PRIVACY OP HET INTERNET

OPTIMALE STRATEGIE VOOR DE INTERNETGEBRUIKER

Eindwerk voorgedragen door JOKE LAMIN
tot het behalen van het diploma
Bachelor in de Grafische en Digitale Media,
afstudeerrichting Multimediaproductie

Academiejaar 2006-2007

Interne promotor Dhr. P. De Pauw - Waterschoot
Externe promotor Dhr. G. Godderis

Arteveldehogeschool
Opleiding Grafische en Digitale Media - Industrieweg 228 - 9030 Mariakerke

WOORD VOORAF

In het laatste jaar van de opleiding Grafische en Digitale Media aan de Arteveldehogeschool in Gent wordt van de studenten verwacht dat zij een eindwerk schrijven. Aangezien een eindwerk het sluitstuk van een opleiding vormt, moest het onderwerp zowel verband houden met mijn afstudeerrichting Multimediaproductie, als mijn interesse weergeven. Na enig zoek- en schrapwerk koos ik ervoor privacy op het internet aan een onderzoek te onderwerpen.

Mijn eindwerk is bedoeld als praktische gids voor de gewone internetgebruiker, die hierin informatieve en bruikbare gegevens kan terugvinden. Met deze doelstelling voor ogen en in overleg met mijn promotoren heb ik de inhoud van mijn eindwerk vastgelegd.

Ik ben veel dank verschuldigd aan mijn externe promotor de heer G. Godderis, bedrijfsleider van Polaris Creative Solutions, die steeds bereikbaar was voor vragen en die vaak goede raad en bruikbare opmerkingen gaf. Verder wil ik mijn interne promotor de heer P. De Pauw – Waterschoot bedanken voor zijn kritische feedback en praktische aanvullingen op de inhoud. Dankzij deze twee heren is mijn eindwerk geworden tot wat u nu in de handen houdt: een praktische handleiding met een heleboel adviezen, zoals ik deze ook voor ogen had.

Daarnaast mag ik de heer V. Willems niet vergeten te bedanken voor zijn praktische richtlijnen.

Uiteraard wil ik ook mijn ouders bedanken omdat zij mij de kans gaven deze banaba-opleiding te volgen. Ik richt ook een dankwoord naar mijn vriendin voor de steun, de nuttige tips en de waardevolle taaladviezen.

Gent, 30 april 2007

Lamin Joke

Inhoudsopgave

Inleiding

Internet speelt een steeds grotere rol in ons leven, zonder dat we onszelf de vraag stellen welke impact dit medium op onze levens heeft. Overal laat je, zowel bewust als onbewust, informatie achter over jezelf. De een, die bijvoorbeeld een persoonlijk dagboek bijhoudt op een blog, is hier al meer bedreven in dan de ander, die internet misschien alleen gebruikt om e-mails te versturen. Maar hoe je het ook draait of keert: vanaf dat er verbinding gemaakt wordt met het internet worden er sporen nagelaten. Je privacy blijkt ineens niet meer zo privé.

De vraag of privacy op het internet wel bestaat, is een vraag die mij in vele opzichten intrigeert, en die in direct verband staat met vele andere vragen. Welke gegevens zijn er over mij op het internet te vinden? Hoe kan ik mijn privacy op het internet beschermen? Hoeveel controle heb ik als internetgebruiker over mijn eigen gegevens? Wat allemaal onder het begrip 'privacy' verstaan wordt, wordt in het eerste hoofdstuk duidelijk afgebakend.

Als internetgebruiker hoop je dat websites je persoonlijke en vertrouwelijke gegevens respecteren. Dit blijkt in de praktijk al eens anders te verlopen. De online risico's voor de privacy worden uitgebreid besproken in het tweede hoofdstuk.

Als eigenaar van een forum merk ik dat mensen soms totaal verschillend omspringen met hun privacy. Sommigen willen niet dat anderen kunnen zien wanneer zij online zijn, omdat zij dat ervaren als een inbreuk op hun privacy. Andere mensen posten de meest persoonlijke levensverhalen of foto's van hun hele gezin, zonder stil te staan bij de mogelijke gevolgen. Als je je privacy niet voldoende beschermt, kan dit immers gevolgen hebben. Deze worden in het derde hoofdstuk besproken.

Zelf kan je echter al een deel van de schade beperken, door de tips & tricks op te volgen die gegeven worden in het vierde hoofdstuk. Aan deze praktische oplossingen zijn echter pro's en contra's verbonden die je best in het achterhoofd houdt bij het surfen op internet. Gelukkig bestaan er ook wetten en andere initiatieven die helpen bij het beschermen van persoonlijke gegevens, een onderwerp dat grondig onder de loep wordt genomen in het vijfde hoofdstuk.

Voor de bedrijven die ons toegang verschaffen tot het internet, is een belangrijke rol weggelegd in het beschermen van onze privacy. Het beleid dat internetproviders voeren wordt bekeken in het zesde hoofdstuk.

Aangezien dit eindwerk de optimale strategie voor de internetgebruiker wil meegeven, bekijken we naast de thuisomgeving ook de situatie op het werk in het zevende hoofdstuk Hoe zit het met de wetgeving over het privé-internetgebruik op het werk? Mag een werkgever de e-mails van werknemers controleren zonder hen hiervan op de hoogte te brengen?

In het achtste hoofdstuk bespreek ik de test die ik gedurende een maand gevoerd heb om spam te verzamelen. In dit hoofdstuk ga ik in een tweede test op zoek naar persoonlijke informatie van een aantal proefpersonen.

Tot slot probeer ik op basis van al deze informatie tot een optimale strategie te komen voor de internetgebruiker.

1 WAT IS PRIVACY OP HET INTERNET

Volgens Van Dale:

pri•va•cy (de ~ (v.))

1 privéleven

in•ter•net (het ~)

1 wereldwijd netwerk van computers, gebaseerd op een gemeenschappelijk, gestandaardiseerd protocol => digitale snelweg, elektronische snelweg, informatiesnelweg, net

Privacy is een **ruim begrip** dat omschreven kan worden als de gelegenheid van mensen om zich af te zonderen, om storende invloeden van de buitenwereld te ontwijken. Volgens een andere beschrijving is privacy het grondwettelijke recht op bescherming van de persoonlijke levenssfeer. [1] Ruim honderd jaar geleden werd het begrip 'privacybescherming' geïntroduceerd door de Amerikaanse juristen Warren en Brandeis. Zij omschreven het recht op privacy ook wel als het recht om met rust te worden gelaten, 'the right to be left alone'. Het recht op privacy omhelst het recht om relaties aan te knopen met anderen en te onderhouden zonder inmenging door derden. [2]

Mensen hechten belang aan de bescherming van hun privacy. Dit gaat van de bescherming van persoonsgegevens, over de bescherming van het eigen lichaam en de eigen woning, de bescherming van familie- en gezinsleven, tot het recht vertrouwelijk te communiceren via brieven, telefoon, e-mail en dergelijke. Privacy betekent dat dergelijke bescherming en communicatie kan plaatsvinden zonder dat de buitenwereld daar inbreuk op maakt of er zelfs kennis van heeft. Het recht op privacy lijkt vanzelfsprekend, in de 'echte' wereld kunnen personen zich immers afzonderen om vertrouwelijke zaken te bespreken. Op het internet wordt het recht op privacy echter steeds minder controleerbaar. [3]

Privacy op het internet heeft enerzijds betrekking op de persoonlijke of vertrouwelijke gegevens die iemand over zijn privéleven achterlaat op het wereldwijde web, en anderzijds op de gegevens die door derden via het internet te verzamelen zijn. Een internetgebruiker denkt misschien onopgemerkt en anoniem op het internet te kunnen surfen, in werkelijkheid is dat anders. Privacy bestaat immers bijna niet op internet. Vanaf dat er op een computer verbinding gemaakt wordt met het internet om te surfen, chatten of e-mailen, worden de eerste sporen nagelaten die door derden opgepikt en gevolgd kunnen worden. De sporen die nagelaten worden, hoe ze opgepikt worden, en wat ertegen gedaan kan worden komen in dit eindwerk aan bod.

Privacy op het internet betekent niet hetzelfde als **veiligheid op het internet**. Veiligheid gaat over computerbeveiliging en beperkt zich meestal tot (het beschermen tegen) schadelijke invloeden van buitenaf, in tegenstelling tot privacy dat betrekking heeft op persoonlijke gegevens die via het internet te vinden zijn. [4]

[1] XS4ALL, *Privacy verklaring*, internet, http://www.xs4all.nl/overxs4all/privacy/, 2007-04-21.
[2] ICRI - INTERDISCIPLINARY CENTRE FOR LAW & ICT, *Privacy*, internet, http://www.law.kuleuven.ac.be/icri/david/E_Privacy.php, 2004-06-01.
[3] WIKIPEDIA, *Privacy*, internet, http://nl.wikipedia.org/wiki/Privacy, 2007-04-22.
[4] LUDIT – LEUVENS UNIVERSITAIR DIENSTENCENTRUM VOOR INFORMATICA EN TELEMATICA, *Hou je computer veilig*, internet, http://ludit.kuleuven.be/software/beveiliging/, 2007-03-26.

Deze twee begrippen kunnen niet volledig losgekoppeld worden van elkaar aangezien een onvolledige computerbeveiliging kan leiden tot inbreuken op de online privacy, en omgekeerd kan een gebrekkige bescherming van de persoonlijke gegevens ertoe leiden dat schadelijke invloeden de computer bereiken.

Met betrekking tot privacy op het internet zijn er twee categorieën mensen te onderscheiden. Enerzijds zijn er de **mensen die sceptisch staan ten opzichte van internet**, die denken dat elke pop-up een virus is, en die internet enkel gebruiken om spelletjes te spelen of e-mails te versturen. Zij zullen niet zo snel persoonlijke gegevens prijsgeven op het internet, al is het maar omdat ze er geen flauw idee van hebben wat een blog of een forum is (deze termen komen later nog aan bod).

Anderzijds zijn er de **mensen die blindelings alles aan het internet toevertrouwen** door een eigen blog bij te houden, op forums te posten, eigen profielen aan te maken met daarop foto's en andere persoonlijke informatie in de hoop zo nieuwe mensen te leren kennen of gewoon omdat ze zichzelf op het internet willen zien staan. De 'fifteen minutes of fame' die vroeger zo gewild waren toen televisie het almachtige medium was, zijn nu veranderd in een situatie waarin iedereen die een blog heeft zichzelf uniek, speciaal en belangrijk vindt en zit te wachten tot anderen dit ook ontdekken.

Het is logisch dat over deze laatste groep mensen een heleboel persoonlijk informatie te vinden is. Vaak staan deze mensen er niet eens bij stil dat de informatie die ze nu op internet posten, ook nog gelezen kan worden over vijf jaar, of over tien jaar, enzovoort. Informatie verwijderen van het internet, is immers niet zo eenvoudig. Enkel wanneer je zelf de controle hebt over een website of er een mogelijkheid is om het betreffende profiel te verwijderen (in het geval van een blog bijvoorbeeld) kan je er zeker van zijn dat jouw persoonlijke informatie van het internet verdwijnt. Tenminste, als die informatie intussen niet door andere webservices of websites werd opgeslaan.

"Wat mogen anderen van mij weten? Hoeveel kan ik over mezelf prijsgeven op het internet?"

De belangrijkste regel die je kan toepassen om je eigen privacy op het internet te beschermen is jezelf de vraag stellen of je wil dat anderen dit over jou weten. Uiteindelijk kiest iedereen zelf welke persoonlijke of vertrouwelijk informatie op internet verschijnt. In sommige gevallen kan er geen rechtstreekse controle uitgeoefend worden, wanneer bijvoorbeeld een derde een verhaal vertelt waarin de persoon in kwestie voorkomt.

Wil je niet dat anderen over jou schrijven, dan kan je hen hiervan op de hoogte brengen. In ruil verwachten zij dan waarschijnlijk ook van jou dat je niets over hen schrijft. Het is dan ook logisch dat je over jezelf niets laat rondslingeren op het internet. De kans bestaat altijd dat anderen dit oppikken en ernaar verwijzen, zonder dat je dit eigenlijk wil of zonder dat je toestemming gevraagd wordt. Aangezien je deze informatie meestal zelf op internet geplaatst hebt, kan je hier weinig tegen beginnen.

"Wil ik wel dat anderen informatie over mij op internet kunnen vinden?"

Zowel bedrijven als personen kunnen vanalles over jou te weten komen als je je op het internet begeeft. Hoe actiever je surfgedrag, hoe meer er over jou gevonden kan worden. Door online enquêtes in te vullen, informatie aan te vragen of je in te schrijven op nieuwsbrieven, maak je je interesses kenbaar aan bedrijven.

Bedrijven spelen hierop in door potentiële klanten gerichte reclame en promoties te sturen. Je kan dit beschouwen als een last, omdat je tenslotte niet gevraagd hebt om dergelijke aanbiedingen, maar langs de andere kant kan je het ook beschouwen als doelgerichte advertising. Iedereen ontvangt liever een brief of e-mail van een bedrijf op naam, dan een onpersoonlijke begroeting als 'Geachte heer/mevrouw'.

In sommige gevallen kan het aangenaam zijn gegevens over anderen terug te vinden op het internet. Dit is bijvoorbeeld het geval wanneer je toevallig op gegevens van oude bekenden stuit. Ook kan je lotgenoten leren kennen, of mensen die dezelfde hobby of interesse delen als jezelf. Dus persoonlijke informatie op het internet plaatsen kan ook positieve gevolgen hebben. Dat hier eventueel ook negatieve gevolgen aan vasthangen, neem je er dan maar bij.

2 Mogelijke risico's met betrekking tot de privacy

Als we ons op het internet begeven, bestaat de kans dat we geconfronteerd worden met gevaren die een inbreuk kunnen betekenen op onze privacy. Deze kan je in 2 groepen onderverdelen: enerzijds de directe risico's die algemeen gekend zijn, en anderzijds de indirecte risico's die een zwaardere inbreuk betekenen op de privacy en eerder ongewenst zijn.

Directe risico's zijn eerder bewuste risico's waar de gebruiker zelf een invloed op kan uitoefenen, door bijvoorbeeld voor een alternatieve browser te kiezen. Bij de indirecte risico's is dit niet het geval. De gebruiker heeft zelf weinig controle over de indirecte risico's en kan zich enkel proberen te beschermen tegen deze risico's door bijvoorbeeld pop-upblokkering in te stellen. Indirecte risico's zijn ook niet meteen duidelijk zichtbaar doordat ze bijvoorbeeld op de achtergrond van de computer lopen.

2.1 Directe risico's

Directe risico's zijn de bewuste risico's waar iedereen die op internet surft, sowieso mee geconfronteerd wordt.

2.1.1 Browser

Om op het internet te surfen, wordt een browser gebruikt. Microsoft heeft met Internet Explorer bijna 90% van het marktaandeel van browsers in handen. Daarnaast zijn er echter nog andere spelers op de markt, waarvan Mozilla Firefox, Safari en Opera de bekendsten zijn.

Omdat een browser noodzakelijk is wanneer men zich op het internet begeeft, en omdat deze een toegangspoort vormt tot internet, is het belangrijk dat deze voldoet aan een paar veiligheidsvereisten: [5]

De browser mag geen beveiligingslekken vertonen.
Net zoals bij andere software, kunnen browsers programmeerfouten bevatten. Hackers gebruiken deze fouten om in te breken in andere computers. Wanneer er toch een lek gevonden wordt, moet dit zo snel mogelijk gedicht worden door bijvoorbeeld de nieuwste updates te installeren.
Logischerwijs gaan hackers zich eerder richten op een browser die een groot marktaandeel bezit, aangezien ze dan meer kans hebben op slagen.

De browser moet veilig met cookies kunnen omgaan.
Zoals eerder vermeld vormen cookies niet direct een beveiligingsprobleem, maar kunnen ze een gevaar voor de privacy vormen. Een goede browser laat toe dat de gebruiker zelf instellingen betreffende cookies kan aanpassen.

[5] LUDIT, *Een veilige browser*, internet, http://ludit.kuleuven.be/software/beveiliging/browser.html, 2007-03-26.

De browser moet ongewenste pop-up-vensters kunnen blokkeren.
Pop-up-vensters zijn meestal kleine browservensters met reclame die boven het huidige browservenster verschijnen wanneer een website bezocht wordt. Pop-under-vensters verschijnen onder het huidige browservenster en zijn dus niet meteen zichtbaar. Deze advertenties vormen vaak de oorzaak van ongewenste spyware. Een goede browser biedt de mogelijkheid ongewenste pop-ups (en pop-unders) te blokkeren, en gewenste pop-ups toe te laten. Wat spyware is, komt verder nog aan bod.

De browser moet het automatisch uitvoeren van onveilige programma's kunnen tegenhouden.
Tijdens het surfen worden bezoekers soms door onbetrouwbare websites naar bepaalde pagina's gelokt waar automatisch onveilige software op de achtergrond uitgevoerd wordt, zonder dat de gebruiker er weet van heeft. Dit ongewenste uitvoeren van onveilige programma's vormt een bedreiging voor de veiligheid van een computer en voor uw privacy. Een goede browser vraagt toestemming aan de gebruiker voordat mogelijk onveilige programma's uitgevoerd worden.

2.1.1.1 Internet Explorer

Internet Explorer wordt standaard geïnstalleerd onder Microsoft Windows, en is daardoor dé standaardbrowser op de meeste computers. Op een bepaald moment genoot Internet Explorer zelfs een bijna-alleenheerschappij van 95 procent. Dankzij de komst van een reeks alternatieven, slinkt dat marktaandeel nu stilaan weer.

Doordat Internet Explorer met een huidig marktaandeel van 90 procent nog steeds de meest populaire browser is, trekt dit uiteraard meer hackers aan dan een browser met een veel kleiner marktaandeel. Vroeger werden op vrij regelmatige basis nieuwe ernstige lekken in de software ontdekt, en miste de browser een aantal basisfunctionaliteiten voor veilige software, zoals het blokkeren van pop-ups en controle op automatisch uitvoeren van software. Zo kreeg spyware vrij spel op Internet Explorer, waardoor deze browser al snel synoniem stond voor 'onveilig'.

De laatste jaren is Microsoft bezig aan een inhaalbeweging op het gebied van veiligheid. In de meest recente versie van Internet Explorer krijgt spyware bijna geen kans meer en worden pop-ups automatisch geblokkeerd.

Internet Explorer wordt ook niet langer ontwikkeld als apart product, waardoor de nieuwe beveiligingsfunctionaliteiten enkel beschikbaar zijn wanneer de gebruiker onder Windows XP werkt en Service Pack 2 geïnstalleerd heeft. Gebruikers van andere Windows-versies krijgen enkel nog de kritische updates aangereikt. Dit betekent dat in Explorer-versies die niet onder Windows XP draaien, sowieso veiligheidsfunctionaliteiten ontbreken.

2.1.1.2 Mozilla Firefox

Deze browser vertoont – volgens Mozilla zelf – een minimum aan beveiligingslekken. Door de ingebouwde update-functie blijft de browser up-to-date, de cookie-instellingen kunnen door de gebruiker beheerd worden, pop-ups worden standaard geblokkeerd, en de automatische uitvoering van programma's wordt tegengehouden. Firefox voldoet dus grotendeels aan de veiligheidsvereisten.

In Firefox worden geregeld beveiligingslekken gevonden, maar Mozilla Foundation doet er dan alles aan om deze zo snel mogelijk te dichten. In heel 2004 was Internet Explorer slechts 9 dagen volledig beschermd tegen alle bekende lekken, voor Firefox was dit meer dan 290 dagen.

2.1.1.3 Safari

Safari is de standaardbrowser op Mac. Via de Software Updates worden gevonden veiligheidslekken onmiddellijk gedicht. De browser blokkeert pop-ups en is verder minder vatbaar voor schadelijke software omdat de meeste malware (virussen, spyware,…) specifiek voor Windows ontwikkeld wordt en dus enkel onder Windows schade kan aanrichten.

2.1.1.4 Opera

Ook hier geldt het verhaal dat weinig krakers hun pijlen richten op een browser met een klein marktaandeel. Verhalen over Opera-veiligheidslekken duiken dan ook zelden op. Deze browser beschikt ook over een ingebouwd antiphishingsysteem, pop-ups kunnen geblokkeerd worden en cookie-instellingen kunnen aangepast worden. [6]

2.1.2 Cookies

Cookies zijn kleine tekstbestandjes die door een website aangemaakt worden en bijgehouden worden in cache op de computer. De cookies bevatten meestal informatie over de acties die op een website ondernomen worden: welke voorkeuren gekozen worden, welke pagina's bezocht worden, ... [7]

Deze informatie wil de website graag bijhouden. Dit kan beschouwd worden als een vorm van privacyschending, maar over het algemeen is er geen probleem omdat een cookie in principe alleen maar kan gelezen worden door de bijhorende website. Aangezien cookies persoonlijke informatie over surfgedrag en mogelijk zelfs vertrouwelijke informatie zoals kredietkaarten en wachtwoorden bevatten, moet er voorzichtig mee omgesprongen worden.

Een goedaardig gebruik van cookies is bijvoorbeeld het geval bij een website die in twee talen bestaat. De website houdt de persoonlijke taalvoorkeur bij in een cookie. Cookies kunnen ook kwaadaardig bedoeld zijn. Zo kan een cookie van een verkoopwebsite bijvoorbeeld een Visanummer opslaan.

Tracking cookies zijn cookies die de bedoeling hebben het surfgedrag van gebruikers in kaart te brengen. Dit is geen virus en kan ook niet gebruikt worden om malware zoals virussen en spyware op een computer te plaatsen. Cookies zijn bedoeld om het leven van de surfer gemakkelijker te maken, niet om het surfgedrag te volgen. Eigenaars die tracking cookies verspreiden beweren dat door het gebruik van tracking cookies, beter kan ingespeeld worden op persoonlijke wensen van de gebruiker. Zo kunnen banners getoond worden die de gebruiker meer aanspreken, omdat ze passen in zijn profiel. Deze targeted advertising wordt direct marketing genoemd. [8]

[6] OPERA, *Security*, internet, http://www.opera.com/products/desktop/security/, 2007-04-22.
[7] LUDIT, *Cookies*, internet, http://ludit.kuleuven.be/software/beveiliging/cookies.html, 2007-03-26.
[8] JAWWI, *Cookies*, internet, http://www.jawwi.nl/malware/cookies.html, 2007-03-26.

2.1.3 E-mail

Bij een inschrijving via het internet, zoals bijvoorbeeld op digitale nieuwsbrieven en op fora, is het opgeven van een e-mailadres noodzakelijk. Hierbij wordt gevraagd of dit e-mailadres al dan niet aan derden mag doorgegeven worden. Wanneer u hiervoor toestemming geeft, kunnen uw gegevens doorgegeven worden aan anderen die u vervolgens ook zullen contacteren via e-mail.

Aangezien e-mail voor privédoeleinden een ander karakter heeft dan professionele e-mails, is het belangrijk dat dit onderscheid behouden wordt. Persoonlijke e-mails wenst u liever niet in uw professionele inbox te ontvangen, en professionele contacten stuurt u liever geen e-mail vanaf uw adres *knuffelbeertje@hotmail.com*.

2.1.4 Licenties

Bij software die op legale wijze verkregen werd, zitten vaak systemen ingebouwd die controle uitoefenen over het kopiëren, gebruiken en aanpassen van deze software. De maker van een computerprogramma heeft automatisch het auteursrecht daarop. Om de ontwikkelde programma's beschikbaar te stellen aan derden, moet de auteur in een licentie toestemming geven voor bepaalde handelingen, zodat derden de software kunnen gebruiken. [9]

Er bestaan verschillende soorten softwarelicenties; de drie belangrijkste zijn freeware, shareware en open source. **Freeware** is de bekendste licentie. Duizenden programma's werken onder deze licentie, maar de meeste van deze programma's hebben ook een shareware-tegenhanger. De freeware-versies zijn meestal populairder omdat ze gratis te verkrijgen zijn. De broncode wordt niet vrijgegeven en staat onder auteursrecht. Aan freeware-programma's mag niets veranderd worden. Het bekendste voorbeeld is Windows Media Player.

Shareware is ook gratis te verkrijgen, maar na een bepaalde periode van gebruik moet er wel voor betaald worden. Tegenwoordig zijn er van bijna elk programma wel trail-versies beschikbaar, zoals bijvoorbeeld van Adobe InDesign. Meestal zijn dit versies die gedurende een proefperiode gebruikt kunnen worden, en na deze proefperiode moet er betaald worden indien men dit programma nog verder wil gebruiken.

Open source software is eigenlijk ook freeware, met als enige verschil dat ook de broncode kan gedownload worden. Aan deze code mag vanalles aangepast worden, zonder toestemming van de auteur. Voordeel hiervan is dat foutjes en aanpassingen snel gemaakt kunnen worden. Dit leidt tot meer stabiele en beter werkende software. Linux en Firefox zijn bekende open source programma's. [10]

De meeste licenties beperken het aantal computers waarop de software kan worden geïnstalleerd of het aantal gebruikers dat deze software mag gebruiken. Bij vrije software krijgt de gebruiker nauwelijks beperkingen opgelegd. Een mogelijke beperking kan zijn dat de gebruiker de software niet tegen betaling mag doorverkopen of dat de naam van de auteur op kopieën vermeld moet worden. [11]

[9] IUS MENTIS, *Het kiezen van een software licentie*, internet, http://www.iusmentis.com/computerprogrammas/licenties/kiezen/, 2007-04-14.
[10] INFO NU, *Softwarelicenties*, internet, http://pc-en-internet.infonu.nl/software/850-softwarelicenties.html, 2007-04-14.
[11] WIKIPEDIA, *Softwarelicentie*, internet, http://nl.wikipedia.org/wiki/Softwarelicentie, 2007-04-14.

Via het internet kan gecontroleerd worden of licenties nageleefd worden. Zo heeft Microsoft in juli 2005 het programma **Windows Genuine Advantage (WGA)** ontwikkeld. Dit programma wil gebruikers die een volledige licentie van Windows bezitten extra voordelen bieden, en Microsoft helpen zijn intellectuele eigendom te beschermen en het illegale gebruik van Windows bestrijden. Met WGA wil Microsoft voornamelijk softwarepiraterij de kop indrukken. In juni 2006 werd WGA uitgebreid met een service die WGA Notifications genoemd wordt. Deze service meldt mensen die een illegale versie van Windows draaien dat ze mogelijk het slachtoffer zijn van softwarepiraterij, en reikt hen een oplossing aan voor dit probleem.

Dit programma heeft twee taken: enerzijds valideren en anderzijds meldingen geven. Het valideren houdt in dat er vastgesteld wordt of er een geldige licentie aanwezig is voor de Microsoft-software die op een computer draait. De meldingen wijzen de gebruiker er af en toe op dat er problemen kunnen zijn met de licentie van de Windows-versie of herinneren de gebruiker eraan dat er nieuwe updates beschikbaar zijn. Om de geïnstalleerde software te kunnen valideren, moet WGA bepaalde gegevens aangaande de configuratie van de computer verzamelen.

De volgende gegevens worden verzameld:

- merk en model van de computer;
- gegevens over het besturingssysteem en andere programma's die Genuine Advantage gebruiken;
- land- en taalinstellingen;
- uniek nummer dat door WGA aan de computer wordt toegekend (Globally Unique Identifier of GUID);
- product-id en productcode;
- BIOS-naam, revisienummer en revisiedatum;
- serienummer van de harde schijf.

Naast de hierboven vermelde configuratiegegevens wordt ook informatie verstuurd met betrekking tot de installatie van WGA en het resultaat van de validatiecontrole. Wanneer de computer verbinding maakt met een WGA-website of WGA-server wordt het IP-adres van deze computer tijdelijk geregistreerd. Aan de hand van het IP-adres wordt bepaalde informatie over de computer vastgesteld. Deze informatie bevat de geografische locatie, Internet Service Provider (ISP) en domeinnaam. Volgens Microsoft behoort het verwijderen van deze logbestanden waarin de IP-adressen worden opgeslaan, ook tot de standaardprocedure. Informatie die door Microsoft wordt verzameld, wordt nooit gebruikt om de identiteit van een gebruiker te achterhalen of contact op te nemen, zo verklaart Microsoft. [12]

Toch kan dit programma als een duidelijk probleem met betrekking tot de privacy gezien worden. Mensen vragen immers niet om deze meldingen, ze willen niet dat hun computer onbewust gecontroleerd wordt door Microsoft zonder dat ze hier zelf veel controle over hebben.

[12] MICROSOFT, *Legitieme Microsoft-software*, internet, http://www.microsoft.com/genuine/Facts.aspx?displaylang=nl, 2007-04-14.

2.1.5 Digital Rights Management (DRM)

DRM is de technologie waarmee digitale bestanden beveiligd worden om illegale verspreiding te voorkomen en vrij gebruik van digitale content te beperken. Zo kan de auteur of de verdeler bepalen welke handelingen mogen gebeuren met bepaalde bestanden zonder dat de gebruiker daar expliciet toestemming voor moet vragen. De gebruiker kan deze bestanden dan enkel openen wanneer hij hiervoor een licentie heeft. In deze gebruikslicentie worden de rechten en de plichten van de gebruiker vastgelegd. Omdat er bij deze technologie veel beperkingen worden opgelegd aan de gebruiker, wordt deze ook wel Digital Restrictions Management genoemd. Een beperking kan zijn dat een bepaald liedje slechts twintig keer gratis beluisterd mag worden. Bekende voorbeelden van DRM-systemen voor audio en video zijn **Windows Media DRM** van Microsoft en **FairPlay** van Apple.

Voorstanders van DRM zijn ervan overtuigd dat zonder DRM piraterij vrij spel krijgt. Bedrijven zien hun inkomsten dalen door de illegale kopieën die gratis of tegen een lage prijs worden aangeboden via het internet. Dit heeft een invloed op de kwaliteit van wat er wel nog uitgebracht wordt, omdat er minder producten uitgebracht worden waar dan ook nog eens minder geld voor beschikbaar is.

Tegenstanders vinden dat het gebruik van digitale content vrij moet zijn. Door het gebruik van DRM blijft de controle over het gebruik van digitale bestanden volledig in handen van de producenten. Zij bepalen wat, waar en wanneer door DRM beschermde bestanden kunnen afgespeeld worden, waardoor de klant beperkt wordt in zijn vrijheid. Deze te sterke beperkingen vormen een belangrijk punt van kritiek.

Een ander punt van kritiek is dat er niet bepaald is wat er met de kopieerbeveiliging gebeurt na het verlopen van het auteursrecht. De beschermingstermijn van het auteursrecht loopt tot 70 jaar na het overlijden van de auteur. Maar het belangrijkste punt van kritiek is dat consumenten hun gekochte digitale bestanden slechts op bepaalde toestellen kunnen gebruiken. Muziek die werd gedownload via **iTunes** kan bijvoorbeeld enkel op een computer of een iPod afgespeeld worden, andere MP3-spelers kunnen deze nummers niet afspelen.

Zo liet de Europese Commissaris voor Consumentenbescherming, Meglena Kuneva, in maart 2007 volgende uitspraak noteren: "*Vindt u het normaal dat een cd door elke cd-speler kan worden afgespeeld, maar dat u een liedje dat u op iTunes koopt alleen kunt beluisteren op een iPod? Wel, ik niet. Dat moet veranderen.*". Met deze uitspraak verhoogt ze de druk op Apple om zijn verkochte muziekbestanden toegankelijk te maken voor alle draagbare muziekspelers. Al sinds de lancering van de iTunes Music Store in april 2003 krijgt Apple immers veel kritiek op zijn politiek.

Wie nu via de online muziekwinkel iTunes Music Store een liedje koopt, krijgt dat niet in het meest gangbare formaat, MP3, toegestuurd maar in AAC-formaat. Die bestanden zijn voorzien van de FairPlaytechnologie waardoor ze op maximaal vijf computers gespeeld kunnen worden en enkel op draagbare muziekspelers die AAC-ondersteunen. Met andere woorden: enkel op MP3-spelers die door Apple gemaakt worden, de zogenaamde iPods.

