

Secure Computing Magazine

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

INDEX

Wijziging van het Wetboek van Strafrecht ivm computercriminaliteit (computercriminaliteit III.)

Wijziging van het Wetboek van Strafvordering ivm computercriminaliteit (computercriminaliteit III)

Beoordelingskader grooming

Meer dan driekwart seksueel getinte foto's en berichten worden verstuurd via Snapchat

Nederland zorgt voor veilig e-mailverkeer

1 Miljoen bezoekers voor Veiliginternetten.nl

De cloud stopt niet bij een grens

Security trends tijdens MWC 2017

Avira en Kaspersky beste tools voor verwijderen malware

Politie gaat aanbieders kinderporno op P2P-netwerken waarschuwen

Windows Vista nadert einde ondersteuning

Dit zijn de meest succesvolle phishingmails

Aantal ransomware-families met 752 procent toegenomen

Mag de politie computerreparateurs betalen om te dataspitten?

Kaspersky Lab ontdekt StoneDrill

Cybercriminelen stelen en herwerken gevaarlijke Petya-ransomware

Amazon werkt mee in moordzaak

Kaspersky software updater

Unchecky

AKTUEEL

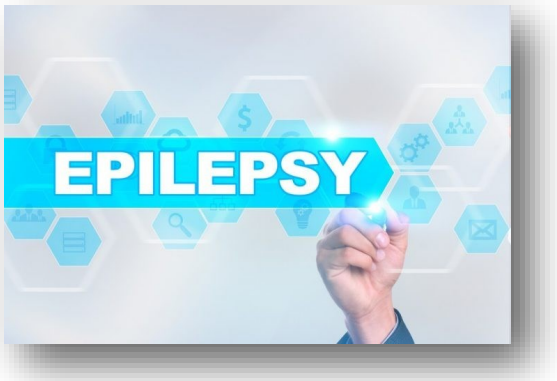
Man opgepakt voor uitlokken epileptische aanval via Twitter

De Amerikaanse autoriteiten hebben een man opgepakt die Twitter zou hebben gebruikt om een epileptische aanval uit te lokken bij een journalist. Het slachtoffer kreeg eind vorig jaar via de berichtendienst een knipperende afbeelding toegestuurd.

Journalist Kurt Eichenwald opende het bericht in december en zag de boodschap ''je verdient een epileptische aanval vanwege je berichten'' en een fel flitslicht. De tweet miste zijn uitwerking niet. Eichenwald kreeg volgens The Washington Post inderdaad een aanval.

Experts verklaarden in de krant ***dat het gaat om een nieuw soort misdrijf, dat qua ernst vergelijkbaar is met het versturen van een bombrief*** of het bewust teweeg brengen van een gevaarlijke allergische reactie.

De opgepakte verdachte, een 29-jarige man uit Salisbury, wordt verdacht van cyberstalking. Voor Eichenwald is de nachtmerrie nog niet achter de rug. Hij stelde dat meer dan veertig mensen hem inmiddels vergelijkbare afbeeldingen hebben gestuurd.



Rubrieken:

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

Wijziging van het Wetboek van Strafrecht ivm computercriminaliteit (computercriminaliteit III.)

(Deze wet treedt in werking op een bij koninklijk besluit te bepalen tijdstip, dat voor de verschillende artikelen of onderdelen daarvan verschillend kan worden vastgesteld.)

Artikel 54a komt te luiden:

Artikel 54a Een tussenpersoon die een communicatiedienst verleent bestaande in de doorgifte of opslag van gegevens die van een ander afkomstig zijn, wordt bij een strafbaar feit dat met gebruikmaking van die dienst wordt begaan als zodanig niet vervolgd indien hij voldoet aan een bevel als bedoeld in artikel 125p van het Wetboek van Strafvordering.

Artikel 80sexies komt te luiden:

Artikel 80sexies Onder geautomatiseerd werk wordt verstaan een inrichting die bestemd is om langs elektronische weg gegevens te verwerken en op te slaan of over te dragen.

Na artikel 138b wordt een artikel toegevoegd, luidende:

Artikel 138c Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft degene die opzettelijk en wederrechtelijk niet-openbare gegevens die zijn opgeslagen door middel van een geautomatiseerd werk, voor zichzelf of voor een ander overneemt.

Artikel 139e komt te luiden:

Artikel 139e Met gevangenisstraf van ten hoogste zes maanden of geldboete van de vierde categorie wordt gestraft degene die, gebruik makende van een technisch hulpmiddel waarvan de aanwezigheid niet op duidelijke wijze kenbaar is gemaakt, opzettelijk en wederrechtelijk van een persoon, aanwezig in een woning of op een andere niet voor het publiek toegankelijke plaats, een afbeelding vervaardigt.

Artikel 139f komt te luiden:

Artikel 139f 1. Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft degene die niet-openbare gegevens: a. verwerft of voorhanden heeft, terwijl hij ten tijde van de verwerving of het voorhanden krijgen van deze gegevens wist of redelijkerwijs had moeten vermoeden dat deze door misdrijf zijn verkregen; b. ter beschikking van een ander stelt, aan een ander bekend maakt of uit winstbejag voorhanden heeft of gebruikt, terwijl hij weet of redelijkerwijs moet vermoeden dat het door misdrijf verkregen gegevens betreft. 2. Niet strafbaar is degene die te goeder trouw heeft kunnen aannemen dat het algemeen belang bekendmaking van de gegevens vereiste.

Artikel 139g vervalt.

Na artikel 184a wordt een artikel ingevoegd, luidende:

Artikel 184b Hij die opzettelijk niet voldoet aan een bevel van de officier van justitie, bedoeld in artikel 125k, vierde lid, van het Wetboek van Strafvordering, wordt gestraft met gevangenisstraf van ten hoogste drie jaren of geldboete van de vierde categorie.

Artikel 273d wordt gewijzigd als volgt:

1. In het eerste lid worden de woorden ‘openbaar telecommunicatienetwerk of openbare telecommunicatiedienst’ vervangen door: openbaar communicatienetwerk of openbare communicatiedienst.
2. In het tweede lid worden de woorden ‘niet-openbaar telecommunicatienetwerk of nietopenbare telecommunicatiedienst’ vervangen door: niet-openbaar communicatienetwerk of niet-openbare communicatiedienst.



Online handelsfraude wordt strafbaar gesteld (art. 326d Sr). Hiermee wordt de mogelijkheid geboden strafrechtelijk op te treden tegen personen die een beroep of gewoonte maken van het aanbieden van goederen of diensten op het internet, zonder de intentie om de goederen of diensten daadwerkelijk te leveren.

Wijziging van het Wetboek van Strafvordering ivm computercriminaliteit (computercriminaliteit III)

In artikel 67, eerste lid, onderdeel b, wordt na “139d, eerste en tweede lid,” ingevoegd: 139f,. (wordt dus een VH-feit)

In Titel IV komt het opschrift van de Zevende afdeling te luiden: ZEVENDE AFDELING Doorzoeking ter vastlegging van gegevens en onderzoek in een geautomatiseerd werk

Na artikel 125j wordt een artikel ingevoegd, luidende: Artikel 125ja > 1. In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, kan de officier van justitie, indien het onderzoek dit dringend vordert, bevelen dat een opsporingsambtenaar als bedoeld in artikel 141, onder b, of een buitengewoon opsporingsambtenaar als bedoeld in artikel 142, eerste lid, onder b, binnendringt in een geautomatiseerd werk of een daarmee in verbinding staande gegevensdrager, bij de verdachte in gebruik, en met een technisch hulpmiddel onderzoek doet met het oog op:

a. het vaststellen van de aanwezigheid van gegevens of het bepalen van de identiteit of locatie van het geautomatiseerde werk of de gebruiker;

b. het overnemen van gegevens die in het geautomatiseerde werk of een daarmee in verbinding staande gegevensdrager zijn verwerkt, of die eerst na het tijdstip van afgifte van het bevel worden verwerkt, voor zover redelijkerwijs nodig om de waarheid aan de dag brengen;

c. de ontoegankelijkmaking van gegevens;

d. een bevel als bedoeld in de artikelen 126l, 126m, 126s, 126t, 126zf of 126zg;

e. een bevel als bedoeld in de artikelen 126g, 126o of 126zd, eerste lid, onder a. In het belang van het onderzoek kunnen gegevens worden vastgelegd.

