wil de rechtbank vooral voorkomen dat de man weer naar Thailand of Cambodja gaat, landen waar de man naar eigen zeggen iedere winter komt om seks te hebben.

———————————————————-

De rechter in Den Bosch heeft een man (22, uit Rosmalen) tot drie jaar celstraf veroordeeld voor internetoplichting. De verdachte, een 'oplichter pur sang' aldus het OM, verstuurde phishingmails. Een stuk of twintig mensen trapten daar in en raakten in totaal duizenden euro's kwijt. Bij deze 'grootgebruiker van andermans identiteit' zoals het OM hem noemde, werd onder meer een schoenendoos vol paspoorten en bankpasjes gevonden. De man, die al een jaar vastzit, moet in totaal vierduizend euro schadevergoeding betalen. De straf is conform de eis van het OM.

———————————————————

De rechtbank heeft een man (26, uit Emmeloord) veroordeeld tot anderhalf jaar celstraf (een jaar voorwaardelijk) en opname in een psychiatrische kliniek. De verdachte stuurde zijn ex-vriendin, nadat ze het uitgemaakt had, in twee maanden tijd maar liefst 19 duizend appjes. Meerdere berichtjes bevatten een doodsbedreiging. De man reed verder regelmatig door haar straat, probeerde via haar moeder contact te krijgen en versperde haar een keer de weg. Ook toen bedreigde hij haar. Naar eigen zeggen kwam dat door zijn coke-verslaving. Het OM eiste behalve de celstraf ook tbs maar de rechtbank vond 'tbs-light' voldoende.

———————————————————-

De rechtbank in Utrecht heeft een man (60) veroordeeld tot een (maximale) werkstraf van 240 uur, en contact- en straatverbod en 3000 euro schadevergoeding voor het belagen van zijn ex-vriendin, haar vrienden en familie en haar werkgever. De verdachte stuurde honderden e-mails en andere berichten, maakte een facebookpagina aan namens het slachtoffer en annuleerde zelfs haar vakanties. Ook bekladde hij, met watervaste stiften, haar huis, auto en kliko. De man moet ook het camerasysteem vergoeden dat de vrouw aanschafte om bewijs tegen hem te verzamelen.

———————————————————-

In de VS staat een vrouw terecht voor betrokkenheid bij de zelfdoding van haar vriendje Conrad. Die jongen (18) sms'te intensief met zijn vriendin Michelle over zijn depressie. Toen hij schreef dat hij nog steeds 'vastbesloten' was om zichzelf te doden, sms'te ze terug dat ze blij was dat te horen. 'Het is tijd schatje, dat weet je'. De jongen stierf een paar uur later in zijn met koolstofmonoxide gevulde auto op een parkeerplaats. De rechtszaak tegen Michelle, inmiddels 20, loopt al sinds 2015. Ze is aangeklaagd voor dood door schuld. Uit het smsverkeer, dat nu openbaar is, blijkt volgens de aanklagers dat ze haar vriendje heeft aangemoedigd. 'Je zegt dat je het gaat doen, maar je doet het nooit', schreef Michelle onder meer. 'You just have to do it [..] Tonight is the night. It's now or never'. Michelle kan twintig jaar celstraf krijgen. Haar advocaat stelt dat ze juist heeft geprobeerd om Conrad van zelfdoding te weerhouden. Bovendien, zegt die advocaat, vallen haar sms'jes onder vrijheid van meningsuiting. Dat pleidooi werkte in een eerdere rechtszaak waarin iemand was aangeklaagd voor het aanzetten tot zelfmoord. Die man werd uiteindelijk veroordeeld (tot zes maanden cel) voor hulp bij zelfmoord, een veel lichter delict. De vrouw is inmiddels schuldig bevonden.

———————————————————-

Er komt geen strafzaak tegen de persoon die een foto op facebook zette van de jongen die wordt verdacht van moord op het meisje Savannah uit Bunschoten. 'Dit is de moordenaar van Savannah', schreef de onbekende bij de foto. De ouders van de jongen deden aangifte omdat hun privacy zou zijn geschonden, maar het OM heeft de zaak gesepo-neerd. Aangifte alleen is te weinig voor strafvervolging, aldus het bericht. Maar er werd geen formele klacht ingediend, waardoor de zaak nu afgerond is. De politie zegt 'stevig' gesproken te hebben met de plaatser van het facebook-bericht.

———————————————————-

INDEX

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	

INDEX

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

INDEX

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

INDEX

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.