Apple reageerde op alle kritiek door te verklaren dat FairPlay enkel de toepassing van DRM of kopieerbeveiliging is die verplicht wordt door de platenlabels. Apple richtte een brief naar deze bedrijven

[13] MJK DISC, *Auteursrecht*, internet, http://www.kopieer-cd.be/sabam/auteursrecht.jsp, 2007-04-14.
[14] WIKIPEDIA, *Digital Rights Management*, internet, http://nl.wikipedia.org/wiki/Digital_Rights_Management, 2007-04-14.

om DRM af te schaffen, in de overtuiging dat dit mensen zal aanmoedigen legaal muziek te downloaden. In dezelfde brief opperde Apple nog dat minstens de helft van het volledige iTunesaanbod eind 2007 onbeveiligd te koop zal zijn. [15]

Vanaf mei 2007 zal alle muziek van platenmaatschappij EMI onbeveiligd op iTunes aangeboden worden. EMI is een van de vier grote muziekmaatschappijen in de wereld en herbergt artiesten zoals Robbie Williams, Coldplay en Moby. Met deze beslissing wordt de eerste voorzet gegeven om legaal aangekochte muziek niet langer te beperken door de aanwezigheid van DRM-software. [16]

Het **grote nadeel van DRM** is dus dat het de persoonlijke vrijheid beperkt van de consument die zijn product nochtans volstrekt legaal verkregen heeft. Aangezien geen enkel DRM-systeem volledig waterdicht is, blijven illegale kopieën verkrijgbaar op het internet, die bovendien nog eens DRM-vrij zijn. Enkel de consument die zijn product legaal aangekocht heeft, zit met de beperkingen opgelegd door de DRM-systemen. [17]

2.1.6 Forums en blogs

Internetforums en blogs zijn twee populaire middelen waar gebruikers hun meningen, vragen en opmerkingen kwijt kunnen.

Een **forum** heeft meestal een algemene startpagina die onderverdeeld is in verschillende thema's. Per thema staan verschillende onderwerpen waarop gereageerd kan worden door de leden. Meestal moet een gebruiker zich registreren alvorens hij een bericht kan posten. Hiervoor maakt een gebruiker een account aan onder een bepaalde nickname en met een avatar, dit zijn respectievelijk een naam en een afbeelding die getoond zal worden bij de berichten die deze gebruiker post. De onderwerpen en het niveau van de discussie kan enorm verschillen afhankelijk van de thema's. De leden zelf kunnen ook nieuwe onderwerpen aanbrengen of reageren op de bestaande onderwerpen. [18]

Een **blog** is een website waar regelmatig nieuwe informatie op verschijnt die omgekeerd chronologisch weergegeven wordt, met het meest recente bericht bovenaan. De informatie die op dergelijke site gegeven wordt kan gaan van persoonlijke aard zoals een dagboek, tot een serieuze blog waarbij de actualiteit of politiek besproken wordt. Gebruikers hebben de mogelijkheid om op elk bericht te reageren. Dit persoonlijke karakter maakt blogs interessant voor bezoekers. [19]

Forums en blogs staan open voor iedereen waardoor ze een unieke ontmoetingsplaats kunnen vormen voor mensen met bepaalde meningen en opvattingen. Maar die openheid houdt ook risico's in voor de privacy wanneer er niet voorzichtig mee wordt omgesprongen. Een forum beschikt meestal over een ruim archief dat tot vele jaren kan teruggaan. Berichten die jaren geleden gepost werden op een forum zijn dus nu waarschijnlijk nog steeds terug te vinden. Berichten die nu online geplaatst worden, zullen er over enkele jaren nog steeds staan. Op internet worden immers weinige zaken volledig gewist.

[15] DECAESTECKER, B., *Eurocommissaris valt over muziekmonopolie Apple*, De Morgen, 2007-03-13.
[16] MEEUS, R., *iTunesmuziek van EMI onbeveiligd maar duurder*, De Morgen, 2007-04-03.
[17] COMPUTERTAAL, *Wat is DRM?*, internet, http://www.computertaal.info/modules/articles/article.php?id=680, 2006-10-06.
[18] WIKIPEDIA, *Internetforum*, internet, http://nl.wikipedia.org/wiki/Internetforum, 2007-04-20.
[19] WIKIPEDIA, *Weblog*, internet, http://nl.wikipedia.org/wiki/Blog, 2007-04-28.

Verder is het perfect mogelijk voor een persoon om zich op een forum of een blog een totaal andere persoonlijkheid aan te meten. Zich anders voordoen dan in het echte leven is geen enkel probleem; er wordt een nickname of bijnaam gekozen die helemaal niets met de echte naam te maken heeft, gegevens hoeven niet allemaal ingevuld te worden en niemand checkt of een persoon echt is wie hij zegt dat hij is. Omdat deze anonimiteit zo verleidelijk is, maken personen hier wel eens misbruik van door berichten te posten op een forum of een blog die kwetsend, uitdagend of neerbuigend bedoeld zijn. Bij online communicatie worden berichten sowieso al snel verkeerd geïnterpreteerd omdat de factor 'lichaamstaal' ontbreekt die aan woorden en zinnen meer duiding kan geven. Wanneer dit gegeven in combinatie gebracht wordt met mensen die misbruik willen maken van hun anonimiteit, is het niet meer dan logisch dat dit al snel resulteert in hevige online discussies en relletjes.

Andere persoonlijke websites zoals profielen (bijvoorbeeld LookNmeet), fotosites (bijvoorbeeld Flickr) of spaces (bijvoorbeeld Windows Live Spaces) kunnen hier ook bij geplaatst worden. De hoeveelheid persoonlijke gegevens die een gebruiker prijsgeeft op dergelijke websites, kiest hij tenslotte zelf. Niemand wordt verplicht om zijn foto's of gegevens voor het gehele internet tentoon te spreiden.

Iedereen heeft recht op vrije meningsuiting. Als er echter (foutieve) informatie over anderen wordt meegedeeld, hebben deze op hun beurt recht op antwoord. Het internet wordt vaak gebruikt om anoniem kritiek te leveren op bepaalde mensen. Aangezien iedereen echter ook recht op privacy heeft, moet erop gelet worden dat de vrije meningsuiting niet eindigt in de privacyschending van derden. De naamvermelding (of vermelding van andere persoonlijke gegevens) van derden moet kunnen op een website, maar enkel wanneer de betreffende personen hiervan op de hoogte gebracht werden en hiervoor hun toestemming gaven.

2.1.7 Chatprogramma's

Chatprogramma's maken gebruik van instant messaging, onmiddellijke berichtgeving. Dit is een manier om via internet te communiceren met anderen. De term 'instant' wijst op het grote verschil met e-mail. Een e-mail kan altijd verstuurd worden ook wanneer de contactpersoon zijn computer niet gebruikt, maar instant messaging werkt enkel wanneer de contactpersoon aanwezig is. Dan kan er reëel met elkaar 'gepraat' worden via het internet, wat chatten genoemd wordt.

Enerzijds bestaan er chatprogramma's met chatrooms zoals IRC en anderzijds zijn er de chatprogramma's die werken met vriendenlijsten zoals MSN Messenger. Op de chatrooms kan iedereen inloggen en chatten met mensen die hij/zij niet kent zonder dat er eerst software moet gedownload worden, omdat alles web-based is. Bij chatprogramma's die werken met vriendenlijsten is dit niet het geval en moet het programma eerst gedownload worden. Bij vriendenlijsten moet er ook steeds wederzijdse toestemming gegeven worden voordat er met elkaar gechat kan worden. [20]

Het gevaar voor de privacy ligt in het feit dat mensen tegen een beeldscherm vaker meer durven zeggen dan in een reëel gesprek. Ook het feit dat chatters zich anoniem wanen omdat ze de persoon aan de andere kant niet in het echte leven kennen, speelt hierbij een belangrijke rol. Sommige mensen vertellen hun hele levensverhaal, gaande van dagdagelijkse zaken tot problemen of geheimen waar ze mee

[20] WIKIPEDIA, *Chatprogramma*, internet, http://nl.wikipedia.org/wiki/Chatprogramma, 2006-10-07.

zitten, immers gemakkelijker aan een onbekende. Gesprekken die via chatprogramma's verlopen, ontsporen gemakkelijker dan persoonlijke gesprekken, want net zoals bij een forum of een blog ontbreekt de non-verbale communicatie om de tekst te duiden.

Daarnaast wordt er tijdens het chatten vaak een webcam aangezet. Het is logisch dat deze een bedreiging vormt voor de privacy aangezien deze beelden opgenomen en dan verspreid kunnen worden.

2.1.8 IP-adres

Om verbinding te kunnen maken met het internet, krijgt iedere computer een uniek nummer toegewezen, het IP-adres waarbij IP staat voor Internet Protocol. Om het mogelijk te maken dat computers met elkaar kunnen communiceren, hebben ze een eigen vast IP-adres nodig. Bij het communiceren worden dan deze adressen met elkaar verbonden.

Een internetprovider kan altijd achterhalen welke persoon op welk tijdstip welk IP-adres gebruikte. Belgische providers houden een jaar lang de surfgegevens van gebruikers bij, dit is zo bij wet bepaald.

Wanneer een persoon naar een site surft, wordt er een www-adres getoond. Dit adres verwijst naar een IP-adres. Een DNS-server maakt deze vertaling. Elke keer er naar een site gesurft wordt, wordt het IP-adres meegestuurd naar die site. Servers bewaren al deze IP-adressen in log-files, en zo ook de rest van de surfgeschiedenis. Met wat kennis van zaken kunnen uit deze log-files hele delen uit je privéleven gereconstrueerd worden. Hier geldt ook de regel dat deze gegevens enkel met een gerechtelijk bevel mogen overgedragen worden aan de politie.

Enkel wanneer er daartoe een gerechtelijk bevel gegeven wordt, mag een internetprovider deze gegevens doorgeven aan de politiediensten. Inhoud van websites, chatlogs of inhoud van verzonden mails worden niet bewaard. In opdracht van een onderzoeksrechter kunnen politiediensten providers wel verplichten het internetverkeer van een bepaalde klant af te luisteren. [21]

[21] INTERNETJOURNALISTIEK, *Hoe privé is privacy op het internet?*, internet, http://www.internetjournalistiek.be/dossiers/detail_privacy.php?nieuwsid=96, 2003-12-07.

2.2.1 Spyware

Spyware is de verzamelnaam voor software die op de achtergrond informatie verzamelt over een computergebruiker en deze doorstuurt naar een externe partij. De term komt van het Engelse *spy* dat spion betekent, en het achtervoegsel *ware* dat aangeeft dat het om software gaat. Deze spion zal zich voornamelijk bezig houden met het verzamelen van vertrouwelijke informatie, maar bijvoorbeeld ook pop-ups laten verschijnen zelfs wanneer er niet op internet gesurft wordt. De informatie die verzameld wordt, gaat van eerder onschuldige gegevens zoals welke sites bezocht worden, tot vertrouwelijke informatie zoals gebruikersnamen en paswoorden, en in extreme gevallen zelfs kredietkaartnummers. Op regelmatige basis sturen de spyware-programma's de verzamelde informatie door naar een centrale databank, waar alle gegevens worden opgeslaan en doorverkocht aan derden.

Spyware wordt vaak onopgemerkt geïnstalleerd samen met andere software die gedownload wordt van het internet. Dit is vaak het geval bij dubieuze software zoals peer-to-peer programma's. Nu programmamakers minder inkomsten uit verkoop halen door het illegaal kopiëren van software, zoeken ze andere manieren om geld te verdienen. Spyware toevoegen aan programma's behoort dan tot de mogelijkheden. [22]

Aangezien spyware op de achtergrond draait, kan dit de werking van de computer vertragen. In tegenstelling tot virussen hebben spyware-programma's geen destructieve bedoelingen; spyware zal geen gegevens op een computer vernietigen of aanwezige software beschadigen. Het enige dat deze programma's doen, is informatie verzamelen over de computergebruiker en deze doorsturen. Maar daarin rust net het grote gevaar van spyware aangezien deze programma's een inbreuk betekenen op de privacy.

Een vorm van spyware zijn **keyloggers**, dit zijn programma's die op de achtergrond van een computer draaien en alle toetsaanslagen bijhouden. Alle letters die ingedrukt worden op een toetsenbord, inclusief vertrouwelijke gegevens zoals gebruiksnamen en paswoorden, worden in een bestand bijgehouden en dit wordt dan doorgestuurd naar een centrale databank. Keyloggers worden meestal onbewust samen met andere software binnengehaald, of via een e-mailbijlage, een virus of een Trojaans paard.

Er bestaan echter ook legitieme keyloggers die alle toetsaanslagen wegschrijven naar de harde schijf zodat bij een computercrash verloren informatie teruggevonden kan worden. Iemand kan dus opzettelijk een dergelijk programma installeren om zo vertrouwelijke informatie te achterhalen.

Browser Hijackers of **browserkapers** zijn een andere vorm van spyware. Deze nemen een deel van de browser over door bijvoorbeeld een zoekbalk te installeren die niet meer weggaat of een bepaalde startpagina in te stellen die niet meer veranderd kan worden. Op de achtergrond verzamelen deze spyware-programma's informatie om deze later door te sturen. [23]

Adware of **advertentieondersteunende software** is een minder bedreigende soort van spyware. Elke softwareapplicatie die advertenties weergeeft wanneer het draait, bevat adware. Deze software kan ook

[22] WIKIPEDIA, *Spyware*, internet, http://nl.wikipedia.org/wiki/Spyware, 2007-04-24.
[23] LUDIT, *Spyware, keyloggers en browserkapers*, internet http://ludit.kuleuven.be/software/beveiliging/watisspyware.html, 2005-04-21.

advertenties weergeven in een pop-upvenster. Adware biedt enerzijds **voordelen voor de eigenaars** van de software doordat de kosten voor de ontwikkeling terugverdiend worden, en anderzijds **voor de gebruiker** doordat de prijzen van de applicatie laag gehouden worden. Sommige adwareprogramma's verzamelen persoonlijke informatie over een gebruiker en sturen deze door naar derden, zonder dat de gebruiker hier weet van heeft. Dit wordt dan beschouwd als spyware. Niet alle adwareprogramma's houden echter persoonlijke gegevens bij over de gebruiker, dus niet alle adware is spyware.

2.2.2 Virussen

Spywareprogramma's worden vaak beschouwd als virussen. Beide worden geïnstalleerd zonder dat de gebruiker er weet van heeft en beide hebben nadelige gevolgen voor de computer en zijn gebruiker. Maar er zijn ook verschillen. Zo kopieert een virus zichzelf om andere computers te kunnen infecteren. Spyware daarentegen kopieert zichzelf in het algemeen niet. Virussen verspreiden zichzelf, doordat gebruikers onvoorzichtig omspringen met hun computer, zo onopvallend mogelijk. Spyware echter wordt geïnstalleerd doordat een gebruiker bewust onveilige of illegale software downloadt.

Een computervirus is een vorm van schadelijke software (malware). Deze programma's gaan zich nestelen in andere programma's of bestanden. Een virus kan zichzelf vermenigvuldigen, en wil andere computers ook besmetten. Verspreiding van het virus gebeurt wanneer bijvoorbeeld besmette bestanden doorgestuurd worden. Toegebrachte schade kan gaan van vervelende nevenwerkingen zoals de computer die trager draait, tot destructief gedrag zoals wissen van bestanden of wissen van de harde schijf. Virussen brengen dus schade toe aan software of aan bestanden.

Een **worm** is een virus dat zichzelf automatisch en direct over een netwerk verspreidt. Hierbij zijn geen handelingen van de computergebruiker nodig. Een worm zit ook niet vast aan andere bestanden, maar kan zichzelf verspreiden op een zelfstandige manier. Verspreiding gebeurt meestal aan de hand van e-mailadressen die op de computer aanwezig zijn. Een worm veroorzaakt meer netwerkverkeer waardoor andere programma's trager gaan werken en soms volledig stilvallen. De moderne virussen zijn bijna allemaal wormen.

Een **Trojaans paard of Trojan horse** lijkt op het eerste zicht een nuttig programma, maar blijkt bij nader inzien schade te veroorzaken aan een computer, een vergiftigd geschenk dus. Trojaanse paarden zijn programma's die andere dingen doen dan wat ze zeggen te doen, zoals bijvoorbeeld een computer toegankelijk maken voor andere virussen. Trojaanse paarden worden verspreid via internet, bijvoorbeeld als bijlage bij een e-mail die van een betrouwbare bron lijkt te komen of samen met software die via internet gedownload kan worden.

Een **hoax** heeft niets met echte virussen te maken, maar betreft een valse viruswaarschuwing. Iedereen kent de e-mails wel die waarschuwen voor een nieuw virus, waarbij taal gebruikt wordt die schrik wil aanjagen (genre 'dit virus wist onmiddellijk de harde schijf'). Meestal gaat het om een verzonnen virus. Een echte viruswaarschuwing zou immers veel zakelijker opgesteld zijn. De gebruiker wordt aangemoedigd de bewuste mail zo snel mogelijk door te sturen naar alle contactpersonen. Dit resulteert in een gigantische maar vooral nutteloze mailstroom. [24]

[24] LUDIT, *Virussen, wormen, Trojaanse paarden en hoaxen*, internet, http://ludit.kuleuven.be/software/beveiliging/virus.html, 2005-04-21.

2.2.3 Pop-ups

Pop-ups zijn kleine browservensters die reclame bevatten en die tijdens een surftocht ineens verschijnen boven het huidige browservenster. Pop-unders verschijnen onder het huidige browservenster. Deze reclamevensters vertonen zich bij het bezoeken of verlaten van een bepaalde site. Spyware komt vaak binnen via verdachte sites, wat te vermijden is door deze sites niet te bezoeken. Maar spyware kan ook binnengehaald worden via pop-ups, en deze zijn veel moeilijker om te ontwijken. Zelfs veilig surfgedrag kan niet garanderen dat er geen pop-ups zullen opduiken. [25]

Soms horen pop-ups gewoon bij een site en dan vormen ze geen enkel risico voor de privacy of veiligheid.

2.2.4 Spam

Spam of **UCE**, wat staat voor **Unsolicited Commercial E-mail**, is ongevraagde en bijna altijd ongewenste e-mail. Meestal gaat het om commerciële boodschappen die aan vele mensen tegelijk verstuurd worden. De afzenders van deze e-mails zijn niet bekend bij de ontvanger.

De gigantische hoeveelheid ongewenste mail maakt tegenwoordig meer dan de helft uit van de verstuurde e-mails. Dit houdt ongemak in voor zowel personen als bedrijven. Spam verstoort immers het e-mailverkeer, zeker omdat het met duizenden tegelijk verstuurd wordt, het reduceert productiviteit in een bedrijf, het betekent tijdsverspilling en bovendien irriteert het de ontvanger. De meeste spamboodschappen bestaan daarnaast nog eens uit aanstootgevende of illegale inhoud. Voor bedrijven die spammen betekent elektronische post een eenvoudige en goedkope manier om hun boodschap naar duizenden ontvangers te versturen, maar voor de ontvangers staat spam gelijk aan ellende. [26]

In ons land, en in de meeste andere landen, is spam wettelijk niet toegelaten, maar het bestrijden van spam is geen prioriteit voor de politie.

2.2.5 Reclame

Sinds 2003 is met de wet op e-commerce of e-handel in België een soft opt-in regime van kracht. Dit betekent dat elektronische post voor reclamedoeleinden enkel met voorafgaande toestemming gestuurd mag worden. Op deze regel zijn enkele uitzonderingen (zie hoofdstuk 5 over de wetgeving met betrekking tot privacy op het internet). [27]

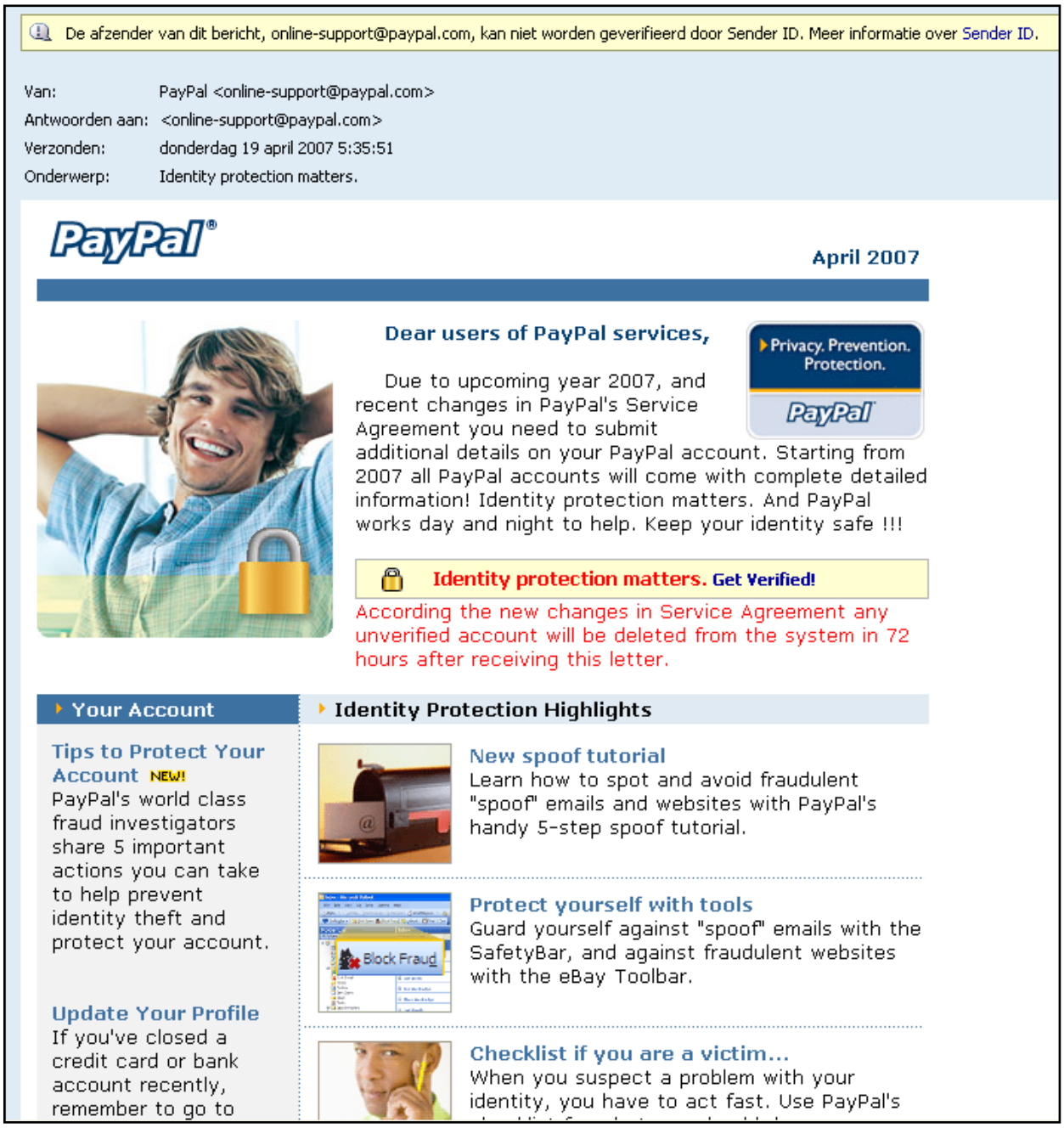
2.2.6 Phishing

Bij phishing draait het om het misleiden van de gebruiker door deze een e-mail te sturen waarin gevraagd wordt bepaalde gevoelige informatie prijs te geven. De afzender van de e-mail doet zich voor

[25] LUDIT, *Het blokkeren van pop-ups*, internet, http://ludit.kuleuven.be/software/beveiliging/popup.html, 2005-04-21.
[26] LUDIT, *Wat is spam?*, internet, http://ludit.kuleuven.be/software/beveiliging/watisspam.html, 2005-04-21.
[27] E-PRIVACY, *Soft opt-in regime in België*, internet, http://www.e-privacy.be/dossier.html, 2007-03-28.

als een betrouwbare instantie, bijvoorbeeld als een bank. In de mail wordt meestal verwezen naar een site waar de ontvanger zijn gevoelige informatie zoals paswoorden of kredietkaartinformatie kan ingeven. Deze site ziet er betrouwbaar uit omdat deze in dezelfde stijl is opgemaakt als bijvoorbeeld de originele site van de bank (zie bijlage I voor de nagemaakte website en bijlage II voor de echte website van **PayPal**). [28]

Phishing e-mails zijn gemakkelijk te herkennen omdat ze onpersoonlijk zijn. In principe zullen ze u nooit aanspreken met uw naam, terwijl bedrijven dit net wel proberen te doen wanneer ze u een e-mail sturen. Phishing e-mails verzoeken u zo snel mogelijk de gevraagde persoonlijke informatie door te geven, en meestal wordt er gedreigd met maatregelen wanneer u niet binnen een bepaalde termijn reageert. In deze e-mails wordt soms gezegd dat uw gegevens verloren gegaan zijn waardoor u verzocht wordt deze opnieuw in te geven. De meeste phishing e-mails zijn ook opgesteld in het Engels of in gebrekkig Nederlands. Hieraan kunt u deze e-mails herkennen.



Afb. 1: Een voorbeeld van een phishing-mail

[28] LUDIT, *Phishing*, internet, http://ludit.kuleuven.be/software/beveiliging/phishing.html, 2005-04-21.

Een gulden regel tegen phishing is: wees waakzaam en kritisch. Normaal gezien zal een bank u bijvoorbeeld nooit via het internet vragen om uw financiële informatie, net zoals uw werkgever geen e-mails zal sturen om uw paswoorden te vragen. Bij twijfel kan u steeds de afzender controleren, want bij phishing blijkt het afzenderadres meestal vervalst.

2.2.7 Webstatistieken

Webstatistieken geven een overzicht van de activiteiten die bezoekers ondernemen op een website. Door het analyseren van deze statistieken kan het succes van een site gemeten worden en kunnen er verbeteringen doorgevoerd worden. De software die deze statistieken genereert en bijhoudt, draait vaak op de webserver waar de website staat. Er bestaan ook bedrijven die online webstatistieken aanbieden, **Nedstat** is hiervan een bekend voorbeeld.

Webstatistieken geven informatie over:

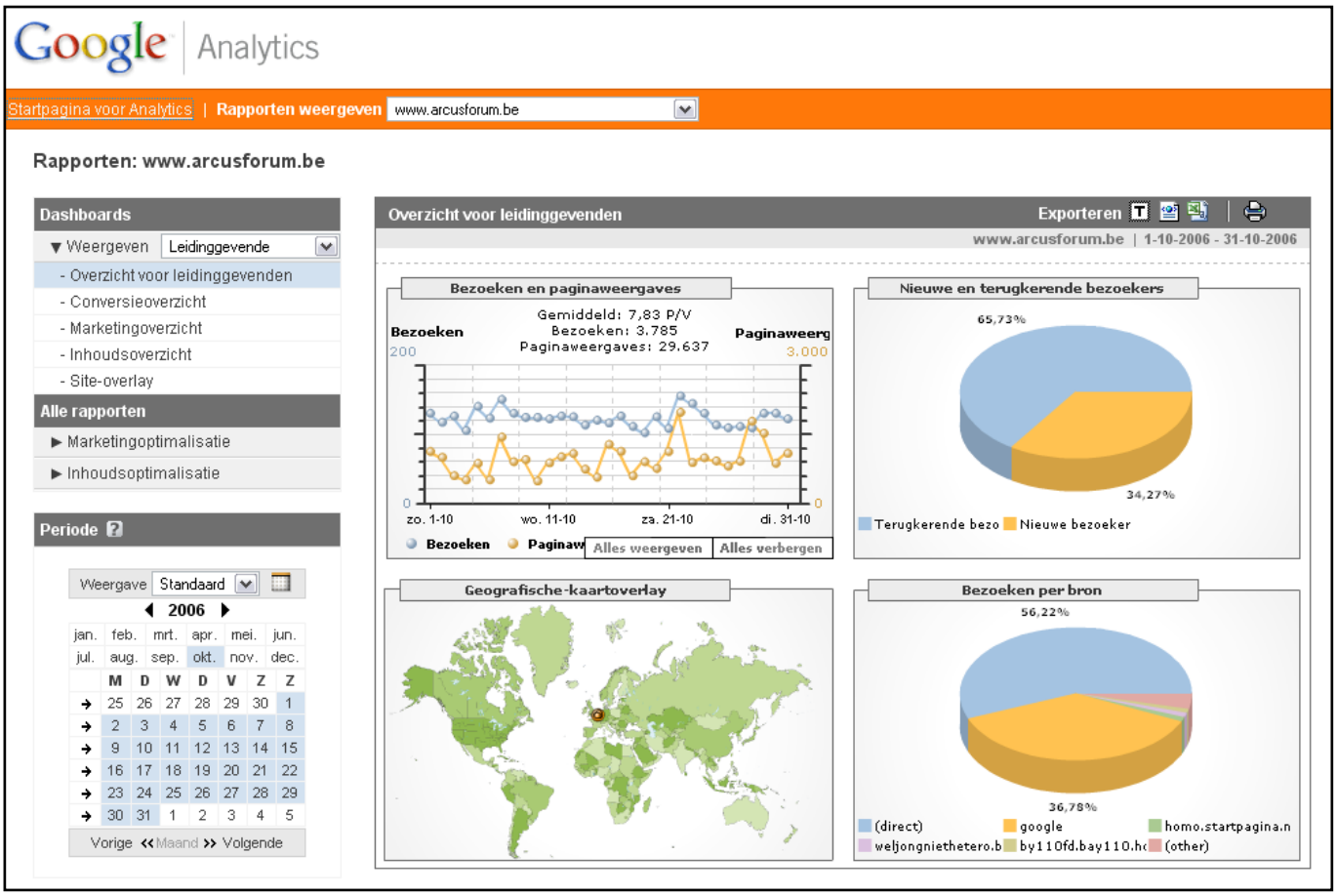
- welke pagina's het meest bezocht worden;
- het aantal bezoekers;
- de tijd die bezoekers doorbrengen op een bepaalde site;
- hoe bezoekers op een bepaalde site terechtkomen;
- bezoekers die al dan niet terugkeren na hun eerste bezoek aan een bepaalde site;
- welke pagina bezoekers als laatste bezoeken op een bepaalde site.

Verder kunnen gegevens verzameld worden over de computer waarmee de site bekeken wordt. Het is bijvoorbeeld mogelijk om te zien welke browser de bezoeker heeft, welk besturingssysteem hij gebruikt, in welke tijdzone hij zich bevindt, tot zelfs de resolutie van zijn beeldscherm. [29]

Webstatistieken gaan op volgende manier tewerk. Bij iedere verbinding tussen een bepaalde site en een gebruiker, worden pagina's opgevraagd. Deze verwijzen naar bestanden die op een server staan. Bij het oproepen van een pagina wordt het bijhorende bestand verstuurd naar de computer van de bezoeker. Alle data die samenhangt met dit bestand kan worden vastgelegd en weergegeven in grafieken en tabellen. [30]

Een ander bekend voorbeeld van statistieken voor analyse van websitebezoek is **Google Analytics**. Op volgende afbeelding is te zien welke gegevens zoal opgevraagd kunnen worden.

[29] ZO WERKT, *Webstatistieken: overige*, internet, http://www.zowerkt.nl/internet/web/webstatistieken_overige.html, 2007-03-29.
[30] WIZZBIT, *Wat zijn webstatistieken?*, internet, http://www.wizzbit.nl/index.php?id=34, 2007-03-29.



Afb. 2: Een screenshot van Google Analytics (voor grotere versie: zie bijlage III)

De vier grafieken in dit rapport bieden een momentopname van de bezoeken aan de website. [31] Weergegeven worden:

- het totale aantal bezoeken aan en paginaweergaves van de website, het gemiddelde aantal paginaweergaves per bezoek (P/V) en het aantal bezoeken en paginaweergaves voor een bepaalde periode;
- het aantal nieuwe en terugkerende bezoekers;
- uit welke plaatsen de meeste bezoekers naar de website komen;
- de belangrijkste verwijzende bronnen.

Eigenaars van een website kunnen op basis van deze grafieken resultaten bekend maken over het bereik, het gebruik en de effectiviteit van hun website. Bezoekers van sites zijn zich niet altijd bewust van het feit dat hun gegevens verzameld worden. Nochtans wordt dit meestal wel in kleine lettertjes vermeld op sites onder het onderdeel 'privacybeleid'.

Als internetgebruikers zich niet realiseren dat een website dergelijke informatie verzamelt, kan dit gezien worden als een soort schending van privacy. Meestal gaat het echter over redelijk onschuldige informatie waarbij gegevens niet geïndividualiseerd worden, en waardoor er dus niet van een echte inbreuk op de privacy gesproken kan worden.

[31] GOOGLE ANALYTICS, *Nieuw: Google Analytics, geavanceerd, eenvoudig, gratis*, internet, http://www.google.com/analytics/nl-NL/index.html, 2007-03-29.

2.2.8 Peer-to-peer- of P2P-software

Met P2P-software kunnen muziek, video's, bestanden en softwareprogramma's wereldwijd via het internet worden gedeeld. Met P2P-programma's zoals **Kazaa**, **LimeWire**, **BitTorrent**, en **BearShare** kan er online gezocht worden naar andere gebruikers om bestanden met hen te delen. In peer-to-peer-netwerken (of P2P) zijn alle computers gelijkwaardig. Iedere computer kan op elk moment gelijk welke rol opnemen. Van gebruikers die downloaden, wordt een tegenprestatie verwacht. Op de computer wordt een map opengesteld zodat andere gebruikers de bestanden die hierin aanwezig zijn, op hun beurt kunnen downloaden.