2. Het bevel, bedoeld in het eerste lid, is schriftelijk en vermeldt:

- a. het misdrijf en indien bekend de naam of anders een zo nauwkeurig mogelijke aanduiding van de verdachte;
- b. de feiten of omstandigheden waaruit blijkt dat de voorwaarden, bedoeld in het eerste lid, zijn vervuld;
- c. een aanduiding van de aard en functionaliteit van het technische hulpmiddel, bedoeld in het eerste lid, dat wordt gebruikt voor de uitvoering van het bevel;
- d. het onderdeel of de onderdelen, genoemd in het eerste lid, met het oog waarop het bevel wordt gegeven;
- e. ten aanzien van welk deel van het geautomatiseerde werk of van de daarmee in verbinding staande gegevensdrager en welke categorie van gegevens aan het bevel uitvoering wordt gegeven.

3. Het bevel, bedoeld in het eerste lid, wordt gegeven voor een periode van ten hoogste vier weken. Het kan telkens voor een periode van ten hoogste vier weken worden verlengd.

4. Het bevel, bedoeld in het eerste lid, kan slechts worden gegeven na schriftelijke machtiging op vordering van de officier van justitie te verlenen door de rechter-commissaris. De machtiging vermeldt de onderdelen van het bevel en de periode waarvoor de machtiging van kracht is.

5. Het bevel, bedoeld in het eerste lid, kan schriftelijk en met redenen omkleed worden gewijzigd, aangevuld, verlengd of beëindigd. Bij dringende noodzaak kunnen de beslissing van de officier van justitie en de machtiging van de rechter-commissaris mondeling worden gegeven. De officier van justitie en de rechter-commissaris stellen deze in dat geval binnen drie dagen op schrift.

6. Bij of krachtens algemene maatregel van bestuur worden regels gesteld omtrent: a. de opslag, verstrekking en plaatsing van het technische hulpmiddel, bedoeld in het eerste lid; b. de technische eisen waaraan het technische hulpmiddel moet voldoen, onder meer met het oog op de onschendbaarheid van de vastgelegde gegevens; c. de vastlegging van gegevens over de uitvoering van het bevel en de werking van het technische hulpmiddel.



Wijziging van het Wetboek van Strafvordering ivm computercriminaliteit (computercriminaliteit III)

Artikel 125k wordt gewijzigd als volgt:

1. In het eerste lid worden de woorden ‘artikel 125i of artikel 125j’ vervangen door: artikel 125i, artikel 125j of artikel 125ja.

2. Het derde lid komt te luiden: Het bevel, bedoeld in het eerste en tweede lid, wordt niet gegeven aan de verdachte behoudens in de gevallen, bepaald in het vierde lid. Artikel 96a, derde lid, is van overeenkomstige toepassing.

3. Er worden vier leden toegevoegd, luidende:

1. In geval van verdenking van een terroristisch misdrijf of het misdrijf, bedoeld in artikel 240b, tweede lid, van het Wetboek van Strafrecht, kan de officier van justitie, indien het onderzoek dit dringend vordert, aan de verdachte het bevel richten toegang te verschaffen tot een geautomatiseerd werk of delen daarvan, tot een gegevensdrager of tot versleutelde gegevens. De officier van justitie geeft het bevel niet dan nadat de verdachte in de gelegenheid is gesteld te worden gehoord. De verdachte is bevoegd zich bij het horen door een raadsman te doen bijstaan.

2. Het bevel, bedoeld in het vierde lid, is schriftelijk en vermeldt: a. het misdrijf en de naam van de verdachte; b. de feiten of omstandigheden waaruit blijkt dat de voorwaarden, bedoeld in het vierde lid, zijn vervuld; c. een zo nauwkeurig mogelijke aanduiding van het geautomatiseerde werk, de gegevensdrager of de te ontsleutelen gegevens en de termijn waarbinnen, alsmede de wijze waarop de toegang dient te worden verschaft.

3. Het bevel, bedoeld in het vierde lid, kan slechts worden gegeven na voorafgaande schriftelijke machtiging, op vordering van de officier van justitie te verlenen door de rechter-commissaris.

4. De verdachte dient gevolg te geven aan het bevel, bedoeld in het vierde lid, door de opsporingsambtenaar toegang te verschaffen tot het geautomatiseerde werk of delen daarvan, de gegevensdrager of tot versleutelde gegevens dan wel door kennis omtrent de beveiliging ter beschikking te stellen.



Na artikel 125o wordt een artikel ingevoegd, luidende: Artikel 125p 1. In geval van verdenking van een strafbaar feit kan de officier van justitie aan een aanbieder van een communicatiedienst het bevel richten om terstond alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om bepaalde gegevens die worden opgeslagen of doorgegeven, ontoegankelijk te maken, voor zover dit noodzakelijk is ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten. De officier van justitie stelt degene tot wie het bevel is gericht in de gelegenheid te worden gehoord. De verdachte is bevoegd zich bij het horen door een raadsman te doen bijstaan. 2. Het bevel, bedoeld in het eerste lid, is schriftelijk en vermeldt:

a. het strafbare feit en indien bekend de naam of anders een zo nauwkeurig mogelijke aanduiding van de verdachte;

b. b. de feiten en omstandigheden waaruit blijkt dat ontoegankelijkmaking van de gegevens noodzakelijk is om het strafbare feit te beëindigen of nieuwe strafbare feiten te voorkomen;

c. c. welke gegevens ontoegankelijk moeten worden gemaakt. 3. Artikel 125o, tweede lid, eerste volzin, is van overeenkomstige toepassing.

Het bevel, bedoeld in het eerste lid, kan slechts worden gegeven na voorafgaande schriftelijke machtiging, op vordering van de officier van justitie te verlenen door de rechter-commissaris.

Wijziging van het Wetboek van Strafvordering ivm computercriminaliteit (computercriminaliteit III)

In de artikelen 126na en 126ua wordt, onder vernummering van het vierde lid tot het vijfde lid, telkens een nieuw vierde lid toegevoegd, luidende: 4. Bij dringende noodzaak kan het bevel mondeling worden gegeven. De opsporingsambtenaar stelt in dat geval het bevel binnen drie dagen op schrift.

Artikel 126zh, tweede lid, komt te luiden: 2. Artikel 126n, tweede tot en met zevende lid, is van overeenkomstige toepassing.

Artikel 126zi, tweede lid, komt te luiden: 2. Artikel 126na, derde tot en met vijfde lid, is van overeenkomstige toepassing.

In artikel 126bb, tweede lid, onderdeel b, wordt de zinsnede “bedoeld in artikel 126m, derde lid, onderdeel c, artikel 126t, derde lid, onderdeel c” vervangen door: bedoeld in artikel 126m, tweede lid, onderdeel c, artikel 126t, tweede lid, onderdeel c.



Aan artikel 354 wordt een lid toegevoegd, luidende: 3. In de gevallen, bedoeld in artikel 353, eerste lid, neemt de rechtbank tevens een beslissing over het bevel, bedoeld in artikel 125p, indien een dergelijk bevel nog niet is opgeheven.

Artikel 552a wordt als volgt gewijzigd:

1. Het eerste lid wordt als volgt gewijzigd:

a. De zinsnede “over de vordering medewerking te verlenen aan het ontsleutelen van gegevens,” wordt vervangen door: over het bevel toegang te verschaffen tot een geautomatiseerd werk of delen daarvan, tot een gegevensdrager of tot versleutelde gegevens dan wel kennis omtrent de beveiliging daarvan ter beschikking te stellen,.

b. Er worden twee volzinnen toegevoegd, luidende: De belanghebbenden kunnen zich voorts schriftelijk beklagen over een bevel tot het ontoegankelijk maken van gegevens, bedoeld in artikel 125p. Over het beklag, bedoeld in de vorige volzin, beslist het gerecht zo spoedig mogelijk.

2. In het derde lid wordt na de zinsnede “ontoegankelijkmaking van de gegevens” ingevoegd: of het bevel, bedoeld in de artikelen 125k en 125p,.

3. In het vierde lid, eerste volzin, wordt na de zinsnede “is geschied” ingevoegd: of het bevel, bedoeld in de artikelen 125k en 125p, is gegeven.

4. Er wordt een lid toegevoegd, luidende: 8. Acht het gerecht het beklag, bedoeld in het eerste lid, tweede volzin, gegrond, dan kan het het bevel geheel of gedeeltelijk opheffen.

Artikel 592, tweede lid, eerste volzin, komt te luiden: De kosten van het nakomen van een vordering tot het verstrekken van gegevens of tot het medewerking verlenen aan het ontsleutelen van gegevens krachtens de artikelen 125k, 126m, 126n, 126na, 126nc tot en met 126ni, 126t, 126u, 126ua, 126uc tot en met 126ui, 126zg, 126zh, 126zi en 126zja tot en met 126zp kunnen de betrokkene uit ’s Rijks kas worden vergoed.

