Secure Computing

Nieuwsbrief Maart 2013

W.Bosgra taakaccenthouder digitale criminaliteit

In dit nummer:

Toename phishing mails
Aangifte doen: wat is er nodig
Valse Flash player
Open WiFi
Ongewenste software uitschakelen
Defacen
Voorkom online-kaping

en meer…….

Dit digitale magazine wordt verzorgd door Secure Computing.

Doel is bewustwording van wat u doet met de computer , kennis opdoen gericht op de opsporing van strafbare feiten (cybercrime) en veilig computergebruik.

U kunt deze nieuwsbrief opslaan op uw eigen "Home"-omgeving en als naslagwerk blijven gebruiken.

Indien u dit magazine tevens in uw eigen thuisomgeving bewaart, kunt u gebruik maken van de ingebouwde hyperlinks.



E-mail? klik hier !

Er sprake van een toename van het aantal gevallen waarbij bankrekeninghouders een zogenaamde phishingmail ontvangen en naar een vervalste website worden geleid.

Alle grote banken zijn hierdoor getroffen. Dit principe gaat op voor elke bank die de mogelijkheid van internetbankieren aanbiedt.

Voorbeelden van deze trojans zijn:
•Spyeye
•Zeus
•Carberp (A,B, etc.)
•Win32/Msposer.A alias Lamewar.vtg
•MS Removal Tool

Besmetting kan plaatsvinden na ontvangst van een mail, met het verzoek om een zipfile te openen of een hyperlink in die mail aan te klikken. Waarna men naar een site wordt geleid waar de besmetting vervolgens plaatsvindt.

Daarnaast kan het activeren van invoegbestanden op een besmette website, het downloaden van foto's en pdf-bestanden ook voorbesmetting zorgen.

Vermoedelijke werkwijze.

De oplichter kijkt één op één mee met de niets vermoedende bankrekeninghouder, neemt de controle van de pc over en heeft dus ook controle over de verbinding met de server van de bank.

De bankrekeninghouder ervaart dit als het 'blijven hangen' van de pc. Vermoedelijk wordt op dat moment het beeldscherm, toetsenbord en muis bevroren. Steeds vaker wordt ook gemeld dat er hulpschermen in beeld verschijnen, waarin om aanvullende informatie (TAN-code of signeercode) wordt gevraagd. De oplichter plaatst op dat moment, niet zichtbaar voor de rekeninghouder, een extra overboekingsopdracht. De hoogte van de overboekingen is afhankelijk van de bestedingsruimte op de rekening(en) van het slachtoffer.

Op het moment dat de rekeninghouder de TAN-code of de code op de e-dentifier/random reader intypt om de eigen betaalopdracht uit te voeren, geeft hij/zij in feite opdracht tot het uitvoeren van de betaling die de cybercrimineel heeft klaargezet.

De eigen betaalopdracht wordt niet altijd uitgevoerd. Weinig rekeninghouders controleren daarna de uitgevoerde betaalopdrachten en zien dus ook niet dat er een niet gewenste betaalopdracht wordt uitgevoerd. Zij die dat wel doen, melden steeds vaker dat de frauduleuze overboekingen voor hem/haar zelf onzichtbaar zijn gemaakt. De cybercrimineel en de bank zien die overboekingen uiteraard wel.





Aangifte doen

aangifte doen van phishing of trojans, beantwoord dan de volgende vragen:

1. Welk besturingssysteem is op de pc geïnstalleerd (versienummer)?
2. Van welke firewall wordt er gebruik gemaakt?
3. Welke antivirussoftware op de pc geïnstalleerd is (naam en versie)?
4. Wordt die software regelmatig geüpdate en wanneer was de laatste keer?
5. Wanneer werd de pc voor het laatst gescand?
6. Welke virussen/trojans werden recentelijk in quarantaine geplaatst (naam, datum)?
7. Is er recentelijk een mail ontvangen c.q. een website bezocht waarbij gevraagd werd
software te installeren?
Zo ja, is die mail (over een niet bezorgd postpakket bijvoorbeeld) er nog of is bekend
welke website het betrof? Tip: prullenbak en geschiedenis browser raadplegen.
Welke software diende te worden geinstalleerd?
8. Mail aanwezigt, stel deze veilig (opslaan op usb-stick als .msg).
Noteer datum en tijd van die mail.
9. Noteer de header-gegevens van die mail.
10 Verliep de sessie internetbankieren anders dan anders (bevriezen beeld). Zo ja, wat gebeurde er dan precies?





11. Heeft de bank gevraagd een antivirusprogramma uit te voeren?
Zo ja, wat waren de resultaten van die scan en werd de gevonden software verwijderd?
12. Wat is het rekeningnummer?
13. Welke bedrag werd er overgeboekt en wanneer was dat?
14. Indien men de TAN-code per sms ontvangt, wat was de tekst van deze sms? (TAN-code is gekoppeld aan de som van de overboekingen)
15. Wat was het begunstigde rekeningnummer en op wiens naam stond dat rekeningnummer?
Indien er sprake is van een overboeking naar een buitenlands rekeningnummer, wat was het IBAN en BIC nummer?
16. Breng een kopie van het bankafschrift mee bij het doen van aangifte.
17. Is de overboeking door de bank gestorneerd?

Cybertaal



Hier zijn enkele tips over hoe u criminelen die het op uw mobiele apparaat hebben voorzien, kunt dwarsliggen:

Reageer niet op een sms-bericht of voicemail van een geblokkeerd of onbekend nummer. Als u niet weet met wie u spreekt, is er een goede kans dat u dat ook helemaal niet wilt weten.

· Download niets tenzij u zeker weet dat het van een betrouwbare bron afkomstig is. Dit geldt zeker voor downloads en bijlagen van geblokkeerde of onbekende gebruikers.

· Reageer niet op e-mails, sms-berichten of telefoontjes waar u niet om gevraagd hebt en waarin om persoonlijke gegevens wordt gevraagd.

· Klik nooit op links of bijlagen in ongevraagde e-mails.

· Als u naar de website van een zakelijke of financiële instelling wilt gaan, moet u het webadres rechtstreeks in de adresbalk typen.

· Controleer apps voordat u ze downloadt. Download nooit een app via een link in een sms-bericht.

Wat is bezemen? (Video Eng.)

Bezemen is een vorm van cyberpesten. Het woord 'bezem' is straattaal voor hoer.
Bezemen staat dan ook voor het online afschilderen van een meisje als hoer. Jongeren halen foto's van social media websites, monteren die achter elkaar en zetten beledigende of bedreigende seksistische teksten in het filmpje. Soms zelfs met namen, mailadressen en telefoonnummers van de slachtoffers in beeld. Daarna zetten ze er muziek onder en wordt het eindresultaat op YouTube geplaatst. Eenmaal op internet is het moeilijk om de filmpjes er vanaf te halen en gaan ze een eigen leven leiden. Bezemen is strafbaar omdat er sprake kan zijn van smaad en/of laster, belediging en soms zelfs discriminatie of bedreiging.

Wat is sexting? (Video Eng.)

"Sexting" bestaat uit de Engelse woorden "sex" en "texting" (dit laatste woord betekent: sms'en). Sexting is het sturen van seksueel getinte berichten of pikante foto's of video's, meestal via je mobiele telefoon.





Het gebruik van SMS(short messaging services) technologie om persoonlijke informatie zoals wachtwoorden en dergelijke te achterhalen middels het infecteren van de telefoon of aangesloten netwerken.

(video (Eng.)

Wat is Vishing?

U ontvangt een voicemail van uw bank en krijgt te horen dat er een dringend probleem is met uw pas en/of rekening. De stem klinkt officieel, dus waarom zou u eraan twijfelen?

U krijgt een gratis telefoonnummer dat u moet bellen. Dit nummer verbindt u door met een systeem dat vraagt naar uw rekeningnummer, pincode en andere persoonlijke gegevens. Net als bij een ***smishing*** aanval gebruiken de dieven uw informatie om bijvoorbeeld creditcards en bankpassen te kopiëren. Zo kunnen ze uw legitieme rekeningen leeghalen en u het leven zuur maken.

Soms krijgt u te horen dat u zich op een website moet aanmelden. Zodra u dat doet, wordt er vanaf de site vaak malware gedownload waardoor dieven toegang krijgen tot alle informatie die in uw telefoon is opgeslagen, waaronder uw contactenlijst.



Hierdoor krijgen ze toegang tot nog meer potentiële slachtoffers.