Hoewel dit een efficiënte technologie is om bestanden uit te wisselen, wordt deze vaak in een negatief daglicht gesteld. Hiervoor zijn twee redenen. Ten eerste worden de wetten op het **auteursrecht overtreden** omdat de bestanden die uitgewisseld worden, vaak auteursrechtelijk beschermd zijn. Miljoenen muziek- en filmliefhebbers liggen niet wakker van deze illegale praktijken en verkiezen een gratis digitale kopie boven een duur origineel exemplaar. Ten tweede worden de computers blootgesteld aan **ongewenste software**. Wanneer bestanden van het internet gedownload worden, kunnen deze virussen, spyware en andere ongewenste software bevatten. [32]

Verder is het ook mogelijk om via peer-to-peerprogramma's de bestanden op de computer van iemand anders te doorzoeken. Mensen die zich hier niet van bewust zijn, lopen gevaar wanneer ze bepaalde delen van hun harde schijf niet afschermen voor downloaders. Wanneer persoonlijke bestanden vrij downloadbaar zijn, zijn daar natuurlijk risico's aan verbonden: identiteitsdiefstal, hacking, ... (zie hoofdstuk 3).

2.2.9 Zoekmachines

Een zoekmachines is een online dienst die informatie zoekt op het internet aan de hand van de zoektermen die ingegeven worden. **Google** is de bekendste, maar daarnaast bestaan er vele andere: **Yahoo**, **AltaVista**, **Hotbot**, **Excite**, **Infoseek**,… Met deze zoekmachines kan natuurlijk ook gezocht worden naar personen. Als de naam van een persoon ergens op het internet staat, is het zeer waarschijnlijk dat de zoekmachine deze naam vindt, tegelijkertijd met andere informatie over deze persoon. Zoekmachines laten soms ook toe te zoeken doorheen nieuwsgroepen op basis van een e-mailadres. [33]

Een naam door een zoekmachine halen levert een schat aan informatie op. De persoon in kwestie hoeft niet eens zelf voor deze informatie gezorgd te hebben. Het probleem bij internetprivacy ligt vaak in de gegevens die anderen over een bepaalde persoon online plaatsen. Om een voorbeeld te geven: bedrijven plaatsen vaak de namen van hun werknemers op hun site, net zoals schoolsites meestal hun leerlingen opsommen met bijhorende studierichting.

In principe heeft een persoon bevoegdheid over de eigen persoonsgegevens, ook als anderen die online plaatsen. Maar in praktijk blijkt het moeilijk deze wettelijke bescherming te laten naleven. Het is onmogelijk alle informatie te screenen die online verschijnt over een bepaalde persoon.

[32] MICROSOFT, *Voordelen en risico's van het delen van bestanden via een peer-to-peer-netwerk*, internet, http://www.microsoft.com/belux/nl/athome/security/online/p2p_file_sharing.mspx, 2005-07-06.
[33] AUSTRALIAN GOVERNMENT – OFFICE OF THE PRIVACY COMMISSIONER, *Protecting your privacy on the Internet*, internet, http://www.privacy.gov.au/internet/internet_privacy/, 2007-03-30.

Verder is het bij inbreuken niet zo evident iets te ondernemen tegen beheerders van een site die zich aan de andere kant van de oceaan bevinden. Bovendien zijn er soms meerdere mensen met dezelfde naam, waardoor sowieso al verwarring kan ontstaan.

Zoekmachines werken zo nauwgezet dat mensen vaak schrikken wanneer ze zichzelf via een zoekmachine opzoeken. Persoonlijke informatie blijkt voor het grijpen te liggen, wat vervelend kan zijn. Extra vervelend is dat op het internet geen informatie verloren gaat. Bij het ondertekenen van een online petitie met naam en voornaam realiseert een persoon zich niet dat dit vaak jaren later nog teruggevonden kan worden door zoekmachines. Hetzelfde geldt voor het posten op forums of blogs. Stel dat een persoon een hele tijd geleden een bericht over alcoholverslaving gepost heeft op een forum. Het spreekt voor zich dat deze persoon daar op een sollicitatiegesprek niet mee geconfronteerd wil worden.

Steeds vaker bereiden personeelsverantwoordelijken zich voor op een sollicitatie door de naam van de sollicitant door een zoekmachine te halen. Zo kan de werkgever relevante informatie vinden met betrekking tot bijvoorbeeld eerdere werkervaringen, maar er zal evengoed irrelevante informatie tevoorschijn komen.

Om duidelijk te maken hoeveel persoonlijke informatie via een site als Google gevonden kan worden, deed de nieuwssite News.com in 2005 een test door **Eric Schmidt**, algemeen directeur van Google, zelf te 'googlen'. Dertig minuten volstonden om informatie te vinden over zijn salaris, hobby's, politieke voorkeur en woonplaats. Schmidt zelf was niet opgezet met de zaak en kondigde een tijdelijke informatiestop af tegenover **News.com**. Dit voorbeeld maakt duidelijk dat er meer persoonlijke gegevens te vinden zijn via zoekmachines dan een persoon soms verwacht. [34]

Google registreert de zoekopdrachten van miljoenen gebruikers en bewaart deze. Dat resulteert in gedetailleerde informatie over het zoekgedrag. Concurrerende zoekmachines bewaren het zoekgedrag van hun gebruikers ook, maar omdat Google naar eigen zeggen de meeste gebruikers heeft, levert dat een krachtige database van persoonlijke interesses op. [35]

[34] VISTERIN, W., *Onvindbaar blijven op het net*, internet, http://www.optiseo.be/onvindbaarophetnet.htm, 2005-11-29.
[35] NIBURU, *Google-baas ontdekt nadeel van zoekmachine*, internet, http://www.niburu.nl/index.php?showarticle.php?articleID=9203, 2005-09-20.

2.3.1 Integratie van televisie en internet

Dankzij de groeiende interesse voor integratie tussen televisie en internet wordt de droom van marketeers werkelijk: one-to-one marketing. In tegenstelling tot massamarketing, waarbij een onpersoonlijk bericht naar een grote groep mensen gestuurd wordt, wordt met one-to-one marketing een persoonlijk bericht naar een individuele persoon gestuurd. Wanneer digitale televisie en internet gecombineerd worden, is het mogelijk perfect te volgen naar welke programma's er gekeken wordt. Op die manier kunnen marketeers te weten komen waar de interesses van de kijker liggen, en hierop gaan inspelen door de kijker doelgerichte advertenties voor te schotelen. Als een persoon bijvoorbeeld vaak naar kookprogramma's kijkt, zullen er advertenties voor kookboeken getoond worden.

Met interactieve digitale televisie (**iDTV**) heeft de kijker via het tv-scherm toegang tot allerlei mogelijkheden zoals interactiviteit in tv-uitzendingen (stemmen, meespelen), programma's opnemen op de harde schijf, films en programma op aanvraag, communicatie (e-mails versturen en chatten), enzovoort. De populariteit van **YouTube**, de website waar iedereen filmpjes kan uploaden en bekijken, bevestigt eveneens de stelling dat mensen steeds vaker zelf willen beslissen wanneer ze naar welke programma's kijken. Met **Joost** willen de makers van **Kazaa** (peer-to-peersysteem) en **Skype** (gratis internettelefonie) nog een stapje verder gaan. Met Joost moet het mogelijk zijn zelf te kiezen wanneer er naar welke programma's gekeken wordt, en ondertussen te discussiëren met iedereen die naar hetzelfde programma kijkt.

Bij Joost zullen de kijkgewoontes van elke gebruiker geregistreerd kunnen worden. De makers geloven heel wat geld uit advertenties te kunnen halen omdat adverteerders veel beter dan bij een traditionele zender het profiel van de kijkers zullen kennen. Alle fans van een bepaald programma zoals bijvoorbeeld Lost of Prison Break zijn op hetzelfde moment bereikbaar voor adverteerders. Via andere wegen als mailinglists en dergelijke zullen ze nog meer te weten kunnen komen over de kijkers. Op die manier wil Joost samen met de adverteerders het mogelijk maken veel minder maar veel doelgerichtere advertenties uit te zenden. [36]

Dit komt de kijkervaring ten goede, aangezien er niet constant reclameblokken zullen zijn die de programma's onderbreken. Langs de andere kant wordt wel bijgehouden naar welke programma's elke gebruiker kijkt, wat ook beschouwd kan worden als een inbreuk op de privacy.

2.3.2 Elektronische identiteitskaart of eID

België telde op 19 maart 2007 bijna vijf miljoen actieve eID-kaarten. Tegen 2008 zal het merendeel van de Belgen een eID hebben en 31 december 2009 is het definitieve einde van het papieren tijdperk. De eID is de wettelijke identiteitskaart voor Belgen. Wat met de papieren identiteitskaart mogelijk was (identiteit bewijzen en reizen naar EU-landen) is nog steeds mogelijk, maar wordt nu uitgebreid met volgende functionaliteiten: identiteit bewijzen via het internet, een elektronische handtekening plaatsen of officiële documenten aanvragen en formulieren invullen via het internet.

[36] DECAESTECKER, B., *Joost mag weten hoe de toekomst van tv eruitziet*, De Morgen, 2007-04-06.

Naarmate de eID ingeburgerd geraakt, zal ze voor steeds meer toepassingen gebruikt kunnen worden: bijvoorbeeld als bibliotheekkaart, als handtekening voor aankopen via het internet, als toegangssleutel tot het bedrijfsnetwerk of tot veilige chatruimtes, als identiteitsbewijs bij online reservatie van een hotel, ...

De eID-kaart bevat een microchip die adresgegevens bevat en elektronische gegevens (zogenaamde digitale certificaten) die de identiteit van een persoon bevestigen wanneer de eID in een kaartlezer wordt gestopt. Via deze kaartlezer kunnen bijvoorbeeld documenten elektronisch ondertekend worden. [37]

De drie belangrijkste diensten die nu gebruikt kunnen worden samen met een eID, zijn:
• **informatie opvragen en doorsturen:** rijksregistergegevens kunnen gecontroleerd worden, de personenbelasting kan online doorgestuurd worden;
• **elektronische handtekening:** e-mails kunnen aangetekend verzonden worden, documenten kunnen voorzien worden van een wettige handtekening;
• **veilige toegang:** bij **Selor** krijgt een persoon toegang tot de persoonlijke selectie van vacatures, binnenkort zal het mogelijk zijn bepaalde chatruimtes te koppelen aan de eID zodat bijvoorbeeld enkel kinderen toegang krijgen.

De eID zal steeds een belangrijkere rol gaan spelen. Zowel overheid als privé-ondernemingen zullen gretig gebruik willen maken van de mogelijkheden van de eID om nieuwe diensten aan te bieden. Het nut van deze diensten is het leven gemakkelijker maken, maar langs de andere kant roept deze kaart ook vele vragen op, waar niet steeds een duidelijk antwoord op te vinden is. Hoe zit het bijvoorbeeld met de veiligheid van de kaart zelf en de software die nodig is om de kaart te lezen, is er misbruik mogelijk, weegt het opgeven van 'anonimiteit' op tegen de voordelen, wordt het internet veiliger met het gebruik van de eID, …

Verder werkt de eID-kaart met een pincode, net zoals een bankkaart. Het lijkt dus waarschijnlijk dat misbruik mogelijk is wanneer iemand de pincode van de eID van een andere persoon kent. Met betrekking tot deze kwestie en andere vragen die in verband staan met veiligheid op het internet, heeft de Belgische overheid een website opgesteld die 'binnenkort' online bereikbaar zal zijn. Die 'binnenkort' vermeldt evenwel geen specifieke datum. [38]

[37] FEDICT – FOD INFORMATIE- EN COMMUNICATIETECHNOLOGIE, *Over eID*, internet, http://eid.belgium.be/nl/navigation/12000/index.html, 2007-04-20.
[38] FEDICT, *Meer weten over eID en veiligheid op je pc?*, internet, http://www.s-days.be, nog niet bereikbaar.

3 Gevolgen van gebrekkige bescherming

3.1 Algemene gevolgen

De algemene gevolgen van een gebrekkige bescherming van persoonlijke gegevens op het internet kunnen zeer uiteenlopend zijn. Spyware en virussen zorgen ervoor dat een computer geïnfecteerd raakt, gegevens begint te versturen, trager loopt, en eventueel zelfs geformatteerd moet worden.

Bij het surfen op internet en dan vooral bij het gebruiken van zoekmachines is de gebruiker er meestal niet van bewust dat zijn sporen op het internet gevolgd en bewaard worden. Aangezien zoektermen vaak een weerspiegeling zijn van werkelijke interesses, kunnen deze – wanneer ze gecombineerd worden – vaak verwijzen naar een bepaalde persoon.

Wanneer iemand op een forum of een blog allerlei persoonlijke informatie prijsgeeft, kan dit door zoekmachines opgepikt worden. Degene die dit postte, heeft dan nog weinig controle over wie deze gegevens kan bekijken. In ieder geval is het moeilijk om volledige controle te bewaren over privégegevens aangezien ook andere mensen informatie online kunnen plaatsen, al dan niet met medeweten van de persoon in kwestie.

Wanneer een kwaadwillige persoon in het bezit komt van deze persoonlijke gegevens, kan hij overgaan tot stalking of chantage via het internet. Identiteitsdiefstal is nog een stapje verder, maar behoort ook tot de mogelijkheden van criminelen.

3.2 Vrijgeven van zoekgeschiedenis

In augustus 2006 speelde zich in de Verenigde Staten het **America Online (AOL)** privacy-schandaal af. De zoekgeschiedenis van 658 000 AOL-gebruikers over een periode van drie maanden werd gepubliceerd op de site van AOL's nieuwe zoekmachine. De bedoeling was om wetenschappers en statistici inzicht te geven in de manier waarop mensen omgaan met internet. Aan de hand van een zoekterm kon gekeken worden welke gebruikers, aangeduid met een gebruikersnummer, deze zoekterm reeds eerder ingevoerd hadden. Verder was het mogelijk om via het specifieke gebruikersnummer te kijken welke zoektermen deze persoon voordien allemaal ingegeven had. Persoonlijke gegevens van de gebruikers werden wel verwijderd voordat de zoekmachine online werd geplaatst. [39]

Op zich lijkt het een handig gegeven om zo gelijkaardige zoektermen te vinden die in verbinding staan met wat oorspronkelijk gezocht werd, maar wie de zaak verder onderzoekt, ontdekt dat het via bepaalde gegevens mogelijk is om de identiteit van de gebruiker te achterhalen. Dit was natuurlijk geenzins de bedoeling van AOL, maar lokte wel kritiek uit onder privacyexperts die vinden dat het vrijgeven van dergelijke gegevens een schending van de privacy is. [40]

Deze vrijwillige bekendmaking van zoekgegevens door AOL staat haaks op het feit dat internetbedrijf **Google** in januari 2006 weigerde zoekgegevens van gebruikers door te spelen aan de Amerikaanse

[39] IXQUICK, *Ixquick beschermt uw privacy!*, internet, http://eu.ixquick.com/ned/protect_privacy.html, 2007-03-19.
[40] KAWAMOTO, D. en MILLS, E., *AOL apologizes for release of user search data*, internet, http://news.com.com/AOL+apologizes+for+release+of+user+search+data/2100-1030_3-6102793.html, 2006-08-07.

overheid. [41] Google was echter wel de enige zoekmachine die niet meteen toegaf aan de eisen, in tegenstelling tot **Yahoo**, **Microsoft MSN** en **AOL** die wel meteen de gevraagde zoekgegevens overmaakten aan de Amerikaanse overheid. Enkele maanden later werd Google dan toch door de rechtbank verplicht bepaalde gegevens uit zijn databanken beschikbaar te stellen voor de overheid, die deze gegevens wil gebruiken om een wet door te drukken die kinderporno via het internet bestrijdt.

Deze twee zaken maken duidelijk dat wat iemand op het internet doet, niet altijd binnen de privésfeer blijft. Onder het motto '*Do no evil, fear no evil*' verzamelen zoekmachines gebruikersinformatie. Zoekmachines houden per gebruiker de persoonlijke zoekgegevens bij in zogenaamde log-files: welke zoektermen ingegeven worden, op welk tijdstip, de links waar u op klikt en uw IP-adres. Deze gegevens worden allemaal opgeslagen in bestanden die bijgehouden worden door de zoekmachines. De vraag waarom ze dit doen is moeilijker te beantwoorden dan de vraag waarom ze het niet zouden doen. Er bestaat geen wet die zoekmachines verbiedt de zoekgeschiedenis bij te houden. Dataopslag is goedkoop en bovendien slaan zoekmachines liever data op dan deze te verwijderen. [42]

Soms kan het handig zijn zoekgeschiedenis bij te houden, bijvoorbeeld om fraude tegen te gaan waarbij het ene bedrijf klikt op de advertenties van een concurrent om diens kosten te doen stijgen. Bedrijven kunnen namelijk opteren voor speciale advertentieplaatsen op bijvoorbeeld de site van Google en betalen dan per aangeklikte link een klein bedrag aan Google. Een andere reden die door Google genoemd wordt om de gigantische hoeveelheid aan zoekinformatie te bewaren, is dat er zo betere zoekresultaten bovenaan komen te staan en dat de advertenties zo doelgerichter zijn. [43] Mensen maken namelijk hun interesse kenbaar door de zoektermen die ze ingeven. Aangezien advertenties de belangrijkste bron van inkomsten vormen voor Google, is het wenselijk dat deze advertenties aan de juiste doelgroep aangeboden wordt. Deze mensen zullen sneller geneigd zijn te klikken op advertenties die passen binnen hun interesse.

Meestal blijkt de gebruikersdata die op deze manier verzameld wordt door zoekmachines, voornamelijk gegeerd door onder andere marketingbedrijven, verzekeringsmaatschappijen, … In de gebruikersprofielen bevindt zich immers een schat aan persoonlijke informatie. Zoals duidelijk werd uit het voorbeeld met Google die door de rechtbank verplicht werd bepaalde gegevens vrij te geven, zit ook de overheid achter deze persoonlijke zoekgegevens aan. Hackers en criminele organisaties doen ook hun uiterste best om in het bezit te komen van uw zoekgegevens. Met andere woorden, bij het zoeken op het internet via zoekmachines kan de privacy in het gedrang komen.

De enige zoekmachine die geen privégegevens bijhoudt is **Ixquick**. Vanaf juni 2006 vernietigt deze meta-zoekmachine alle persoonlijke zoekgegevens van haar gebruikers die worden opgeslagen in log-files. Concreet betekent dit dat Ixquick wel nog zoekgegevens bewaart, maar deze kunnen nooit meer gelinkt worden aan een bepaalde persoon, aan een gebruikersnummer of aan een IP-adres. Een programma zorgt ervoor dat het IP-adres verwijderd en overschreven wordt in de log-files. Gebruikers zoeken via Ixquick gelijktijdig in de 14 beste zoekmachines, wat meta-zoeken wordt genoemd, zonder dat hun gegevens geregistreerd worden. Hierdoor genieten ze van een optimale privacy en maximale zoekprestaties. [44]

[41] MEEUS, R., *Amerikaanse overheid eist gegevens van Google op*, De Morgen, 2006-01-20.
[42] MCCULLAGH, D., *FAQ : Protecting yourself from search engines*, internet, http://news.com.com/FAQ+Protecting+yourself+from+search+engines/2100-1025_3-6103486.html, 2006-08-08.
[43] SCHOFIELD, J., *Has the time finally come to stop using Google?*, internet, http://technology.guardian.co.uk/weekly/story/0,,1851363,00.html, 2006-08-17.
[44] DE TELEGRAAF, *Ixquick schakelt 'Big Brother' uit*, internet, http://www.telegraaf.nl/i-mail/45395771/Ixquick_schakelt_%18Big_Brother%19_uit.html, 2006-06-27.

3.3 Identiteitsdiefstal of Identity Theft

Sommige jongeren vinden het leuk om een wachtwoord voor **MSN Messenger** van iemand te weten te komen door speciale software te gebruiken of door het simpelweg te vragen. Met die gegevens kunnen ze dan inloggen op de account van een andere persoon en zich vervolgens voordoen als deze persoon. Dit klinkt redelijk onschuldig, maar het is wel een vorm van identiteitsdiefstal.

Identiteitsdiefstal is namelijk het onrechtmatig gebruikmaken van iemands persoonlijke gegevens. [45] In de eerste twee maanden van 2007 is de dreiging van identiteitsdiefstal met 200 procent toegenomen. Een beveiligingsbedrijf uit de Verenigde Staten geeft aan dat het aantal downloads met kwaadaardige software gestegen is tot 60 000 per dag. In diezelfde periode is er zelfs een maximum genoteerd van 140 000 downloads op een dag. [46]

Bij phishing wordt een persoon gemaild met de vraag persoonlijke informatie zoals paswoorden of kredietkaartgegevens te onthullen. Vaak maakt phishing deel uit van een strategie om de identiteit te stellen van de onschuldige ontvanger van de mail. De oplichters proberen zoveel mogelijk over een bepaalde persoon te weten te komen zodat ze die gegevens kunnen gebruiken om in naam van die persoon illegale praktijken uit te oefenen. In de Verenigde Staten wordt bijvoorbeeld vaak een krediet geopend op naam van die persoon. Verder kunnen er met deze gegevens accounts aangemaakt worden bij banken of bij winkels op het internet, maar de informatie kan ook gebruikt worden om iemand via e-mail af te persen.

Identiteitsdiefstal is problematisch aan het worden, voornamelijk in het Engelse taalgebied. Jaarlijks verdienen criminelen miljarden euro's door met gestolen inloggegevens artikelen te kopen en deze bij tussenpersonen te laten afleveren. De tussenpersonen voorkomen dat de echte misdadigers kunnen opgespoord worden. Een consumentenorganisatie deed in 2005 een onderzoek waaruit bleek dat een op vier Engelsen ooit het slachtoffer werd van identiteitsfraude. In de **Verenigde Staten** werd in 2005 voor meer dan vijftig miljoen dollar schade geleden als gevolg van identiteitsdiefstal. Hier werd wel rekening gehouden met het stelen van gegevens in de fysieke leefomgeving. Het stelen van een kredietkaartbonnetje waarop alle benodigde gegevens vermeld staan is immers voldoende om iemands kredietkaart te gebruiken. In 2006 was de schade door identiteitsfraude in de V.S. afgenomen tot 47 miljard dollar.

In december 2006 werden in **Nederland** phishingmails onderschept waarbij klanten van een **PayPal**-dienst gevraagd werden hun gegevens op een nagemaakte site van de betaaldienst in te geven. [47] PayPal is een dienst die het mogelijk maakt om online betalingen te verzenden en te ontvangen. [48]

Nog in Nederland moest de bank **ABN Amro** in maart 2007 klanten waarschuwen voor een nep e-mail die afkomstig lijkt van de bank en die gebruikers aanspoort gegevens in te vullen op een nagemaakte ABN Amro-website. [49]

[45] TAALTELEFOON, *Identiteitsdiefstal*, internet, http://www.vlaanderen.be/servlet/Satellite?cid=1126670405504&pagename=taaltelefoon%2FPage%2FArticle&c=Page, 2002-12-16.
[46] WEBWERELD, *Dreiging identiteitsdiefstal met 200 procent toegenomen*, internet, http://www.webwereld.nl/ref/rss/45705, 2007-03-28.
[47] EJURE, *Phishingmail richt zich op Nederlandse PayPalklanten*, internet, http://www.ejure.nl/f_dossier/dossier_id=171/news_id=3734/news.html, 2006-12-13.
[48] PAYPAL, *De eenvoudige snelle veilige manier om te betalen*, internet, http://www.paypal.nl/nl, 2007-04-02.
[49] WEBWERELD, *ABN AMRO waarschuwt voor phishing e-mail*, internet, http://www.webwereld.nl/articles/45591/abn-amro-waarschuwt-voor-phishing-e-mail.html, 2007-03-21.

3.4 Computerinbraak of hacking

Computerinbraak of hacking is het op een of andere manier ongeoorloofd binnendringen in een computersysteem. Een gebruiker maakt hierbij verbinding met een netwerk, een server of een bestand zonder dat hij daarvoor de toestemming heeft. Inbreken in andermans computer is bij wet verboden. Niemand mag dus op een andere computer rondsnuffelen zonder dat de eigenaar hiervoor toestemming gegeven heeft.

Computers en systemen van anderen kunnen om verschillende redenen interessant zijn voor criminelen. Door middel van hacking kunnen zij immers persoonlijke gegevens bemachtigen zoals bankgegevens, loginnamen en wachtwoorden. Soms zoeken ze ook naar bedrijfsgevoelige informatie. Daarnaast kunnen inbrekers of hackers er ook op uit zijn om de ruimte op een andere computer te misbruiken. Ze kunnen bijvoorbeeld een website op een computer plaatsen, zodat de eigenaar betaalt voor het verkeer op die website. Ook kunnen ze illegale bestanden zoals video's of software op een computer opslaan. Vervolgens gaan anderen deze bestanden downloaden van deze computer. Dat maakt de eigenaar van de gehackte computer medeplichtig aan heling. Verder kunnen criminelen schadelijke programma's installeren en van op afstand controleren, bijvoorbeeld om spam te versturen of om andere computers aan te vallen, zonder dat de eigenaar hier maar iets van vermoedt. [50]

Er is ook een onderscheid te maken tussen white en black hacking. **White-hat hackers** zijn de 'goeden', zij die computers hacken als hobby of om de aandacht op veiligheidslekken te vestigen. **Black-hat hackers** of **crackers (krakers)** zijn de 'kwaden', zij die computers kraken met criminele bedoelingen. De eerste groep is meestal niet uit op persoonlijke gegevens, maar gaat eerder computers hacken voor het plezier, de tweede groep daarentegen is er wel op uit om vertrouwelijke gegevens te bemachtigen. [51]

3.5 Cyberstalking

Stalking of belaging is het herhaaldelijk lastigvallen, achtervolgen, contacteren of bedreigen van een persoon. Bij cyberstalking gebeurt dit via internet: via forum, chatprogramma, e-mail. Het slachtoffer ervaart stalking als een zware inbreuk op de privacy. Dit verziekt het leven soms zodanig dat er psychische schade opgelopen wordt.

Omdat er geen fysiek contact aan te pas komt, wordt het online lastigvallen en bedreigen vaak als minder erg beschouwd dan fysieke stalking. Daarnaast gebeurt cyberstalking meestal anoniem en vanaf grote afstand, maar daarom betekent dit nog niet dat de dreiging minder groot of reëel is. Internet maakt immers een steeds groter deel uit van ons persoonlijke en professionele leven, waardoor stalkers niet alleen **makkelijk aan persoonlijke informatie** geraken, maar ook nog eens veel kansen tot communicatie krijgen. Door de grote hoeveelheid aan persoonlijke informatie die op het internet beschikbaar is, kan een cyberstalker gemakkelijk veel te weten komen over een potentieel slachtoffer.

Verder voelen cyberstalkers zich veilig door de **anonimiteit** die heerst op internet. Potentiële stalkers kunnen of willen hun slachtoffer vaak niet via de telefoon benaderen. Het internet lijkt hen ideaal om

[50] XS4ALL, *Wat is computerinbraak?*, internet, http://www.xs4all.nl/veiligheid/inbraak/index.php, 2007-04-03.
[51] INFORMATION SECURITY, *White Hat/Black Hat Hackers*, internet, http://www.yourwindow.to/information-security/gl_whitehatblackhathackers.htm, 2007-04-22.

hun slachtoffer lastig te vallen of te bedreigen omdat zij dan anoniem kunnen werken. Het gebruiksgemak en het onpersoonlijke karakter van internetcommunicatie verlagen de barrières voor cyberstalking. Voor de dader lijken de risico's kleiner. Hij waant zich in een voordelige positie. Het slachtoffer heeft geen idee wie de dader is: een vorige geliefde, een totale vreemde, of gewoon iemand die een grap wil uithalen.

Cyberstalkers kunnen ver gaan in hun bedreigingen en intimidaties. Zo kunnen er speciale programma's gebruikt worden om op bepaalde of willekeurige tijdstippen berichten te versturen zonder fysiek aanwezig te zijn bij de computer. Een cyberstalker kan ook andere internetgebruikers aansporen om een slachtoffer lastig te vallen of te bedreigen via een forum of chatroom. Dit uit zich in bijvoorbeeld controversiële of verleidelijke berichten waaronder naam, telefoonnummer of e-mailadres van het slachtoffer geplaatst worden.

De inspanningen van cyberstalkers zijn minimaal, maar de impact op slachtoffers is groot. Zij worden gedwongen hun sociale leven te beperken of aanpassen uit angst ook fysiek lastig te worden gevallen. Slachtoffers van stalking gaan proberen aan hun belagers te ontkomen door te verhuizen en door te veranderen van telefoonnummer, e-mail en soms zelfs van werk. Wanneer de stalking blijft aanhouden, krijgen slachtoffers vaak psychische problemen. Zij gaan bijvoorbeeld lijden aan angstgevoelens, chronische slaapstoornissen, vermoeidheid of hoofdpijn. Stalking heeft in ieder geval een ingrijpende invloed op het leven van het slachtoffer.

Aangezien er niet altijd direct contact is tussen de cyberstalker en zijn slachtoffer, is het moeilijk voor justitie en politie om de stalker te identificeren, te lokaliseren en te arresteren. Vaak vormt cyberstalken trouwens, net zoals bij fysieke stalking, een voorbode op meer serieus agressief gedrag. Hieruit kan besloten worden dat cyberstalking een groeiend probleem vormt in de huidige samenleving. [52]

[52] SOCIOSITE, *CyberStalking: belaagd op het internet*, internet, http://www.sociosite.org/cyberstalking.php, 2006-05-04.

4 TIPS & TRICKS VOOR HET BESCHERMEN VAN DE PRIVACY

Mogelijke oplossingen tegen de gevaren die uw privacy op het internet bedreigen, zijn overal beschikbaar. De oplossingen die hier volgen zijn bedoeld voor de **modale thuisgebruikers** en beschermen reeds een groot deel van de privacy, maar uiteraard zijn er nog meer oplossingen.

4.1 ALGEMENE TIPS

Zonder rekening te houden met de specifieke activiteiten die op een computer verricht worden, zijn er een paar **algemene regels** die een computergebruiker sowieso in het achterhoofd dient te houden: [53]

- installeer beveiligingssoftware op de computer;
- geef nooit wachtwoorden of vertrouwelijke informatie door aan onbekenden;
- beveilig een draadloos netwerk;
- bewaar rekeningnummers, wachtwoorden en dergelijke op een veilige plaats;
- doe enkel elektronische bankverrichtingen op betrouwbare websites;
- pas op met het prijsgeven van persoonlijke informatie op websites.

Er zijn ook enkele richtlijnen die de hoeveelheid **spam** in een mailbox kunnen beperken:

- reageer nooit op spammails, ook niet door erop te antwoorden;
- laat een e-mailadres nooit zomaar achter op een website, een forum of een blog;
- gebruik chatprogramma's enkel om te chatten met bekenden;
- beperk het aantal e-mailadressen: hoe meer e-mailadressen, hoe meer kans op spam;
- vul geen formulieren in op onbetrouwbare websites;
- maak geen e-mailadressen van anderen zomaar openbaar.

Om het risico op **virussen en spyware** te verlagen, zijn er ook enkele vuistregels:

- open nooit bestanden die in e-mails zitten die verstuurd werden door onbekenden;
- open ook nooit bijlagen bij verdachte e-mails, ook al werden deze verstuurd door bekenden;
- pas op met het uitwisselen van bestanden via peer-to-peernetwerken;
- wees voorzichtig met gratis software, laat deze eerst scannen door een antivirusprogramma;
- download geen gratis bestanden of programma's tenzij de aanbieder betrouwbaar is;
- vermijd onbetrouwbare websites zoals pornowebsites of websites met illegale software;
- klik nooit op advertenties die u wijsmaken dat u gewonnen heeft of dat de computer gevaar loopt.

Om te vermijden dat u het slachtoffer wordt van **phishing of oplichterij**, zijn hier enkele tips waar best op gelet wordt:

- ga nooit in op een commercieel voorstel van een onbekende afzender;
- ga nooit in op een e-mail die vraagt om bankgegevens of wachtwoorden in te vullen;
- besef dat een e-mail die er officieel en echt uitziet, dat daarom niet automatisch ook is;

[53] SPAMSQUAD, *Checklist met adviezen voor een veilig internetgedrag*, internet, http://www.spamsquad.be/nl/fiches/fiche21.html?q=, 2007-04-04.