Beoordelingskader grooming

Grooming is strafbaar gesteld in artikel 248e Wetboek van Strafrecht (Sr.):

"Hij die door middel van een geautomatiseerd werk of met gebruikmaking van een communicatiedienst een persoon van wie hij weet of redelijkerwijs moet vermoeden dat deze de leeftijd van zestien jaren nog niet heeft bereikt, een ontmoeting voorstelt met het oogmerk ontuchtige handelingen met die persoon te plegen of een afbeelding van een seksuele gedraging waarbij die persoon is betrokken, te vervaardigen wordt, indien hij enige handeling onderneemt gericht op het verwezenlijken van die ontmoeting, gestraft met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie"

Ontmoeting

Bij grooming staat de ontmoeting centraal. Het door middel van een geautomatiseerd werk of met gebruikmaking van een communicatiedienst communiceren met een minderjarige, is niet strafbaar, ook niet als de inhoud van het gesprek een ontuchtige toonzetting had. De strafbaarheid ontstaat pas wanneer de verdachte een voorstel tot een ontmoeting doet en daaraan een uitvoeringshandeling verbindt. Causaal verband tussen de voorafgaande communicatie en het voorstel annex uitvoeringshandeling is vereist.



De ontmoeting moet strekken tot het verrichten/ondergaan van seksuele handelingen en/of het vervaardigen van een afbeelding daarvan. Niet is vereist dat de seksuele handelingen daadwerkelijk hebben plaatsgevonden, of dat er sprake is geweest van een begin van uitvoering. Als dat wel het geval is geweest, dan is er vaak samenloop met andere strafbare feiten zoals verkrachting, etc.

De verdachte moet willens en wetens een voorstel tot een ontmoeting hebben gedaan, gevolgd door een op de verwezenlijking van die ontmoeting gerichte uitvoeringshandeling. Het voorstel tot de ontmoeting moet zich kenmerken door een zekere vastheid. Het voorstel tot de ontmoeting moet zijn gevolgd door een handeling gericht op het realiseren van de ontmoeting, oftewel een concrete uitvoeringshandeling. Voorbeelden van uitvoeringshandelingen zijn: het zich begeven naar een afgesproken plek, het voorzien van het slachtoffer van een routebeschrijving naar de afgesproken plek, het kopen van treinkaartjes of toegangsbewijzen.

De tijd en datum voor de ontmoeting hoeft niet concreet vast te staan om te komen tot grooming, maar omdat wel een uitvoeringshandeling wordt vereist, moet de voorgenomen ontmoeting vaak wel concreet worden (vlg o.a. rechtbank 's-Hertogenbosch, 28 december 2011, LJN: BU9341).

Ontuchtige handelingen

Van grooming is alleen sprake wanneer het minderjarige slachtoffer wordt bewogen tot het plegen van seksuele handelingen die in strijd zijn met de sociaal-ethische norm. Wanneer het gaat om voorstellen tot seksuele contacten tussen minderjarigen onderling, en er ook sprake is van instemming, is er uiteraard geen sprake van grooming.

Leeftijd: jonger dan 16 jaar

Alleen wanneer het voorstel tot de ontmoeting wordt gedaan aan een minderjarige, jonger dan 16 jaar is er sprake van grooming. Bewezen moet worden dat de verdachte had moeten weten dat de minderjarige de leeftijd van 16 jaar nog niet had bereikt. Hij moet voorwaardelijk opzet hebben gehad op de leeftijd. Wanneer de verdachte de aanmerkelijke kans op de koop heeft toegenomen dat de persoon aan wie hij het voorstel tot de ontmoeting heeft gedaan jonger kan zijn dan 16 jaar, is dit voldoende voor grooming.

Meer dan driekwart seksueel getinte foto's en berichten worden verstuurd via Snapchat

Snapchat is het sexting-medium onder Nederlandse jongeren. Dit blijkt uit recent onderzoek onder jongeren van 12 tot 17 jaar in het kader van Safer Internet Day (7 februari). Maar liefst 76,1% van de naaktfoto's of foto's in ondergoed wordt verstuurd via dit medium. Ook WhatsApp (47,8%) en Facebook (9%) zijn populair. Dat dit soort beelden het vaakst worden gepost op Snapchat is niet geheel verwonderlijk, want jongeren zien Snapchat als het meest persoonlijke sociale netwerk. Foto's worden op Snapchat niet automatisch op internet opgeslagen, waardoor het medium onterecht veilig lijkt voor sexting. Meisjes doen iets vaker aan sexting dan jongens.

Bijna een kwart (23%) heeft wel eens een naaktfoto of foto in ondergoed ontvangen. Meisjes ontvangen vaker 'sexts' (24,5%) dan jongens (21,6%). Zij doen zelf ook iets vaker aan sexting: 7,1% van de meisjes tegenover 5,5% van de jongens tussen 12 en 17 jaar heeft wel eens een naaktfoto of foto in ondergoed naar iemand gestuurd.

Praten helpt

Uit het onderzoek dat de Universiteit van Amsterdam in opdracht van Kliksafe uitvoerde blijkt dat ouders veruit de belangrijkste informatiebron (77,2%) voor jongeren zijn als het gaat om online risico's. "Als er thuis veel over het onderwerp wordt gesproken, werkt dat risico-verlagend," zegt Bert Jan Peters, directeur van Kliksafe. "Hierbij blijken vragend en belangstellend informeren ("Vertel eens…") en een wederzijds gesprek (samen afspraken maken) aanmerkelijk beter te werken dan eenrichtingsverkeer (met opdrachten en preken) en onderhandelen ("Als jij dit doet, mag je dat")". De meerderheid van de ouders kiest voor de constructieve eerste twee manieren van communiceren.

"Vooral onder jongeren in de leeftijd 12 tot 17 jaar kan sexting voor grote problemen zorgen," zegt Marjolijn Bonthuis, Safer Internet Centre Nederland. *"Dat Snapchat zo populair is, komt mede doordat de gebruikers denken dat hun foto of bericht binnen no-time verdwenen is. Uit Snapchat misschien, maar daarbij wordt vaak vergeten dat een screenshot snel gemaakt én verspreid is. Zo kan een pikante foto die je voor je vriend of vriendin maakte je nog jaren blijven achtervolgen".*

In Nederland bespreekt 93% van de ouders het internetgedrag van hun kind(eren) en 65,1% heeft het specifiek over sexting. Na roken geven ouders over dit onderwerp de meeste voorlichting.

Sexting is dom

De bewustwording van het risico op verspreiding van 'sexts' is aanzienlijk toegenomen. Uit de nieuwe cijfers blijkt dat 9 op de 10 jongeren verwacht dat de beelden verder verspreid worden, terwijl 64% dat zeker weet. Vorig jaar wist slechts 10% dit zeker.

Volgens driekwart van de jongeren (74,5%) sturen leeftijdsgenoten seksueel getinte foto's vooral door naar anderen om zelf cooler of populairder te lijken. Maar ruim de helft van de jongeren (52,2%) vindt leeftijdsgenoten die aan sexting doen dom. Tegelijkertijd is het niet zo dat een jongere van wie een pikante foto circuleert altijd wordt verstoten door zijn of haar vrienden. In tegendeel, jongeren steunen elkaar. Bijna 7 op de 10 jongeren geeft aan dat hun vrienden op hun steun kunnen rekenen als er een naaktfoto van hen op internet zou circuleren.



Nederland zorgt voor veilig e-mailverkeer

Bedrijfsleven, brancheorganisaties en overheid gaan gezamenlijk misbruik zoals phishing en het afluisteren van e-mail aanpakken. Daartoe hebben zij met steun van het ministerie van Economische Zaken de 'Veilige E-mail Coalitie' opgericht.

In de coalitie nemen de volgen partijen deel: PostNL, KPN, Betaalvereniging Nederland, DDMA, Thuiswinkel.org, VNO-NCW, MKB-Nederland, Stichting Zeker-OnLine, Dutch Datacenter Association, Stichting DINL, XS4ALL, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (Rijks-CIO), Fraudehelpdesk, Nederland ICT en de Belastingdienst. De deelnemers aan de 'Veilige E-Mail Coalitie' gaan binnen hun organisaties aan de slag met het invoeren van maatregelen voor het beveiligen van e-mailverkeer. Daarvoor wordt gebruik gemaakt van gezamenlijk vastgestelde standaarden.



Op die manier kan zowel phishing als het afluisteren van e-mail worden tegengegaan. Daarnaast gaan zij het gebruik van e-mailbeveiliging verder versnellen door onderlinge kennisdeling en promotie. De betrokken partijen nodigen andere bedrijven en overheden uit om zich aan te sluiten en gebruik te maken van de kennis binnen de coalitie. Marcel Krom, CIO bij PostNL: "We zijn zelf vergevorderd met de implementatie van de moderne e-mailbeveiligingsstandaarden. Maar we realiseren ons dat alle partijen in het mail-ecosysteem mee moeten doen om het echt te laten werken. Daarom sluiten we graag aan bij de coalitie."