Vishing lost een hoop problemen van traditionele phishing scams op. Er is geen sprake van duidelijke spelfouten, wazige logo's of andere indicaties die erop wijzen dat er iets mis is. In plaats daarvan hoort u een zelfverzekerde, gezaghebbende stem die u vertelt over een probleem dat u onmiddellijk moet oplossen.

SSID

De afkorting SSID staat voor Service Set Identifier (SSID). Het is een naam waarmee een draadloos toegangspunt zichzelf bekend maakt.

Zo gebruikt routerfabrikant Belkin de standaardnaam "Belkin54g" voor veel van haar apparaten. Deze naam verschijnt bijvoorbeeld wanneer iemand zijn laptop aanzet en op zoek gaat naar een draadloos netwerk.

Het wijzigen van de SSID is belangrijk wanneer je duidelijk wilt maken welk netwerk gevonden wordt. Je kunt de naam van je organisatie gebruiken.

Aan de andere kant kan iedereen in je directe omgeving je draadloze netwerk op deze manier herkennen. Door de SSID-identificatie uit te schakelen wordt je toegangspunt onzichtbaar voor iedereen. Alleen wie de naam kent kan toegang krijgen.

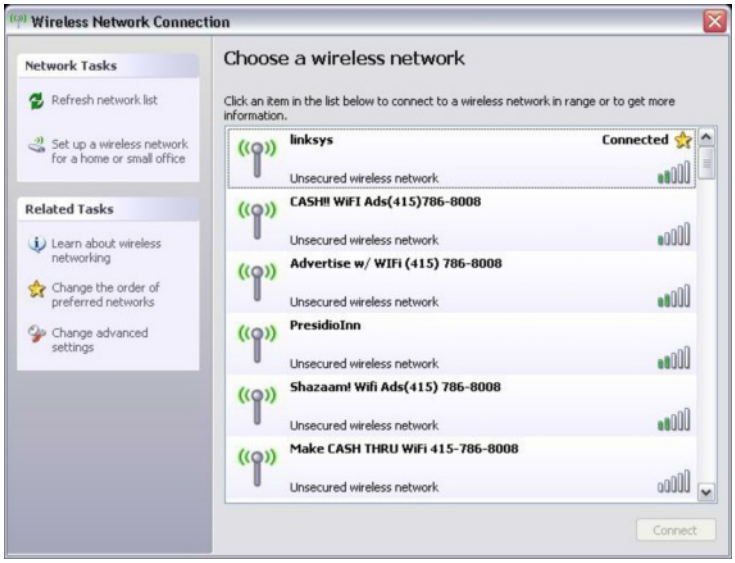
Routers en access points (toegangspunten) worden geconfigureerd via een webinterface.

1. Start Internet Explorer.

2. Typ in de adresbalk het IP-adres van het apparaat (staat in de handleiding of zoeken via Google).
3. Je ziet een webpagina met instellingsopties voor je apparaat. Zoek de optie om SSID uit te schakelen (disable). Hoe dit precies gaat is niet aan te geven omdat elke fabrikant hiervoor andere schermen en interfaces hanteert.

4. Gebruik een knop als Save Settings of Apply Changes om je wijzigingen op te slaan.
Voor bestaande gebruikers, die al verbinding hadden met het draadloze netwerk, verandert er niets. Nieuwe medewerkers daarentegen zullen je draadloze netwerk nu niet meer kunnen vinden.

Dit los je als volgt op:
1. Start de laptop van de medewerker, open het configuratiescherm en klik op de icoon van de draadloze netwerkverbinding.
2. Ga naar de Eigenschappen en klik daar op de knop Configureren om de Netwerknaam (SSID)handmatig in te stellen. Het kan ook zijn dat er een wizard wordt gestart.



Valse Flash Player-update verspreidt politievirus

Om internetgebruikers met ransowmare te infecteren, ook bekend als politievirussen, gebruiken cybercriminelen naast drive-by downloads ook social engineering. Bij drive-by downloads worden internetgebruikers automatisch met malware geïnfecteerd als ze hun software niet hebben gepatcht. Veel ransomware gebruikt deze tactiek, maar inmiddels wordt ook social engineering toegepast.

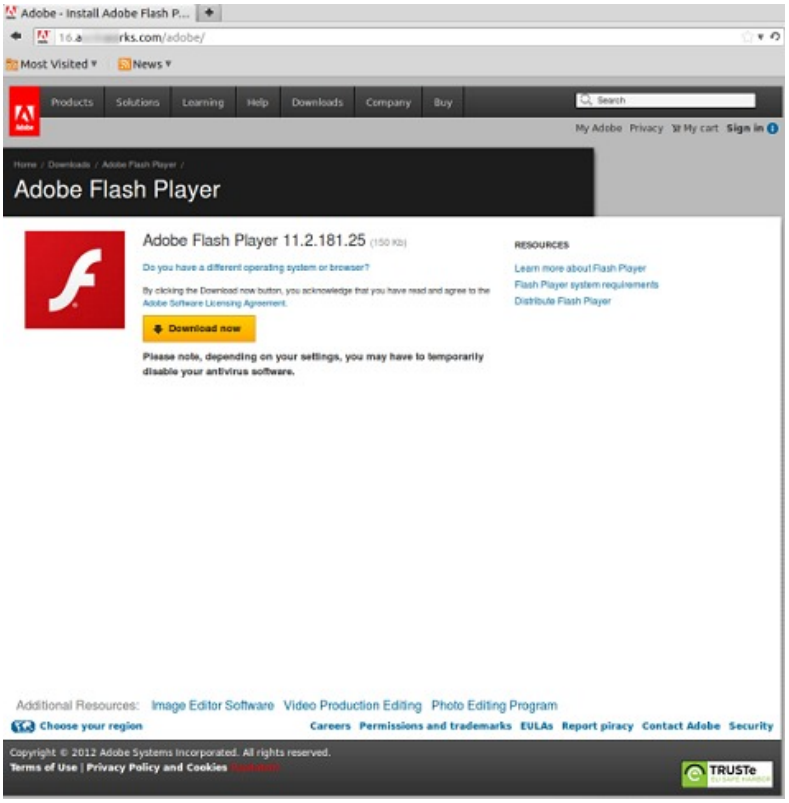
Internetgebruikers worden naar een valse versie van de Adobe Flash Player website geleid, waar ze een update voor Flash Player wordt aangeboden. In werkelijkheid is dit malware. De website gebruikt twee opties om bezoekers te besmetten. De eerste manier is via een pop-up die de gebruiker vraagt om het bestand flash_player_updater.exe te downloaden.

Adresbalk
De tweede optie is de downloadknop, die het bestand update_flash_player.exe aanbiedt. Hoewel de bestanden hetzelfde zijn, vertonen ze verschillend gedrag. Naast het stelen van wachtwoorden van FTP, telnet, SSH, SMTP, IMAP en POP3 accounts, installeert optie 1 ransomware, terwijl optie 2 adware installeert.

De ransomware is een bekende variant die in naam van een opsporingsdienst of politiekorps de computer vergrendelt. De gebruiker moet vervolgens een bepaald bedrag betalen om weer toegang tot zijn gegevens te krijgen.

De infectie is eenvoudig te voorkomen.

Gebruikers moeten namelijk de adresbalk controleren, waaruit blijkt dat ze niet op de echte Adobe-website zitten.



Houd uw Adobe Flash Player altijd up-to-date. Hoewel het bekend staat om zijn vele veiligheidslekken en dito updates, is het voor veel websites onontbeerlijk.

Download alleen van dit adres: (let op> vink eerst de extra optie McAfee Security Scan uit!)

http://get.adobe.com/nl/flashplayer/

Een veilige smartphone in tien stappen

1. Gebruik een pincode of wachtwoord
Vergrendel je startscherm met een pincode of wachtwoord voor het geval je telefoon wordt gestolen, of je hem verliest. Stel je telefoon zo in dat hij na enkele minuten zonder activiteit automatisch vergrendelt. Ook de traditionele wachtwoordregel is hier van tel: gebruik verschillende wachtwoorden voor de belangrijkste accounts die je op het toestel gebruikt.

2. Behoud de standaard beveiligingsinstellingen
Wijzigingen aanbrengen in de beveiligingsinstellingen, of je telefoon jailbreaken of rooten, ondermijnt de ingebouwde bescherming van het toestel, en maakt je meer kwetsbaar voor een aanval. Laat de instellingen dus best zoals ze zijn.

3. Maak een back-up van je data
Maak een back-up van alle contacten en bestanden op je telefoon. Je kan ze bewaren op je computer, een extern opslagmedium, of in de cloud. Op die manier zijn je gegevens veilig, voor het geval je telefoon wordt gestolen of gewist.