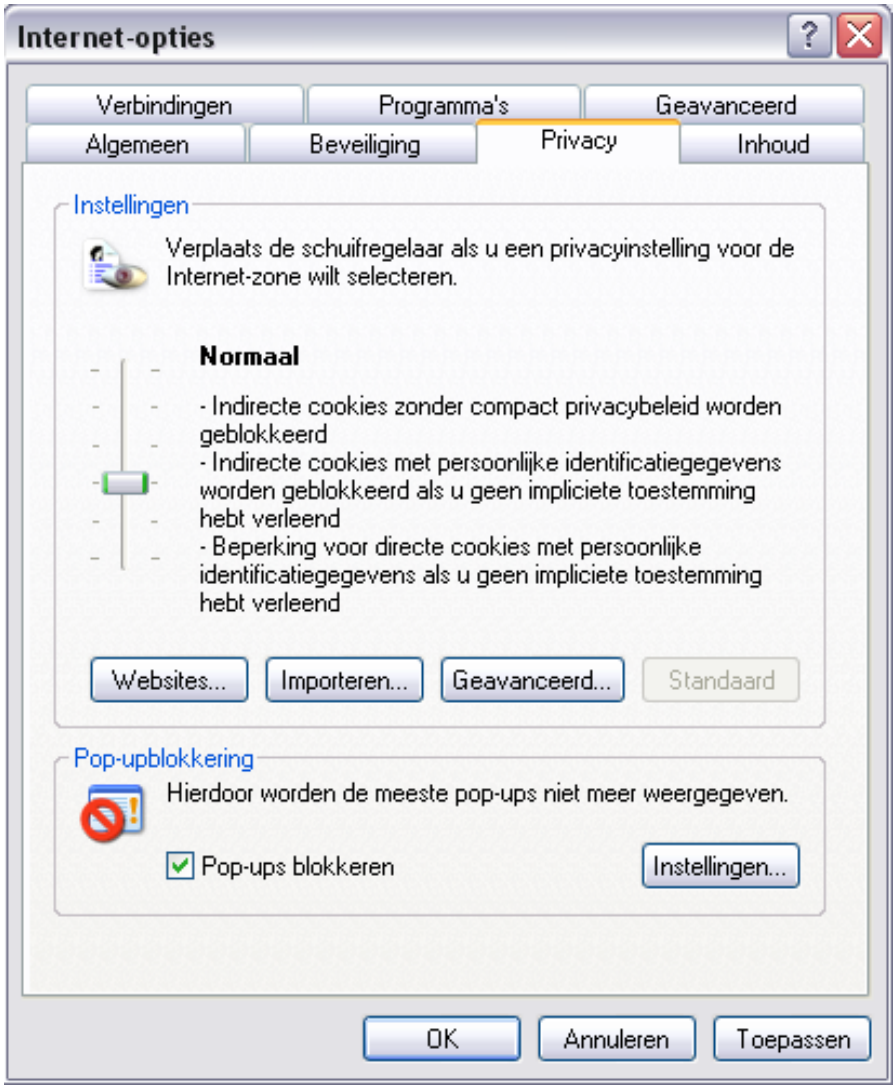
- schrijf nooit geld over aan onbekenden enkel op basis van een e-mail;
- verander wachtwoorden geregeld.

Enkele tips die hierboven vermeld staan, worden in de volgende puntjes verder uitgewerkt, aangevuld met verdere raadgevingen.

4.2 Optimale instellingen voor browser

4.2.1 Internet Explorer

In de meeste browsers kan perfect ingesteld worden hoe er met cookies en pop-ups moet omgegaan worden. In Internet Explorer staat een standaardniveau van cookiebescherming aan, tenzij dit anders ingesteld wordt door de gebruiker. Deze instellingen zijn te vinden via Extra (Tools) en dan Internet opties (Options), en daar naar het tabblad Privacy te gaan. [54]

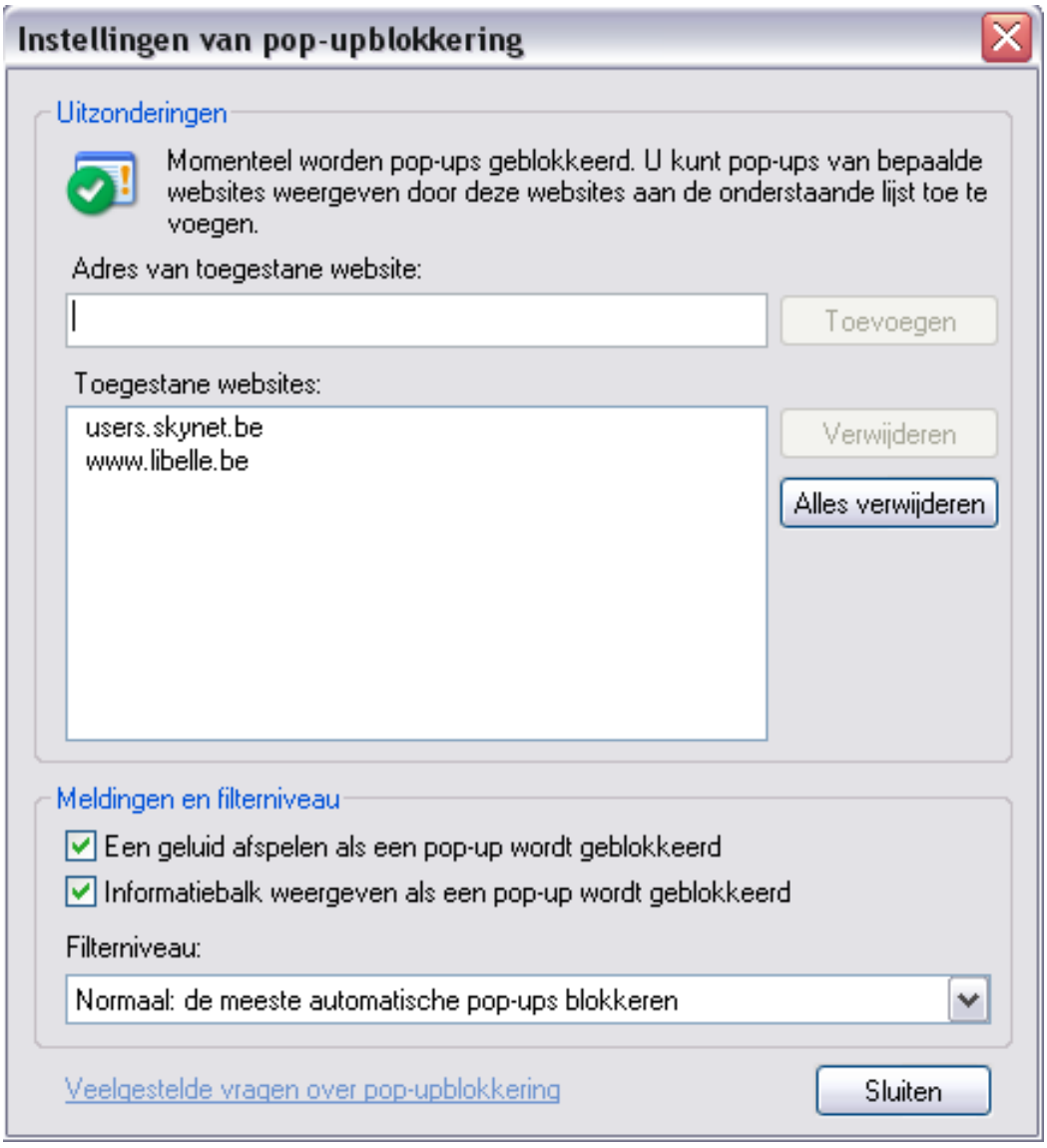


Afb. 3: Instellingen voor privacy in Internet Explorer

[54] LUDIT, *Cookie-instellingen*, internet, http://ludit.kuleuven.be/software/beveiliging/cookie-settings.html, 2007-04-01.

De instellingen voor **cookies** gaan hier van het niveau waarop alle cookies geaccepteerd worden, over laag, normaal en hoog naar het niveau waarop alle cookies geblokkeerd worden. Alle cookies blokkeren is een drastische maatregel, want om op sommige sites te kunnen surfen, moet het gebruik van cookies toegelaten zijn. Door op Websites (Sites) te klikken, kan per website geregeld worden of de bijhorende cookies altijd moeten toegestaan of geblokkeerd worden. Cookies kunnen in een keer verwijderd worden door voor deze optie te kiezen op het hoofdscherm van Internet opties.

Verder kan in dit privacytabblad ingesteld worden hoe Internet Explorer met **pop-ups** moet omgaan. Bij het klikken op Instellingen komt volgend venster tevoorschijn:

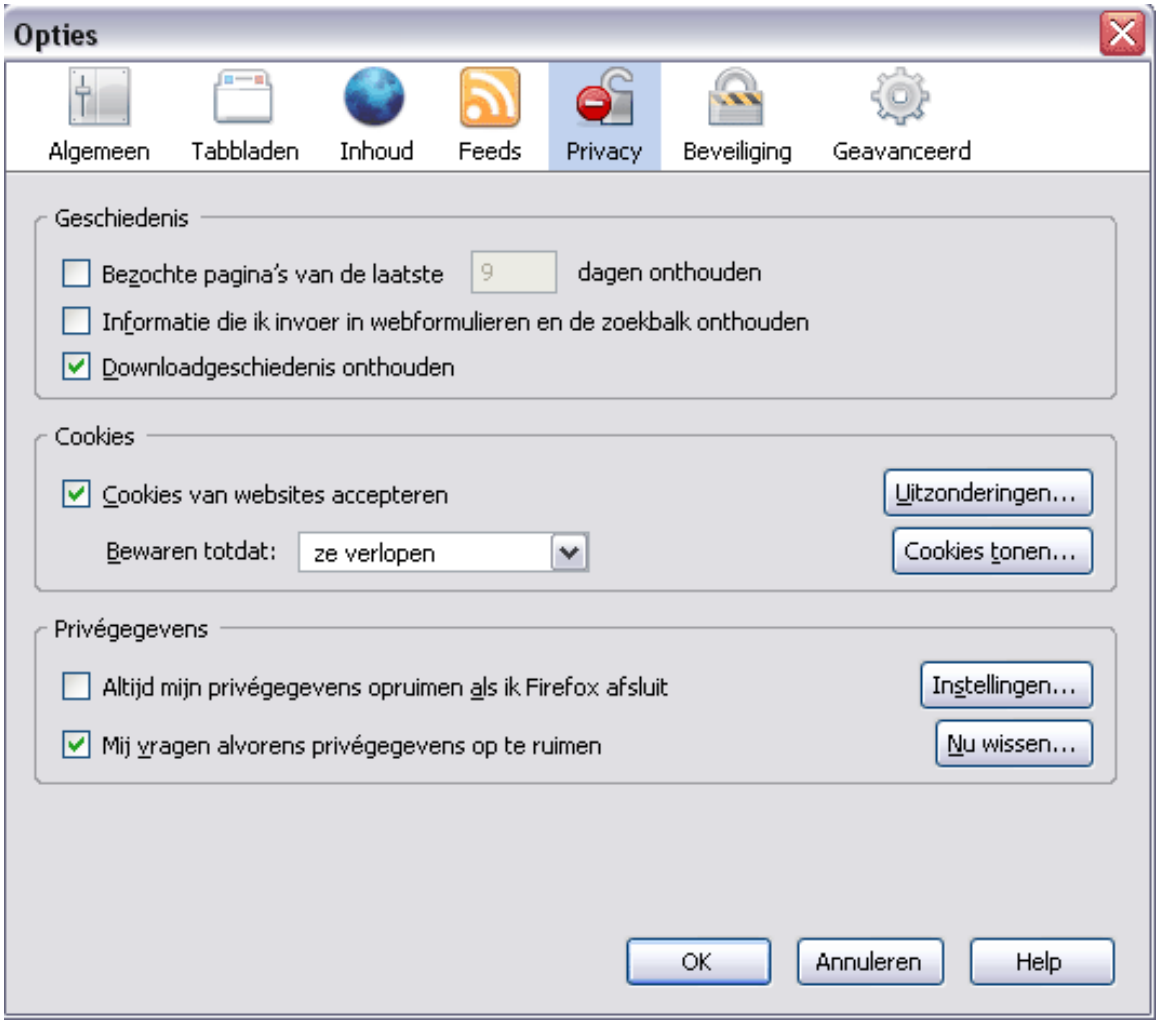


Afb. 4: Instellingen voor pop-upblokkering in Internet Explorer

Pop-ups worden standaard geblokkeerd. In dit venster kan dan bepaald worden van welke sites wel pop-ups worden toegelaten. De meldingen wanneer een pop-up geblokkeerd wordt, kunnen hier aangepast worden. Verder is het mogelijk het filterniveau aan te passen: hoog (alle pop-ups blokkeren), normaal (de meeste automatische pop-ups blokkeren) of laag (pop-ups van beveiligde websites toestaan).

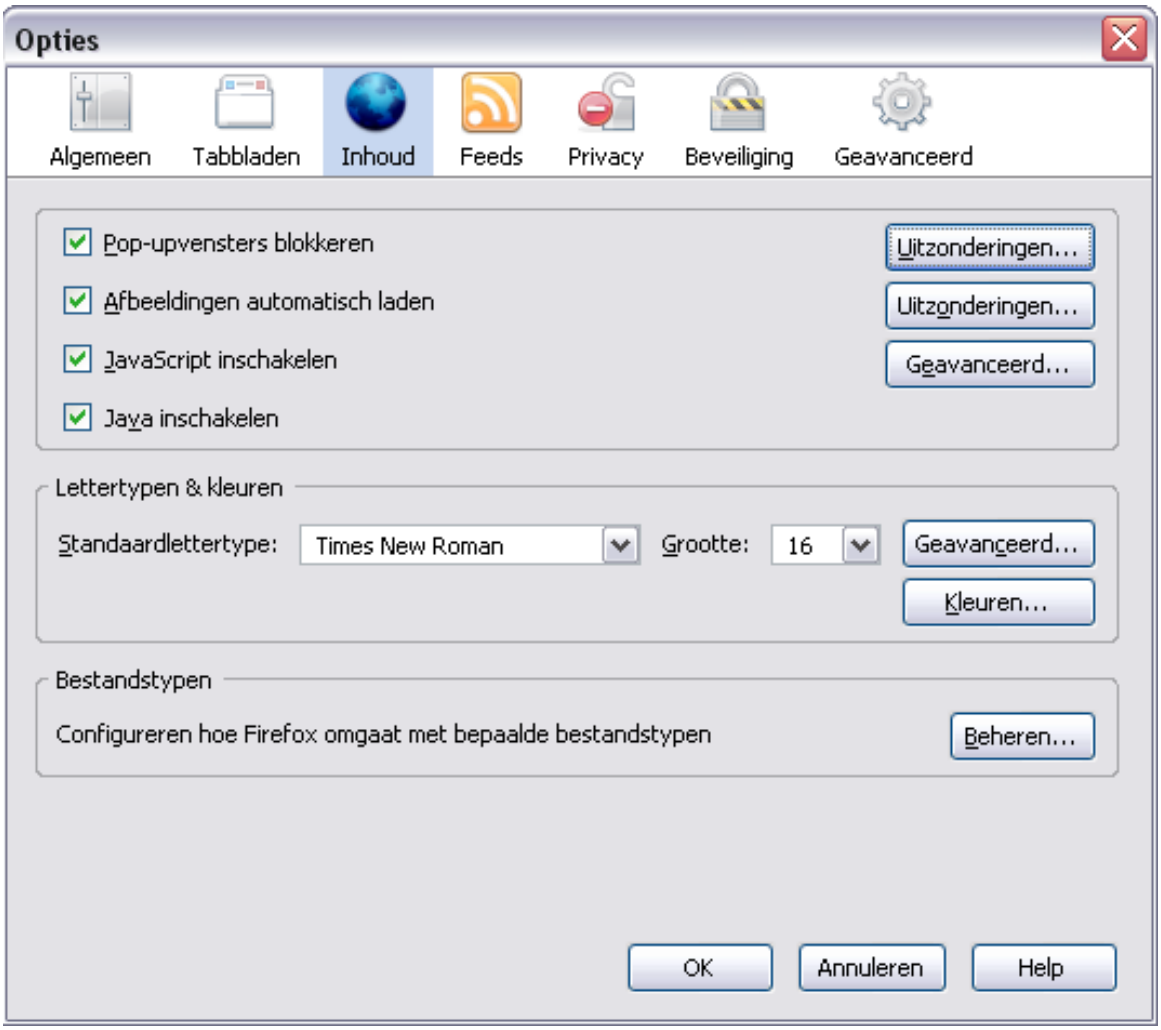
4.2.2 Mozilla Firefox

In Firefox kunnen cookie-instellingen geregeld worden via Extra (Tools) en dan Opties (Options), tabblad Privacy.



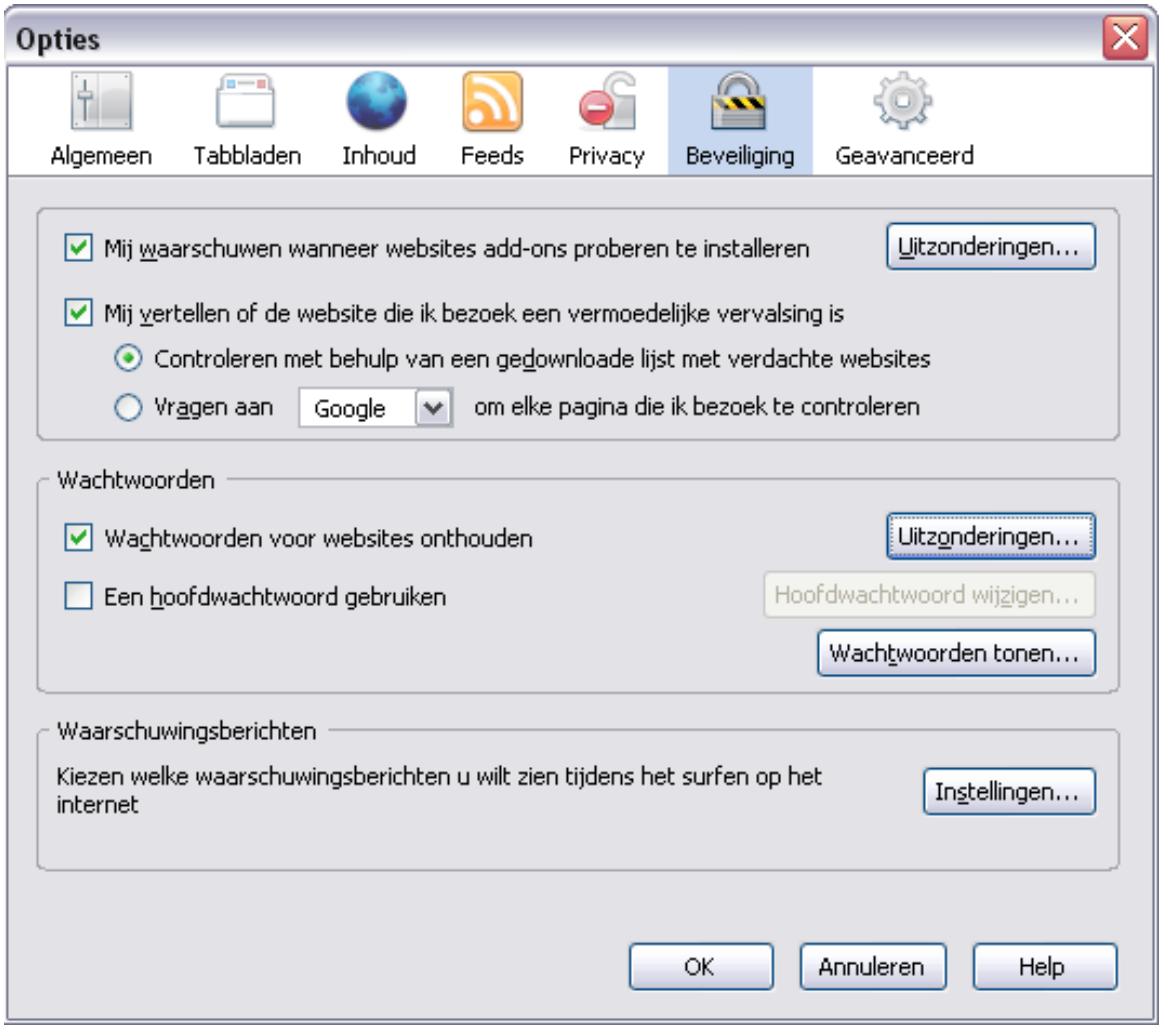
Afb. 5: Instellingen voor privacy in Mozilla Firefox

Hier kan ingesteld worden hoe lang **cookies** bewaard moeten worden: tot ze verlopen, tot Firefox afgesloten wordt of elke keer vragen. Bij uitzonderingen kan er gekozen worden cookies van bepaalde sites te blokkeren, toe te staan of enkel toe te staan gedurende een sessie.



Afb. 6: Instellingen voor pop-upblokkering in Mozilla Firefox

Onder het tabblad Inhoud vinden we bij Firefox de optie om **pop-upvensters** te blokkeren. Via Uitzonderingen kunnen websites opgenomen worden waarvan pop-ups altijd toegelaten worden. Dit werkt dus op een gelijkaardige manier als bij Internet Explorer.



Afb. 7: Instellingen voor beveiliging in Mozilla Firefox

Dit tabblad **Beveiliging** is het antwoord van Firefox op het phishing-fenomeen. Firefox 2 (de nieuwste versie van de browser) is uitgerust met **Phishing Protection**, dat standaard staat ingeschakeld. De instellingen zijn te wijzigen via dit tabblad.
Mozilla Firefox beschermt tegen phishing door de websites die bezocht worden te vergelijken met een lijst sites die bekend staan als phishing-sites. Deze lijst staat op de computer en wordt regelmatig automatisch ge-update. Door de aanwezigheid van deze lijst op een computer komt de privacy niet in gevaar, want er worden geen gegevens over het surfgedrag doorgestuurd naar Mozilla. [55]
Wanneer een website bezocht wordt die in de lijst met verdachte websites staat, volgt deze melding:

Afb. 8: Weergave in Mozilla Firefox bij het bezoeken van een vermoedelijk vervalste website

[55] PLANET INTERNET, *Firefox 2 onder de loep*, internet, http://www.planet.nl/planet/show/id=74274/contentid=790387/sc=92e365, 2006-12-23.

4.2.3 Safari

In Safari zijn de instellingen met betrekking tot cookies eenvoudig en beperkt tot één scherm. Via Voorkeuren (Preferences) in het Safari-menu kan gekozen worden voor het tabblad Beveiliging (Privacy).[56]

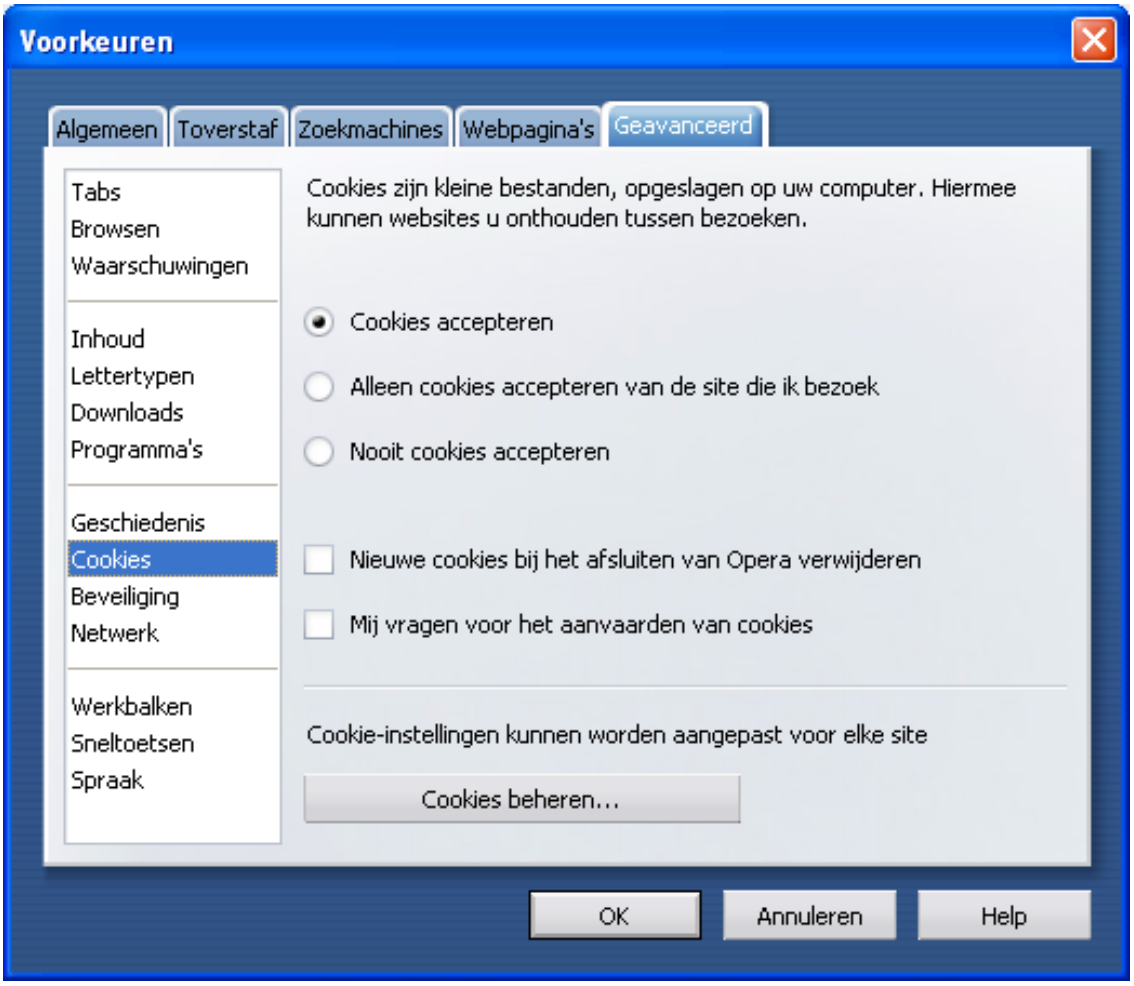
Afb. 9: Instellingen voor beveiliging in Safari

Er zijn drie mogelijke instellingen om **cookies** te accepteren: altijd, nooit of alleen van sites die ik bezoek. Via Toon cookies kunnen de cookies bekeken worden en eventueel verwijderd worden. Ook de mogelijkheid om pop-upvensters te blokkeren, bevindt zich in dit scherm.

4.2.4 Opera

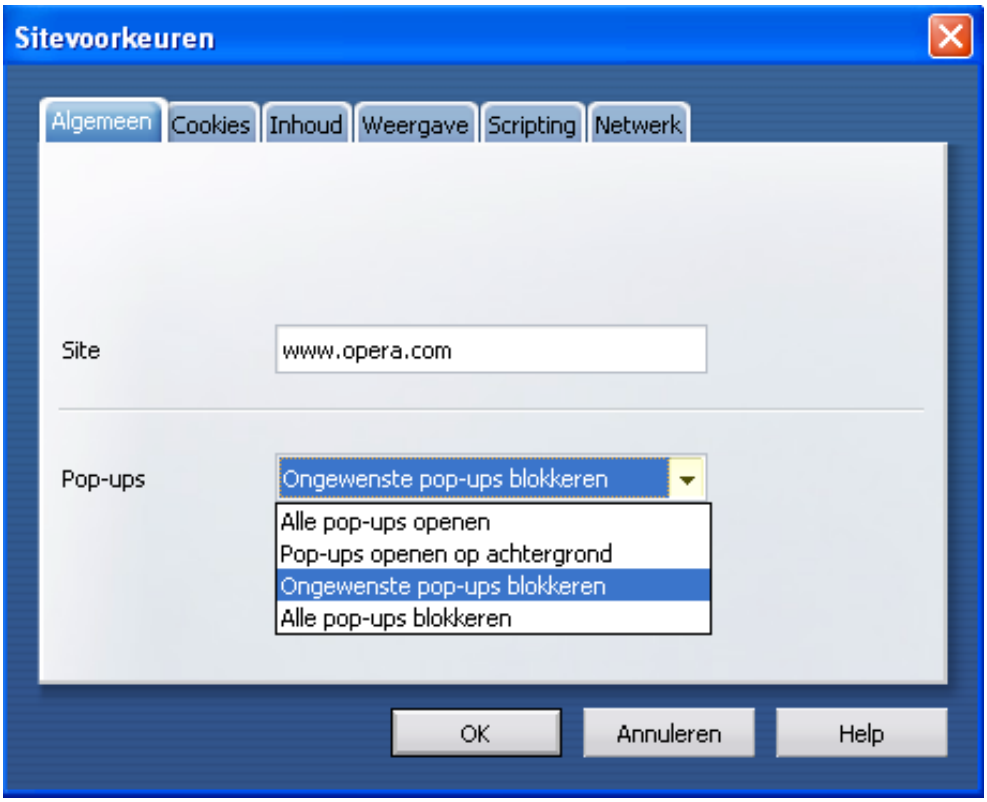
Via Extra (Tools) kan er gekozen worden voor Voorkeuren (Preferences), en dan Geavanceerd (Advanced). Hier kunnen de instellingen voor **cookies** aangepast worden.

[56] LUDIT, Cookie-instellingen, internet, http://ludit.kuleuven.be/software/beveiliging/cookie-settings.html, 2007-04-01.



Afb. 10: Instellingen voor cookies in Opera

Via de sneltoets F12 kunnen de instellingen voor **pop-ups** veranderd worden.



Afb. 11: Instellingen voor pop-ups in Opera

4.3 ADBLOCKERS

Adblockers kunnen een aanvulling vormen op de instellingen van een browser, doordat ze advertenties blokkeren op websites. Advertenties zijn meestal ongewenst omdat het even kan duren voor ze inladen en omdat ze soms verwijzen naar onbetrouwbare websites. Een bekende adblocker is **AdBlock Plus**, een uitbreiding van **Firefox** die toelaat om selectief afbeeldingen te blokkeren op websites. Concreet houdt dit in dat advertentiebanners geblokkeerd worden op websites en dus niet meer zichtbaar zijn. [57]

Wanneer advertenties en banners zichtbaar staan op een website, kan dit aangepast worden door rechts te klikken op de afbeelding en te kiezen voor 'AdBlock' in het menu dat verschijnt. Door een * als wildcard te gebruiken, kunnen bijvoorbeeld alle afbeeldingen op een bepaalde website geblokkeerd worden. Ook kan er gekozen worden voor een standaard filtering waardoor de meeste advertenties geblokkeerd zullen worden. [58]

Het nadeel is dat er websites zijn die het gebruik van dergelijke adblockers niet toestaan. **Tweakers.net** bijvoorbeeld, Nederlands grootste informatie- en communitysite voor tweakers (dit zijn mensen met een grote interesse in computers), heeft in de voorwaarden onder de bepaling aangaande advertenties volgende regel opgenomen:

> "Omdat Tweakers.net een gratis dienst van Tweakers.net BV is, wordt er op de pagina's reclame gemaakt. Het weren van deze reclame op welke manier dan ook is verboden. Deze reclame zorgt voor het voortbestaan van Tweakers.net BV. Overtreding van deze regel kan reden zijn voor onmiddellijke uitsluiting."
> Bron: http://tweakers.net/my.tnet/?action=reg

4.4 ANONYMIZER

Een **Internet Service Provider (ISP)** zoals **Telenet** of **Belgacom** verzorgt de toegang tot internet. Een proxyserver, die een soort buffer vormt tussen een computer en het internet, regelt het internetverkeer en slaat een kopie op van aangevraagde pagina's zodat ze een volgende keer sneller bekeken kunnen worden. Alle aanvragen die hij krijgt, worden bewaard in **logbestanden**. Bovendien bewaren de meeste websites op hun beurt ook nog eens logbestanden van de bezoekers die ze krijgen. In die logbestanden wordt bijgehouden welk IP-adres welke pagina's en welke afbeeldingen heeft opgevraagd en wanneer. Dat IP-adres is een uniek adres waarmee elke computer geïdentificeerd kan worden. Zonder IP-adres kan er niet op het internet gesurft worden. Dat betekent dat er niet anoniem gesurft kan worden.

Een provider gebruikt logbestanden om fouten op te sporen en beheerders van een website kunnen er bezoekersaantallen uit afleiden. Wanneer de politie online criminaliteit op het spoor is, komen diezelfde logs goed van pas. Providers zijn immers verplicht de identiteit van hun klanten bekend te maken als de politie daar om vraagt.

[57] LUDIT, *Aangeraden extenties*, internet, http://ludit.kuleuven.be/software/netwerk/firefox/aangeraden-ext, 2007-04-01.
[58] MOZILLA, *Firefox Add-ons: Adblock Plus*, internet, https://addons.mozilla.org/en-US/firefox/addon/1865, 2007-04-01.