E-mail populair maar ook kwetsbaar
E-mail is een zeer veel gebruikt communicatiemiddel. Miljoenen Nederlanders verzenden en ontvangen dagelijks samen tientallen miljoenen e-mailberichten. Onveilige e-mail zorgt helaas dagelijks voor misbruik en schade. Gelukkig kan e-mail veiliger. Daarvoor is het wel belangrijk dat verzenders en ontvangers in de gehele keten moderne beveiligingsmaatregelen en daarbij behorende standaarden toepassen. Steeds meer partijen doen dat al.

De standaarden waar de 'Veilige E-mail Coalitie' voor staat, zorgen ervoor dat internetcriminelen niet zomaar uit naam van andermans e-mailadres phishingmails kunnen versturen. Daarnaast helpen ze om het afluisteren van bedrijfs- en privacy-gevoelige informatie in e-mails te voorkomen. Door het open karakter van deze standaarden zijn die voor alle organisaties beschikbaar.

1 Miljoen bezoekers voor Veiliginternetten.nl

Dat Veiliginternetten.nl in 2016 ruim 1 miljoen unieke bezoekers heeft getrokken, is een mooie mijlpaal, twee jaar na de lancering, maar vooral een teken dat steeds meer mensen actief werk maken van veilig internetten. Ook het rapportcijfer van een 7,5 is bovengemiddeld goed voor een website.

Dit betekent niet dat 2017 een rustig jaar zal worden. De redactie blijft doorlopend werken aan het verbeteren en updaten van de content en het brengen van nieuws in relatie tot praktische stap-voor-stap uitleg.

Met een eigen startpagina en specifieke content, afgestemd op wat ondernemers kunnen doen en laten om veilig te internetten, heeft het MKB (en andere zakelijke gebruikers) medio 2016 een eigen én herkenbare plek gekregen op de website: www.veiliginternetten.nl/zakelijk.

De cloud stopt niet bij een grens

De keurmerken Zeker-OnLine (Nederland), Label Cloud (Frankrijk) en Trusted Cloud (Duitsland) hebben een overeenkomst getekend voor samenwerking om MKB'ers in Europa zekerheid te geven over de kwaliteit en betrouwbaarheid van online diensten. De samenwerking is getekend op de tweede Frans-Duitse conferentie over digitale economie in Berlijn.
De keurmerken stellen de betrouwbaarheid van cloudapplicaties in Nederland, Frankrijk en Duitsland vast. Samen met de Europese Commissie werken deze landen aan Europese harmonisatie van eisen aan online diensten.

Voor welk probleem, een oplossing?

Het gebruik van cloudtechnologieën en big data biedt aanzienlijke kansen voor ondernemers ten aanzien van productiviteit en flexibiliteit. Daarnaast versterkt deze technologie het innovatie- en het concurrentievermogen van ondernemers. Met name bij kleine en middelgrote ondernemingen zijn er vaak nog aarzelingen om gebruik te maken van cloudtechnologieën omdat de data daadwerkelijk wordt overgedragen en de gebruiker een sterke afhankelijkheid creëert van een cloudleverancier. De belangrijkste vragen van ondernemers hebben betrekking op de veiligheid van de infrastructuur, de bescherming van persoonsgegevens, de naleving van de wet en regelgeving, continuïteit en beschikbaarheid van de dienst maar ook vragen over de inbedding van cloudapplicaties in de totale IT-systeem van een bedrijf. De antwoorden en garanties op deze vragen zijn vaak moeilijk te krijgen.
De MKB'er heeft over het algemeen zelf niet de kennis en toegang om een cloudprovider op deze elementen te beoordelen. Dit betekent dat er een risico bestaat dat deze bedrijven hun concurrentiepositie op de internationale markt verliezen. Dit is de reden waarom de Europese Commissie en de overheden het gebruik van cloudtechnologieën onder het MKB promoten. Er is vanuit de Europese Commissie dan ook uitdrukkelijk voor gepleit om vanuit de drie keurmerken tot harmonisatie te komen.



Keurmerken Trusted Cloud, Label Cloud en Zeker-OnLine

De drie keurmerken hebben gemeen dat ze de betrouwbaarheid vaststellen van cloudapplicaties voor cloudleveranciers in Nederland, Frankrijk en Duitsland. De wereldwijde cloud computing-markt ontwikkelt zich snel. In Frankrijk, Nederland, Duitsland en Oostenrijk en Zwitserland zijn er nationale initiatieven voor de ontwikkeling van standaarden en certificaten/labels voor het gebruik van cloudtechnologieën. De drie keurmerken delen het uitgangspunt dat ondernemingen en gebruikers bij uitbesteding van activiteiten naar de cloud erop moeten kunnen vertrouwen dat de cloudleverancier handelt in het belang van de ondernemer en zorg draagt voor een betrouwbare dienst. Daarbij maken alle drie de keurmerken gebruik van:

Een openbaar normenkader

Onafhankelijk toezicht op toekennen van keurmerken

Minimale eisen ten aanzien van de betrouwbaarheid van de infrastructuur en applicatie

Principes en best practices voor het bepalen van noodzakelijke maatregelen.

Bron: Zeker-Online

Eugene Kaspersky schetst security trends tijdens MWC 2017

Eugene Kaspersky van het gelijknamige securitybedrijf wil dat we als maatschappij de lat hoger leggen voor security. Maar de realiteit is dat we volgens hem te weinig mensen hebben.

Het was een donkere maar toch amusante uiteenzetting van de Russische securityexpert op MWC. "Alle systemen zijn kwetsbaar", gevolgd door een slide met aanvallen uit 2016: 448 miljoen voor Windows en 22 miljoen voor Android. Maar ook Macs kregen 40.000 aanvallen te verwerken en Linux zo'n 30.000. iOS lijkt het onaantastbaarst, zeker in verhouding tot het aantal toestellen: 600 op een jaar tijd. "Veel mensen denken dat ze veilig zijn op een Mac, maar dat is fout. Waarom zijn er minder aanvallen op Macs? Omdat het moeilijk is om Mac engineers te vinden (die malware of andere aanvallen kunnen ontwikkelen).

Maar Kaspersky komt hier niet praten over de dingen waarvan we weten dat ze gehackt worden. Hij heeft het over het stroomnetwerk. "In 2003 was er een enorme black-out in het Noordoosten van de VS. Het was geen hacking, maar plots kon niemand het netwerk controleren, want ook de communicatie met de systemen werkte niet meer omdat ze zich hadden uitgeschakeld uit zelfbescherming."

"Maar in 2016 was er wel een cyberaanval op een stroomnetwerk, dat van Oekraïne. Hackers kregen controle over de systemen. Weet je wat dat betekent? Geen liften, geen internet, geen mobiele netwerken. Dit soort scenario's bestaan. We leven in een wereld gebaseerd op systemen die veertig tot vijftig jaar geleden zijn ontwikkeld, toen er nog geen hackers bestonden."

"Ik droom van een wereld met systemen die niet onhackbaar zijn. Maar de realiteit is dat we daarvoor alles moeten aanpassen. En eerlijk gezegd, daar hebben we niet genoeg mensen voor. We hebben te weinig securityingenieurs in de wereld. Zeg dus gerust tegen je kinderen dat ze securityingenieur moeten worden. Ze zullen weinig vakantie hebben, maar veel geld verdienen. En dan kunnen ze meteen voor mij komen werken", aldus een geanimeerde Eugene Kaspersky.



Maar onder de entertainende toon gepaard met een sappig Russisch accent zit wel een ernstige kern: onze maatschappij steunt verder op systemen die weliswaar hun stabiliteit hebben bewezen, maar zijn ontwikkeld in een tijd voor het internet en voor je van buitenaf kritieke infrastructuur kon beheren.

Die technologie grondig aanpassen kost tijd, geld en mensen. Mensen zijn er niet genoeg, en in praktijk zullen veel dingen niet worden aangepast tot er effectief een veiligheidsprobleem opduikt. In een wereld waar bepaalde landen of groeperingen hun hand er niet voor omdraaien om een ander land te bestoken met gerichte hacks of grootschalige aanvallen, brengt Kaspersky een boodschap met stof tot nadenken.

Avira en Kaspersky beste tools voor verwijderen malware

In het geval een Windowscomputer met malware besmet raakt kan er het beste software van Avira of Kaspersky Lab worden gebruikt om de infectie te verwijderen, zo blijkt uit een nieuwe test van het Duitse testlab AV-Test. Gedurende een periode van 12 maanden werden 8 virusscanners en 7 speciale verwijdertools met tientallen echte infecties getest. Alleen Avira en de Kaspersky Virus Removal Tool scoorden 100 procent.