4. Installeer enkel apps van vertrouwde bronnen
Apps van onbetrouwbare bronnen kunnen schadelijk zijn. Je doet er daarom best aan om je apps uit een officiële appwinkel te downloaden. Lees ook eens een paar reviews, en vergelijk of de website van de ontwikkelaar consistent is met de link in de appwinkel.



5. Weet welke toegang je aan een app geeft
Applicaties maken vaak gebruik van persoonlijke gegevens, zoals je contacten of je locatie, om bepaalde diensten aan te bieden. Kijk dus goed na waar je allemaal in toestemt bij het installeren van een app.

6. Voorzie toegang vanop afstand
Veel smartphones beschikken standaard over de mogelijkheid om je toestel vanop afstand te lokaliseren of de gegevens te wissen. Is dit geen standaardfunctie op je toestel, dan kan je er in de meeste gevallen een app voor installeren.

7. Installeer software-updates en patches
Nog zo'n klassieker die we ook kennen van de pc. Installeer telkens de laatste updates voor je besturingssysteem en applicaties, of laat ze automatisch bijwerken als je toestel het toelaat. Een smartphone die volledig up-to-date is, loopt minder risico besmet te worden.

8. Wees voorzichtig op publieke wifi-netwerken
Wanneer je verbinding maakt met een onbeveiligd publiek netwerk, is het altijd mogelijk dat er een cybercrimineel op de loer ligt. Beperk je gebruik van publieke hotspots en verbind liever met vertrouwde (beveiligde) netwerken, of maak gebruik van je mobiele internetverbinding.

9. Wis een oude telefoon voor je hem weg doet
We gebruiken onze smartphone dagelijks, en het toestel bezit dan ook heel wat persoonlijke informatie. Wanneer je een oude telefoon afdankt, kun je hem best eerst volledig wissen en de fabrieksinstellingen herstellen.

10. Maak melding bij diefstal
Beschermen tegen cyberaanvallen is één ding, maar wat als je telefoon wordt gestolen? Doe allereerst aangifte bij de politie, maar neem ook contact op met je provider. Zij kunnen zowel je simkaart en je gsm blokkeren. In het geval dat je bankverrichtingen uitvoerde met het toestel, neem je best ook even

Mobiele bedreigingen

We gebruiken steeds meer mobiele devices in ons dagelijkse leven. En steeds vaker worden deze mobiele devices zowel zakelijk als privé gebruikt. Met deze toenemende mobiliteit willen we uiteraard ook overal toegang tot het internet hebben. De noodzaak van een goede beveiliging van de, inmiddels traditionele, desktop is wel bekend, maar hoe zit het met de beveiliging van de verschillende mobiele apparaten?

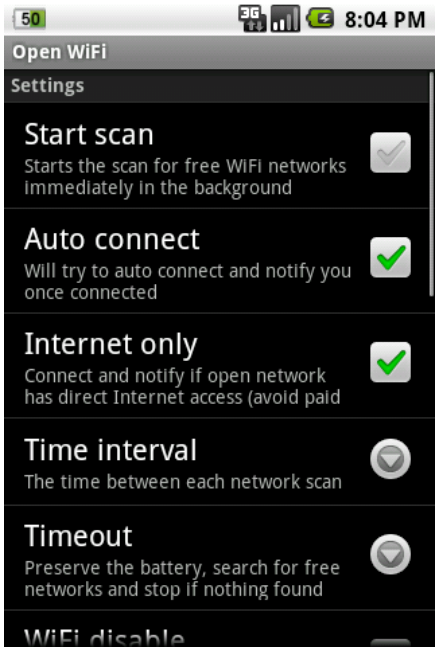
Uit ons onderzoek blijkt dat maar weinig mensen zich bewust zijn van het feit dat het beveiligen van mobiele apparaten van groot belang is. Zo maakt slechts 20 procent van de Android-gebruikers gebruik van een beveiligingsapp. Voor cybercriminelen is het daarom kinderspel om via deze mobiele devices binnen te dringen.

We verwachten dat bedreigingen op apparaten met Android een grote vlucht zullen nemen en dat de belangrijkste bedreiging dit jaar dan ook afkomstig zal zijn van kwaadaardige Android apps. Waren er eind 2012 nog 350.000 kwaadaardige Android apps, zal dit in 2013 naar verwachting uitgroeien tot een miljoen.

De gevaren
Iedereen heeft het wel eens gedaan; gebruik maken van een openbaar en onbeveiligd Wi-Fi netwerk. Even je email checken, twitteren of gewoonweg het laatste nieuws volgen. Toch breng je hiermee je eigen online veiligheid snel in gevaar. Iedereen die het netwerk gebruikt kan in theorie namelijk zien wat je doet; van het zien van de websites die je hebt bezocht tot het toegang krijgen tot jouw mail.

De do's en dont's voor openbare Wi-Fi-netwerken

Maar betekend dit dat je een dergelijk openbare Wi-Fi hotspot in geen enkel geval mag gebruiken? Natuurlijk is het beter om je online activiteiten te beperken tot je eigen beveiligde netwerk, maar mocht het nu echt nodig zijn, is er een aantal zaken die je kunt ondernemen om de risico's te beperken. Daarom hier enkele do's en dont's voor het gebruiken van een openbaar Wi-Fi netwerk:



Controleer je eigen instellingen als je buiten de deur bent. Zorg ervoor dat je device niet automatisch verbinding maakt met een Wi-Fi netwerk, maar zorg dat je altijd eerst toestemming moet geven. Maak alleen verbinding wanneer het echt nodig is en zorg er daarnaast voor dat het automatisch delen van bestanden niet is geactiveerd.

Het is een open deur, maar onthoud dat een openbaar netwerk openbaar is en pas daar je surfgedrag op aan. Check dus niet zomaar je bankzaken, maar houd het luchtig.

Wanneer een openbare gelegenheid gratis Wi-Fi heeft, controleer dan eerst de naam van het netwerk voordat je hier verbinding mee maakt. Cybercriminelen zetten namelijk dummy netwerken op waarbij je, zodra je er verbinding mee maakt, direct in de val loopt. Verifieer daarom altijd eerst de naam van het netwerk bij de gelegenheid waar je bent voordat je het internet op gaat.

Laat je niet misleiden door te denken dat een Wi-Fi hotspot in een openbare gelegenheid, bijvoorbeeld in een café of restaurant, waarbij je een wachtwoord ontvangt veilig is. Iedereen die erom vraagt ontvangt tenslotte dit wachtwoord en dat geldt dus ook voor criminelen.

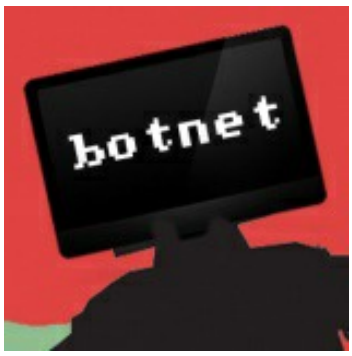
Ben je buiten de deur en wil je toch creditcard informatie invullen of bankzaken controleren, zorg dan dat het webadres met 'https' begint. De 's' staat voor 'secure' en het laat daarmee zien dat de website veilig is. Let er tevens op dat sommige websites 'https' alleen gebruiken voor hun inlog pagina en je daarna gewoon weer doorsturen naar de normale 'http' pagina. Op je mobiele telefoon is het overigens soms lastig te zien of je gebruik maakt van 'https'.

Verander de wachtwoorden die je hebt gebruikt tijdens het gebruiken van een openbaar Wi-Fi netwerk zodra je weer op een beveiligd netwerk bent.

Probeer, indien mogelijk, een Virtual Private Network (VPN) te gebruiken.



OPINIE:



Botnets of botnetwerken zijn speciale netwerken van computers. Je kunt zeggen dat een botnet computers 'kaapt'. Zonder toestemming van de eigenaren worden op hun computers programma's geïnstalleerd. Daarmee kan iemand ze op afstand gebruiken. Meestal worden de computers in een botnetwerk gebruikt voor allerlei vormen van cybercrime. Zonder dat de eigenaar dat merkt!

Wilt u uw eigen pc controleren op de aanwezigheid van een botnet, download dan hier een van de gratis botnetscanners (DE-ckeaner)
Uw heeft de keus tussen Kaspersky en Avira.

Het neerhalen van botnets is zinloos. Private ondernemingen zoals Digital Investigation en Microsoft moeten met hun handen van botnetservers afblijven. "Ze veroorzaken alleen maar meer ruis."