Een site als **Privacy.net** maakt duidelijk dat anonimiteit op het internet bijna niet bestaat. Op deze site wordt de privacy van een computer gecheckt. Gegevens als IP-adres, besturingssysteem, browser, schermresolutie en dergelijke meer worden probleemloos opgehaald door deze site. Op zich lijkt dit niet zo erg omdat dit geen belangrijke gegevens zijn, maar dit vormt slechts de basis om een profiel samen te stellen. Marketeers of andere geïnteresseerden kunnen een persoon volgen door in databases te gaan rondneuzen of door externe klantengegevens aan te kopen. Op allerlei manieren kunnen zij persoonlijke informatie te weten komen over een bepaalde persoon: welke websites die hij bezoekt, naar welke websites hij regelmatig terugkeert, wat hij online aankoopt, welke programma's hij downloadt, welke interesses hij heeft, ... [59]

Rekening houdend met de mogelijke gevolgen die een gebrekkige bescherming van privacy op het internet met zich meebrengt (zie vorig hoofdstuk), is het belangrijk zich bewust te zijn van deze dreiging. Soms is het aangewezen bepaalde informatie voor anderen verborgen te houden, en om dus even **anoniem te surfen**. Dat betekent niet noodzakelijk dat er iets te verbergen valt. In landen waar een streng politiek regime heerst, kan het wenselijk of zelfs levensnoodzakelijk zijn om anoniem te surfen. Strikt genomen heeft iedereen recht op privacy en anonimiteit zonder zich daarvoor te hoeven verantwoorden.

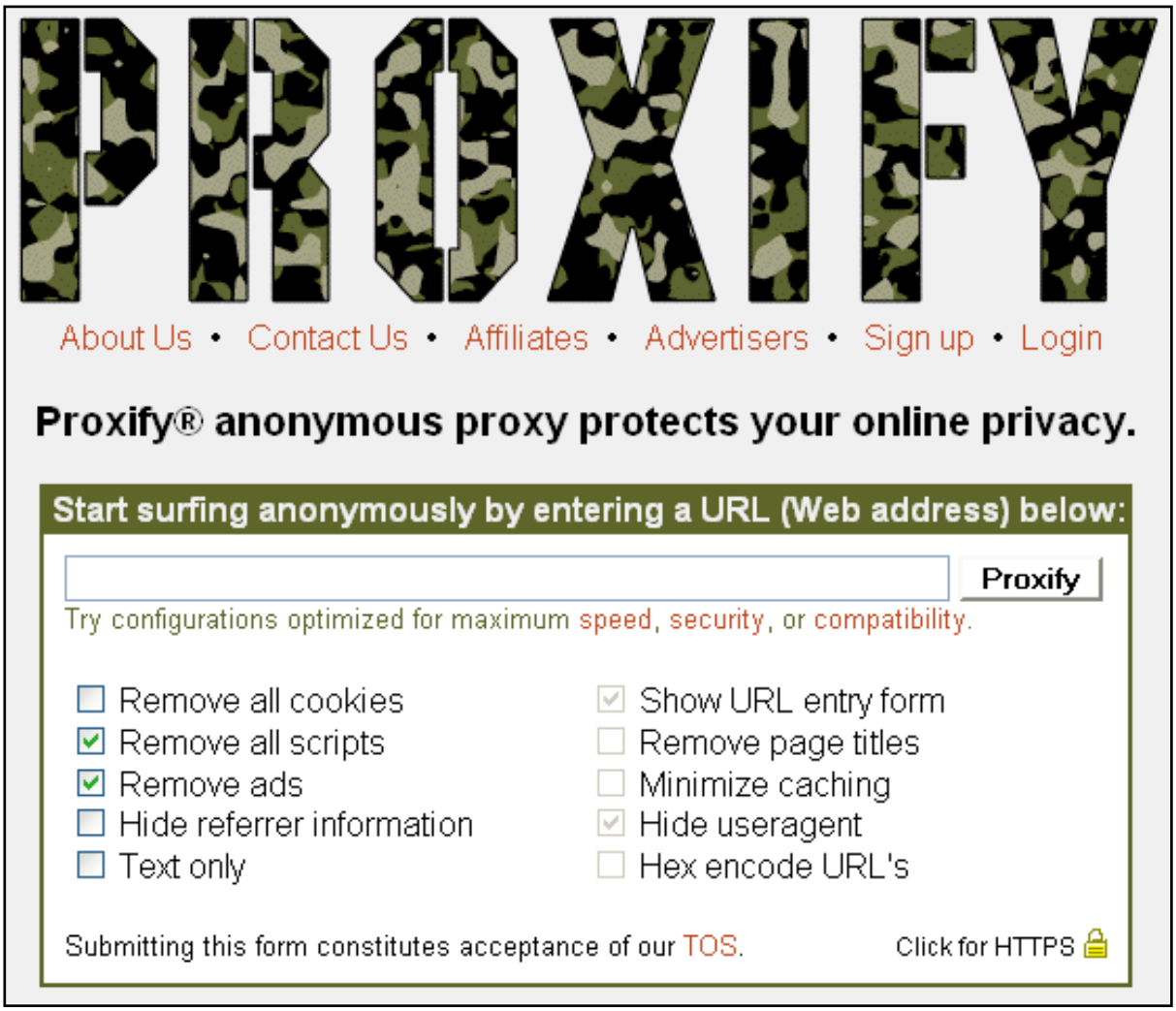
Om vrijwel anoniem te surfen, blijken anonymizers de meest geschikte oplossing. Zij beloven dat ze alle sporen wissen die iemand maakt op het internet en dat er geen gegevens met betrekking tot de identiteit van de gebruiker kunnen achterhaald worden. Er bestaan twee soorten anonymizers: de anonieme proxyservers en websites (of software) die toelaten anoniem een andere website te bezoeken. [60]

Anonieme proxyservers op het internet fungeren als een soort tussenschakel, zodat de originele computer niet meer getraceerd kan worden. Deze proxyservers zorgen ervoor dat het internetverkeer van een computer omgeleid wordt naar een server die het IP-adres verbergt voor de websites die bezocht worden. Hierdoor wordt een **IP-adres niet bekend** gemaakt aan de bezochte websites. Maar de eigen provider kan het dataverkeer wel onderscheppen. Een ander **nadeel** is dat dergelijke servers meestal erg traag en onbetrouwbaar zijn. Bovendien kan niet nagegaan worden of een anonieme proxyserver wel degelijk doet wat hij beloofd heeft.

De andere categorie van anonymizers zijn **webdiensten die toelaten anoniem websites te bezoeken**. De werking is eenvoudig: via de website van een anonymizer kan het adres ingegeven worden van een andere website, de anonymizer doet de rest en toont de desbetreffende pagina binnen het oorspronkelijke venster.

[59] HCCNET, *Anoniem surfen*, internet, http://home.hccnet.nl/t.amerongen/Anonymizers.htm, 2007-04-02.
[60] INTERNETJOURNALISTIEK, *Surfen in het geniep*, internet, http://www.internetjournalistiek.be/dossiers/detail_privacy.php?nieuwsid=99, 2007-04-02.

Proxify.com is een anonieme proxyservice die iedereen toelaat om privé en veilig te surfen op het internet. In tegenstelling tot andere proxyservers is Proxify zeer eenvoudig in gebruik en hoeft er niets geïnstalleerd te worden. De mate van privacybescherming kan gekozen worden. In het invulveld wordt het adres ingegeven van de website, daarna wordt er geklikt op 'Proxify' en meer hoeft er niet gedaan te worden. Nadeel is wel dat er een advertentiebanner verschijnt eens de gevraagde site werd opgehaald en dat Flash-animaties blijkbaar onderdrukt worden (zie bijlage IV). [61]



Afb. 12: Screenshot van de anonieme proxyservice Proxify.com (zie bijlage V voor groter formaat)

The-Cloak.com behoort tot de tweede categorie van anonymizers. Op The Cloak wordt het adres van een website ingetypt en vervolgens verzonden via Secure Socket Layer (SSL), dit is een encryptie- of codeermethode die ook gebruikt wordt bij beveiligd betalingsverkeer via het internet. De server van The Cloak surft naar de pagina in kwestie en stuurt deze terug naar de oorspronkelijke browser. Het dataverkeer kan wel onderschept worden, maar niet ontcijferd, ook niet door de provider. In de adresbalk komt achter de url van The Cloak het gevraagde adres te staan (zie bijlage VI). [62]

[61] PROXIFY, *Anonymous Proxy protects your online privacy*, internet, http://proxify.com/, 2007-04-02.
[62] THE CLOAK, *Free anonymous web surfing*, internet, http://www.the-cloak.com/anonymous-surfing-home.html, 2007-04-02.

Afb. 13: Screenshot van de anonymizer webdienst The-Cloak.com

Deze manier lijkt perfect om anoniem te surfen, maar blijkt ook niet helemaal onschuldig. Anonymizers bewaren zelf echter ook logbestanden. The Cloak vermeldt zelfs openlijk op de site dat wanneer bevoegde instanties vragen om gegevens van hun gebruikers, ze dat niet kunnen weigeren. [63] Een andere populaire anonymizer, **JAP**, kreeg in 2003 op bevel van een Duitse rechter een maatregel opgelegd waardoor de politie surfers nu wel kan betrappen op het bezoeken van illegale sites. Na de aanslagen op de WTC-torens van elf september 2001 zagen anonymizers van het eerste uur **Freedom** en **SafeWeb** zich genoodzaakt ermee te stoppen, aangezien de Amerikaanse overheid van mening was dat terroristen anoniem afspraken maakten via het internet.

Anonymizer **Surfola** werkte in juli 2003 mee aan een onderzoek van de FBI, terwijl in de privacy policy nochtans vermeld staat dat ze onder geen enkel beding gegevens als namen, adressen en e-mailadressen doorgeeft aan derden.
Een andere reden die zorgt voor de tanende populariteit van anonymizers, is het feit dat surfen via een anonymizer net de aandacht trekt. Enkel mensen die iets te verbergen hebben, gebruiken dergelijke diensten, is de overtuiging van de politie. Dus door dergelijke diensten te gebruiken, worden gebruikers als verdacht beschouwd, terwijl ze net anoniem het internet willen doorkruisen. [64]

[63] THE CLOAK, *Terms and Conditions, Abuse Policy and Privacy Policy*, internet, http://www.the-cloak.com/terms.html, 2007-04-02.
[64] INTERNETJOURNALISTIEK, *Surfen in het geniep*, internet, http://www.internetjournalistiek.be/dossiers/detail_privacy.php?nieuwsid=99, 2007-04-02.

4.5 Aanvullende software

Op kleinschaliger niveau kan er gekeken worden naar de situatie thuis, op school of op het werk. Wanneer meerdere mensen toegang hebben tot dezelfde computer, kan er perfect nagegaan worden welke websites reeds eerder bezocht werden. Zoektermen die in Google werden ingetypt, blijven bewaard en kunnen door iedereen bekeken worden. De computer geregeld opkuisen is de beste remedie om dergelijke sporen te verwijderen. Er bestaan tientallen meestal gratis programma's die tijdelijke bestanden, cookies en andere surfgegevens opruimen.

Ccleaner is een dergelijk gratis programma dat het computersysteem optimaliseert en de privacy beschermt. Ongebruikte en tijdelijke bestanden worden verwijderd, waardoor het besturingssysteem sneller werkt en er plaats vrijkomt op de harde schijf. Cookies, de browsergeschiedenis, de lijst met recent geopende bestanden, log-bestanden, alle onnodige bestanden die anders op de computer blijven staan worden verwijderd.

Er kan zelf aangegeven worden wat wel en wat niet opgeruimd moet worden (zie bijlage VII). Ook index.dat-bestanden kunnen verwijderd worden. Alle websites die op een computer worden bezocht, worden opgeslagen in dit index.dat-bestand. Het nut hiervan wordt nergens bekend gemaakt door Microsoft. Dit bestand kan vele megabytes groot zijn en bevat privacygevoelige informatie. [65]

Een ander gratis programma dat gemaakt is om spyware op een computer te detecteren en te verwijderen is **Spybot – Search & Destroy**. Spyware wordt niet altijd door gewone anti-virusprogramma's gevonden. Wanneer er ineens een nieuwe toolbar in Internet Explorer verschijnt of wanneer de startpagina van de browser veranderd is en deze niet gewijzigd kan worden, is er hoogstwaarschijnlijk spyware aanwezig op de computer.

Spyware is echter niet altijd zichtbaar. Steeds vaker draaien deze schadelijke programma's op de achtergrond van de computer en heeft de gebruiker niet door dat de computer geïnfecteerd is. Spyware verzamelt informatie over het surfgedrag van de gebruiker en stuurt deze door naar bedrijven die geld verdienen met het samenstellen van marketingprofielen en doorverkopen aan reclamebedrijven. Spybot-S&D verwijdert spyware, adware, dialers (ongewenste inbelverbindingen), keyloggers, Trojans, usage tracks (geschiedenis van websites die bezocht werden en bestanden die geopend werden op een computer) en andere mogelijke virussen en bedreigingen. De gebruiker kiest zelf welke bedreigingen verwijderd worden (zie bijlage VIII). [66]

Ontwikkelaar Lavasoft omschrijft **Ad-Aware** als het meest populaire anti-spywareprogramma voor computergebruikers met bijna een miljoen downloads per week. Deze gratis versie biedt de gebruiker een geavanceerde bescherming tegen spyware. Net zoals Ccleaner en Spybot-S&D is Ad-Aware een **on-demand-scanner**. Dit betekent dat ze niet permanent op de achtergrond draaien, maar slechts beginnen met scannen nadat de gebruiker hierom gevraagd heeft. Dat is beter voor de snelheid en het geheugen van de computer, maar vraagt langs de andere kant wel voldoende discipline van de gebruiker die zelf de scan moet starten.

[65] DOWNLOAD FREEWARE, *Ccleaner*, internet, http://www.downloadfreeware.nl/ccleaner.php, 2007-04-03.
[66] SPYBOT – SEARCH & DESTROY, *Overzicht*, internet, http://www.safer-networking.org/nl/spybotsd/index.html, 2007-04-03.

Ad-Aware biedt ook een betalende versie, die **real-time** werkt en dus constant op de achtergrond alle bestanden scant. De gratis versie kan spyware en tracking cookies detecteren en verwijderen, aangepaste scans uitvoeren, browser hijackers blokkeren en bestanden in quarantaine plaatsen (zie bijlage IX). [67]

4.6 Firewall

Een firewall is een systeem dat een computer of een computernetwerk beschermt tegen eventuele inbreuken via een extern netwerk waarmee ze verbonden zijn. Een firewall werkt met regels over wat wel en niet mag in de communicatie tussen een computer en de andere computers op het internet. Indringers zoals fysieke personen (hackers), wormvirussen of spyware worden door een firewall tegengehouden. Een goede firewall werkt in twee richtingen: zowel verdacht verkeer van het internet naar een computer toe wordt gescand, als omgekeerd. Dit is nodig aangezien sommige virussen of spyware gaan proberen vanop een computer gegevens of spam naar het internet te versturen.

Aangezien de tips zich tot thuisgebruikers beperken, hoeven niet alle verschillende soorten firewalls besproken te worden. Naast de personal of persoonlijke firewall bestaan er immers ook firewalls voor kleine netwerken en voor grote netwerken op bedrijfsniveau. Een persoonlijke firewall is een programma dat een individuele computer beschermt tegen de bedreigingen van het internet. Versies van Windows XP die **Service Pack 2** (een veiligheidsupdate) geïnstalleerd hebben, beschikken over een ingebouwde firewall. Deze is echter beperkt tot het analyseren van bedreigingen van het internet naar een computer toe, en niet omgekeerd. Aangeraden is een aparte persoonlijke firewall te gebruiken. Dat is een makkelijk te installeren programma dat ook door beginners gebruikt kan worden en weinig onderhoud vraagt, behalve natuurlijk af en toe de meest recente versie installeren.

In het begin komt een firewall vrij vaak automatisch vragen wat er moet gebeuren met een programma dat voor de eerste keer gebruikt wordt, en dat verbinding zoekt met het internet. Een firewall verwittigt de gebruiker hiervan en vraagt of dat wel degelijk de bedoeling is. Wanneer het programma te vertrouwen is, antwoordt de gebruiker bevestigend en kan het programma verbinding maken met het internet. Deze goedkeuring wordt onthouden voor de volgende keren dat het programma gebruikt wordt. Zo zal de firewall steeds minder vragen stellen, maar toch de echte bedreigingen tegenhouden.

Wanneer er eenmaal toestemming gegeven is aan een programma om verbinding te maken met het internet, zal de firewall dit altijd toelaten. Dit houdt risico's in wanneer een programma niet volledig te vertrouwen is, zoals bijvoorbeeld het geval is met P2P-programma's als **Kazaa**. Als de firewall dit programma toelaat verbinding te maken met het internet, kunnen eventuele virussen of spyware die via Kazaa toekomen niet tegengehouden worden.

Een firewall kan gezien worden als een muur waarin een lange rij 'deuren' zitten, die **poorten** worden genoemd. Elk programma dat verbinding maakt met het internet, gebruikt één of meerdere van die poorten. De browser krijgt bijvoorbeeld poort 80 toegewezen.Via een firewall kan geregeld worden dat een programma via een bepaalde poort communiceert met het internet. Alles wat niet expliciet toegelaten wordt, blijft geblokkeerd. [68]

[67] LAVASOFT, *Ad-Aware SE Personal*, internet, http://www.lavasoftusa.com/products/ad-aware_se_personal.php, 2007-04-03.
[68] SPAMSQUAD, *Installeer een firewall: houd de hackers buiten*, internet, http://www.spamsquad.be/nl/fiches/fiche28.html, 2007-04-03.

4.7 VIRUSSCANNER

Omdat virussen ongemerkt een computer kunnen binnendringen, is het noodzakelijk hier goed tegen beschermd te zijn. Een virusscanner kan virussen opsporen en zo een computer 'genezen'. Voorkomen is echter beter dan genezen. Een virusscanner detecteert dan ook virussen voor ze de computer kunnen infecteren. [69]

Een **on-access-scanner** draait **permanent** op de achtergrond en scant bestanden voordat ze geopend worden. Deze virusscanner vertraagt de computer wel. Een **on-demand-scanner** voert scans uit van een bestand, een map of een gehele schijf maar **enkel op aanvraag**, dus wanneer de gebruiker dit wil. Dit kan meestal gepland worden zodat dit bijvoorbeeld wekelijks gebeurt. On-demand-scanners worden meestal gebruikt om eventueel reeds actieve virussen op te sporen en te verwijderen, in tegenstelling tot on-access-scanners die tot doel hebben infectie van het systeem te voorkomen. [70]

Belangrijk is wel dat de gebruiker op regelmatige basis nieuwe updates installeert om de virusscanner up-to-date te houden. Virusdetectie is immers afhankelijk van een database met gekende virusdefinities. Aangezien er voortdurend nieuwe virussen en bedreigingen opduiken en deze zich snel verspreiden, is vaak updaten geen overbodige luxe. De meeste virusscanners kunnen automatisch updaten.

Een goed antivirusprogramma moet **verschillende taken** uitvoeren. Alle activiteiten op een computer moeten op de achtergrond gecontroleerd worden. Er moet regelmatig een **volledige systeemscan** uitgevoerd worden, zodat er geen virussen onopgemerkt blijven. Wanneer het mis gaat, biedt dit programma een **noodoplossing** in de vorm van een bootdisk. Dit is een diskette of CD waarmee de computer herstart kan worden wanneer die door virussen niet meer werkt. **Bestandsbijlagen** van inkomende e-mails worden gescand door het antivirusprogramma.

Verder moet een virusscanner **verdachte activiteiten en scripts** in de gaten houden. Virussen hebben immers de typische eigenschap om zich verder te verspreiden, bijvoorbeeld via het zenden van mails naar contacten in een e-mailprogramma. Antivirusprogramma's zullen deze activiteiten opmerken en de gebruiker hierop wijzen. Scripts, stukjes software op een website die een bepaalde taak verrichten, worden ook geobserveerd. Zij worden immers soms gebruikt om virussen te verspreiden. [71]

Om een computer te vrijwaren van virussen is een goede virusscanner een absolute noodzaak. Twee virusscanners naast elkaar draaien, lijkt misschien dubbel zo veilig, maar in werkelijkheid zullen ze elkaar tegenwerken. Bekende virusscanners als **Norton AntiVirus** [72] en **McAfee VirusScan Plus** [73] bieden **tegen betaling** een uitgebreid pakket aan gaande van virusdetectie tot het blokkeren van spyware en wormen. Thuisgebruikers hebben meestal weinig zin om te betalen voor dergelijke diensten als er ook **deftige alternatieven** bestaan die **gratis** beschikbaar zijn.

[69] LUDIT, *Het gebruik van een virusscanner*, internet, http://ludit.kuleuven.be/software/beveiliging/virusscanner.html, 2007-04-04.
[70] HET COMPUTERVIRUS, *Antivirusprogramma*, internet, http://www.wobotje.com/computervirus/bescherming_programma.htm, 2007-04-04.
[71] SPAMSQUAD, *Installeer een antivirusprogramma*, internet, http://www.spamsquad.be/nl/fiches/fiche24.html?q=, 2007-04-04.
[72] SYMANTEC, *Norton AntiVirus 2007*, internet, http://www.symantec.com/home_homeoffice/products/overview.jsp?pcid=is&pvid=nav2007, 2007-04-04.
[73] MCAFEE, *McAfee VirusScan Plus: Essentiële pc-beveiliging*, internet, http://nl.mcafee.com/root/package.asp?pkgid=276, 2007-04-04.

Avira AntiVir Personal Edition is een dergelijk deftig alternatief. AntiVir is een gratis antivirusprogramma dat een computer beschermt tegen virussen, wormen, Trojans en dialers. De real-time monitoring gebeurt door het on-access gedeelte van dit pakket, Virus Guard. Na installatie staat dit pictogram in het systeemgebied van de taakbalk, rechtsonder dus.

AntiVir beschikt ook over een on-demand gedeelte dat via een ingebouwde agenda scans kan plannen en uitvoeren. Wat er gebeurt met gedetecteerde virussen kan de gebruiker zelf bepalen: automatisch herstellen, verwijderen of verplaatsen naar de quarantainemap. Wanneer virusfdefinities verouderd zijn, haalt AntiVir de nieuwste updates automatisch binnen. [74]

Een andere virusscanner die dezelfde gratis diensten aanbiedt, is **AVG Free Edition**. AVG biedt real-time bescherming en downloadt automatisch en iedere dag de laatste updates. Via het on-access gedeelte Control Center kan er naar het on-demand gedeelte Test Center gegaan worden waar er gekozen kan worden welke bestanden of schijven gescand moeten worden (zie bijlage X). Verder beschikt AVG over een mailscanner die e-mails controleert op virussen nog voor ze gelezen worden. [75]

4.8 Parental Control

Het internet heeft geen grenzen zodat ouders bezorgd zijn wanneer ze hun kinderen laten surfen op het web. Parental Control software is software die ouders in staat stelt de toegang tot websites en programma's te controleren. Gevoelige inhoud wordt geblokkeerd. Eventueel kan zelfs ingesteld worden hoe lang kinderen achter de computer mogen zitten. [76]

CyberPatrol is software tegen betaling voor ouderlijk internettoezicht. [77] In Nederland biedt Orange **Parental Control** aan – ook tegen betaling – waarmee toegang tot internet en programma's gecontroleerd kan worden. [78] **Parental Control Bar** is gratis software die een extra werkbalk installeert in de browser die werkt met een wachtwoord. Met dit wachtwoord wordt overgeschakeld van kind- naar volwassenmodus en omgekeerd. [79]

In **Windows Vista** zit een nieuw onderdeel Ouderlijke Beveiliging (of Parental Control). Aparte Parental Control software is niet meer nodig. Met deze software kunnen ouders precies bepalen wat hun kinderen op de computer kunnen doen: welke spelletjes hun kinderen mogen spelen, welke programma's ze kunnen gebruiken, naar welke websites ze mogen surfen en wanneer. Ouders kunnen immers het computergebruik beperken tot bepaalde tijdstippen, ook wanneer ze zelf niet thuis zijn.

[74] SURFNET, *Virussen bestrijden*, internet, http://www.surfkit.nl/info/beveiliging/virussen_bestrijden.jsp, 2007-04-04.
[75] GRATIS SOFTWARE SITE, *Beschrijving AVG Anti-Virus Free*, internet, http://www.gratissoftwaresite.nl/avg.html, 2007-04-04.
[76] ORANGE, *Parental Control: Bescherm je kinderen*, internet, http://www.orange.nl/overige_produkten/veiligheid/parental_control/, 2007-04-06.
[77] CYBERPATROL, *Oplossingen voor ouderlijk internettoezicht van CyberPatrol*, internet, http://www.cyberpatrol.com/Software_voor_ouderlijk_internettoezicht.htm, 2007-04-06.
[78] ORANGE, *Parental Control: Bescherm je kinderen*, internet, http://www.orange.nl/overige_produkten/veiligheid/parental_control/, 2007-04-06.
[79] ZDNET, *Parental Control Bar 4.0.3: Uw oogappels kunnen veilig surfen*, internet, http://www.zdnet.nl/downloads.cfm?id=64284, 2007-04-06.

Het scherm Ouderlijke Beveiliging is bereikbaar via Gebruikersaccounts en Ouderlijk toezicht. Hier kunnen de instellingen aangepast worden (zie bijlage XI). Er kunnen bijvoorbeeld ook activiteitsrapporten bekeken worden waarin vermeld wordt hoe de kinderen de computer gebruikt hebben. Het pictogram Ouderlijke Beveiliging is altijd zichtbaar in het systeemvak zodat kinderen weten dat dit is ingeschakeld.

Via het beheerscherm kan beheerd worden wanneer kinderen de computer mogen gebruiken. Op een rooster met alle dagen van de week en alle uren van de dag kan dit ingesteld worden. Standaard mogen kinderen de computer 24 uur per dag en zeven dagen per week gebruiken. Om dit te beperken, kunnen er tijden en dagen aangeduid worden die geblokkeerd worden voor de kinderen. Wanneer die periode nadert, wordt er een kwartier en een minuut voordat de geblokkeerde periode begint, een melding weergegeven. Als de tijd verstreken is voordat het kind zich afmeldt, wordt de sessie onderbroken. Deze blijft wel actief op de achtergrond, zodat de sessie een volgende keer hernomen kan worden.

Naast blokkering op tijd is er ook blokkering mogelijk op inhoud. Hiervoor heeft Windows Vista een webfilter die sites met ongepaste inhoud blokkeert. Er kan gekozen worden voor strenge of soepele censuur. Verder kan het downloaden van bestanden via chatprogramma's tegengehouden worden, maar er kan evengoed ingesteld worden dat chatprogramma's niet gebruikt mogen worden. Aan spelletjes kan gevraagd worden of ze voldoen aan een bepaalde norm, voordat ze opgestart kunnen worden. [80]

4.9 E-MAILADRESSEN BESCHERMEN

De publicatie van een e-mailadres op een webpagina is vatbaar voor **spambots**. Een spambot is een robot die e-mailadressen van websites en nieuwsgroepen verzamelt voor bedrijven die spam willen versturen. Alle e-mailadressen die het tegenkomt, slaat de spambot op. Meestal worden e-mailadressen vermeld in de vorm van 'info@domein.be' of 'klik hier om te mailen'. In de html-code wordt er een mailto-functie toegevoegd die ervoor zorgt dat een e-mailprogramma, bijvoorbeeld **Outlook**, wordt geopend wanneer een surfer op deze link klikt. Deze manier is de meest gebruikte en gemakkelijkste manier om bezoekers contact te laten opnemen met de eigenaars van de website, maar tegelijk de meest ontvankelijke voor spam.

Naast spambots bestaan er ook nog **spiders** of **crawlers**. [81] Normaal gezien worden deze spiders gebruikt om websites te bezoeken en de hyperlinks, dit zijn verwijzingen op het internet, te volgen. Zoekmachines maken bijvoorbeeld gebruik van spiders. Maar er bestaan ook spiders die het internet afschuimen op zoek naar e-mailadressen. Dergelijke software werd speciaal ontwikkeld om het @-teken of de mailto-functie te herkennen als e-maillink en vervolgens op te slaan in een database. Deze database met e-mailadressen wordt gebruikt om spam te versturen. Dergelijke databases worden ook vaak aan derden aangeboden via het internet. [82]

[80] DE DIGITALE REVOLUTIE, *Ouderlijke controle (parental control) in Vista*, internet, http://www.dedigitalerevolutie.tv/toontext.asp?id=17982, 2007-04-06.
[81] CONBA, *Zoekmachines: hoe werken ze?*, internet, http://www.conba.be/showunieuws.asp?archief=1&language=NL&IDnr=1248, 2006-09-25.
[82] INFOTALIA, *Bescherm uw e-mailadres tegen spam!*, internet, http://www.infotalia.be/nl/ict/internet_detail.asp?id=102, 2007-04-07.

Voor een webmaster is het belangrijk om zich te beschermen tegen spambots en spiders, want anders is het onbegonnen werk spam van gewone e-mails te onderscheiden. Een mogelijke oplossing is geen e-maillinks meer plaatsen, maar het e-mailadres verbergen door het op volgende manier te typen: info at domein punt be. Het voordeel is dat spambots of spiders een e-mailadres niet meer als dusdanig zullen herkennen, maar het nadeel is dat bezoekers niet meer kunnen klikken op een link om een e-mail rechtstreeks te versturen.

Een andere methode is het opnemen van de mailto-link in JavaScript. Dat ziet er zo uit:

```
<script type="text/javascript">
document.write("<a href='mailto:info@domein.be'>Stuur me een email</a>");
</script>.
```

Maar ook dit blijkt geen perfecte oplossing. Het e-mailadres wordt immers nog steeds vermeld in de broncode van de pagina, en kan dus nog steeds opgepikt worden door spambots en spiders. [83]

Er bestaat nog een betere oplossing: het e-mailadres coderen. Dit houdt in dat elk karakter door een numerieke waarde vervangen wordt. Info@domein.be wordt zo omgezet tot info@domein.be waarbij i staat voor de letter i, n voor de letter n, f voor de letter f, enzovoort. Een site die deze omrekening maakt is **Blinfotec.org**. [84] Door het gecodeerde e-mailadres te gebruiken op een website, wordt het spambots en spiders al een stuk lastiger gemaakt.

Op de meeste websites moet er geregistreerd worden vooraleer er bijvoorbeeld kan deelgenomen worden aan een wedstrijd. Een gebruiker die zijn e-mailadres niet overal wil rondstrooien kan ervoor kiezen een speciale wegwerpaccount aan te maken die enkel gebruikt wordt voor wedstrijden of onbelangrijke registraties. Dat er ook spam toekomt op dit adres, is dan niet zo erg. Er bestaat echter een website die bedoeld is voor dergelijke doeleinden: **Spam.la**. Wanneer voor een onbelangrijke registratie gevraagd wordt een e-mailadres in te vullen, kan de gebruiker bijvoorbeeld naam@spam.la ingeven. Op de website kan hij vervolgens de activatiemail terugvinden. [85]

Use spam.la email addresses for throw-away site registrations.

All email sent to any_address@spam.la is publicly readable right here.

Only show me messages sent to: @spam.la filter (optional)

To	From	Click Subject To Read Email	Age
e2e401@spam.la	"usiverify-e2e-07-sg02-d...	FW: a5377316a5f25fc38fd7e04c888193ba	0 secs
johynjohn@spam.la	"Carrie Diggs"	It dolton whichever chassell	1 sec
e2e401@spam.la	"usiverify-e2e-07-sg02-d...	FW: 609e7529a6cd1e97cb94cd0eb7f530d5	2 secs
e2e401@spam.la	"usiverify-e2e-07-sg01-d...	FW: d02267e877888424f4a5c953d7f289db	2 secs

Afb. 14: Screenshot van de website Spam.la

[83] MIJN HOMEPAGE, *Je emailadres coderen*, internet, http://www.mijnhomepage.nl/artikelen/wd/emailadres-coderen.php, 2007-04-07.
[84] BLINFOWEB, *Email encoder*, internet, http://www.blinfotec.org/tools/emailencoder.html, 2007-04-07.
[85] SPAM.LA, *Fight spam, use an anonymous @spam.la address!*, internet, http://www.spam.la/, 2007-04-07.

4.10 Robinson-lijst

Een andere manier om een e-mailadres te beschermen tegen ongewenste e-mail, is de Robinson-lijst. Door zich in te schrijven in de Robinson e-maillijst maakt een persoon kenbaar dat hij geen informatie meer wil ontvangen via e-mail over producten of diensten van bedrijven. Langs de andere kant mogen er dan ook geen promoties of kortingen meer gestuurd worden via e-mail. Het e-mailadres dat opgegeven wordt, wordt uitgesloten van alle commerciële acties. Bedrijven waar de gebruiker klant van is of waar hij uitdrukkelijke toestemming aan heeft gegeven om via e-mail contact op te nemen, mogen uiteraard wel e-mails blijven sturen.