De virusscanners werden op twee manieren getest. De eerste keer werden ze al op een besmette computer geïnstalleerd. Bij de tweede test waren ze al op de computer actief, maar werden ze tijdelijk uitgeschakeld om de malware te installeren, en daarna weer ingeschakeld. Vervolgens werd er gekeken of de malware het verwijderen voorkwam, of er actieve malware-onderdelen niet door de virusscanner werden verwijderd, of er onschuldige bestanden achterbleven en als laatste of de malware echt volledig werd verwijderd en het systeem hersteld.

Avira scoort zoals gezegd 100 procent, op de voet gevolgd door Kaspersky en Malwarebytes. De twee scanners laten elk een onschuldig bestand van de malware-infectie achter, waardoor ze net naast de eerste plek grijpen. Helemaal onderaan eindigt Microsoft Security Essentials. De virusscanner weet uiteindelijk 68 van de 78 gebruikte malware-exemplaren te verwijderen. In vier gevallen weet de malware het verwijderen te voorkomen en in vier andere gevallen worden de actieve malware-onderdelen niet door Security Essentials verwijderd.

Bron: Eugene Kaspersky / AV-Test

Politie gaat aanbieders kinderporno op P2P-netwerken waarschuwen

Europese politiediensten gaan in samenwerking met Europol de aanbieders van kinderporno op peer-to-peer (P2P) netwerken waarschuwen, zo heeft Europol vandaag bekendgemaakt. Volgens Europol spelen dergelijke netwerken een zeer belangrijke rol bij het verspreiden van kinderporno.

De opsporingsdienst richtte zich dan ook op de aanbieders op deze netwerken, wat tot aanhoudingen en veroordelingen leidde. "Hoewel deze aanpak een positieve impact had om de dreiging te verminderen en het aantal vervolgingen te vergroten, wordt kinderporno nog steeds op internet benaderd", stelt Europol. Het nu aangekondigde Police2Peer-initiatief moet misbruik voorkomen en ervoor zorgen dat overtreders begrijpen dat ze met de politie te maken zullen krijgen.

Hiervoor gaat de politie zelf bestanden aanbieden die op kinderporno lijken en van een ander persoon met dezelfde interesses afkomstig lijken. Het gaat echter niet om een afbeelding, maar een waarschuwing van de politie. De waarschuwing wijst de persoon in kwestie op zijn handelen en geeft advies hoe hij of zij hulp kan zoeken. "Als iemand begint met het downloaden van wat kinderporno lijkt te zijn of illegale bestanden zelf op het netwerk beschikbaar gemaakt, zullen we onze bestanden met hen delen", aldus Europol.

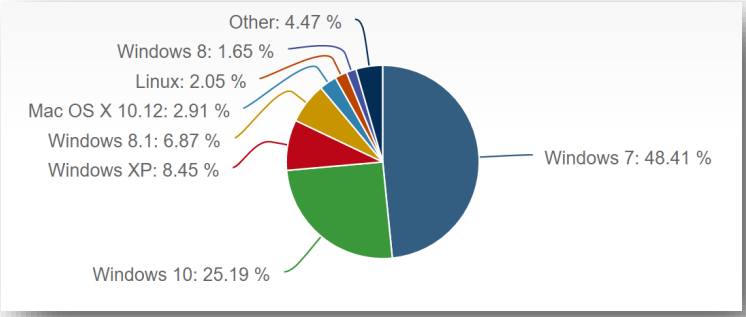
"Op deze manier maken we het glashelder dat deze netwerken geen schuilplaats zijn voor mensen die kinderen misbruiken. ze kunnen elke keer dat ze dit soort materiaal uploaden politie tegenkomen", zegt Bjorn-Erik Ludvigsen van de Noorse politie en leider van het initiatief. Naast de waarschuwingen is er ook een website online verschenen waar mensen hulp kunnen vinden. Europol benadrukt dat het geen informatie over bezoekers van de website voor onderzoeken zal gebruiken.

Windows Vista nadert einde ondersteuning

Op 11 april 2017 zet Microsoft de ondersteuning voor Windows Vista stop. Dat betekent dat het 10 jaar oude besturingssysteem vanaf dan niet langer updates zal ontvangen. Vista was de opvolger van het immens populaire Windows XP, maar had het bijzonder moeilijk om de grote schoenen van zijn voorganger te vullen.

Het OS werd geplaagd door bugs, onvolledige features en trage prestaties, waardoor veel gebruikers bleven vasthouden aan XP. Volgens de recentste cijfers van NetMarketShare heeft Windows Vista vandaag nog een wereldwijd marktaandeel van 0,78% ten opzichte van 8,45% voor Windows XP, hoewel de ondersteuning voor dat systeem al in 2014 werd stopgezet.

U wordt dus aangeraden over te stappen naar een meer recent besturingssysteem.



Dit zijn de meest succesvolle phishingmails

Het is nog steeds veel te gemakkelijk om werknemers erin te luizen met een phishingaanval. Dat stelde beveiligingsbedrijf MWR Infosecurity vast. Het bedrijf simuleerde 100 phishing-campagnes bij 48 grote bedrijven, in totaal goed voor één miljoen gebruikers. De resultaten zijn ontluisterend: als een phisher zijn strategie goed heeft uitgekiend, kan hij ruim één op de tien overhalen om niet alleen zijn gebruikersnaam en wachtwoord in te voeren, maar eveneens om een bestand te downloaden.

Een bedrijfsnetwerk is maar zo sterk als zijn zwakste schakel. Indien een hacker erin slaagt om ransomware op een enkel toestel te krijgen binnen een bedrijf, kan dat voldoende zijn om het hele netwerk op de knieën te krijgen. Bij de grote bedrijven uit de studie zou dat neerkomen op een fikse rekening aan losgeld.

Uit het onderzoek blijkt dat de risico's het kleinst zijn bij het ontvangen van een factuur. Voldoende mensen blijken een kwaadwillige e-mail met vervalste factuur te herkennen, zelfs wanneer die van een ander e-mailadres binnen het bedrijf komt. Dat betekent voornamelijk dat gebruikers niet snel geneigd zijn om een verdacht bestand te downloaden dat rechtstreeks in hun inbox terechtkomt. 5 op 1000 werknemers openden uiteindelijk het bestand.

Wanneer het bestand echter wordt aangereikt via een externe pagina, liggen de kaarten anders. Wie uitgenodigd wordt door zijn IT-helpdesk om zijn gegevens na te kijken voor de migratie naar een andere e-maildienst (het bedrijf zou zogezegd overstappen), ziet er blijkbaar geen graten in om zijn gegevens te verstrekken en een bestand te downloaden. 79 op 1000 werknemers openden een bestand.

Wanneer de HR-afdeling een beoordelingssysteem rondstuurt, strandt het aantal gedupeerden op 94 werknemers die een verdacht bestand openden. Voor een kortingsbon waren dat 104 werknemers. De winnaar was echter een vriendschapsverzoek voor een sociaal medium. 99 werknemers openden uiteindelijk een verdacht bestand. Het cijfer ligt lager dan bij de kortingsbon, maar het aantal mensen dat op de link naar de externe webpagina klikte, lag hier het hoogst. Vaak is dat voor een gerichte hack voldoende om een computer te injecteren met malware. MWR laat verder optekenen dat slechts drie procent van alle gecontacteerde werknemers de (gesimuleerde) aanvallen rapporteerde. Niet alleen zijn werknemers dus te weinig bezig met veiligheidscontroles wanneer ze e-mails ontvangen, ze laten eveneens na om anderen op de hoogte te brengen.

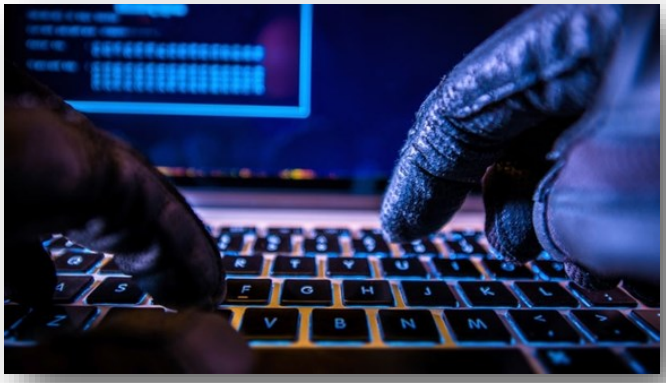
Het viel MWR overigens op dat er zelfs flagrante fouten in een e-mail of op een webpagina mogen staan, zonder dat deze een belletje doen rinkelen. Zo kwam het in de simulaties regelmatig voor dat een e-mailadres slechts vaagweg leek op het officiële domein van het bedrijf, of werd de naam van het bedrijf verkeerd geschreven.