Dat zegt cybercrime-expert Limor Kessems van beveiligingsbedrijf RSA. Ze vindt het onbegrijpelijk dat een bedrijf als Digital Investigation de hand heeft weten te leggen op 750 GB aan data dat door een botnet is gestolen van duizenden Nederlandse bedrijven. "Zo'n hostingbedrijf dat dat zomaar afgeeft aan een private onderneming heeft zijn zaken niet echt goed op een rijtje. Dat Digital Investigation vervolgens met de data in zijn maag zit en overheid en opsporingsdiensten niet goed weten om te gaan met de situatie, tekent de onbenulligheid van zo'n ondoordachte actie."

Kessems refereert daarbij onder meer ook aan Microsoft, dat zich op de borst slaat als meervoudig neerhaler van botnets. "Wat hebben ze daarmee nu allemaal bereikt? Niets. De criminelen achter de botnets gaan gewoon door, met andere servers en een groot deel van de bots is nog steeds onder hun controle. Het is niet meer dan public relations. Ze frustreren de werkelijke aanpak van botnets met die zinloze acties."
'Pak criminelen, niet de botnets'

De cybercrime-ambassadeur van RSA vindt dat de aanpak van botnets in het hoekje van de opsporingsdiensten moet blijven. Die werken volgens haar wat langzamer en veel meer achter de schermen doordat zij de criminelen achter de botnets proberen te pakken in plaats van de snelle maar veel kleinere winst te halen in het sluiten van C&C-servers. "Daar gaat het om, het pakken van de criminlen. Dat is een hels karwei. De ontwikkelaars van Zeus, SpyEye, Citadel, ze zijn allemaal van de aardbodem verdwenen."

De criminelen achter de malware zijn zeer voorzichtig, zegt Kessems. Zo eens in de maand wordt er malware verkocht en de ontwikkelaars zijn continu bezig met nieuwe technieken in te bouwen. Zo heeft de maker van Zeus een nieuwe variant op de markt gebracht, Zeus p2p, dat nu mondjesmaat aan andere criminelen wordt verkocht. "

Het is een strijd, maar geen verloren strijd voor de bestrijders van cybercriminelen. Het meest effectief is het zo moeilijk mogelijk maken voor criminelen om geld te verdienen. In Finland is de winst uit fraude met internetbankieren nagenoeg nul. Het banksysteem is zo robuust met zoveel beveiligingsmaatregelen dat het voor consumenten al moeilijk genoeg is om ermee om te gaan, laat staan voor cybercriminelen. Dat systeem wordt nergens anders ter wereld gekopieerd, omdat het simpelweg te gebruiksonvriendelijk is. Maar dus wel effectief."

RSA®
The Security Division of EMC

Problemen oplossen door ongewenste software uit te schakelen

Uninstall-tools

Is het uninstaller-bestand nergens te vinden en biedt de setup geen soelaas dan kan een van onderstaande tools wellicht nog uitkomst bieden:

MyUninstaller download: www.nirsoft.net/utils/myuninst.html, negeer de waarschuwing). Omdat via View, Advanced Mode, Quiet Uninstall meerdere programma's tegelijk verwijderd kunnen worden, werkt deze tool beduidend efficiënter dan de standaard deïnstallatieprocedure.

Revo Uninstaller Freeware download: www.revouninstaller.com een goed alternatief voor de standaard deïnstallatieprocedure.

PC Decrapifier (download: www.pcdecrapifier.com voor het geautomatiseerd verwijderen van ongewenst door de fabrikant geïnstalleerde software.

Restanten van programma's definitief verwijderen:

Je zou misschien verwachten dat de reguliere uninstall-bestanden gewoon netjes een programma verwijderen, zonder restjes (zoals programmabestanden en registerwaarden) achter te laten. Als gevolg van niet-verwijderde bestanden kunnen problemen ontstaan bij het installeren van een nieuwere versie of zelfs het installeren van alternatieve software onmogelijk maken .
Ga dus met gezond verstand te werk en maak eventueel gebruik van onderstaande reparatietool:

Microsoft Fix-it

Redenen om software uit te schakelen

Er zijn redenen genoeg om software uit te schakelen: wat te denken van de lange opstarttijd, virussen, ongewenste software, pop-ups, een trage en onhandelbare PC, een trage internetverbinding, etc. Het gebeurt iedereen wel eens dat er (per ongeluk of expres) software wordt geïnstalleerd waar u zich uiteindelijk meer aan irriteert dan baat bij heeft.

Zo bevat een nieuw aangeschafte, voorgeïnstalleerde computer vaak reclamesoftware, en wordt gratis software voorzien van ongewenste toevoegingen. In het ergste geval heeft u te maken met virussen, pop-ups, een hoge processorbelasting of een trage internetverbinding.

Probeer software eerst op de normale manier te verwijderen

Er zijn computergebruikers die denken dat geïnstalleerde software kan worden verwijderd door simpelweg de bestanden uit de programmamap Program Files en/of Program Files (x86) te verwijderen of zelfs door alleen de snelkoppeling uit het startmenu of het Windows 8 startvenster te knikkeren... Het mag duidelijk zijn dat dit niet de juiste manier is!
Ooit geïnstalleerde software kan het beste op de reguliere manier worden verwijderd via het onderdeel Software (XP)/Programma's en onderdelen (8/7/Vista) in het configuratiescherm (in Windows 8 ook te bereiken via de optie Installatie ongedaan maken in de app-balk die wordt getoond na activeren van een snelkoppeling in het startvenster of App-overzicht) zodat zowel de programmabestanden alsook de bijbehorende registerwaarden netjes worden verwijderd.

Alternatieve manieren om een programma te verwijderen

Is het programma niet opgenomen in deze lijst dan zal een alternatief moeten worden gezocht. Wellicht heeft het programma een snelkoppeling naar het uninstallprogramma in het startmenu (Windows 7 en ouder) of App-overzicht (Windows 8) achtergelaten.
De uninstaller kan vaak ook nog worden teruggevonden in de betreffende programmamap onder C:\Program Files en/of C:\Program Files (x86) (zoek hier naar een bestand met een naam als UNINSTALL.EXE, meestal voorzien van een prullenbak-icoontje).
In veel gevallen kan de software ook met het gedownloade installatiebestand weer worden verwijderd.

TIP: Werkt de uninstaller niet meer? Probeer de software dan eens opnieuw te installeren, wellicht kan het programma daarna wèl op de juiste manier worden verwijderd.

Dit is natuurlijk alleen mogelijk wanneer de origineel geïnstalleerde software nog beschikbaar is!

Bewaar daarom altijd het gedownloade installatiebestand van de geïnstalleerde software, het is namelijk nooit zeker of deze later nog van pas kan komen.





Defacen van website

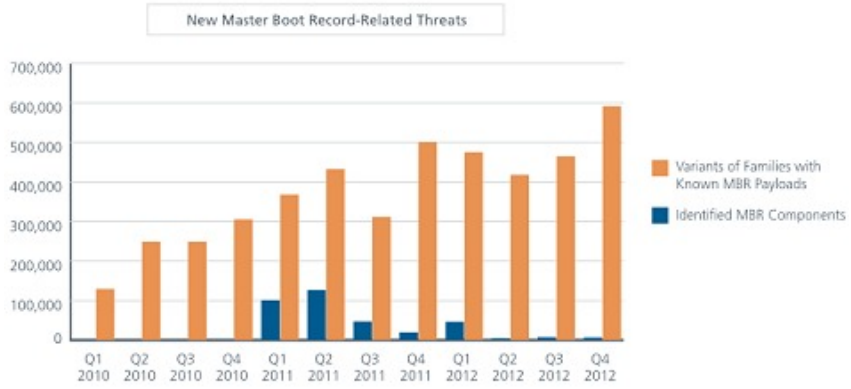
Het defacen van een site is een vorm van vandalisme die grofweg het elektronisch equivalent is van graffiti spuiten. De site wordt gehackt en de inhoud van de pagina's wordt aangepast of vervangen, meestal met beledigende of expliciete tekst en foto's.

Defacen is een vorm van onbruikbaar maken of vernielen van gegevens en dus strafbaar (art. 350a lid 1)

Toename rootkits die harde schijf infecteren

In het vierde kwartaal van 2012 is het aantal rootkits en andere malware die de Master Boot Record (MBR) van harde schijven kan infecteren met maar liefst 27% gegroeid en heeft zo een nieuw hoogtepunt bereikt. De MBR bevat verschillende gegevens over het soort en de locatie van de logische partities van de harde schijf. Door zich in de MBR te verstoppen zijn rootkits vaak lastiger te vinden.