Deze lijst geldt enkel voor inwoners van België. Enkel de 450 bedrijven die lid zijn van het **Belgisch Direct Marketing Verbond (BDVM)** zijn verplicht deze Robinson-lijst te gebruiken, dus andere niet-aangesloten bedrijven kunnen wel nog e-mails versturen naar de personen op de Robinson-lijst. De impact van deze lijst is bijgevolg eerder beperkt aangezien enkel de leden van het BDMV zich ertoe verbonden hebben de lijst te respecteren. Bovendien is de grote meerderheid van spam afkomstig uit het buitenland. [86]

4.11 Cryptografie

Met betrekking tot cryptografie (of versleuteling) en handtekeningen via het internet bestaan er verschillende technologieën. Zo kunnen datastromen versleuteld worden, wat bijvoorbeeld gebeurt bij online bankieren. In dit geval kan verkeer afgeluisterd worden, maar is de data zodanig versleuteld dat deze data vrijwel onleesbaar is. [87] Cryptografie is echter een uitgebreid en technisch onderwerp en binnen dit eindwerk is het de bedoeling dat de aandacht vooral gaat naar de modale internetgebruiker. Deze heeft weinig boodschap aan een technische uitleg over cryptografie. Daarom wordt dit onderwerp hier niet verder in detail besproken.

Wat wel nuttig kan zijn voor de internetgebruiker, is het feit dat e-mails ook beveiligd kunnen worden door de inhoud ervan te gaan versleutelen. Om tegen te gaan dat e-mails onderschept en gelezen kunnen worden door de verkeerde personen (bijvoorbeeld door Echelon, dat in het volgende hoofdstuk besproken wordt), is er de software **Pretty Good Privacy (PGP)** die zich vasthecht aan een e-mailprogramma. [88] Dit is een manier om e-mails te versleutelen waarbij de tekst door PGP wordt omgezet in numerieke waarden. De versleutelde e-mail wordt dan bij de ontvanger vertaald naar het origineel. Iemand die de e-mail onderschept en wil lezen, ziet enkel een onleesbare resem aan letters en cijfers.

PGP werkt met twee sleutels: een publieke en een geheime sleutel. Zowel de zender als de ontvanger moeten PGP-sleutels aanvragen. De publieke sleutel mag openbaar gemaakt worden. Als er een e-mail verstuurd wordt naar iemand, moet de publieke sleutel van deze persoon gekend zijn. Met behulp van deze sleutel codeert PGP de e-mail. Op de computer van de ontvanger wordt de e-mail automatisch door de geheime sleutel vertaald naar de originele versie. Zonder deze geheime sleutel kan de e-mail niet gelezen worden. [89]

[86] ROBINSONLIST, *Hoe werkt de Robinson-lijst?*, internet, http://www.robinsonlist.be/, 2007-04-07.
[87] CAMPUS TU DELFT, *Cryptografie en digitale handtekeningen*, internet, http://campus.tudelft.nl/live/pagina.jsp?id=5198149a-657f-495f-a658-a58a67d2cc4d&lang=nl, 2007-04-09.
[88] PGPI, *The International PGP Home Page*, internet, http://www.pgpi.org/, 2007-04-09.
[89] DE DIGITALE REVOLUTIE, *Echelon en het versleutelen van mail*, internet, http://www.dedigitalerevolutie.tv/toontext.asp?id=9749, 2007-04-09.

4.12 Voorzichtigheid en gezond verstand

Naast alle mogelijke maatregelen die een persoon kan nemen om zijn privacy op het internet te beschermen, is de belangrijkste regel: wees voorzichtig en gebruik uw gezond verstand. Denk na voordat u iets online plaatst. Wees alert wanneer u software wil installeren waarvan u niet zeker weet of het betrouwbaar is.

Blijf kritisch. Een programma is niet per definitie goed omdat velen het gebruiken. Populaire programma's of besturingssystemen zijn vanzelfsprekend ook populair bij degenen die er misbruik van willen maken. Kies dus alternatieven. Besturingssystemen als **Mac OS X** of **Linux** zijn minder gevoelig voor spyware en virussen. **Internet Explorer** heeft ook zwakke plekken, **Mozilla Firefox** is een goed alternatief. Een nadeel van alternatieve browsers is dat websites soms niet functioneren zoals ze in Internet Explorer doen. [90]

[90] XS4ALL, *Checklist: Gezond verstand*, internet, http://www.xs4all.nl/veiligheid/checklist/verstand.php, 2007-04-08.

5 Wetgeving

5.1 Verenigde Staten van Amerika

De Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, gekend als de USA PATRIOT Act of kortweg de **Patriot Act** is een Amerikaans wetsvoorstel dat door president Bush werd opgenomen in de wetgeving op **26 oktober 2001**, 45 dagen na de aanslagen van 11 september 2001. De wet heeft als doel meer mogelijkheden te geven aan de Amerikaanse overheid om informatie te vergaren over mogelijk terrorisme en wordt gebruikt als een middel in de Amerikaanse oorlog tegen het terrorisme.

In de wet wordt geregeld dat Amerikaanse justitie en inlichtingendiensten meer macht krijgen dan voorheen: zonder gerechterlijk bevel kunnen ze informatie verzamelen, telefoongesprekken afluisteren of bewakingsopdrachten uitvoeren. E-mailverkeer kan zomaar gecontroleerd worden en gevoelige persoonlijke gegevens kunnen zonder grondige reden bekeken worden. [91]

Voorstanders hopen dat de wet meer mogelijkheden geeft aan de overheid om terrorisme voortijdig op te sporen en zo aanslagen te voorkomen. **Tegenstanders** hebben kritiek op de Patriot Act omdat deze wet de burgerrechten van de Amerikaanse bevolking zou schenden en dan voornamelijk op het gebied van privacy. Dit wordt door de overheid weerlegd door te stellen dat het leven zonder angst het hoogste burgerrecht is, en dus per definitie belangrijker is dan de bescherming van privacy. Daarnaast wordt de wet als stigmatiserend beschouwd omdat het vooral de immigranten en buitenlandse bezoekers viseert. [92]

Om gegevens over het surfgedrag van internetgebruikers te verkrijgen, wordt het **Carnivore Surveillance System** gebruikt dat door het Federal Bureau of Investigation (FBI) ontwikkeld werd. De Amerikaanse senaat keurde dit computersysteem via de Patriot Act goed om zo terrorisme op te sporen. Met dit systeem wordt er verbinding gemaakt met het netwerk van internetproviders om zo digitale communicatie te onderscheppen en te bewaren. [93]

Voordat de Patriot Act in het leven geroepen werd, bestond **Echelon** reeds, de codenaam voor het wereldwijde spionagenetwerk van de Verenigde Staten, het Verenigd Koninkrijk, Canada, Australië en Nieuw-Zeeland. Tussen deze landen werd in **1948** het United Kingdom – USA Communications Intelligence Agreement gesloten, gekend als het **UKASA-akkoord**. Echelon staat onder controle van de Amerikaanse NSA (National Security Agency). Via een wereldwijd netwerk van satellieten kan Echelon telefoon-, fax- en e-mailverkeer aftappen, om zo terroristen op te sporen en om aanslagen te voorkomen.

Alle onderschepte communicatie wordt via Echelon-computersystemen doorzocht op de aanwezigheid van bepaalde trefwoorden die zijn opgenomen in de Echelon Dictionaries. Deze Dictionaries bevatten lijsten van verdachte trefwoorden die afgeluisterd moeten worden zoals bijvoorbeeld explosieven,

[91] PLANET INTERNET, *Amerika twee jaar later*, internet, http://www.planet.nl/planet/show/id=67777/contentid=399682/sc=ebc27c, 2003-09-11.
[92] WIKIPEDIA, *USA PATRIOT Act*, internet, http://nl.wikipedia.org/wiki/USA_PATRIOT_Act, 2006-11-29.
[93] ACCELERATED GLOBAL, *Anti-Terrorism Technology: Carnivore Surveillance System*, internet, http://accelerated-promotions.com/consumer-electronics/usa-patriot-act-carnivore.htm, 2007-04-19.

aanslag, computerterrorisme, samenzwering, top secret, clandestien, bedreiging, regering, en nog veel meer. [94] Wanneer dergelijke trefwoorden gevonden worden in de communicatie, wordt dit doorgegeven aan analisten die dit verder onderzoeken. Wanneer er redenen zijn om personen te verdenken van (al dan niet nog te plegen) misdrijven kunnen gegevens doorgespeeld worden aan bevoegde instanties die verdachten in het oog kunnen houden. [95]

Voorstanders van Echelon stellen dat wie niets te verbergen heeft, ook geen bezwaar ken hebben tegen het gebruik van deze afluistermethode. Maar volgens het recht op privacy mag een dergelijke inbreuk op de persoonlijke levenssfeer enkel wanneer iemand verdacht wordt van een misdrijf indien er hiervoor aanwijzingen bestaan. Het gevaar van dergelijke spionagenetwerken als Echelon is dat de democratische regels met betrekking tot de privacybescherming met de voeten getreden worden. Daardoor ontstaat er een gevaar op misbruik van gegevens.

5.2 Europese Unie

Artikel 8 paragraaf 1 van het **Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM, 1950)** stelt dat iedereen recht heeft op eerbiediging van zijn privéleven, zijn gezinsleven, zijn huis en zijn briefwisseling. Dit grondbeginsel is de ultieme verdediging tegen inbreuken op de e-privacy. Wanneer andere beschikbare rechtsmiddelen ontoereikend blijken, kan nog steeds dit artikel ingeroepen worden ter verdediging van de privacy.

In **1981** werd de **Conventie voor de Bescherming van Individuen met betrekking tot de Automatische Verwerking van Persoonlijke Gegevens nr. 108** opgericht. Hierbij wordt de privacy beschermd bij de verwerking van persoonsgegevens door middel van nieuwe informatie- en communicatiesystemen. Deze Conventie nr. 108 is nog steeds relevant omdat ze ook gevolgd dient te worden in domeinen die buiten het bereik vallen van het Europese rechtssysteem.

Het recht op de privacy en het recht op de bescherming van persoonsgegevens werden ook opgenomen in het **Charter van de Fundamentele Rechten van de Europese Unie** en in het wetsvoorstel voor de **Europese Grondwet**.

Richtlijn 95/46/EG

Deze richtlijn van het Europees Parlement en de Raad van **24 oktober 1995** betreffende de **bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens** vormt nog steeds de algemene norm op het vlak van de bescherming van persoonsgegevens. Deze richtlijn wordt beschouwd als de basisregel in de Europese Unie die altijd van toepassing is, zowel online als offline. [96]

Deze richtlijn vertrekt van het principe dat de verwerking van persoonsgegevens alleen wettelijk is als de persoon in kwestie daarvoor nadrukkelijk zijn/haar toestemming gegeven heeft. Daarnaast wordt

[94] RENSE, *The list of Carnivore and Echelon keywords*, internet, http://www.rense.com/general66/scgh.htm, 2007-04-19.
[95] WIKIPEDIA, *Echelon*, internet, http://nl.wikipedia.org/wiki/ECHELON, 2007-04-22.
[96] OBSERVATORIUM VAN DE RECHTEN OP HET INTERNET, *Juridisch kader: wetgeving, Privacy en andere fundamentele vrijheden*, internet, http://www.internet-observatory.be/internet_observatory/home_nl.htm, 2007-04-10.

een grote verantwoordelijkheid gelegd bij de lidstaten. In artikel 3 paragraaf 2 wordt gesteld dat de richtlijn niet van toepassing is op werkzaamheden die te maken hebben met openbare veiligheid, defensie, staatsveiligheid en op strafrechterlijke activiteiten van de lidstaten. De nationale overheden hebben zelf het recht om te bepalen wanneer een afwijking van de gegevensbescherming toelaatbaar is, zo stelt artikel 13. In artikel 27 staat dat de Europese Unie hen aanmoedigt om nationale gedragscodes op te stellen. In artikel 28 wordt aan de lidstaten gevraagd om elk een onafhankelijke instantie op te richten die toezicht moet houden op de correcte toepassing van de regels.

De Europese Unie richt in artikel 29 een werkgroep op met de naam 'Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens', ook bekend als 'Werkgroep Artikel 29', die een adviserende rol krijgt toegewezen. Verder bepaalt de richtlijn ook dat de overdracht van persoonsgegevens naar landen buiten de Europese Unie enkel mogelijk is als de landen in kwestie voldoende bescherming bieden.

Richtlijn 2000/31/EG

Deze richtlijn van het Europees Parlement en de Raad van **8 juni 2000** handelt over **bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt**. In deze richtlijn wordt aangegeven dat de lidstaten er steeds voor dienen te zorgen dat, als ze ongevraagde commerciële communicatie via elektronische post toestaan, de verzender van dergelijke berichten ertoe verplicht is ervoor te zorgen dat de ontvanger van de boodschap deze meteen duidelijk en ondubbelzinnig bij ontvangst kan identificeren als een reclameboodschap.

De lidstaten moeten ook maatregelen nemen die ervoor zorgen dat dienstverleners die via de elektronische post ongevraagde commerciële communicatie versturen, de opt-out registers regelmatig raadplegen en ook respecteren. Dergelijke opt-out registers bevatten gegevens van natuurlijke personen die dergelijke commerciële communicatie niet wensen te ontvangen. [97]

Richtlijn 2002/58/EG

Deze richtlijn betreffende de **verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie** werd op **12 juli 2002** goedgekeurd. Deze wordt ook de richtlijn betreffende privacy en elektronische communicatie (of korter 'privacyrichtlijn') genoemd en verduidelijkt de bepalingen van de algemene norm, richtlijn 95/46/EG. De nieuwe richtlijn is enkel bedoeld voor publieke netwerken, en niet voor kleinschalige netwerken zoals deze in bedrijven. De privacyrichtlijn legt immers strenge beperkingen op die te zwaar zouden doorwegen in kleine netwerken. [98]

De lidstaten werden verplicht wetten op te stellen die het vertrouwelijke karakter van elektronische communicatie moeten waarborgen door het onderscheppen en controleren van dergelijke communicatie te verbieden. Verder wordt met deze richtlijn het langer dan noodzakelijk opslaan van verkeers-

[97] DE MUYNCK, H., *Informatica: Juridische aspecten – een overzicht*, Uitgeverij Lannoo NV, Tielt, 2004, Hoofdstuk 9: Europese Richtlijn 'Elektronische handel' p. 113-122.
[98] INTERNETJOURNALISTIEK, *E-privacy in een Europese context*, internet, http://www.internetjournalistiek.be/dossiers/detail_privacy.php?nieuwsid=94, 2007-04-10.

gegevens verboden. De bewaring van dergelijke gegevens wordt door de Raad van Europa beperkt tot drie maanden. In het kader van een gerechtelijk onderzoek of bij bedreiging van de openbare orde of van de staatsveiligheid mag de gegevensbescherming wel opgegeven worden.

Door de richtlijn worden de lidstaten van de Europese Unie verplicht om vanaf **oktober 2003 ongewenste communicatie of spam** te **verbieden**. Het versturen van elektronische post voor commerciële doeleinden is enkel toegelaten na toestemming van de geadresseerde, dit wordt het opt-in systeem genoemd. Het probleem van spam is daardoor niet opgelost aangezien elektronische berichten die van buiten de Europese Unie verstuurd worden, niet onder deze regelgeving vallen.

Met betrekking tot **cookies** werd in deze richtlijn bepaald dat internetgebruikers voldoende informatie moeten krijgen over het doel van cookies. Ze moeten eveneens het recht krijgen deze te weigeren. [99]

5.3 België

5.3.1 Wettelijke bepalingen

Wet van 21 maart 1991

Deze wet betreffende de **hervorming van sommige economische overheidsbedrijven** bevat een hoofdstuk over geheimhouding van gesprekken en bescherming van de persoonlijke levenssfeer. Deze wet wordt ook de **Belgacomwet** genoemd omdat deze wet ook en zelfs hoofdzakelijk de bedoeling had het statuut van Belgacom en zijn personeel te regelen. Het centrale artikel in dit hoofdstuk is artikel 109terD dat onder meer de kennisname van het bestaan van andermans communicatie verbiedt zonder de voorafgaande toestemming van alle communicerende partijen.

Wet van 14 juli 1991

Deze wet betreffende de **handelspraktijken en de voorlichting en bescherming van de consument**, kortweg de **wet op de handelspraktijken**, stelt dat het versturen van ongevraagde reclame per e-mail of spam toegelaten is voor zover de ontvanger ervan duidelijk en ondubbelzinnig kan zien dat het om reclame gaat en hij de boodschap onmiddellijk kan verwijderen als hij niet geïnteresseerd is in dergelijke berichten. [100]

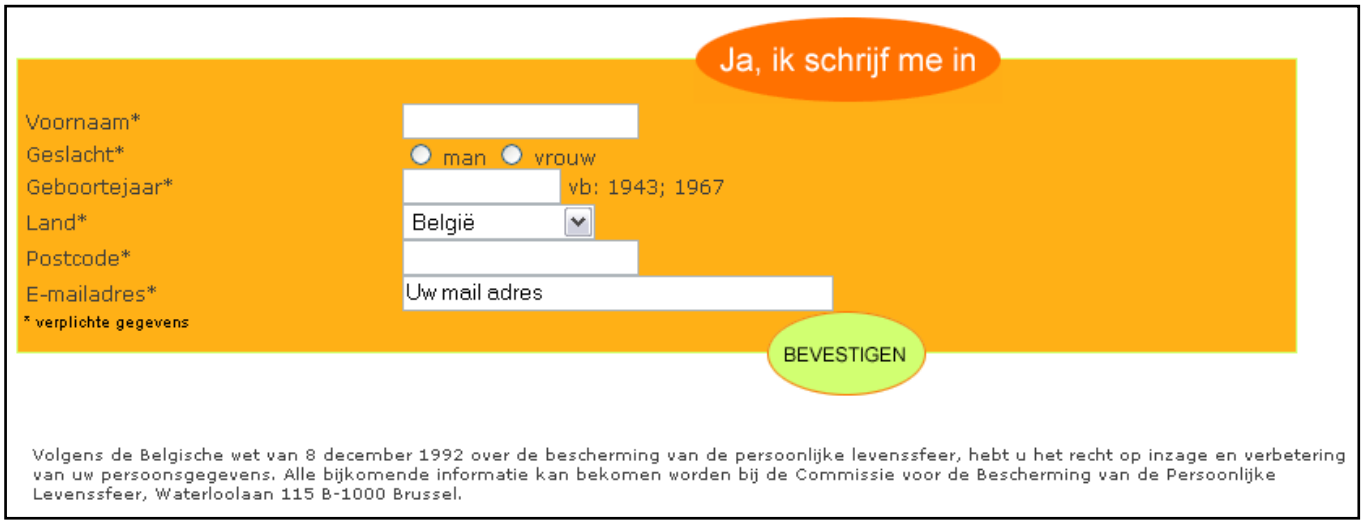
Wet van 8 december 1992

Deze wet tot **bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens**, de zogenaamde '**wet verwerking persoonsgegevens**', is één van de belangrijkste Belgische wetten die de privacy van de burger beschermt. Het doel ervan wordt vastgelegd in artikel 2:

[99] DE MUYNCK, H., *Informatica: Juridische aspecten – een overzicht*, Uitgeverij Lannoo NV, Tielt, 2004, Hoofdstuk 1: Juridische aspecten inzake de persoonlijke levenssfeer en de verwerking van persoonsgegevens, p. 15-25.
[100] DE MUYNCK, H., *Informatica: Juridische aspecten – een overzicht*, Uitgeverij Lannoo NV, Tielt, 2004, Hoofdstuk 6: Juridische aspecten met betrekking tot reclame per e-mail (spam), p. 81-90.

iedere natuurlijke persoon heeft in verband met de verwerking van persoonsgegevens die op hem betrekking hebben, recht op bescherming van zijn fundamentele rechten en vrijheden, waaronder de bescherming van de persoonlijke levenssfeer.

Bij deze wet werd een onafhankelijke controle-autoriteit voor gegevensbescherming opgericht: de **Commissie voor de bescherming van de persoonlijke levenssfeer**. Deze Commissie staat in voor de naleving en de interpretatie van deze privacywet. In het privacystatement op websites wordt vaak verwezen naar deze wet (zie afbeelding hieronder). Zo willen bedrijven duidelijk maken dat hun privacybeleid conform deze wet is. Over deze wet en de Commissie volgt hierna (zie 5.2.2) meer informatie.



Afb. 15: Screenshot van de inschrijving op de nieuwsbrief van de website E-gezondheid.be

Wet van 30 juni 1994

De wet van 30 juni 1994 ter **bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privécommunicatie en –telecommunicatie** is ook bekend als de **Afluisterwet**. Deze bevat de belangrijkste Belgische reglementeringen die verband houden met de bescherming van de vertrouwelijkheid van privé(tele)communicatie. Het afluisteren, kennisnemen en opnemen van andermans privé(tele)communicatie zonder de toestemming van alle deelnemers is verboden. Hierbij worden openbare gezagsdragers onderworpen aan een strenger regime dan particulieren. Bij het onderzoeken van bepaalde zwaarwichtige strafbare feiten kan een uitzondering worden gemaakt op dit verbod. Indien afluisteren absoluut nodig is om de ware toedracht van een misdrijf te achterhalen is het toegelaten de privé(tele)communicatie van een verdachte voor een beperkte tijd af te luisteren of op te nemen.

Wet van 11 december 1998

De **Europese richtlijn 95/46/EG** werd in deze wet omgezet naar Belgisch recht via een aanpassing van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

Wet van 28 november 2000

Met de wet van **28 november 2000** betreffende **informaticacriminaliteit** verplicht de Belgische overheid telecombedrijven en providers om verkeers- en locatiegegevens gedurende **minstens 12 maanden** bij te houden. De bewaring van dergelijke gegevens wordt met de **Europese richtlijn 2002/58/EG** door de Raad van Europa beperkt tot drie maanden, een periode die in richtlijn 95/46/EG reeds werd vastgelegd. Met deze wet wordt computerinbraak of hacking ook uitdrukkelijk strafbaar gesteld. [101]

Collectieve arbeidsovereenkomst nr. 81 van 26 april 2002

CAO 81 tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische online communicatiegegevens werd op 26 april 2002 gesloten in de Nationale Arbeidsraad. CAO 81 bepaalt de controle die de werkgever kan uitoefenen op de elektronische online communicatiegegevens wanneer een werknemer daar gebruik van maakt.

In de CAO worden eerst de beginselen waaraan iedere controle moet voldoen bepaald. Deze beginselen zijn **finaliteit** (doelstellingen van de controle moeten omschreven worden), **proportionaliteit** (er mag geen inmening zijn in de persoonlijke levenssfeer) en **transparantie** (iedereen moet vooraf ingelicht worden). Hierna wordt in de CAO gedefinieerd welke voorlichting aan de werknemers gegeven moet worden, op welke gegevens controle uitgeoefend mag worden, en de maatregelen die de werkgever kan nemen wanneer zich een probleem voordoet.

Wet van 11 maart 2003

De Europese richtlijn 2002/58/EG stelt dat het versturen van elektronische post voor commerciële doeleinden enkel toegelaten is na toestemming van de geadresseerde, volgens het zogeheten opt-in systeem. Met de wet van 11 maart 2003 betreffende **bepaalde juridische aspecten van de diensten van de informatiemaatschappij** was België het eerste land in de Europese Unie dat deze bepaling opnam in haar nationale wetgeving. De verzending van **spam** zonder voorafgaande toestemming van de ontvanger werd hierdoor **verboden**, op enkele uitzonderingen na.

De verzender van de reclame dient duidelijke en begrijpelijke informatie te verschaffen over het feit dat de ontvanger van de reclame het recht heeft zich te verzetten tegen het in de toekomst nog ontvangen van reclame. Er moet vermeld worden op welke manier dit verzet kan worden doorgegeven. Om misbruiken tegen te gaan werd in de wet ook bepaald dat het verboden is voor verzenders het e-mailadres of de identiteit van een derde te gebruiken of informatie te vervalsen of te verbergen. [102]

Gegevens die na de inwerkingtreding van deze wet ingezameld worden, mogen in principe niet zonder toestemming van de ontvanger gebruikt worden om reclame te verzenden. Wat eerder ingezamelde

[101] PISA – PROVIDING INFORMATION ABOUT INTERNET SECURITY ASPECTS, *Wetgeving: Inbraak*, internet, http://pisa.belnet.be/pisa/nl/juridisch/crack.htm, 2007-04-14.
[102] DE MUYNCK, H., *Informatica: Juridische aspecten – een overzicht*, Uitgeverij Lannoo NV, Tielt, 2004, Hoofdstuk 6: Juridische aspecten met betrekking tot reclame per e-mail (spam), p. 81-90.

gegevens betreft, heeft de Commissie een overgangsbeleid gevoerd naar Frans voorbeeld. Ondernemingen die op wettelijke wijze een adressenbestand verzameld hebben, kregen tot 31 december 2003 de tijd om hun klanten te contacteren om te vragen of zij in de toekomst nog commerciële boodschappen willen ontvangen. Mensen die hun toestemming niet gaven, moesten uit het adressenbestand geschrapt worden. [103]

Het Koninklijk Besluit van 4 april 2003

In dit KB tot **reglementering van het verzenden van reclame per elektronische post** werden belangrijke bepalingen opgenomen die een uitbreiding vormen op de wet van 11 maart 2003.

Een bedrijf dient geen voorafgaande toestemming te vragen bij **eigen klanten** wanneer aan volgende drie voorwaarden voldaan wordt:

- Het bedrijf heeft de contactgegevens van de betrokkene rechtstreeks verkregen in het kader van de verkoop van een product of dienst, bijvoorbeeld via een online bestelformulier. Hierbij moet de privacywet gerespecteerd zijn, wat bijvoorbeeld betekent dat de gegevens niet onrechtmatig verkregen mogen zijn.
- De gegevens zullen enkel gebruikt worden voor gelijkaardige producten en diensten die het bedrijf zelf levert.
- Het bedrijf geeft de klanten bij de gegevensverzameling de mogelijkheid om zich kosteloos en op een gemakkelijke manier te verzetten tegen het gebruik van hun gegevens.

Verder moet een bedrijf geen voorafgaande toestemming vragen om reclame via e-mail te sturen naar **rechtspersonen**, indien aan de volgende twee voorwaarden voldaan wordt:

- de contactgegevens moeten onpersoonlijk zijn;
- de producten waarvoor reclame gemaakt wordt, zijn bestemd voor de rechtspersoon.

Met betrekking tot het kosteloos en gemakkelijk verzet tegen het ontvangen van reclame via elektronische post wordt gesteld dat de dienstverlener verplicht is om:

- binnen een aanvaardbare termijn en per e-mail een ontvangstbewijs te leveren dat de vraag bevestigt om geen reclame meer te ontvangen;
- binnen een aanvaardbare termijn de nodige maatregelen te treffen om de wil van deze persoon na te leven;
- lijsten bij te werken met personen die hun wil kenbaar hebben gemaakt om niet langer reclame per elektronische post te ontvangen.

[103] OBSERVATORIUM VAN DE RECHTEN OP HET INTERNET, *Juridisch kader: wetgeving, Privacy en andere fundamentele vrijheden*, internet, http://www.internet-observatory.be/internet_observatory/home_nl.htm, 2007-04-14.

5.3.2 Basisprincipes van de wet verwerking persoonsgegevens

De wetgever stelt uitdrukkelijk dat iedere natuurlijke persoon recht heeft op bescherming van zijn persoonlijke levenssfeer wanneer het gaat om de verwerking van de op hem betrekking hebbende persoonsgegevens. De wet is niet van toepassing op de verwerking van persoonsgegevens voor huishoudelijk of persoonlijk gebruik. [104]

Persoonsgegevens

Onder persoonsgegevens wordt hier iedere informatie verstaan betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Gegevens betreffende rechtspersonen vallen hier dus niet onder. Een persoon is identificeerbaar als hij direct of indirect kan worden geïdentificeerd, bijvoorbeeld aan de hand van een identificatienummer of specifieke elementen kenmerkend voor zijn fysieke, fysiologische, psychische, economische, culturele of sociale identiteit.

Verwerking

Onder verwerking valt elke bewerking met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procédés. Het gaat hier over bijvoorbeeld het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, gebruiken en verspreiden van informatie. Voordat wordt overgegaan tot verwerking van gegevens dient hiervan aangifte te worden gedaan bij de Commissie voor de bescherming van de persoonlijke levenssfeer.

Voorwaarden waaraan de persoonsgegevens moeten voldoen:

- Ze moeten eerlijk en rechtmatig worden verwerkt. Gegevens mogen dus niet verzameld worden voor een vals doel of zonder medeweten van de betrokken persoon.
- De gegevens moeten verkregen worden voor specifiek omschreven en gerechtvaardigde doeleinden.
- De persoonsgegevens moeten relevant zijn. Er mag niet gevraagd worden naar overbodige gegevens die irrelevant zijn.
- Ze moeten nauwkeurig zijn en indien noodzakelijk, worden bijgewerkt.
- De persoonsgegevens mogen niet langer dan noodzakelijk worden bewaard.

Situaties waarin de wetgever de verwerking van persoonsgegevens toelaat:

- wanneer de betrokkene daarvoor vrijwillig zijn ondubbelzinnige toestemming heeft gegeven;
- wanneer de verwerking noodzakelijk is voor de uitvoering van een overeenkomst, bijvoorbeeld wanneer een bestelling moet geleverd worden;
- wanneer de verwerking nodig is om een verplichting na te komen, bijvoorbeeld personeelsgegevens die moeten doorgegeven worden aan de Rijksdienst voor Sociale Zekerheid (RSZ);
- wanneer de verwerking noodzakelijk is om het vitaal belang van de betrokkene te beschermen, bijvoorbeeld persoonsgegevens die noodzakelijk zijn voor de behandeling van een medisch spoedgeval;
- wanneer de verwerking noodzakelijk is voor het vervullen van een taak van openbaar belang of een taak die deel uitmaakt van de uitoefening van het openbaar gezag, bijvoorbeeld de Post die adreswijzigingen bijhoudt;
- wanneer de verwerking noodzakelijk is in het kader van het gerechtvaardige belang van degene die de gegevens verwerkt.

[104] DE MUYNCK, H., *Informatica: Juridische aspecten – een overzicht*, Uitgeverij Lannoo NV, Tielt, 2004, Hoofdstuk 1: Juridische aspecten inzake de persoonlijke levenssfeer en de verwerking van persoonsgegevens, p. 15-25.

Rechten van de betrokken persoon

De betrokken persoon van wie gegevens worden verzameld heeft een aantal rechten toegekend gekregen van de wetgever.

1) recht op informatie: De verantwoordelijke voor de gegevensverwerking moet uiterlijk op het moment dat de gegevens verkregen worden de volgende informatie meedelen:

- de naam en het adres van de verantwoordelijke voor de verwerking
voorbeeld: *"De persoonsgegevens die u hierbij verstrekt worden opgenomen in de bestanden van Belgacom Skynet, Carlistraat 2 , 1140 Evere."*
Bron: http://www.skynet.be

- de doeleinden van de verwerking
voorbeeld: *"Deze gegevens worden door Skynet verwerkt in het kader van de klantenadministratie, marktstudies en met het oog op het voeren van gepersonaliseerde informatie- en promotiecampagnes i.v.m. onze producten en diensten."*
Bron: http://www.skynet.be

- het bestaan van het recht om zich te verzetten tegen de verwerking van de persoonsgegevens, indien het verwerking in het kader van direct marketing betreft
voorbeeld: *"U heeft het recht om u kosteloos te verzetten tegen verwerking van uw gegevens voor direct marketing doeleinden. U kunt uw aanvraag tot inzage, correctie of verzet richten tot de klantendienst."*
Bron: http://www.telenet.be

- de andere partijen met wie de gegevens eventueel worden gedeeld
voorbeeld: zie bijlage XII

- het al dan niet verplichte karakter van het antwoord en de eventuele gevolgen van niet-beantwoording
voorbeeld: *"Op de registratiepagina van Yez wordt u verzocht contact- en facturatiegegevens te verstrekken (zoals naam, adres, e-mail, tel, enz), zodat u objecten kan aanbieden, biedingen kan uitbrengen op Yez en advertenties kan plaatsen. U kan ervoor kiezen bepaalde gegevens niet te verstrekken, maar dit kan uw gebruik van bepaalde faciliteiten van onze site beperken."*
Bron: http://www.yezzz.be

- het bestaan van het recht op toegang tot en verbetering van de persoonsgegevens
voorbeeld: *"U hebt het recht om uw gegevens in te kijken en, zo nodig, te verbeteren. U hoeft daarvoor enkel een brief met een kopie van uw identiteitskaart te sturen naar KBC Bank & Verzekering, PCS, Cliëntenservice, Brusselsesteenweg 100, 3000 Leuven. U kunt uw gegevens ook opvragen via een voorgedrukt formulier dat ter beschikking ligt in uw KBC-bankkantoor."*
Bron: http://www.kbc.be

2) recht op mededeling: De betrokken persoon kan met een gedagtekend en ondertekend verzoek aan de verwerker van de persoonsgegevens informatie vragen in verband met:

- de verwerking van op hem betrekkende gegevens;
- informatie over de doeleinden van deze verwerkingen;
- de categorieën gegevens waarop de verwerkingen betrekking hebben;
- de ontvangers aan wie de gegevens worden verstrekt.