Ten slotte merkte MWR op dat wachtwoordhygiëne nog te vaak wordt achterwege gelaten. 60 procent van de gebruikers volgde exact de minimumvereisten die een bedrijf vooropzette. Dat betekent dat gebruikers slechts het absolute minimum doen om een veilig wachtwoord in te stellen. Bovendien bevatte 13,6 procent van alle wachtwoorden een cijfercombinatie tussen 1940 en 2040. Daarvan eindigde maar liefst de helft op 2016, het jaar waarin het wachtwoord werd aangemaakt.

Lure	Example	% clicked	Of those, % who then provided credentials	Of those, % who then downloaded a file
Financial	Invoice download	10.17	34.40	16.76
Technology	Secure email	14.17	65.02	81.13
Human resources	Appraisal system	18.21	73.86	72.43
Promotional	Discount voucher	19.46	63.26	87.19
Social media	Connection request	23.83	54.23	80.85

Bron: MWR Infosecurity

Aantal ransomware-families met 752 procent toegenomen



Antivirusbedrijf Trend Micro merkte in 2016 een enorme stijging (752 procent) in het aantal ransomware-families op ten opzichte van het jaar ervoor. Dat is ook niet zo vreemd, want het is een lucratieve business.

In 2015 merkte Trend Micro nog 29 ransomware-families op. In 2016 waren dat er al 247. Met name bedrijven zijn daarbij een gewild doelwit. Cybercriminelen haalden er vorig jaar 1 miljard dollar mee binnen.

Van de 81 miljard malware-besmettingen kwam 75 miljard binnen via malafide e-mails. Eerder toonde Kaspersky ook al aan dat er vorig jaar meer phishing -aanvallen plaatsvonden. De kans op een virus is dus het grootst via besmette mailtjes.

Kwetsbaarheden

Trend Micro ontdekte daarnaast ook nog honderden kwetsbaarheden in besturingssystemen en software. Daarbij viel op dat het aantal lekken in Microsoft-producten behoorlijk terugliep, van circa 180 in 2015 naar 90 in 2016.

Bij Apple- en Android-producten steeg het aantal ontdekte kwetsbaarheden juist.

Groot fraudebotnet in Android-reclames ontdekt

Het fraudebotnet Chamois misleidde gebruikers om ze op advertenties in Android te laten klikken. Hierdoor werden er apps geïnstalleerd en sms'jes verzonden.

Chamois werd ontdekt door Google, dat inmiddels maatregelen heeft getroffen om het netwerk te blokkeren. Volgens de zoekgigant is Chamois één van de grootste botnets in zijn soort.

Het botnet gebruikt misleidende afbeeldingen in advertenties, om ervoor te zorgen dat gebruikers hierop zouden tikken. Hierdoor worden er pop-ups geopend waardoor bepaalde sites onrechtmatig bezoekverkeer krijgen.



Bij het aantikken van de advertenties kan er ook een app worden geïnstalleerd zonder dat het slachtoffer hier toestemming voor geeft. Daarnaast verzendt Chamois soms sms-berichten naar betaaldiensten, waardoor er geld bij het slachtoffer wordt afgeschreven.

Chamois werd ontdekt door Google tijdens een routinecontrole, waarna de apps met deze advertenties door Google werden geblokkeerd.

Volgens Google gebruikt Chamois meer dan 100.000 regels aan code, die afkomstig lijkt te zijn van professionele ontwikkelaars.

Mag de politie computerreparateurs betalen om te dataspitten?

De Amerikaanse FBI zou sinds 2007 medewerkers van de Geek Squad, een computerreparatiedienst van elektronicaketen Best Buy, betaald hebben om als informanten te dienen. Dat meldde Tweakers onlangs. De reparateurs spitten door binnengebrachte computers heen op zoek naar bijvoorbeeld kinderporno. De truc daarachter zou zijn dat de reparateurs dat kunnen zonder gerechtelijk bevel of zelfs maar verdenking, en dat die dan daarna een aangifte doen dat wél grond is voor een verdenking en juridische actie. Hoe zou dat in Nederland uitpakken?



Ook bij ons geldt natuurlijk dat de politie niet zomaar in computers mag snuffelen. Een officier van justitie zou bevel geven tot doorzoeking, en meestal is daarvoor toestemming van de rechter-commissaris nodig. Dat vereist al een stevige verdenking van een misdrijf, op de bonnefooi eens gaan zoeken is niet toegestaan.

Privépersonen zijn niet aan die regels gebonden. Als een reparateur dus bij herstelwerk iets strafbaars aantreft, dan is hij bevoegd daar aangifte van te doen. Hij heeft geen toestemming nodig van een overheidsinstantie om te zoeken naar strafbare informatie of om aangifte te mogen doen.

Het maakt zelfs niet uit of de reparateur toestemming van de eigenaar had om op die plek te gaan zoeken. Snuffelen zonder grondslag kan een probleem zijn – contractbreuk, misschien zelfs computervredebreuk – maar dat maakt het aldus verkregen bewijsmateriaal niet onbruikbaar voor Justitie. In theorie zou de reparateur dan vervolgd worden voor die computervredebreuk, parallel aan de rechtszaak tegen de eigenaar voor hetgeen dat er gevonden is middels die computervredebreuk.

Het punt is hier alleen wel: dit is niet zomaar wat tegenkomen, of zelfs maar snuffelen uit nieuwsgierigheid en wat tegenkomen. Dit is werken in opdracht van de politie. En dán val je ook als burger onder die regels voor de politie. Bewijs dat uit zo'n betaalde snuffelopdracht komt, is dus onbruikbaar bij ons.

Kaspersky Lab ontdekt StoneDrill



Het Global Research & Analysis Team van Kaspersky Lab heeft nieuwe geavanceerde wiper-malware ontdekt, genaamd StoneDrill. Net als Shamoon, een andere beruchte wiper, vernietigt StoneDrill alles op de geïnfecteerde computer. Daarnaast heeft StoneDrill geavanceerde anti-detectietechnieken en spionagehulpmiddelen in zijn arsenaal. Naast doelen in het Midden-Oosten is nu ook een StoneDrill-doelwit ontdekt in Europa. Dit terwijl in het Midden-Oosten gebruikte wipers eerder niet in het wild werden ontdekt.

StoneDrill – een wiper met connecties
Het is nog niet bekend hoe StoneDrill wordt overgedragen, maar eenmaal aanwezig op de aangevallen machine injecteert het zichzelf in het geheugenproces van de voorkeursbrowser van de gebruiker. Tijdens dit proces gebruikt het twee geavanceerde anti-emulatietechnieken, gericht op het misleiden van beveiligingsoplossing die op de machine van het slachtoffer is geïnstalleerd. De malware begint vervolgens bestanden op de schijf van de computer te vernietigen. Tot dusverre werden ten minste twee doelwitten van de StoneDrill wiper geïdentificeerd, één in het Midden-Oosten en de andere in Europa.

Bron: Arnoud Engelfriet / Kaspersky

Cybercriminelen stelen en herwerken gevaarlijke Petya-ransomware

Een groep cybercriminelen gebruikt de Petya-ransomware om geld af te troggelen van slachtoffers, maar vermomt de malware zodat ze de originele bedenkers niets moeten betalen.

Ransomware wordt vaak verspreid volgens een 'as-a-service'-model. Cyberciminelen kunnen kant-en-klaarpakketten aanschaffen waarmee ze de ransomware meteen kunnen gebruiken om de toestellen van slachtoffers te besmetten en te versleutelen. In ruil voor het gebruik van de malware, krijgen de originele bedenkers van de code een percentje van de winst. De uitvinders van de beruchte Petya-ransomware kunnen echter naar hun geld fluiten: een groep criminelen heeft een manier bedacht om de code achter de ransomware aan te passen, en gebruikt het cyberwapen zonder te betalen. Door de aanpassingen wordt de nieuwe vorm van de malware bovendien niet herkend door beveiligingssystemen, meldt Kaspersky Lab die de ransomware het eerst op het spoor kwam.

PetrWrap wordt de nieuwe vorm van ransomware gedoopt. Voor de slachtoffers die met de malware besmet worden, is er weinig verschil in resultaat. Het toestel in kwestie zal crashen, en tijdens het herstartproces wordt de toegang tot de harde schijf van het apparaat versleuteld. De criminelen hebben wel de moeite genomen om verwijzingen naar de originele ransomware te verwijderen. Zo zien slachtoffers niet meer de kenmerkende, flitsende schedel verschijnen, en wordt ook de naam Petya nergens vermeld in de instructies op het scherm.

Om de originele Petya-ransomware te verhullen, en de versie te gebruiken zonder te betalen aan de bedenkers, creëerden de criminelen een "speciale module" die de ransomware à la minute kan patchen. "Dat is wat de nieuwe malware zo uniek maakt," schrijven cybersecurity-analisten bij Kaspersky Lab. PetrWrap dwingt de Petya-malware om anderhalf uur te wachten voor de uitvoering, waarna de code tijdens het lanceren wordt aangepast. De patch zorgt er onder andere voor dat de criminelen niet bij de Petya-eigenaars moeten aankloppen om de decryptiesleutels te genereren.