Zelfs het formatteren van de harde schijf kan in dit geval de infectie niet verhelpen. Hoewel deze MBR-aanvallen nog altijd een relatief klein percentage vertegenwoordigen van de totale hoeveelheid pc-malware, verwacht anti-virusbedrijf McAfee dat dit in 2013 zal uitgroeien tot één van de belangrijkste aanvalsvormen.





Live Messenger-gebruikers in april naar Skype

Gebruikers van chatprogramma Windows Live Messenger, in Nederland beter bekend als MSN, moeten in april overstappen op Skype. Dat heeft Microsoft bekendgemaakt.

Op 15 maart wordt Messenger via Skype officieel in gebruik genomen, al is het al enige tijd mogelijk om via de internetbelapp in te loggen met een Microsoft-naam en -wachtwoord. In de loop van april wordt Messenger echter ontoegankelijk gemaakt. Op 8 april begint het bedrijf met het afsluiten van toegang voor Engelstalige gebruikers. De rest van de wereld volgt in de rest van die maand.

De achterliggende infrastructuur van het netwerk blijft voorlopig nog wel online. Windows Phone-gebruikers en gebruikers van chatprogramma's van derden kunnen ook de komende tijd gewoon nog inloggen. Wel bestaan er al plannen om ook deze versies af te sluiten.



Hoe je Androidtelefoon voorbereiden op zijn pensioen



Je Androidtelefoon heeft je goed gediend, maar ooit is het tijd om afscheid te nemen. Op dat ogenblik kan je best al je privégegevens van de telefoon verwijderen.

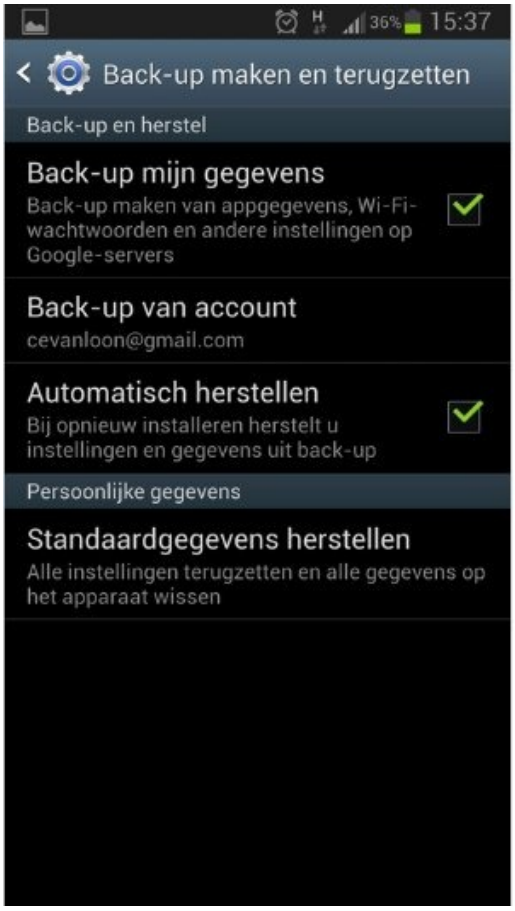
Als je nu een nieuwe telefoon koopt, moet je huidige telefoon met pensioen. Je kan hem in de schuif leggen, verkopen op het internet of cadeau doen aan een neefje of nichtje. In elk geval is het verstandig om al je privégegevens even van je telefoon te halen. Enkel zo kan je je privacy beschermen.

Je Androidtelefoon die afzwaait staat vol met e-mail, foto's, berichten en documenten. Eerst en vooral moet je eens nagaan wat je niet kwijt wil. De foto's zet je best in de cloud met een dienst als Dropbox. Hetzelfde geldt voor je documenten die lokaal opgeslagen zijn. De bestanden opslaan op de geheugenkaart is niet zo verstandig, omdat het mogelijk is dat Android versleuteling toepast. Die versleutelde gegevens zijn achteraf onbruikbaar.

Om je berichten over te hevelen naar een andere telefoon heeft Android een handige functie. Deze vind je op Samsungtelefoons bij de instellingen onder de kop 'Back-up maken en terugzetten'. Andere merken hebben vaak een soortgelijke optie.

Als je zeker bent dat een reservekopie hebt van alle gegevens die je wil houden, kan je aan het wissen slaan. Daarvoor kies je onder Instellingen voor 'Standaardgegevens herstellen'. Daar klik je op 'Apparaat resetten'. De telefoon doet al het nodige om de telefoon opnieuw in te stellen en alle gebruikersgegevens te wissen.

Je kan veiligheidshalve ook nog de geheugenkaart uit het toestel halen om zeker te zijn dat je geen gegevens achterlaat.





Boost je router in tien stappen

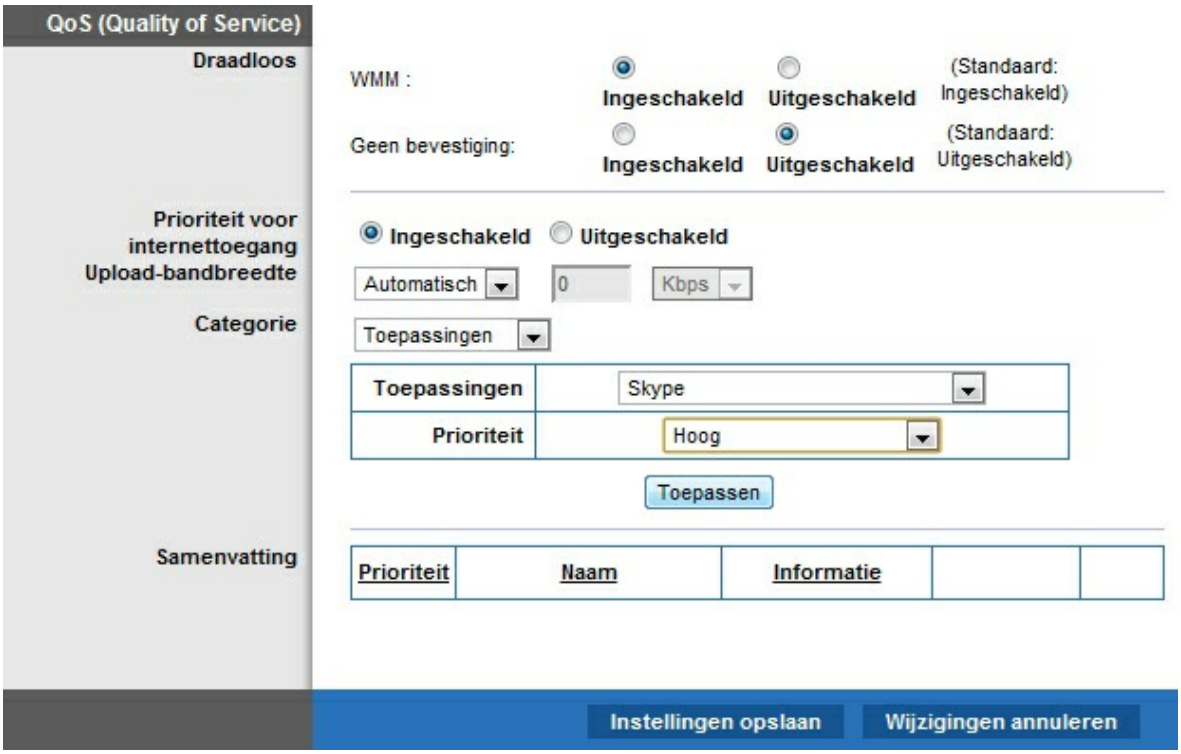
Dankzij een draadloze router kan je hele netwerk het internet op. Zorg er wel voor dat de router optimaal is ingesteld, zodat iedereen vlot kan surfen. We tonen je waar je moet kijken.



De meeste routers zitten bomvol instellingen, maar waar vind je die? Als er geen software bij de router zit, zal je in de handleiding het IP-adres moeten opzoeken. Als je dat adres, meestal 192.168.0.1 of 10.0.0.1, intypt in je browser, krijg je toegang tot de routerinstellingen.

1. Firmware updaten
Het eerste dat je nu na het aanmelden best doet, is de routerfirmware updaten. Zo'n firmware-update brengt immers meer stabiliteit, nieuwe functies of snellere draadloze verbindingen. Soms kan dat updaten gebeuren vanuit de webinterface zelf, maar meestal zal je op de website van de routerfabrikant een bestand moeten downloaden, om dit vervolgens te uploaden naar de router. Opgelet: alle routerinstellingen worden na zo'n update normaal gezien gewist, dus maak best eerst een back-up.