3) recht op verbetering: Iedereen is gerechtigd om alle onjuiste persoonsgegevens die op hem betrekking hebben, kosteloos te doen verbeteren.

4) recht op verzet: Indien de persoonsgegevens verkregen worden in het kader van direct marketing mag de betrokkene zich kosteloos en zonder enige reden tegen de verwerking van de op hem betrekking hebbende persoonsgegevens verzetten.

De verantwoordelijke van een website is verplicht op voorhand bepaalde informatie in verband met de verzameling van persoonsgegevens te verstrekken aan de bezoeker van de website. De volledige informatie van het gevoerde privacybeleid dient toegankelijk te zijn vanaf de startpagina van de website, maar eveneens op elke plaats waar de persoonsgegevens online worden verzameld. Dit gebeurt door middel van een link die een specifieke titel draagt, meestal 'privacystatement', 'privacybeleid' of kortweg 'privacy'. Een voorbeeld van een privacybeleid is te vinden in bijlage, zie bijlage XIII: het privacybeleid van Telenet.

Commissie voor de bescherming van de persoonlijke levenssfeer

De taken van deze Commissie kunnen samengevat worden in vier punten:

- aanbevelingen geven aan de regering omtrent iedere zaak die te maken heeft met de toepassing van de grondbeginselen van de bescherming van de persoonlijke levenssfeer;
- de getekende en gedateerde klachten onderzoeken die haar worden toegestuurd;
- aangifte doen bij de procureur des Konings van de misdrijven waar zij weet van heeft;
- ieder jaar bij de Wetgevende Kamers een verslag indienen over haar werkzaamheden.

5.4 Zelfregulering

In plaats van enkel een beroep te doen op de wettelijke bepalingen, zijn er een aantal instanties die zelf initiatieven hebben genomen om de internetgebruikers te beschermen tegen spam.

Zo is er het initiatief van het **Belgisch Direct Marketing Verbond (BDMV)** dat de zogenaamde **Robinson-lijst** aanbiedt, wat reeds werd aangehaald in het vorige hoofdstuk.

Een ander initiatief werd genomen door de vereniging van de Belgische internetaanbieders **Internet Service Providers Association (ISPA)**. Deze werken samen een procedure uit die ervoor moet zorgen dat alle internetleveranciers op een uniforme manier zullen optreden tegen spam. Tot op heden volgt elke provider een eigen politiek tegen spam die er voornamelijk uit bestaat dat bepaalde spamfiltersoftware ter beschikking wordt gesteld van de klanten.

ISPA werkt samen met de informele werkgroep **Spamsquad** die bestaat uit academici, overheidsvertegenwoordigers, rechtsgeleerden en professionelen uit de informaticasector. Deze organisatie houdt zich bezig met het onderzoeken van spam en het uitwerken van oplossingen om spam actief te bestrijden.

TRUSTe is ook een dergelijk initiatief dat zich bezighoudt met de privacy van internetgebruikers. TRUSTe is een onafhankelijke non-profit organisatie die het eerste online privacyprogramma ontwikkelde. Met dit programma wordt gecontroleerd of websites te vertrouwen zijn met persoonlijke gegevens van websitebezoekers door te vergelijken of het privacystatement op een website overeenkomt met de regels met betrekking tot eerlijke handelspraktijken die door het U.S. Department of Commerce en de Federal Trade Commission zijn uitgeschreven. Wanneer het privacystatement van een website beantwoordt aan de eisen, mag de website de TRUSTe-privacyzegel plaatsen (zie bijlage XIV).

6 Beleid van internetproviders

Een Internet Service Provider (ISP) of kortweg internetprovider is een organisatie die de internettoegang verzorgt. In België houden internetproviders een jaar lang surfgegevens bij. Dit is bij wet bepaald. De inhoud van bezochte websites, van chatgesprekken of van verstuurde e-mails wordt niet bewaard. De politie kan in opdracht van een onderzoeksrechter internetproviders wel verplichten het internetverkeer van een bepaalde klant af te luisteren.

Privacybescherming van de Belgische internetgebruiker zit in meerdere wetten vervat, die in het vorige hoofdstuk werden opgesomd. Ook de Europese regelgeving met betrekking tot privacybescherming dient gevolgd te worden in België. De aansprakelijkheid van ISP's is moeilijk te bepalen. Er bestaat momenteel geen Belgische wetgeving die de aansprakelijkheid van de internetproviders specifiek en duidelijk vastlegt. Slechts enkele beslissingen uit de rechtspraak bakenen de aansprakelijkheid van de ISP's enigszins af.

6.1 Wetgeving

De rechtspraak is niet eensgezind, omdat bepaalde arresten veel aandacht krijgen in de media en zo onzekerheid zaaien bij de internetproviders. Eén principe wordt vaak vernoemd: de provider is enkel aansprakelijk wanneer hij weet dat hij toegang verleent tot onwettige sites en hij hieraan niets doet. In de meeste gevallen van overtreding wordt de ISP in kort geding (volgens een snelprodedure) voor de rechter gedagvaard. De rechter verplicht de provider dan alle onwettige informatie te verwijderen tegen een dwangsom. Zolang de onwettige informatie niet verwijderd is, moet de ISP een bepaald bedrag betalen per dag. Het gebeurt zelden dat de rechter de provider veroordeelt en beslist dat hij aansprakelijk is.

Het Europees Parlement en de Raad hebben op 8 juni 2000 **richtlijn 2000/31/EG** opgesteld betreffende bepaalde juridische aspecten van de elektronische handel in de interne markt, die ook de richtlijn inzake **elektronische handel** wordt genoemd. In de richtlijn wordt bepaald dat de aansprakelijkheid van de provider wegvalt onder bepaalde omstandigheden en voor bepaalde soorten van activiteiten. Afhankelijk van de rol die de ISP heeft, gelden andere voorwaarden die de provider vrijstellen van aansprakelijkheid.

Wanneer de provider de rol van gewone informatiedrager heeft, is hij vrijwel geheel vrijgesteld van aansprakelijkheid. Maar bij **opslag van informatie in cache** en bij **hosting-activiteit** kan de provider onder bepaalde voorwaarden aansprakelijk worden gesteld. Caching is de automatische, tussentijdse en tijdelijke opslag van informatie met als enige doel de latere doorgifte van die informatie doeltreffender te maken. Als de internetprovider zich strikt houdt aan zijn rol, wordt hij niet aansprakelijk gesteld zolang hij onmiddellijk informatie verwijdert of de toegang ertoe onmogelijk maakt, wanneer een gerechtelijke of administratieve instantie hem dit bevolen heeft of wanneer de provider zelf weet heeft van de onwettige aard van de informatie.

Wanneer de provider weet heeft van onwettige activiteiten of dergelijke activiteiten opmerkt, moet hij **onmiddellijk handelen om de informatie te verwijderen of de toegang daartoe onmogelijk te maken** als hij die mogelijkheid heeft. Dit principe laat ruimte tot interpretatie. Telkens de ISP door een derde (geen bevoegde instantie) wordt gewezen op onwettige informatie, moet hij zelf uitmaken of de inhoud al dan niet verdacht of onwettig is. De inhoud is onwettig als het gaat om overduidelijke inbreuken: pedofiele afbeeldingen, aansporing tot rassenhaat of –discriminatie, aanzetting tot moord of wanbedrijven, duidelijke vervalsing, beledigende uitspraken, enzovoort. In dergelijke gevallen moet de ISP onmiddellijk de inhoud verwijderen of de toegang ertoe onmogelijk maken als hij die mogelijkheid heeft.

In sommige gevallen kan de inhoud omstreden zijn, zonder daarom duidelijk onwettig te zijn: lasterlijke of beledigende uitspraken, gewelddadige boodschappen, pornografische teksten of afbeeldingen, persoonsgegevens die zonder toelating worden gepubliceerd, ... In dergelijke gevallen is het voor de provider moeilijk om op te treden. De rechtspraak raadt de ISP aan snel op te treden om de rechten van derden te beschermen.

Verder wordt in de richtlijn gesteld dat een internetprovider **geen algemene toezichtverplichting** heeft. Een provider is niet verplicht om toe te zien op de informatie die ze doorstuurt of bewaart, noch om actief te zoeken naar feiten of omstandigheden die op onwettige activiteiten duiden. Toch kunnen bevoegde autoriteiten een tijdelijk en gericht toezicht opleggen als dit nodig is om de staatsveiligheid, de verdediging en de openbare orde te bewaren en om strafbare feiten te voorkomen, op te sporen en te vervolgen. [105]

6.2 SURFARCHIEVEN

De Belgische wetgeving eist dat elke internetprovider een jaar lang alle oproepgegevens van zijn klanten opslaat. Die informatie is nodig voor het opsporen en vervolgen van strafbare feiten. Uit de Belgische wetgeving blijkt niet duidelijk wat verstaan wordt onder 'oproepgegevens'. De Europese richtlijn is op dat vlak duidelijker en vermeld dat de door de elektronische gegevens afgelegde weg bewaard mag worden, net als de tijdstippen van communicatie, het volume, het gebruikte protocol (ftp, e-mail, …) en netwerk, de locaties en het formaat van de berichten. [106]

Internetprovider **Belgacom** bevestigt enkel die gegevens bij te houden waar de wetgeving om vraagt en de informatie die nodig is met het oog op de facturering. Informatie die verzameld wordt omvat volgende gegevens: wie inlogt en met welke login, hoe lang werd ingelogd en welk volume werd gedownload. Er worden geen gegevens verzameld over welke websites bezocht werden, wat gedownload werd, naar wie gemaild werd, of met wie gechat werd. Belgacom houdt, zoals de Belgische wetgeving het voorschrijft, de oproepgegevens een jaar bij. [107]

[105] FOD ECONOMIE KMO MIDDENSTAND EN ENERGIE, *Aanbevelingen inzake de aansprakelijkheid van de internetprovider*, internet, http://mineco.fgov.be/information_society/enterprises/providers_internetguide/Providers1_nl-03.htm#P283_34529, 2007-04-16.
[106] SOUFFREAU, B., *Providers houden jaar lang surfgegevens bij*, internet, http://www.internetjournalistiek.be/dossiers/detail_privacy.php?nieuwsid=93, 2003-12-07.
[107] BELGACOM, *Online Privacy Policy*, internet, http://www.belgacom.be/home/gallery/content/e-services/conditions/nl/privacy.pdf, 2007-04-16.

Scarlet houdt ongeveer dezelfde gegevens bij: wanneer iemand zich op het internet aanlogt, wanneer hij weer aflogt en hoeveel bits verstuurd worden. Inhoud van websites, e-mails of chats wordt niet bijgehouden, omdat het enerzijds niet haalbaar is en anderzijds niet toegelaten is door de privacywet van 8 december 1992. De verzamelde informatie wordt gebruikt voor meerdere doeleinden: voor facturatie, voor de controle van gebruikerslimieten, voor politiediensten wanneer zij gegevens van klanten nodig hebben (welk IP-adres aan wie toebehoort bijvoorbeeld) en voor de monitoring van het netwerk. In het laatste geval is de informatie steeds anoniem, en dus niet gelinkt aan een bepaalde klant. Scarlet verwijdert sommige informatie al na drie tot zes maanden, meestal zijn dit gegevens die nodig zijn voor het opstellen van de facturen. Andere informatie blijft twaalf maanden in het bezit van Scarlet. [108]

Op de site van **Telenet** is terug te vinden dat het bedrijf zich houdt aan de Belgische privacywetgeving. Telenet verzamelt ook informatie over de conditie van het netwerk voor intern gebruik. [109]

6.3 Samenwerking met politie en gerecht

Volgens een ruwe schatting schakelt de Belgische politie maandelijks een duizendtal keer de internetproviders in om via een IP-adres de naam van de klant te kunnen achterhalen. Die gegevens worden gebruikt in onderzoeken naar spam, hacking, illegale en pornografische inhoud. De politie kan **in het kader van een strafrechtelijk onderzoek** en **na vordering door de onderzoeksrechter** aan een internetprovider vragen het internetverkeer van een bepaalde klant af te luisteren, maar in de praktijk gebeurt dit niet vaak.

Onder **afluisteren** valt het onderscheppen van e-mails, de inventarisatie van het surfgedrag (bezochte websites en gevoerde chatgesprekken) en het scannen van bepaalde computers. Het in beslag nemen en onderzoeken van de computer van een verdachte valt hier niet onder. [110]

6.4 Internetcensuur

Op aanvraag van de regering kunnen bepaalde websites gecensureerd of geblokkeerd worden. Zo wordt in **China** geregeld internetcensuur toegepast. China is op vijf punten verbonden met het wereldwijde internet. Het grootste gedeelte van de filtering vindt bij deze vijf gateways plaats, maar ook op het niveau van ISP's, internetcafés en andere aanbieders wordt gefilterd. Zo kan de toegang tot websites met politiek gevoelige of pornografische inhoud geblokkeerd worden. Bovendien hebben ISP's en internetcafés blackboxes geïnstalleerd om alle internetverkeer gedurende 60 dagen te kunnen opslaan, zodat precies kan nagegaan worden wie waar op het internet is geweest. [111]

Daarnaast worden bepaalde zoektermen niet geaccepteerd door zoekmachines in China. Wanneer dat toch geprobeerd wordt, verschijnt eerst 'the page cannot be displayed'. Wanneer het herhaaldelijk geprobeerd wordt, kan de toegang tot de zoekmachine geheel geblokkeerd worden. Blogbeheerders

[108] SCARLET, *Wettelijke vermeldingen en voorwaarden*, internet, http://www.scarlet.be/nl/legal/, 2007-04-16.
[109] TELENET, *Algemene voorwaarden Telenet Internet*, internet, http://www.telenet.be/nl/onlinesupport/thuis/algemene-voorwaarden/algvw_internet.page, 2007-04-16.
[110] SOUFFREAU, B., *Providers houden jaar lang surfgegevens bij*, internet, http://www.internetjournalistiek.be/dossiers/detail_privacy.php?nieuwsid=93, 2003-12-07.
[111] GELE DRAAK, *Internetcensuur in China*, internet, http://www.geledraak.nl/html/showarticle.asp?id=539, 2007-04-18.

staan bepaalde woorden niet toe en zelfs de internetcache (het archief waar kopieën van alle websites worden bijgehouden) van Google wordt gefilterd. Verder aarzelt de Chinese overheid niet om mensen op te pakken die online voor hun mening uitkwamen. De angst om door de overheid gesloten te worden, heeft veel bedrijven doen besluiten zelfcensuur toe te passen. [112]

In **2004** bevestigde **Google** dat het sommige websites niet toont bij de zoekresultaten van zijn Chinese zoekmachine. Links die leiden naar websites die door de Chinese overheid geblokkeerd worden, worden niet opgenomen tussen de zoekresultaten.

In **2005** blokkeerde de Chinese overheid de toegang tot de Chinese versie van **Wikipedia**, een online encyclopedie die door vrijwilligers wordt samengesteld. Niet alleen de Chinese versie werd gecensureerd, ook de toegang tot anderstalige versies van Wikipedia werd geblokkeerd. De Chinese Wikipedia bevat veel artikels over gevoelige onderwerpen die nog steeds taboe zijn in China. In **2006** werd de blokkade na ruim een jaar weer opgeheven.

Nog in **2006** kondigde **Google** de **speciale Chinese versie** aan van zijn zoekmachine, met als webadres de Chinese extentie .cn. Google ging akkoord met de eisen van de Chinese regering om zoekresultaten te censureren. Internetgebruikers konden voordien bijna geen gebruik maken van Google omdat de zoekresultaten met vertraging werden afgebeeld. De zoekmachine werd zo goed als onbruikbaar door de blokkades die de regering had opgelegd om ongewenste informatie te weren.

Google zal webcontent censureren die de Chinese regering als ongewenst beschouwd. Voorbeelden van verboden webcontent zijn pagina's over de onafhankelijkheid van Taiwan of over de slachting op het Tiananmenplein in 1989. Wanneer een Chinese internetgebruiker verboden zoekresultaten opvraagt, krijgt hij een melding dat de zoekresultaten zijn verwijderd om te voldoen aan lokale wetten. Soortgelijke meldingen worden ook in **Duitsland** en **Frankrijk** gebruikt waar het wettelijk verboden is om nazi-propaganda op een website te vermelden. [113]

In **Nederland** maakte internetprovider **UPC** begin **februari 2007** bekend dat ze samen met de politie websites met kinderporno ontoegankelijk maakt voor haar klanten. In navolging va Noorwegen waar dagelijks 6 500 hits naar kinderpornosites geblokkeerd worden, gaat UPC het internet filteren. In samenwerking met de politie die een zwarte lijst heeft opgesteld met kinderporno-adressen, wil het bedrijf ongeveer 3 000 adressen blokkeren. Gebruikers die proberen een dergelijke website te bezoeken krijgen voortaan een pagina te zien waarop wordt vermeld dat de site ontoegankelijk is gemaakt. Andere providers gaan dit voorbeeld volgen, aangezien de pornoliefhebbers anders naar de concurrentie zullen overlopen.

[112] TWEAKERS.NET, *China's grote vuurmuur nader bekeken*, internet, http://tweakers.net/nieuws/40666, 2007-04-18.
[113] PERSONAL COMPUTER MAGAZINE, *Google gaat akkoord met Chinese censuur*, internet, http://www.pcmweb.nl/nieuws.jsp?id=1093324, 2007-04-18.

7 Privacy binnen een bedrijf

7.1 Wetgeving

Met het steeds intensievere gebruik van het internet doen zich steeds vaker problemen voor in de relatie tussen de werkgever en de werknemer die te maken hebben met:

- het tijdens de werkuren surfen op internet voor privé-doeleinden;
- het door de werkgever controleren van de door de werknemer bezochte websites;
- het door de werknemer versturen van persoonlijke e-mails;
- het door de werkgever lezen van e-mails die werden ontvangen door de werknemer.

De meeste van deze problemen vallen onder het begrip 'eerbiediging van het privéleven'. De wetgeving die hierop betrekking heeft, werd reeds in hoofdstuk 5 aangehaald. Aangezien de wettelijke regelingen soms op verschillende manier geïnterpreteerd kunnen worden, hebben werkgevers en werknemers besloten om binnen de **Nationale Arbeidsraad (NAR)** samen aan tafel te gaan zitten om zelf een regeling uit te werken voor deze problematiek. De NAR heeft bevoegdheid om CAO's af te sluiten die bindend zijn op nationaal vlak. De onderhandelingen hebben geleid tot de **Collectieve Arbeidsovereenkomst nr. 81** van **26 april 2002** ter **bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische online communicatiegegevens**.

De CAO definieert het controlerecht van de werkgevers op privé-e-mails en internetverkeer van de werknemers en de daaruit volgende regels op het vlak van bescherming van de persoonlijke levenssfeer van de werknemers. De CAO bepaalt duidelijk aan welke voorwaarden een controle op de elektronische online communicatiegegevens dient te voldoen en geeft aan hoe het zit met de individualisering van gegevens in het kader van de verrichte controles. De CAO heeft niet tot doel regels vast te leggen die de toegang voor de werknemers tot en het gebruik van elektronische online communicatiemiddelen regelen. Dat moet door de werkgever zelf op ondernemingsvlak worden bepaald. [114]

Controleprocedure

De werkgever kan slechts controle uitoefenen om **vier redenen**:

- om ongeoorloofde of strafbare feiten te voorkomen (bijvoorbeeld het kraken van computers) of om feiten te voorkomen die de goede zeden of de waardigheid van andere personen kunnen schaden (het raadplegen van pornografische websites of websites die aanzetten tot discriminatie);
- om de economische en financiële belangen van de onderneming te beschermen (bijvoorbeeld het doorgeven van vertrouwelijke gegevens);
- om de veiligheid van de netwerksystemen te waarborgen;
- om na te gaan of de regels voor het gebruik van e-mail en internet gerespecteerd worden.

[114] DE MUYNCK, H., *Informatica: Juridische aspecten – een overzicht*, Uitgeverij Lannoo NV, Tielt, 2004, Hoofdstuk 11: Informatica en sociaal recht, p. 131-140.

Indien de werkgever dergelijke controles wil uitvoeren, moet er eerst aan **drie voorwaarden** voldaan zijn:

- **het transparantieprincipe:** De werkgever dient zijn werknemers vooraf in te lichten over de controle (de zogenaamde informatieplicht). Een geheime controle is uitgesloten.
- **het proportionaliteitsprincipe:** De controle moet relevant en gepast zijn en mag geen inmenging in de persoonlijke levenssfeer tot gevolg hebben.
- **het finaliteitsprincipe:** De doelstellingen van de controles moeten duidelijk omschreven worden.

Het vooraf informeren van de werknemers moet **collectief** en **individueel** gebeuren. Collectief betekent dat de ondernemingsraad moet ingelicht worden over de doelstellingen van de controle, hoe en wanneer de controle zal gebeuren, welke gegevens verzameld zullen worden, waar de gegevens bewaard zullen worden, … Daarnaast moet iedere werknemer individueel ingelicht worden via bijvoorbeeld het arbeidsreglement, de arbeidsovereenkomst, e-mail of een omzendbrief. Deze inlichting omvat informatie over de doelstellingen van de controle, wat er gecontroleerd gaat worden, hoelang de controle zal duren en hoelang de gegevens bewaard zullen worden. Bovendien moeten de werknemers ingelicht worden over hun rechten, plichten en eventuele beperkingen die er op het internetgebruik rusten en de sancties die aan eventuele overtredingen gekoppeld zijn. [115]

Individualisering van de gegevens

Indien uit controles blijkt dat er onregelmatigheden gebeuren, dient de werkgever een duidelijk omschreven procedure te volgen. Wanneer ongeoorloofde of strafbare feiten vastgesteld worden of feiten die strijdig zijn met de goede zeden of die de waardigheid van andere personen kunnen schaden, of wanneer de bedrijfsbelangen geschonden worden of de veiligheid van de netwerksystemen in het gedrang komt, mag de werkgever onmiddellijk de gegevens individualiseren. Met andere woorden, de werknemer die zich schuldig heeft gemaakt aan de overtreding(en) mag geïdentificeerd worden en er moeten gepaste maatregelen getroffen worden.

Indien blijkt dat de regels voor het gebruik van e-mail en internet niet nageleefd worden, dient de werkgever een **alarmbel-procedure** te volgen. Dit betekent dat de werkgever eerst zijn werknemers inlicht dat er onregelmatigheden zijn vastgesteld en dat de controlegegevens geïndividualiseerd zullen worden als er nieuwe inbreuken worden vastgesteld. De werkgever zal op dat moment ook de voorschriften herhalen die in de onderneming gelden. Nadat er opnieuw misbruik is vastgesteld, mag de werkgever de identiteit van de betrokkene opsporen. Hierna volgt een individueel gesprek tussen de werkgever en de betrokken werknemer, eventueel bijgestaan door de vakbondsafgevaardigde. In dit gesprek krijgt de werknemer de mogelijkheid zich te verantwoorden en zijn daden te rechtvaardigen. Deze bespreking dient te gebeuren voordat er een eventuele sanctie tegen de werknemer wordt uitgesproken. [116]

[115] DE MUYNCK, H., *Informatica: Juridische aspecten – een overzicht*, Uitgeverij Lannoo NV, Tielt, 2004, Hoofdstuk 11: Informatica en sociaal recht, p. 131-140.
[116] DE MUYNCK, H., *Informatica: Juridische aspecten – een overzicht*, Uitgeverij Lannoo NV, Tielt, 2004, Hoofdstuk 11: Informatica en sociaal recht, p. 131-140.

In elk geval heeft de werkgever vanaf het moment dat het beroepsmatige karakter van de communicatie betwist wordt, nooit het recht de inhoud van de elektronische gegevens te bekijken. Dit mag enkel wanneer de werknemer (en andere betrokken partijen bij de communicatie) hiervoor uitdrukkelijk zijn toestemming geeft. [117]

7.2 Privacy van de werknemer in de praktijk

Eind 2006 werd een onderzoek gevoerd naar internetcontroles op de werkvloer bij **80 in Brussel gevestigde bedrijven**. Zowel grote (meer dan 100 werknemers) als kleine ondernemingen uit verschillende sectoren werden ondervraagd. Uit de enquêtes blijkt dat Belgische bedrijven hun werknemers daadwerkelijk controleren op het vlak van internetgebruik en e-mailverkeer. Meestal gebeuren deze controles aan de hand van spysoftware. Positief is dat hier – in tegenstelling tot in de Verenigde Staten waar controle de regel is geworden – de controles meestal pas ingaan als er fraude wordt vermoed. Twee derde van de bedrijven die controles uitvoeren, lichten het personeel in via de ondernemingsraad, aan de hand van richtlijnen of het arbeidsreglement, net zoals het in CAO nr. 81 werd voorzien. Een derde van de bedrijven is dus niet in regel. Vaak zijn dit de grotere bedrijven, die nochtans over een grotere juridische afdeling zouden moeten beschikken.

Controle blijft eigen aan de arbeidsrelatie. Een werkgever heeft het recht om zijn werknemers te controleren. Anderzijds is het logisch dat een werknemer al eens een persoonlijke e-mail verstuurt of even snel iets opzoekt op het internet. Die situatie is door werkgevers en werknemers zelf gecreëerd. Er wordt verwacht dat mensen vrijwel altijd bereikbaar zijn in hun professionele hoedanigheid, zelfs buiten de werkuren. Dan is het niet meer dan normaal dat een werknemer soms even bezig is met privéaangelegenheden op het werk. Bij 90 procent van de ondervraagde ondernemingen werd het gebruik van e-mail en internet voor privédoeleinden toegelaten, uiteraard voor zover het privégebruik de normale beroepsactiviteiten niet stoort.

Zo heeft een **Deens bedrijf** bijvoorbeeld een creatieve oplossing bedacht om tegen te gaan dat werknemers tijdens de werkuren naar pornowebsites surfen. Na het onderzoeken van trends op het internet en internetverkeer op de werkvloer besliste **LL Media** alle werknemers een gratis abonnement op pornosites te geven. Tijdens de werkuren wordt dan wel de toegang tot pornowebsites geblokkeerd. Het bedrijf verwacht dat werknemers door deze maatregel, die beschouwd wordt als een extralegaal voordeel, rustiger en efficiënter kunnen werken. [118]

Opvallend is dat 30 procent van de bedrijven al eens een werknemer moest bestraffen naar aanleiding van onaangepast gebruik van e-mail of internet. Dit onaangepast gebruik wordt anders geformuleerd in CAO nr. 81 dan in het Europees Verdrag voor de Rechten van de Mens. De CAO stelt dat alle professionele e-mails mogen gecontroleerd worden, terwijl de Europese wetgeving duidelijk oplegt dat ook professioneel e-mailverkeer onder het briefgeheim valt.

[117] DE CONINCK, M.P., *Cursus 'Bedrijfseconomische vorming' - Hoofdstuk 7: De wet op de privacy*, p. 1-13.
[118] AFTENPOSTEN, *Dane considers porn fringe benefit*, internet, http://www.aftenposten.no/english/world/article796860.ece, 2004-05-26.

Steeds vaker worden geschillen met betrekking tot onaangepast gebruik van e-mail of internet voor de rechtbank uitgevochten. In bijna ieder geval gaat het om bedrijven die onregelmatigheden vaststellen en daarop besluiten de werknemers te gaan controleren. Wanneer ze eenmaal bewijzen in handen hebben, volgt er vaak een ontslag om dringende redenen. Even vaak vechten de werknemers deze beslissing aan via de arbeidsrechtbank. Uit de praktijk blijkt dat de rechtbanken erg streng zijn als het over de procedure gaat. Vaak gaat de werknemer vrijuit omdat er niet voldaan werd aan de informatieplicht. De bewijsmiddelen die verzameld werden, worden dan niet ontvankelijk verklaard. De informatieplicht of transparantie is dus van groot belang.

Rechtbanken eisen ook dat de controleprocedure strikt gevolgd wordt, want dergelijke procedures en voorschriften regelen immers de vrijheden. Een bedrijf dat wil controleren, kan dit dus maar beter tijdig en uitgebreid communiceren naar de werknemers toe. Tegelijk kan het nuttig zijn voor bedrijven om preventief te werken door de toegang tot bepaalde websites te regelen met speciale filters. Dat is een goed compromis om internetmisbruik tegen te gaan en tegelijkertijd de privacy van de werknemers te vrijwaren. [119]

[119] POPPE, P., *Big Brother als collega: Mag je werkgever je controleren?*, Jobat, 2007-03-31, p. 16-17.

8 De praktijk nader onderzocht

8.1 Spam-test

Om spam te vermijden, worden altijd dezelfde tips gegeven (laat nergens je e-mailadres achter, beantwoord nooit spam, schrijf je niet in op onbetrouwbare websites, …). In deze test ging ik na of het werkelijk zo 'gemakkelijk' is om spam te krijgen, en ging ik net het tegenovergestelde doen van de tips. Verder bekeek ik welke soorten spam er zoal toekwamen. De test liep gedurende een maand en startte op 30 maart 2007.

Peter Jansens werd mijn online undercover persoonlijkheid. Het e-mailadres peterjansens001@hotmail.com werd het adres waar ik spam naartoe ging proberen te lokken. In naam van Peter ging ik verschillende gastenboeken ondertekenen met het bewuste e-mailadres. Ik nam met dit e-mailadres ook deel aan enkele wedstrijden en schreef Peter in op enkele nieuwsbrieven. Daarnaast plaatste ik een zoekertje op een datingsite. Overal waar ik een e-mailadres kon achterlaten, postte ik Peters e-mailadres.

Om nog meer spam te lokken, antwoordde ik op de meeste ongewenste e-mails die toekwamen in Peters mailbox. In Hotmail wordt trouwens een melding weergegeven wanneer je wil antwoorden op spam.

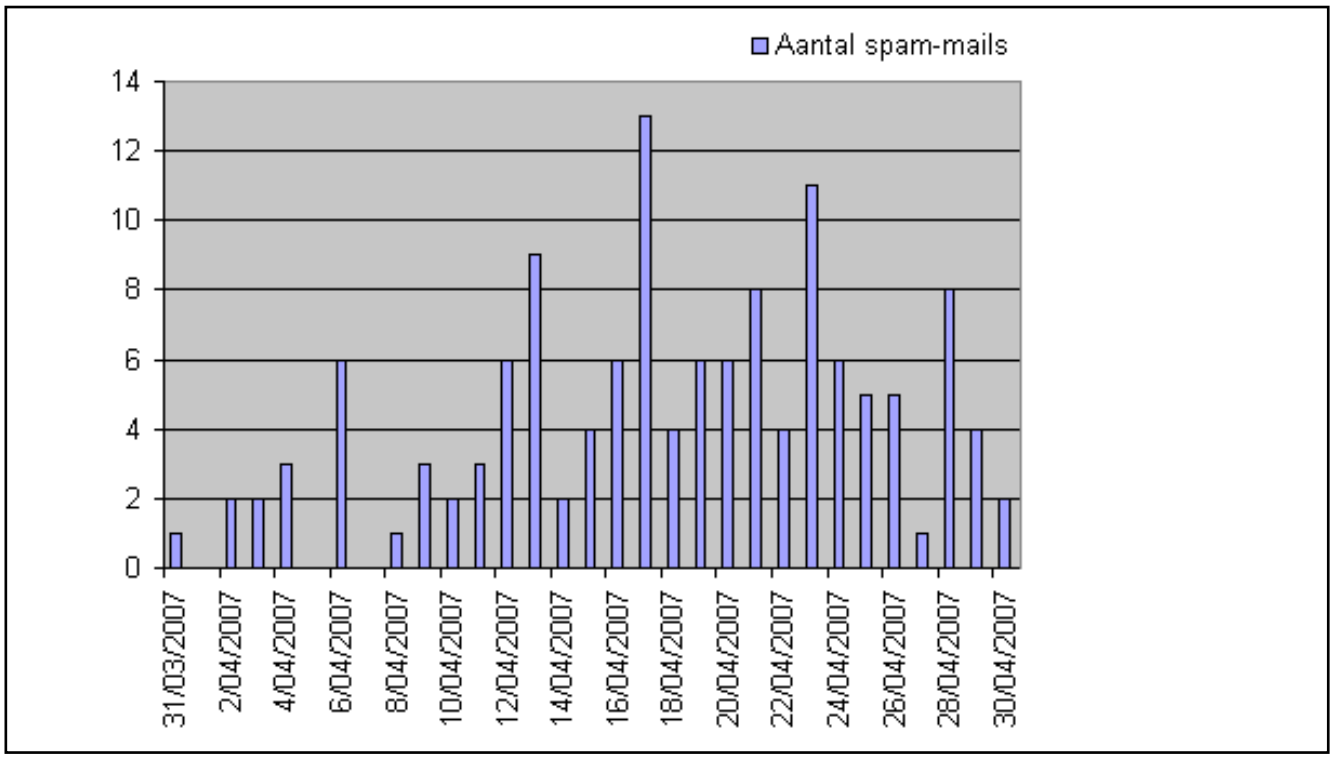
> *"Belangrijk: als je om de een of andere reden op ongewenste e-mail reageert, bevestig je dat je e-mailadres bestaat en is de kans groter dat je meer ongewenste e-mail krijgt in plaats van minder. Klik op de knop Annuleren om ervoor te zorgen dat dit bericht niet wordt verzonden."*

Vriendelijk van hen om me te waarschuwen. Aangezien ik de bedoeling had Peters mailbox bloot te stellen aan spam, sloeg ik deze goede raad van Hotmail dus in de wind. Wanneer er verder de mogelijkheid geboden werd uit te schrijven (unsubscribe), deed ik dat. Het is namelijk bekend dat door te unsubscriben, je jezelf meestal net inschrijft voor andere zaken.