Een decryptietool die slachtoffers kan helpen is voorlopig niet aan de orde, laat Kaspersky weten. Slachtoffers kunnen wel proberen om bestanden te herstellen met andere hulpmiddelen, zoals R-studio.

Amazon werkt mee in moordzaak

Internetgigant Amazon heeft, na een aanvankelijke weigering, beloofd mee te werken met een moordonderzoek in Arkansas, VS. In die zaak blijkt een smart speaker van Amazon bij een gebruiker thuis de gesprekken te hebben opgenomen tussen de mogelijke moordenaar en het slachtoffer.



Dit Echo-apparaat staat continu aan: het reageert net als Siri en soortgelijke apps. Ook in het huis van James Bates stond Echo aan. Bij Bates thuis werd november 2015 ene Victor Collins dood gevonden in het bubbelbad. Het OM vorderde daarop bij Amazon de opgeslagen data maar het bedrijf weigerde, vanwege Bates' privacy.

Onduidelijk is waarom Amazon nu wel meewerkt. Bates zelf verklaarde geen bezwaar te hebben.

Bron: Kaspersky / Amazon

KASPERSKY SOFTWARE UPDATER
Steeds up-to-date

Uiteraard maak je gebruik van een goed antivirusprogramma en zorg je dat je besturingssysteem up-to-date is. Hackers maken steeds meer gebruik van lekken in verouderde versies van populaire programma's.

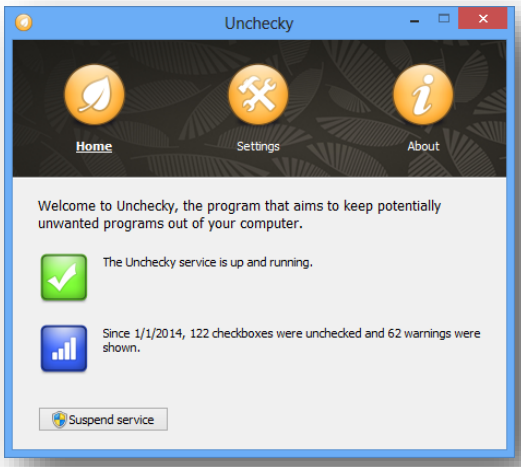
Daarom is het belangrijk dat je ook deze software steeds bijwerkt. Beveiligingsbedrijf Kaspersky brengt Kaspersky Software Updater (https://free.kaspersky.com), een programma dat zoekt naar updates voor je Windows-programma's en dat deze voor je installeert.



UNCHECKY
Ongewenste software automatisch uitvinken

Het gebeurt iedereen… Je installeert een programma, vergeet tijdens de installatieprocedure enkele vinkjes uit te zetten en daardoor worden de instellingen van je browser aangepast, zit je plots opgezadeld met een andere zoekmachine of heb je ongevraagd een extra werkbalk.

Om dit soort ongein te voorkomen is er Unchecky , een Windows-tool die allergisch is voor ongevraagde installatietoevoegingen en die de meeste vinkjes alvast resoluut uitzet.



Bron: Kaspersky / Unchecky

…verder op de website oa ……

ASK.COM TOOLBAR WEER GEBRUIKT VOOR VERSPREIDEN VAN MALWARE

HET VIRTUELE LEVEN VAN EEN KINDERMOORDENAAR

CYBER COMMANDO BEZORGD OVER REAL-TIME VIDEOMANIPULATIE

EEN HACKER MAAKTE MIJN BEDRIJF KAPOT

POLITIE ONTSLEUTELT 3,6 MILJOEN BLACKBERRY PGPBERICTEN

OPGEPAKT VOOR OPLICHTING VIA NEPAPP

MICROSOFT WAARSCHUWT VOOR NIEUWE MICRSOFTSCAM

KEVIN MITNICK GEEFT TIPS OM "ONZICHTBAAR" TE ZIJN

OP INTERNET

LEK IN NEST-BEVEILIGINGSCAMERA'S

…. en meer ……..



…verder op de Facebook pagina oa ……

Verwijder je Google-account

Microsoft blokkeert updates Windows 7 en 8.1 op nieuwe computers

Verwijderde bestanden terughalen met Windows Bestandgeschiedenis

10 tips om meer uit One Drive te halen

De juiste tools om gewiste bestanden te herstellen

ACM waarschuwt kleine ondernemers voor 'lijnkaping'

Zo kun je grondig je laptop of pc schoonmaken

Los de wifi problemen in je huis op: een complete gids

…. en meer ……..

Cops in cyberspace

'Hoe kom je daarbij?' en zelfs 'WTF are you talking about?' Zo reageerde de politie in Mannheim tweets waarin van alles en nog wat werd gesuggereerd toen een automobilist inreed op een stel mensen. Vooral op twitter werd direct geroepen dat de dader wel een moslim zou zijn, dat het een terroristische aanslag was etcetera. De politie reageerde op al die tweets en onderzoekt nu of er maatregelen genomen kunnen worden tegen de afzenders van die 'ongepaste' berichten. Woordvoerder Norbert Schätzle zei tegen Die Welt dat alle berichten worden beoordeeld op 'criminele inhoud'. De persdienst van het korps was urenlang bezig met het ongeluk. 'En nu voor iedereen: de verdachte is een Duitser, geen immigrant!'.

———————————————————

In de 'Turkijerel' zijn niet alleen talloze Nederlandse websites gehackt en tientallen twitter-accounts opeens voorzien van hashtags als #Nazihollanda, maar kwam opeens ook een Amerikaans politiekorps ter sprake. Vanuit Turkije was, vooral via twitter, opgeroepen om de Rotterdamse politie te bellen. 'Call them and make them listen to Dombra, Mehter, Azan and Quran'. Maar het googlen naar het telefoonnummer van de Rotterdam Police ging niet helemaal goed: het nummer dat in de tweet werd vermeld, is van de plaatselijke politie in het kleine stadje Rotterdam in de staat New York – dat stond kennelijk hoger in de Google-ranking … Agenten in het stadje werden vervolgens platgebeld door boze Turken. Volgens Lieutenant Jeffrey Collins van de Rotterdam Police Department kwamen er gemiddeld 900 telefoontjes per uur – en geen diender die wist waar het over ging.

———————————————————-

In Nederland bekijkt de politie de facebookpagina van de Pool Lukasz S. (31) die eind februari in Utrecht een 41-jarige vrouw doodstak. Waar het aanvankelijk leek alsof S. een willekeurig slachtoffer had gekozen, toont de verdachte zich op zijn facebookpagina een vrouwenhater met extreem-rechtse ideeën. S., orthodox lid van de Pinkstergemeente, schrijft dat hij een hekel aan feministen heeft, dweept er met zijn nazi-voorvaderen en blijkt gefascineerd door het IJzeren Kruis. Jezus zelf zou hem verder verteld hebben over een apocalyptische eindstrijd tussen goed en kwaad. Facebookvrienden van S. kennen diens radicale opvattingen, schrijft het AD, dat uit het facebookprofiel van de verdachte afleidt waar deze de laatste maanden doorbracht: vooral in de Veluwse 'bijbelgordel'. OM en politie hebben nog niet gereageerd. Maar waar we in Nederland midden in de discussie zitten over de bewijskracht van uitlatingen op facebook, worden die postings in andere landen door de politie gebruikt om zaken op te lossen. Zo beschreef de man die onlangs in Canada een agent probeerde neer te steken, op zijn facebookpagina zijn liefde voor Vladimir Poetin. 'Russia will defeat everybody', schreef Vitali Savin een half uur voordat hij met zijn mes op de politieman afstormde. Savin, al acht jaar in Canada werkzaam in de olie-industrie, werd even later doodgeschoten door de politie. En in India worden de facebookpostings van Muthukrishnan Jeevanantham (27) nader onderzocht. In zijn postings schreef Jeevanantham, onderzoeker aan de Jawaharlal Nehru Universiteit, over zijn depressies – mogelijk de aanleiding voor zijn zelfmoord vorige maand.

———————————————————

De dierenpolitie waarschuwt voor het kopen van een hondje via facebook of andere sociale netwerken. Aanleiding is de inbeslagname van een zwerfhondje dat via facebook bleek te zijn gekocht door een vrouw uit Alkmaar. Tegen die vrouw is proces-verbaal opgemaakt. Internethandel in honden is een wijdverspreid fenomeen. In een facebookgroep werd onlangs een hond geruild voor een smartphone en op Marktplaats werden op één dag in 2014 maar liefst achttienduizend honden aangeboden. De Koninklijke Hondenbescherming zegt te zijn geschrokken van het grote aantal puppy's dat op facebook wordt aangeboden en heeft Facebook Inc daarom dringend verzocht beter op te letten – het bedrijf beloofde dat ooit maar lijkt er weinig aan te doen.