2. Voorrang aan programma's
Alle data die een router afhandelt, worden in principe gelijkwaardig behandeld. Met Quality of Service (QoS) kan je echter prioriteiten gaan toekennen. Dit kan op basis van de gebruikte poort, het programma, het protocol of zelfs de computer waarvoor het bedoeld is. Belangrijk is dat de upload- en downloadsnelheden die je ingeeft accuraat en realistisch zijn, want onder andere daarop baseert QoS zich om de bandbreedte optimaal in te delen.



3. Schakel WMM in
WMM of Wifi Multimedia borduurt verder op de in tip 2 aangehaalde QoS-technologie, maar is specifiek bedoeld voor multimediatoepassingen zoals videochat of VoIP. Toepassingen waarbij het niet wenselijk is om tegen een onderbreking aan te lopen. Het loont daarom de moeite om WMM in te schakelen in je router, al valt het nog af te wachten of het ook echt iets bijdraagt, in het bijzonder als je al QoS gebruikt. Gewoon proberen dus.

4. Snellere wifi

Deze tip is er eentje voor wie de geavanceerde instellingen van de wifi durft in te duiken. Fabrikanten raden af om daar te gaan rondneuzen, tenzij je écht weet wat je doet, maar wat mij betreft moet je absoluut Frame Burst activeren. Met Frame Burst geactiveerd zullen draadloos verbonden apparaten immers sneller kunnen communiceren. De kans is groot dat deze functie al vanuit de fabriek aangevinkt is, maar als dat nog niet het geval is, kan je dat best zelf even doen. Verlies je regelmatig je wifi-connectie? Probeer dan om Frame Burst uit te schakelen.

5. Back-up de router

Je zal al gemerkt hebben dat zelfs de simpelste router een hoop instellingen herbergt. Eenmaal alles op punt staat, loont het dan ook de moeite om al die instellingen te bewaren. Alle routers bieden de mogelijkheid om hun configuratie op te slaan in een extern back-upbestand (.cfg) dat je ergens veilig bewaart. Vergeet je het wachtwoord, of moet je de router toch ooit eens volledig 'resetten', dan importeer je gewoon dat bestand in je router en ben je snel terug aan het werk.

6. 20 of 40 MHz?

Hoe meer 'ruimte' voor wifi-signalen, hoe hoger de snelheid. Toch staat de kanaalbreedte van wifi doorgaans ingesteld op 20 MHz in plaats van het bredere (en snellere) 40 MHz. Daar is een reden voor: in 20 MHz-modus beperk je de storing voor omliggende netwerken. Zit je echter in een gebied met weinig of geen andere wifi-netwerken, dan zorgt de 40 MHz-modus wellicht voor meer snelheid. Slimme routers bepalen zelf de gewenste modus, maar niets houdt je tegen om handmatig 40 MHz te activeren. Nadeel is wel dat het bereik in deze modus doorgaans wat minder is. Proberen dus!



7. Meerdere routers

NAT of Network Address Translation laat je toe om één publiek IP-adres te delen met verschillende computers en is een essentieel onderdeel van tal van routers. Heb je een netwerk met meerdere routers, zorg er dan voor dat enkel de router die verbonden is met het internet NAT heeft ingeschakeld. Op de andere router(s) moet je NAT uitschakelen.

8. Sneller met WPA2

De toegang tot een wifi-netwerk is meestal afgeschermd via een wachtwoord. Maar wist je dat de gebruikte beveiligingstechniek – WEP, WPA, WPA2 – invloed kan hebben op de draadloze snelheid? Een en ander hangt af van je router en de clients zelf, maar omdat bij WPA2-AES hardwarematige encryptie vereist is, mag deze techniek normaal geen invloed hebben op de snelheid van draadloze verbindingen. Bovendien is WPA2-AES moeilijk te kraken.

9. Zoek de bottleneck

Ontelbaar veel factoren hebben hun invloed op de snelheid van wifi-verbindingen. En soms ontkom je er niet aan om zelf op zoek te gaan naar de bottleneck. Gebruik dan de volgende tools:

Metageek InSSIDer (Windows). Gratis en makkelijk te gebruiken analysetool om het meest geschikte radiokanaal te zoeken.

Jperf (Windows). Een benchmarktool om de snelheid van netwerkverbindingen accuraat te meten.

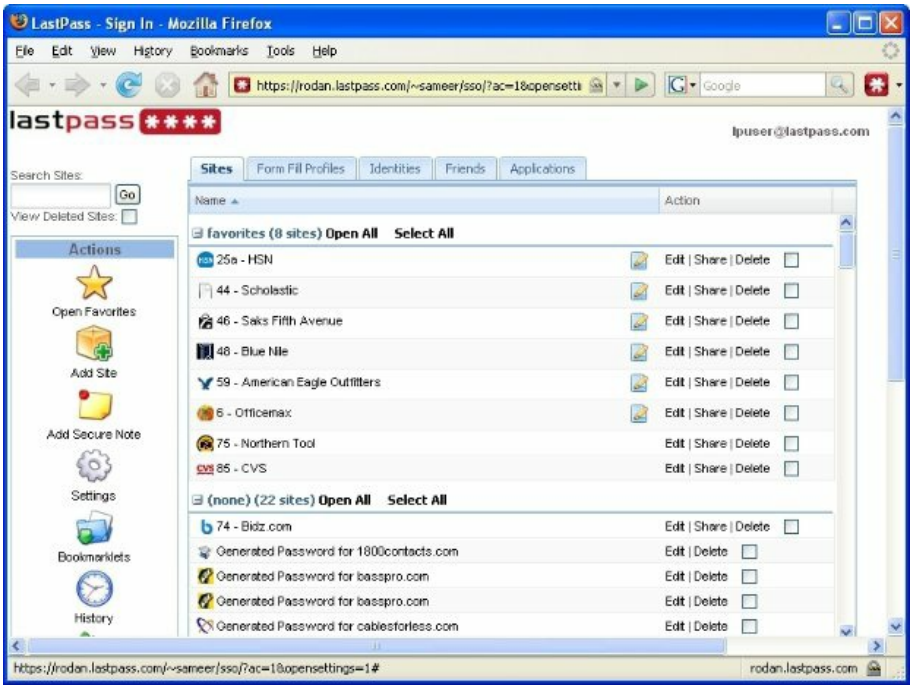
10. Draadloze verbetering

Lukt het je toch niet om in die ene hoek van de kamer draadloos internet te krijgen? Overweeg dan om een access point te plaatsen als je een netwerkkabel in de buurt hebt, of een range extender.

Tien tips om een online kaping te voorkomen

1. Wachtwoordbewaarder

Hoe sterker je wachtwoord, hoe veiliger je online bent. Beter nog: gebruik voor elke dienst een apart wachtwoord om ervoor te zorgen dat niemand je online leven kan plunderen. Je kan natuurlijk nooit alle wachtwoorden onthouden, maar daar bestaan veilige online diensten voor die dat voor jou regelen.



Gebruik bijvoorbeeld LastPass om alje digitale wachtwoorden te beheren. LastPass werkt bovendien op elk denkbaar platform: Windows, Mac, Android, iOS, & noem maar op. Beslist de moeite om eens te proberen.

2. Twee stappen

Een sterk en uniek wachtwoord is belangrijk, maar als je geen risico wil lopen, is een verificatie met twee stappen noodzakelijk. De eerste stap is je gebruikelijke wachtwoord voor die bepaalde dienst, maar daarna wordt – via e-mail of sms bijvoorbeeld – een tweede code verstuurd ter verificatie.

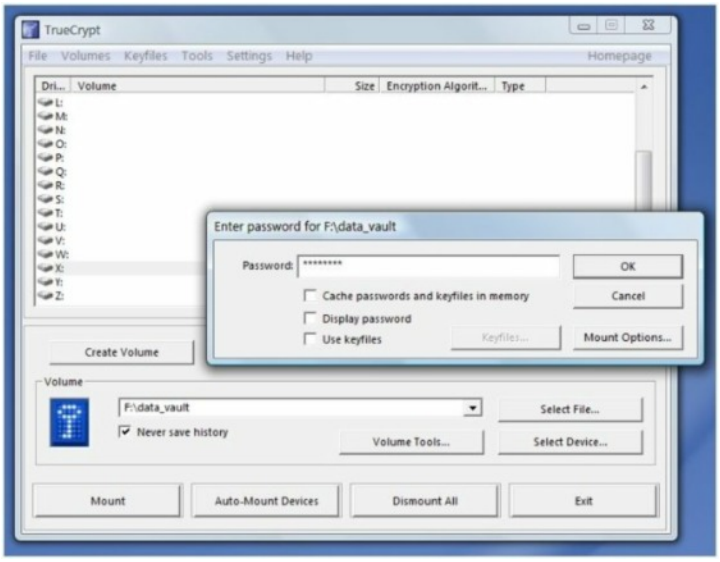
Sinds kort bieden sommige online diensten deze vorm van beveiliging aan. Een mooi voorbeeld is de Authenticator-app van Google. Deze app genereert elke 10 seconden een zescijferige code die je moet invullen wanneer je ergens met je Google-account inlogt. Zo wordt het voor hackers onmogelijk om je account te kapen.

3. WPA2-beveiliging

Het is uiterst belangrijk om online sterke wachtwoorden te kiezen, maar dat geldt ook voor je draadloze thuisnetwerk. Van zodra er iemand kan inloggen op je netwerkje, kan die alle computers nagaan op bestanden, en mogelijk zelfs een virus binnenloodsen. Kies daarom voor je draadloze internetrouter altijd een WPA2-wachtwoordbeveiliging. Die is uiterst moeilijk te kraken in vergelijking met het kwetsbare WEP. Om het wachtwoord van je router te wijzigen, heb je het IP-adres van je toestel nodig. Raadpleeg hiervoor de handleiding van je router.

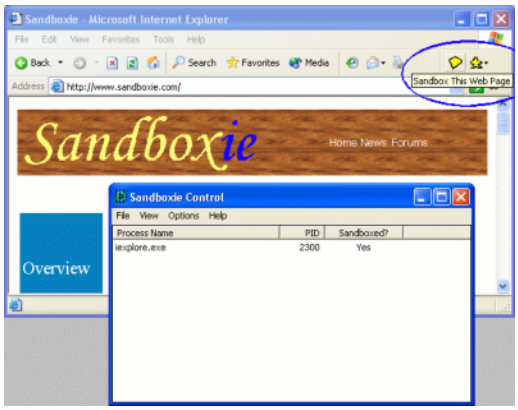
4. Encryptie

Wanneer je gebruik maakt van online opslagdiensten, liggen je bestanden in principe open en bloot op het internet, zij het achter een beveiligde deur. Theoretisch kan er niets mee gebeuren, maar om zeker te zijn kan je je bestanden altijd nog encrypteren.



Gratis softwareprogramma's zoals TrueCrypt zorgen ervoor dat al je bestanden met een wachtwoord naar keuze beveiligd worden. Wie dat wachtwoord niet heeft, kan niks met je bestanden aanvangen.

5. Sandbox



Dankzij een bijzonder Sandbox-systeem draaien Chrome en Internet Explorer 10 in feite in een virtuele machine. Komt er via internet een bedreiging binnen, dan besmet die de virtuele machine, maar niet je computer zelf. Online bankieren is daarom het veiligst in een browser met een Sandbox.

Firefox maakt voorlopig nog geen gebruik van een Sandbox-systeem. Heb je graag deze extra veiligheid, maar wil je niet veranderen van browser? Probeer dan zeker het gratis programma Sandboxie.

Download je toch nog een virus en open je het op je computer, dan ben je natuurlijk wel besmet.

6. Eigen back-up eerst

Tegenwoordig schieten de online clouddiensten als paddenstoelen uit de grond. Overal kan je van gratis online opslag genieten, met variërende opslagcapaciteiten. De ene biedt al wat meer mogelijkheden dan de andere, maar je mag zo'n opslagdienst zeker niet zien als een veilige back-up.

Wanneer er ooit iemand je wachtwoord kaapt, ben je in het slechtste geval in één oogopslag alles kwijt. Zorg daarom altijd voor een extra fysieke back-up ergens in huis. Als die faalt, kan je altijd nog terecht bij je online opslag om die te herstellen naar je nieuwe fysieke back-up, en omgekeerd.

Je zou het jezelf nooit vergeven wanneer die éne belangrijke fotocollectie opeens voor altijd verdwenen is. Online diensten stralen dan wel zekerheid uit, maar iedereen kan wel eens pech hebben.



7. SSL-encryptie

Let telkens goed op de beveiliging van een website waarop je een inlognaam en een wachtwoord aanmaakt. Zeker wanneer je voor elke website dezelfde login en hetzelfde wachtwoord neemt. Elke website waar een SSL-encryptie van toepassing is, geeft je de zekerheid dat je inloggegevens veilig versleuteld worden opgeslagen.
Zonder SSL-encryptie liggen je inloggegevens in feite gewoon te grabbel wanneer een hacker de website kaapt. Niet zo leuk als je overal dezelfde gegevens gebruikt.

Webshops zonder SSL-encryptie zijn daarom niet per definitie onbetrouwbaar wat betalingen betreft. Elke betaling wordt immers omgeleid naar een aparte website, waar gelukkig wel SSL-encryptie is voor optimale veiligheid. Bijna elke website die SSL-encryptie gebruikt, maakt dat ook duidelijk op zijn webpagina of bij de registratie.

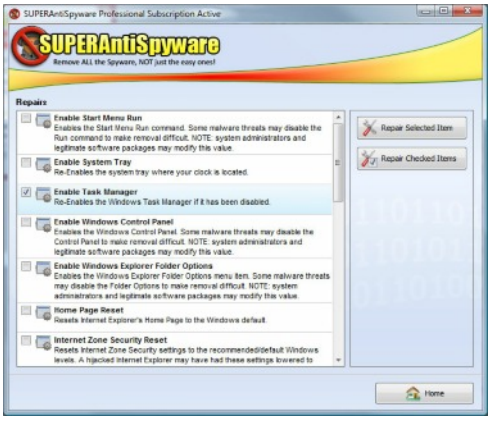
8. Veilige smartphone

De smartphone wint aan populariteit en wordt steeds meer het centrale toegangspunt voor allerlei online diensten. E-mails, kalender, berichten, wachtwoorden, apps, … van zodra iemand je smartphone in handen heeft, kan die vernietigend te werk gaan.

Daarom is het heel belangrijk dat je je smartphone beveiligt met een pincode. Niet alleen om hem in te schakelen, maar ook telkens je hem uit stand-by haalt.

Heb je de mogelijkheid om met een veegpatroon of je gezicht je smartphone te ontgrendelen, dan mag dat natuurlijk ook.

9. Spyware, malware, keyloggers



Online surfen geeft je een gevoel van vrijheid, maar je moet goed oppassen waar je surft en wat je allemaal downloadt. Voor je het weet, wordt er een piepklein, onopvallend stukje software op je computer geïnstalleerd dat je continu in het oog houdt.

Deze zogenaamde spyware of malware kan al je gegevens ontrafelen, en daarna online veel schade aanrichten zonder dat je het zelf doorhebt. Het wordt zelfs nog erger wanneer iemand een keylogger op je computer installeert. Die registreert elke toetsaanslag, waardoor plots al je wachtwoorden blootgegeven worden.

Zorg daarom altijd voor goede software zoals SuperAntiSpyware of Malwarebytes Anti-Malware, en voer regelmatig een volledige scan uit.

10. Privacy

Sommige diensten gebruiken geheime vragen en antwoorden om je wachtwoord te ontgrendelen, zoals de naam van je vrouw of van je huisdier. Onbekenden zouden het antwoord niet mogen weten, maar dankzij sociale websites als LinkedIn en Facebook heeft tegenwoordig niemand nog geheimen. Zorg er daarom altijd voor dat je privacyinstellingen correct ingesteld staan, en dat alleen je vrienden en jijzelf je privégegevens kunnen bekijken. Hoe minder er online over jou te lezen valt, hoe veiliger.



6 tot 8GB

(Je hebt een 64-bit besturingssysteem nodig)

Nu zijn we in het domein van de hardcore prestaties. Als je een gaming pc aan het bouwen bent, raad ik aan om je RAM op te drijven naar 6 of 8GB, afhankelijk van hoeveel je moederbord ondersteunt. Als je een computer voor foto- en videobewerking bouwt, of gewoon graag een snelle machine wilt, beschouw dit dan als een must.
6 of 8GB RAM is ook niet meer zo duur. Laat je het door de fabrikant in een nieuw systeem steken, betaal je natuurlijk een meerprijs . Maar als je het achteraf bijkoopt, kan je zelfs al voor minder dan 50 euro gesteld zijn.

12 tot 16GB

(Je hebt een 64-bit besturingssysteem nodig)

Is het interessant om meer dan 8GB RAM te gebruiken? Natuurlijk wel, maar dan haal je je geld er niet echt meer uit.
Meer dan 8GB RAM wordt pas nuttig en begint pas voor zichzelf te betalen wanneer je verschillende veeleisende programma's tegelijk draait. Vooral als het gaat om foto- en videobewerking, CAD, of 3D-modelleren. Probeer Premiere Pro, Photoshop en After Effects eens tegelijk te draaien op een systeem met 8GB RAM, en verhoog het daarna om het verschil te voelen.