———————————————————-

In Zeeland heeft de politie een man (41, uit Middelburg) aangehouden op verdenking van afpersing van homoseksuele mannen. De verdachte dreigde sekstapes van zijn slachtoffers openbaar te maken als ze niet een grote som geld overmaakten. Toen een slachtoffer aangifte deed, zette de politie een val voor hem op. De verdachte trapte daar in en werd op heterdaad aangehouden.

———————————————————-

In een week tijd heeft de politie in totaal 28 personen aangehouden, allemaal afkomstig uit Noord-Nederland, die worden verdacht van internetoplichting. Een deel van hen 'verkocht' goederen, vaak concertkaarten, maar leverde die nooit. Andere verdachten kwamen in beeld omdat ze als geldezel actief waren. Tegen de verdachten waren ruim tweehonderd aangiftes gedaan, onduidelijk is wat de totale schade is. Één van de verdachten, meldt de politie in een persbericht, is in ieder geval een verslaafde man (24, uit Groningen) tegen wie (door circa vijftig slachtoffers) 17 keer aangifte werd gedaan. In deze zaak is voor 1500 euro conservatoir beslag gelegd.

———————————————————-



Rechtspraak

De rechtbank Midden-Nederland heeft een man (23, uit Utrecht) voor identiteitsfraude en oplichting via Marktplaats veroordeeld tot 18 maanden celstraf (zes voorwaardelijk) en 240 uur taakstraf. De man verkocht producten op Marktplaats, zette foto's daarvan op de site maar beschikte helemaal niet over die spullen. Zo 'verkocht' hij onder meer een schroefmachineset en een duikcomputer. Ook vervalste hij screenshots van bankoverschrijvingen waarmee hij bij anderen concertkaartjes kocht maar niet betaalde. Die kaartjes verkocht hij vervolgens via Ticketswap weer door. Volgens de rechtbank heeft de man door zijn acties 'het wederzijds vertrouwen tussen koper en verkoper' geschonden en zo schade toegebracht. Volgens het OM maakte de man ruim 200 slachtoffers en verdiende hij daarmee ruim 23.500 euro. De verdachte moet meerder slachtoffers schadevergoeding betalen.

———————————————————-

De rechtbank Oost-Brabant heeft een man (27, uit Deurne) veroordeeld tot drie jaar gevangenisstraf en tbs voor onder meer afpersing van een vrouw, ontucht met minderjarige meisjes en het bezit van kinderporno. Tegen de 'gewetenloze' Brian S. was vijf jaar en dwang-tbs geëist. Hij had, toen het minderjarige nichtje van een buurvrouw vermist was, via facebook gesuggereerd dat het meisje door een mensenhandelaar was ontvoerd. Met geld of naaktfoto's en -films kon de vrouw haar nichtje weer veilig terugzien, anders zou ze naar 'een apenland' gestuurd worden. 'Ruil jezelf in', schreef hij aan de vrouw. 'Tot die tijd kruipen ze er op'. Bij een andere vrouw probeerde hij dezelfde truc. Maar de politie kwam de chats snel op het spoor, vooral omdat uit het huis van de man recent nog een vrouw was bevrijd. De verdachte heeft verder via Whatsapp allerlei minderjarige meisjes lastiggevallen. Hij maakte nepaccounts en dwong de meiden om compromitterende foto's van zichzelf te sturen. Een meisje moest zichzelf filmen op het toilet van school, anders verliep 'een deadline' en zou hij de foto's publiceren. De meisjes maakten in totaal dertien seksfilms. Daarmee had hij kinderporno in bezit. De rechtbank hield rekening met het feit dat de verdachte al eens eerder voor kinderporno is veroordeeld. De man moet daarom verplicht in therapie.

———————————————————-

De rechtbank Noord-Nederland heeft een man (33, uit Assen) veroordeeld tot een maand cel, waarvan 29 dagen voorwaardelijk, voor het bezit van zeven kinderpornografische afbeeldingen. Die foto's waren volgens de verdachte 'waarschijnlijk per ongeluk' meegekomen tot hij porno bekeek. De man, werkzaam in de gevangenis in Veenhuizen, liep eind 2015 tegen de lamp toen een collega de politie belde: de verdachte zou hebben geprobeerd een seksafspraak te maken met een minderjarig meisje. Dat meisje bleek zijn eigen vrouw, die als tienermeisje met haar man aan het chatten was. Pas op de afgesproken plek, het Asserbos, bleek dat hij een date met zijn eigen vrouw had. Maar de politie vond op zijn laptop ook chats met echte minderjarigen. De verdachte, een ex-militair met ptss, werd daarom niet vervolgd voor grooming, wel voor kinderporno.

———————————————————

Tien Nederlandse Syriëgangers zijn door het OM bij verstek gedagvaard, onder meer via facebook, twitter en Whatsapp. Bekend is dat de verdachten in het buitenland verblijven maar niet exact waar. De oproepen om (op 23 maart as) bij de rechtbank te verschijnen, konden daarom niet persoonlijk worden uitgereikt. Dan maar via sociale media, ook al hebben politiekorpsen in veel landen al veel sociale-mediakanalen van jihadisten laten afsluiten. De tien, die al lange tijd op de nationale terroristenlijst staan, worden verdacht van deelname aan de jihad en IS. 'Het OM wil hiermee duidelijk maken dat de rechtsstaat geen afscheid heeft genomen van de uitreizigers. De rechtsstaat is op hen van toepassing, of zij nu willen of niet.' Een van de tien is bekeerling Victor Droste (29, uit Raalte) die tegen De Telegraaf zei niet wakker te liggen van de dagvaarding. Droste, voormalig postbode, noemt zich vanaf 2013 Zakariya al-Hollandi en doet naar eigen zeggen aan 'grensbewaking'. Hij kreeg de dagvaarding via facebook messenger. 'Allemaal nogal vaag, vrij lang, een paar pagina's'.

———————————————————

De rechtbank in Den Bosch heeft drie mannen (21 en 23, uit Helmond) taakstraffen opgelegd
voor inbraken, wapenbezit, heling en veel gevallen van internetoplichting. De drie zorgden, begin 2015, voor 'een beerput van ellende' in Helmond toen ze her en der inbraken en de buitgemaakte spullen vervolgens via Marktplaats en een nepwinkel op Instagram probeerden te verkopen. De taakstraffen variëren van tachtig tot tweehonderd uur.

———————————————————

De rechtbank in Utrecht heeft een bejaarde man (71, uit Woerden) veroordeeld tot 240 uur werkstraf en zes maanden 'bijna helemaal voorwaardelijk'. Op een computer van de verdachte waren kinderpornografische afbeeldingen gevonden, materiaal dat de man in de jaren negentig had verzameld. Het onderzoek kwam na een tip dat de man als sekstoerist naar Vietnam wilde reizen. De verdachte werd eerder in Cambodja al een veroordeeld voor ontucht. Naar eigen zeggen gebruikte de man de kinderporno om maar geen ontucht te hoeven plegen. Omdat de verdachte in Nederland een blanco strafblad had, inmiddels in therapie is en 'door zijn hoge leeftijd minder libido' heeft, ging de rechtbank niet mee met het OM dat één jaar cel had geëist (waarvan vier maanden voorwaardelijk). De verdachte hoeft niet terug de cel in, hij zat zijn celstraf uit in voorarrest.

———————————————————-



Bron: Cops in Cyberspace

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

Bron: Overheid.nl

Wetsartikel

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

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

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

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

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

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

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

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

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

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

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

Art. 231b Sr Identiteitsfraude

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

Art. 240b Sr Kinderpornografie

Art. 248e Sr Grooming

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

Art. 273d Sr Schending telecommunicatiegeheim

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

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

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

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

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

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

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

Video

Tek Tok Late Night:

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

You Tube:

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

Help wanted:

Grooming
Sexting
Webcammisbruik
Bedreigd/gechanteerd
Kinderporno
Nepprofiel

Handig

Phishing- / valse e-mails melden:

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

ING Bank: valse-email@ing.nl

Rabobank: valse-email@rabobank.nl

SNS Bank: valse-email@sns.nl

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

Tips voor veilig handelen op Marktplaats

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

www.mijnpolitie.nl/miocheck

Komt de verkoper voor op de website Opgelet op internet ?

Malware ID website met info omtrent verwijderen van infecties

PCrisk verwijderingsrichtlijnen voor spyware en virussen

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

Computer woordenboek

Secure Computing Naslag

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