Hoeveel RAM-geheugen heb je nodig?

1GB

Beschouw 1GB als het absolute minimum. De dagen dat RAM per megabyte gemeten werd, zijn lang voorbij.

1GB RAM is genoeg voor basishandelingen als surfen op het internet - al moet je niet proberen tientallen tabbladen open te laten staan - email, tekstverwerking, en lichte fotobewerking.

Gamen met deze hoeveelheid RAM zal pijnlijk zijn, en taken als beeldverwerking of het rippen van een CD zullen praktisch heel je systeem overnemen. Videobewerking kan je helemaal vergeten.

Ik promoot 1GB RAM niet echt, omdat ik simpelweg niet wil worden beperkt tot maar 1GB. Al gebruik je je computer alleen voor lichte taken, idealiter gebruik je meer dan 1GB.

2GB

Je kan het misschien met minder stellen, maar de kans is groot dat je dan heel veel slechte woorden naar je computer gaat slingeren.

Met 2GB RAM zou je min of meer alles moeten kunnen doen waar een computer toe in staat is: gamen, foto- en videobewerking, Microsoft Office draaien en een dozijn tabbladen laten open staan in je browser, het wordt allemaal ineens mogelijk. De hoeveelheid RAM zal uiteindelijk wel voor een knelpunt zorgen, maar je krijgt tenminste wat echt werk gedaan.

2GB is ook genoeg om zware softwarepakketten als de Adobe Master Collection CS6 te draaien (of dat beweert Adobe toch, maar als je 2.500 euro kan neertellen voor software, dan zou je je ook wat meer RAM moeten kunnen veroorloven!).

3 tot 4GB

Als je met een 32-bit besturingssysteem werkt, zal je met 3 of 4GB geïnstalleerde RAM toch maar toegang hebben tot ongeveer 3,2GB (dit heeft te maken met beperkingen in toewijzing van geheugen). Met een 64-bit besturingssysteem heb je toegang tot de volledige 4GB.

Het verschil tussen een computer met 2GB RAM en 3 of 4GB, is een verschil tussen dag en nacht. Zelfs op een 32-bit systeem, dat de RAM beperkt tot net over 3GB, is de prestatieverbetering de meerprijs waard. Applicaties draaien niet alleen sneller, je kan ook meer programma's tegelijk draaien - handig als je werkt met pakketten als Microsoft Office of Adobe Master Collection.

Als je een 64-bit besturingssysteem hebt, is de upgrade van 2GB RAM een no-brainer.

De meeste Windows 8-systemen - behalve de erg goedkope modellen - komen met 3 of 4GB RAM, terwijl 4GB het minimum is voor alle nieuwe iMacs, MacBooks en MacBook Pro's



Meer ‘blauw online’ tegen internetcriminaliteit

Het inperken van de privacy van internetters, in de strijd tegen cybercrime, is zinloos. Beter leer je computergebrukers hoe ze moeten omgaan met de gevaren van het web.

Daarvoor pleit mr dr Mathieu Paapst, docent en onderzoeker bij het Centrum voor Recht en ICT (RU Groningen). Paapst reageert op het rapport van McAfee dat aantoont dat Nederland ‘een waar paradijs’ is voor cybercriminelen.

De overheid reageerde op dat rapport met voorstellen onze privacy nog meer in te dammen. Volgens Paapst is dat absurd. ‘Daarmee los je nauwelijks iets op. Laat de overheid eerst maar eens zorgen dat burgers – maar vooral ook bedrijven en overheden – zich bewust worden van de risico’s die ze lopen.’

Het is logisch dat Nederland bovenaan die lijst staat, met 6,4 miljoen breedbandaansluitingen, circa 1500 hostingbedrijven, het Europese datacentre van Google en het grootste internetschakelpunt ter wereld. ‘Als je dan gaat tellen waar de meeste inbraken plaatsvinden, is het logisch dat we in de top-3 staan’.

Paapst stoort zich vooral aan de politiek. ‘Omdat we er niet goed in slagen die cybercriminaliteit op te sporen, moeten we dús de privacy van de gebruikers maar opzij zetten’. Het moet eigenlijk andersom zijn: de overheid zou internetgebruikers in staat moeten stellen om hun privacy te kunnen beschermen.

Hij noemt gebrek aan kennis de belangrijkste reden waarom het niet goed gaat. ‘De gemiddelde burger weet niet wat een botnet is. Hoe kan hij zich daar dan tegen beschermen?’

Computergebruikers, bedrijven én overheden moeten veel bewuster worden van de gevaren.

Een van de maatregelen die Paapst voorstelt is meer blauw online.
‘De politie weet vaak niet hoe ze een malafide handelaar op het web kan traceren’.

Blog

VS: Politie stuurt sterfbericht via Facebook

In de staat Georgia heeft de politie een moeder via facebook laten weten dat haar zoon was overleden. Op zich al vreemd, maar nog gekker was dat het verstuurd werd vanaf een anonieme facebookaccount die de politie in Clayton County ooit had gebruikt voor een undercoveractie. En berichten van mensen met wie je niet bevriend bent, komen bij veel mensen automatisch in de spam-box. Dus toen moeder Anna Lamb van ene Misty Hancock – profielfoto: een rapper – bericht kreeg dat zoon Rickie verongelukt was bij een autocrash, werd dat nooit gelezen. Pas drie weken later, op Valentijnsdag nog wel, vond een dochter het bericht, toen ze de computer aan het opschonen was. Volgens de politie was er van alles geprobeerd om met Anna Lamb contact op te nemen en was facebook het enige wat nog restte. Onzin, aldus moeder Lamb. 'Ik werk al dertien jaar op dezelfde plaats. Als ze criminelen kunnen vinden, dan hadden ze mij ook kunnen opsporen. Ze hadden gewoon beter hun best moeten doen.'

Boete voor photoshoppen foto wijkagent

Een 18-jarige jongen moet 500 euro boete betalen omdat hij een foto van wijkagent Johan Dubbeldam uit Hoofddorp had bewerkt. Op het hoofd van Dubbeldam werd een piemel geplakt. De jongen twitterde de foto vervolgens naar de agent. Een politieverzoek om de foto weg te halen, negeerde hij. Waarop hij thuis werd opgepakt. De jongen schikte vervolgens met het OM. Toen de politie twitterde over de boete, ontstond commotie over de boete. Die tweet werd vervolgens verwijderd. Inmiddels worden er van de photoshops weer nieuwe photoshops gemaakt.

Nieuwe zoekmachine voor sociale media

Het 'ultieme cyberspionagewapen', zo noemt Joop.nl het programma RIOT, Rapid Information Overlay Technology, van ontwikkelaar Raytheon. Het programma, nog in ontwikkeling, zou persoonlijke gegevens uit verschillende sociale media bundelen en in kaart brengen. De Britse The Guardian zag op een geheime video over het project hoe het werkte, aan de hand van een fictieve persoon. 'We know where Nick's going, we know what Nick looks like. Now we want to try to predict where he may be in the future.' RIOT toont een spindiagram met relaties en verbanden, koppelt facebookvrienden en twittervolgers, zoekt gps-info uit Foursquare en nog meer. Omdat Nick elke maandagochtend incheckt in zijn sportschool, weet de krant genoeg. 'If you ever want to try to get hold of Nick, you might want to visit the gym at 6am on a Monday.'

Tweetportret van daders mag toch niet

Toen vanaf een terrastafel in het centrum van Alphen aan den Rijn een iphone werd gestolen, ontdekte wijkagent Theo van der Hoek dat de dader op bewakingsbeelden te zien was. Hij nam met zijn mobieltje een foto van die beelden en vroeg zijn volgers op twitter naar de dief uit te kijken. Maar hij had daarvoor natuurlijk eerst toestemming moeten vragen aan het OM. De tweet werd daarom snel weggehaald. 'Politiewerk blijft mensenwerk', twitterde Van der Hoek. Volgens een woordvoerder van de politie was de bedoeling goed. De mogelijke dader is trouwens opgepakt.

Dit magazine verschijnt maandelijks.
De inhoud bestaat uit verzameld werk uit openbare internetbronnen.
Voor zover mogelijk zal de bron worden vermeld.

Gebruikte bronnen voor dit nummer:

Webwereld
Security.nl
Ixquick
Voelspriet
Zdnet
De Waarschuwingsdienst
Europol
Computable
Politiebronnen.nl

Opmerkingen kunt u mailen naar de redacteur.