Wat ook grappig is, is dat in bepaalde spam-mails wordt verwezen naar een website, waar spam vervolgens gerapporteerd kan worden (zie bijlage XV).

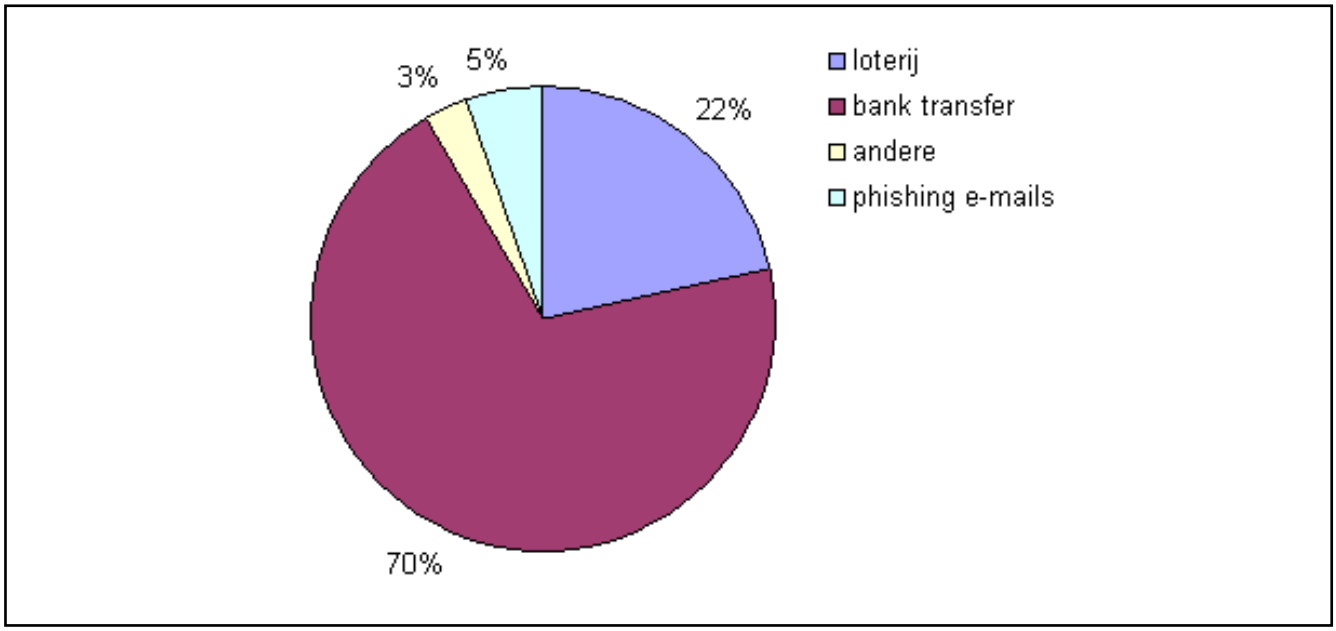
Peterjansens002@hotmail.com werd gebruikt als controleadres om te kijken of hier dezelfde spam-mails zouden toekomen. Dit e-mailadres werd nergens achtergelaten.

De resultaten hield ik bij in een excel-document.



Afb. 16: Grafiek die het aantal spam-mails toont per dag

Uit deze grafiek blijkt dat 17 en 23 april de meest succesvolle spam-dagen waren. Dit waren respectievelijk een dinsdag en een maandag. De dagen vlak na het weekend blijken meestal het populairst om spam-mails te verzenden. De algemene tendens die blijkt uit deze grafiek is dat het aantal spam-mails meestal oploopt naarmate het piekmoment nadert, zijnde net na het weekend. Dit lijkt logisch, aangezien de meeste spam verstuurd wordt naar professionele e-mailadressen en niet naar privé-emailadressen. Mensen checken meestal hun professioneel e-mailadres niet tijdens het weekend, maar wel tijdens de week, of dat is toch de redenering die spam-bedrijven blijkbaar volgen.



Afb. 17: Grafiek die het aantal spam-mails per onderwerp weergeeft

Uit deze grafiek blijkt dat de meeste spam die ik ontving, aanbiedingen waren waarbij ik ofwel een bepaalde banktransfer moet doen in ruil voor (zogezegd) een percentage van dat bedrag, ofwel zomaar

een bepaald bedrag geschonken kreeg. Het addertje onder het gras is hier dat degene die de e-mails ontvangt, meestal zelf eerst een bedrag moet storten aan de verzenders van de e-mail alvorens de zogezegde transactie kan gebeuren.

Verder kreeg ik ook een aantal spam-mails die me kwamen melden dat ik een bepaald bedrag had gewonnen met een of andere loterij. In dezelfde periode kreeg ik ook enkele phishing-mails die mijn gegevens probeerden te achterhalen door te beweren dat bijvoorbeeld mijn Paypal-account dringend vernieuwd moest worden.

De categorie 'andere' bevatte bijvoorbeeld een anonieme e-card die verwees naar een bepaald programma op een verdachte website of een onfrisse business proposal.

Het controleadres ontving in dezelfde periode geen enkele spam-mail.

8.2 Zoektocht naar persoonsgegevens op het internet

Om te achterhalen welke persoonlijke gegevens er over een persoon zoal te vinden zijn op het internet, besloot ik een test te doen. Bij wijze van test heb ik enkele namen van personen ingegeven in enkele zoekmachines om te onderzoeken wat ik zo allemaal over die personen te weten kon komen. Uiteraard heb ik de proefpersonen eerst om hun toestemming gevraagd.

Mijn interne promotor, **de heer Philippe De Pauw - Waterschoot**, werd mijn eerste proefpersoon. Zijn foto en e-mailadres staan zowat bovenaan in de zoekresultaten van Google. Dat hij webmaster/programmeur is op de campus Hoogpoort en campus Mariakerke van de Arteveldehogeschool wist ik natuurlijk al, maar blijkt ook uit de zoekresultaten.

Via zijn profiel op ArtWanted.com kom ik te weten dat hij artistieke ambities koestert. Daar bevinden zich vijf creaties van hem, getiteld 'Heads collisions', 'Landscape', 'Sadness', 'Surrounded Eye' en 'Portrait of a survivor'. Via dit profiel vond ik de link naar zijn persoonlijke blog. Hierop luidt zijn voorstelling als volgt:

> "I am a guy, 29 years old living in Belgium. A litlle country between Holland, Germany, and France. … I have a house in Ghent, the capital city of flanders. I am a teacher, programmer and web designer (mostly programming). I try to do the following things in my spare time: web designing, walking, drawing, cycling, be active also lazy, watching movies, surfing the net, playing with my cat Rocky and try to please my girlfriend :)."

Sinds 2005 werd deze website echter niet meer vernieuwd.

Samen met Patrick De Causmaecker, Peter Demeester en Greet Vanden Berghe organiseerde Philippe De Pauw - Waterschoot een tweede symposium over 'agent technology' en hield daar samen met hen een bespreking over 'agent assistance in lab session planning'.

Verder bestaat er blijkbaar ook een Philippe De Pauw's Website. Op deze website die blijkbaar meer recente informatie bevat, bevindt zich deze blogpost van 13 januari 2007:

> "Today was a busy day, not for renovating my home, i did nothing because we had to visit my girlfriend's family. A gathering in memory of my girlfriend's aunt. All her family members gathered at a church in west-flanders. After a christian service we visited the home of the deseased where we ate sandwiche with hot-dogs, cheese and other things. It tasted great, my stomach filled with tastefull desires.
>
> After chatting a bit, I went back to my home in Ghent, my home-city. Arrived there, my cats were welcomed me, miaaaaauw. The one cat, called Frodo, a male red cat with white stripes. He is 2 years old, with half-long hair. He is not so jumping type, more keep it calm, but now he founds his way to the toop floor getting outside through a window. Now he is so fier because he is climbing roofs but at his pace. The other cat, a male cat called Rocky is now 5 years old. He is black with white spots, he is very active sometimes jumping around, climbing roofs and trees. But at the winter, he sleeps like an angel, almost 18 hours a day. He gives great head-to-heads and spins like a king."

De heer Gys Godderis, mijn externe promotor, was mijn tweede proefpersoon. Verwijzingen naar de website van PolarisNation en zijn e-mailadres zijn zowat overal terug te vinden. Op PolarisNation stond hij in voor de productie en coördinatie.

Op LinkedIn.com heeft hij een profiel waar volgende zaken op te lezen zijn:

> "Gys Godderis, POLARIS Creative Solutions and Events Services Consultant, Belgium
>
> Developer, graphic & webdesigner, allround media designer and Project Manager in a wide variety of business and cultural events/applications. Particularly interested in full-project development, from print 2 event.
>
> Experiences: Blue Note, Festivals, Coca Cola events, Music Awards, Barco 3d modelling, Concert managing, ... Just ask, we'll provide a creative solution !
>
> **Current**
>
> - creative consultant at POLARIS Creative Solution
> - partner / creative consultant Accor Group Europe at Accor Group
> - Owner at POLARIS Creative Backline (Self-employed)
>
> **Past**
>
> - Blue Note Festival at Jasrecords

Education

- Hogeschool voor Wetenschap & Kunst: master, graphic design, 1996-2000
- Katholieke Hogeschool Leuven: master, art
- University of Toronto: post degree, 3d animation and special effects

Industry

Marketing and Advertising"

Gys Godderis zat ook in het stuurcomité van Message in a bottle, een sensibiliseringscampagne van 2005 waarbij de Atlantische Oceaan overgestoken werd in een boot in de vorm van een gigantische fles. Met deze boot werden dan allemaal brieven of messages meegegeven die de aandacht op de levensomstandigheden van de kinderen in de arme landen moet vestigen.

Gys zat ook in het stuurcomité van Humane Connection, een Belgische onafhankelijke organisatie die toegevoegde waarde wil brengen bij ontwikkelingswerk in het Zuiden.

Via Google vond ik ook nog het profiel van Gys op Flickr.com, onder de naam Allure_me_jazz. Hierop staan 118 foto's onderverdeeld in drie albums: artzzz, family en nokia pics.

Uit deze twee voorbeelden kan al blijken dat er heel wat persoonlijk informatie te vinden is op het internet, als je er wat zoekwerk voor over hebt.

Besluit

Uit dit eindwerk blijkt dat privacy een relatief begrip is dat door iedereen een andere invulling kan krijgen. De risico's met betrekking tot privacy die opgesomd werden, kunnen opgedeeld worden in twee groepen. Enerzijds is er de persoonlijke informatie die door de persoon in kwestie zelf op het internet verspreid wordt en waar de gebruiker zich dus bewust van is. Anderzijds is er de informatie die door derden verzameld wordt over een persoon, waar de gebruiker zelf weinig controle over heeft en waar hij zich meestal niet bewust van is.

Wat de eerste categorie betreft, hangt veel af van de eigen interpretatie van privacy. Dit blijkt ook uit de praktijktest waarbij ik persoonlijke gegevens heb gezocht van mijn interne en externe promotor. In hun beroep is het onoverkomelijk en soms zelfs noodzakelijk traceerbaar te zijn op het internet. Als zij op een andere manier hadden omgesprongen met hun persoonlijke gegevens, was het waarschijnlijk moeilijker geweest hen op te sporen. Hieruit kunnen we de optimale strategie afleiden die je als internetgebruiker kunt toepassen om je eigen privacy op het internet te beschermen: stel jezelf de vraag of je wil dat anderen die informatie over jou weten. Uiteindelijk moet het je eigen keuze zijn wat je wil prijsgeven en wat niet. De wetgeving is er om ervoor te zorgen dat anderen hier geen misbruik van maken.

In het tweede geval kunnen de sporen van een internetgebruiker gevolgd worden. De gevolgen van een gebrekkige bescherming van de eigen privacy, kunnen zowel onschuldig (gerichte advertenties) als schadelijk (spyware) tot zelfs gevaarlijk (stalking) zijn. Zoals blijkt uit het hoofdstuk met tips & tricks bestaan er hier voldoende oplossingen voor, zowel betalend als gratis. Sommige oplossingen hebben echter ook een keerzijde, dus is het weer aan de internetgebruiker zelf om te beslissen hoe ver hij wil gaan in het beschermen van zijn privacy. De internetgebruiker moet uiteindelijk zelf de gulden middenweg vinden die zijn privacy het best beschermt.

De optimale strategie voor de internetgebruiker om zijn privacy te beschermen bestaat dus uit een heleboel tips & tricks die naar believen kunnen toegepast worden, aangevuld met een portie gezond verstand.

Daarnaast spelen de wetgeving en het beleid van internetproviders ook een belangrijke rol bij het beschermen van de privacy van de internetgebruiker, tenzij deze strafbare daden stelt. Ook voor de werksituatie is er een wet ontwikkeld die ervoor zorgt dat de werkgever zijn werknemers niet zonder voorafgaande duidelijke informatie mag controleren.

"On the Internet, nobody knows you're a dog." - Peter Steiner, in the New Yorker, 1993-07-05.

Deze cartoon vat mooi de belangrijkste richtlijn van dit eindwerk samen. Iedereen kan eender wat over zichzelf verzinnen op het internet, niemand hoeft te weten wie je werkelijk bent. Als je deze regel in je achterhoofd houdt, zul je minder snel geneigd zijn zelf persoonlijke informatie prijs te geven op het internet. Uiteindelijk beslis je zelf als enige welke gegevens over jou op het internet verschijnen, of zo zou het toch moeten zijn.

LITERATUURLIJST

BOEKEN

• DE MUYNCK, H., Informatica: Juridische aspecten – een overzicht, Uitgeverij Lannoo NV, Tielt, 2004, 148 pagina's.
• VAN KOOTEN, L., PC Beveiligd (vertaling), Uitgeverij Sybex BV, Soest, 2000, 242 pagina's.

CURSUS

• DE CONINCK, M.P., Cursus 'Bedrijfseconomische vorming' - Hoofdstuk 7: De wet op de privacy, p. 1-13.

ARTIKELS

• DECAESTECKER, B., Eurocommissaris valt over muziekmonopolie Apple, De Morgen, 2007-03-13.
• DECAESTECKER, B., Joost mag weten hoe de toekomst van tv eruitziet, De Morgen, 2007-04-06.
• MEEUS, R., Amerikaanse overheid eist gegevens van Google op, De Morgen, 2006-01-20.
• MEEUS, R., iTunesmuziek van EMI onbeveiligd maar duurder, De Morgen, 2007-04-03.
• POPPE, P., Big Brother als collega: Mag je werkgever je controleren?, Jobat, 2007-03-31, p. 16-17.

WEBSITES

• ACCELERATED GLOBAL, Anti-Terrorism Technology: Carnivore Surveillance System, internet, http://accelerated-promotions.com/consumer-electronics/usa-patriot-act-carnivore.htm, 2007-04-19.
• AFTENPOSTEN, Dane considers porn fringe benefit, internet, http://www.aftenposten.no/english/world/article796860.ece, 2004-05-26.
• AUSTRALIAN GOVERNMENT – OFFICE OF THE PRIVACY COMMISSIONER, Protecting your privacy on the Internet, internet, http://www.privacy.gov.au/internet/internet_privacy/, 2007-03-30.
• BELGACOM, Online Privacy Policy, internet, http://www.belgacom.be/home/gallery/content/e-services/conditions/nl/privacy.pdf, 2007-04-16.
• BLINFOWEB, Email encoder, internet, http://www.blinfotec.org/tools/emailencoder.html, 2007-04-07.
• CAMPUS TU DELFT, Cryptografie en digitale handtekeningen, internet, http://campus.tudelft.nl/live/pagina.jsp?id=5198149a-657f-495f-a658-a58a67d2cc4d&lang=nl, 2007-04-09.
• COMPUTERTAAL, Wat is DRM?, internet, http://www.computertaal.info/modules/articles/article.php?id=680, 2006-10-06.
• CONBA, Zoekmachines: hoe werken ze?, internet, http://www.conba.be/showunieuws.asp?archief=1&language=NL&IDnr=1248, 2006-09-25.
• CYBERPATROL, Oplossingen voor ouderlijk internettoezicht van CyberPatrol, internet, http://

www.cyberpatrol.com/Software_voor_ouderlijk_internettoezicht.htm, 2007-04-06.
• DE DIGITALE REVOLUTIE, Echelon en het versleutelen van mail, internet, http://www.dedigitale-revolutie.tv/toontext.asp?id=9749, 2007-04-09.
• DE DIGITALE REVOLUTIE, Ouderlijke controle (parental control) in Vista, internet, http://www.dedigitalerevolutie.tv/toontext.asp?id=17982, 2007-04-06.
• DE TELEGRAAF, Ixquick schakelt 'Big Brother' uit, internet, http://www.telegraaf.nl/i-mail/45395771/Ixquick_schakelt_%18Big_Brother%19_uit.html, 2006-06-27.
• DOWNLOAD FREEWARE, Ccleaner, internet, http://www.downloadfreeware.nl/ccleaner.php, 2007-04-03.
• E-PRIVACY, Soft opt-in regime in België, internet, http://www.e-privacy.be/dossier.html, 2007-03-28.
• EJURE, Phishingmail richt zich op Nederlandse PayPalklanten, internet, http://www.ejure.nl/f_dossier/dossier_id=171/news_id=3734/news.html, 2006-12-13.
• FEDICT – FOD INFORMATIE- EN COMMUNICATIETECHNOLOGIE, Over eID, internet, http://eid.belgium.be/nl/navigation/12000/index.html, 2007-04-20.
• FEDICT, Meer weten over eID en veiligheid op je pc?, internet, http://www.s-days.be, nog niet bereikbaar.
• FOD ECONOMIE KMO MIDDENSTAND EN ENERGIE, Aanbevelingen inzake de aansprakelijkheid van de internetprovider, internet, http://mineco.fgov.be/information_society/enterprises/providers_internetguide/Providers1_nl-03.htm#P283_34529, 2007-04-16.
• GELE DRAAK, Internetcensuur in China, internet, http://www.geledraak.nl/html/showarticle.asp?id=539, 2007-04-18.
• GOOGLE ANALYTICS, Nieuw: Google Analytics, geavanceerd, eenvoudig, gratis, internet, http://www.google.com/analytics/nl-NL/index.html, 2007-03-29.
• GRATIS SOFTWARE SITE, Beschrijving AVG Anti-Virus Free, internet, http://www.gratissoftware-site.nl/avg.html, 2007-04-04.
• HCCNET, Anoniem surfen, internet, http://home.hccnet.nl/t.amerongen/Anonymizers.htm, 2007-04-02.
• HET COMPUTERVIRUS, Antivirusprogramma, internet, http://www.wobotje.com/computervirus/bescherming_programma.htm, 2007-04-04.
• ICRI - INTERDISCIPLINARY CENTRE FOR LAW & ICT, Privacy, internet, http://www.law.kuleuven.ac.be/icri/david/E_Privacy.php, 2004-06-01.
• INFOTALIA, Bescherm uw e-mailadres tegen spam!, internet, http://www.infotalia.be/nl/ict/internet_detail.asp?id=102, 2007-04-07.
• INFO NU, Softwarelicenties, internet, http://pc-en-internet.infonu.nl/software/850-softwarelicenties.html, 2007-04-14.
• INFORMATION SECURITY, White Hat/Black Hat Hackers, internet, http://www.yourwindow.to/information-security/gl_whitehatblackhathackers.htm, 2007-04-22.
• INTERNETJOURNALISTIEK, Dossier: Privacy op het web, internet, http://www.internetjournalistiek.be/dossiers/privacy.php, 2007-04-10.
• IUS MENTIS, Het kiezen van een software licentie, internet, http://www.iusmentis.com/computerprogrammas/licenties/kiezen/, 2007-04-14.
• IXQUICK, Ixquick beschermt uw privacy!, internet, http://eu.ixquick.com/ned/protect_privacy.html, 2007-03-19.
• JAWWI, Cookies, internet, http://www.jawwi.nl/malware/cookies.html, 2007-03-26.
• KAWAMOTO, D. en MILLS, E., AOL apologizes for release of user search data, internet, http://

news.com.com/AOL+apologizes+for+release+of+user+search+data/2100-1030_3-6102793.html, 2006-08-07.
• LAVASOFT, Ad-Aware SE Personal, internet, http://www.lavasoftusa.com/products/ad-aware_se_personal.php, 2007-04-03.
• LUDIT – LEUVENS UNIVERSITAIR DIENSTENCENTRUM VOOR INFORMATICA EN TELEMATICA, Hou je computer veilig, internet, http://ludit.kuleuven.be/software/beveiliging/, 2007-04-04.
• MCAFEE, McAfee VirusScan Plus: Essentiële pc-beveiliging, internet, http://nl.mcafee.com/root/package.asp?pkgid=276, 2007-04-04.
• MCCULLAGH, D., FAQ : Protecting yourself from search engines, internet, http://news.com.com/FAQ+Protecting+yourself+from+search+engines/2100-1025_3-6103486.html, 2006-08-08.
• MICROSOFT, Legitieme Microsoft-software, internet, http://www.microsoft.com/genuine/Facts.aspx?displaylang=nl, 2007-04-14.
• MICROSOFT, Voordelen en risico's van het delen van bestanden via een peer-to-peer-netwerk, internet, http://www.microsoft.com/belux/nl/athome/security/online/p2p_file_sharing.mspx, 2005-07-06.
• MIJN HOMEPAGE, Je emailadres coderen, internet, http://www.mijnhomepage.nl/artikelen/wd/emailadres-coderen.php, 2007-04-07.
• MJK DISC, Auteursrecht, internet, http://www.kopieer-cd.be/sabam/auteursrecht.jsp, 2007-04-14.
• MOZILLA, Firefox Add-ons: Adblock Plus, internet, https://addons.mozilla.org/en-US/firefox/addon/1865, 2007-04-01.
• NIBURU, Google-baas ontdekt nadeel van zoekmachine, internet, http://www.niburu.nl/index.php?showarticle.php?articleID=9203, 2005-09-20.
• OPERA, Security, internet, http://www.opera.com/products/desktop/security/, 2007-04-22.
• PAYPAL, De eenvoudige snelle veilige manier om te betalen, internet, http://www.paypal.nl/nl, 2007-04-02.
• PERSONAL COMPUTER MAGAZINE, Google gaat akkoord met Chinese censuur, internet, http://www.pcmweb.nl/nieuws.jsp?id=1093324, 2007-04-18.
• PGPI, The International PGP Home Page, internet, http://www.pgpi.org/, 2007-04-09.
• PISA – PROVIDING INFORMATION ABOUT INTERNET SECURITY ASPECTS, Wetgeving: Inbraak, internet, http://pisa.belnet.be/pisa/nl/juridisch/crack.htm, 2007-04-14.
• PLANET INTERNET, Amerika twee jaar later, internet, http://www.planet.nl/planet/show/id=67777/contentid=399682/sc=ebc27c, 2003-09-11.
• PLANET INTERNET, Firefox 2 onder de loep, internet, http://www.planet.nl/planet/show/id=74274/contentid=790387/sc=92e365, 2006-12-23.
• PROXIFY, Anonymous Proxy protects your online privacy, internet, http://proxify.com/, 2007-04-02.
• RENSE, The list of Carnivore and Echelon keywords, internet, http://www.rense.com/general66/scgh.htm, 2007-04-19.
• ROBINSONLIST, Hoe werkt de Robinson-lijst?, internet, http://www.robinsonlist.be/, 2007-04-07.
• SCARLET, Wettelijke vermeldingen en voorwaarden, internet, http://www.scarlet.be/nl/legal/, 2007-04-16.
• SCHOFIELD, J., Has the time finally come to stop using Google?, internet, http://technology.guardian.co.uk/weekly/story/0,,1851363,00.html, 2006-08-17.
• SOCIOSITE, CyberStalking: belaagd op het internet, internet, http://www.sociosite.org/cyberstalking.php, 2006-05-04.
• SOUFFREAU, B., Providers houden jaar lang surfgegevens bij, internet, http://www.internetjournalistiek.be/dossiers/detail_privacy.php?nieuwsid=93, 2003-12-07.

• SPAMSQUAD, De Belgische portaalsite in de strijd tegen spam, internet, http://www.spamsquad.be/nl/home.html, 2007-04-04.
• SPAM.LA, Fight spam, use an anonymous @spam.la address!, internet, http://www.spam.la/, 2007-04-07.
• SPYBOT – SEARCH & DESTROY, Overzicht, internet, http://www.safer-networking.org/nl/spybotsd/index.html, 2007-04-03.
• SURFNET, Virussen bestrijden, internet, http://www.surfkit.nl/info/beveiliging/virussen_bestrijden.jsp, 2007-04-04.
• SYMANTEC, Norton AntiVirus 2007, internet, http://www.symantec.com/home_homeoffice/products/overview.jsp?pcid=is&pvid=nav2007, 2007-04-04.
• TAALTELEFOON, Identiteitsdiefstal, internet, http://www.vlaanderen.be/servlet/Satellite?cid=1126670405504&pagename=taaltelefoon%2FPage%2FArticle&c=Page, 2002-12-16.
• TELENET, Algemene voorwaarden Telenet Internet, internet, http://www.telenet.be/nl/online-support/thuis/algemenevoorwaarden/algvw_internet.page, 2007-04-16.
• THE CLOAK, Free anonymous web surfing, internet, http://www.the-cloak.com/anonymous-surfing-home.html, 2007-04-02.
• TWEAKERS.NET, China's grote vuurmuur nader bekeken, internet, http://tweakers.net/nieuws/40666, 2007-04-18.
• OBSERVATORIUM VAN DE RECHTEN OP HET INTERNET, Juridisch kader: wetgeving, Privacy en andere fundamentele vrijheden, internet, http://www.internet-observatory.be/internet_observatory/home_nl.htm, 2007-04-14.
• ORANGE, Parental Control: Bescherm je kinderen, internet, http://www.orange.nl/overige_produkten/veiligheid/parental_control/, 2007-04-06.
• VISTERIN, W., Onvindbaar blijven op het net, internet, http://www.optiseo.be/onvindbaarophetnet.htm, 2005-11-29.
• WEBWERELD, ABN AMRO waarschuwt voor phishing e-mail, internet, http://www.webwereld.nl/articles/45591/abn-amro-waarschuwt-voor-phishing-e-mail.html, 2007-03-21.
• WEBWERELD, Dreiging identiteitsdiefstal met 200 procent toegenomen, internet, http://www.webwereld.nl/ref/rss/45705, 2007-03-28.
• WIKIPEDIA, internet, http://nl.wikipedia.org/wiki/Hoofdpagina, 2007-04-28.
• WIZZBIT, Wat zijn webstatistieken?, internet, http://www.wizzbit.nl/index.php?id=34, 2007-03-29.
• XS4ALL, Veilig internetten, internet, http://www.xs4all.nl/veiligheid/, 2007-04-08.
• ZDNET, Parental Control Bar 4.0.3: Uw oogappels kunnen veilig surfen, internet, http://www.zdnet.nl/downloads.cfm?id=64284, 2007-04-06.
• ZO WERKT, Webstatistieken: overige, internet, http://www.zowerkt.nl/internet/web/webstatistieken_overige.html, 2007-03-29.

BIJLAGEN

Bijlage I: Phishing website van PayPal

Bijlage II: De echte website van PayPal

Bijlage III: Google Analytics

Bijlage IV: Resultaat bij opzoeken van Arteveldehs.be via Proxify.com

Bijlage V: Proxify.com - Een anonieme proxyservice

Bijlage VI: Resultaat bij opzoeken van Arteveldehs.be via The-Cloak.com

Bijlage VII: Aanvullende software - Ccleaner

Bijlage VIII: Aanvullende software - Spybot Search & Destroy

Bijlage IX: Aanvullende software - Ad-Aware SE Personal

Bijlage X: Virusscanner - AVG Free Edition

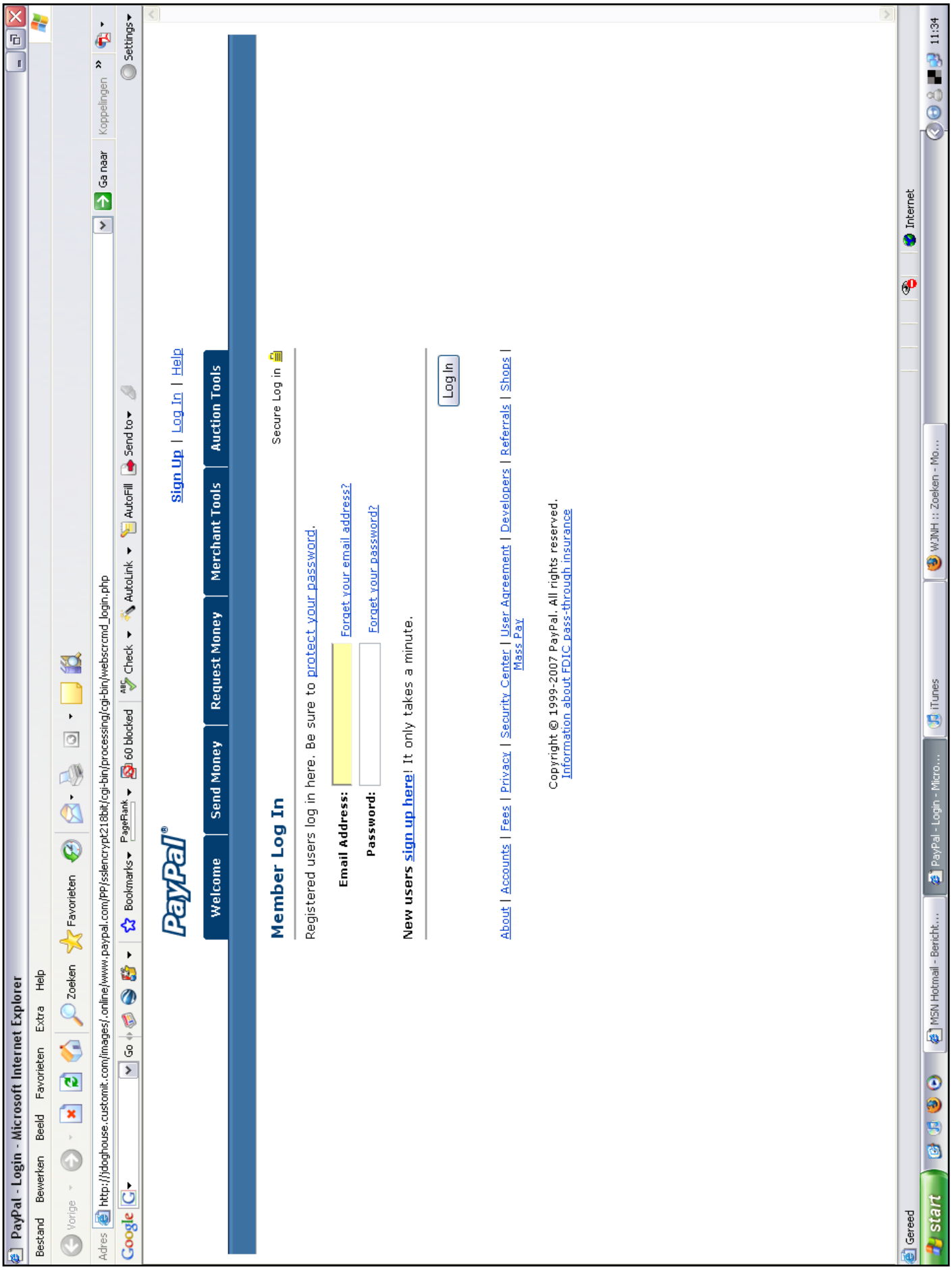
Bijlage XI: Parental Control in Windows Vista

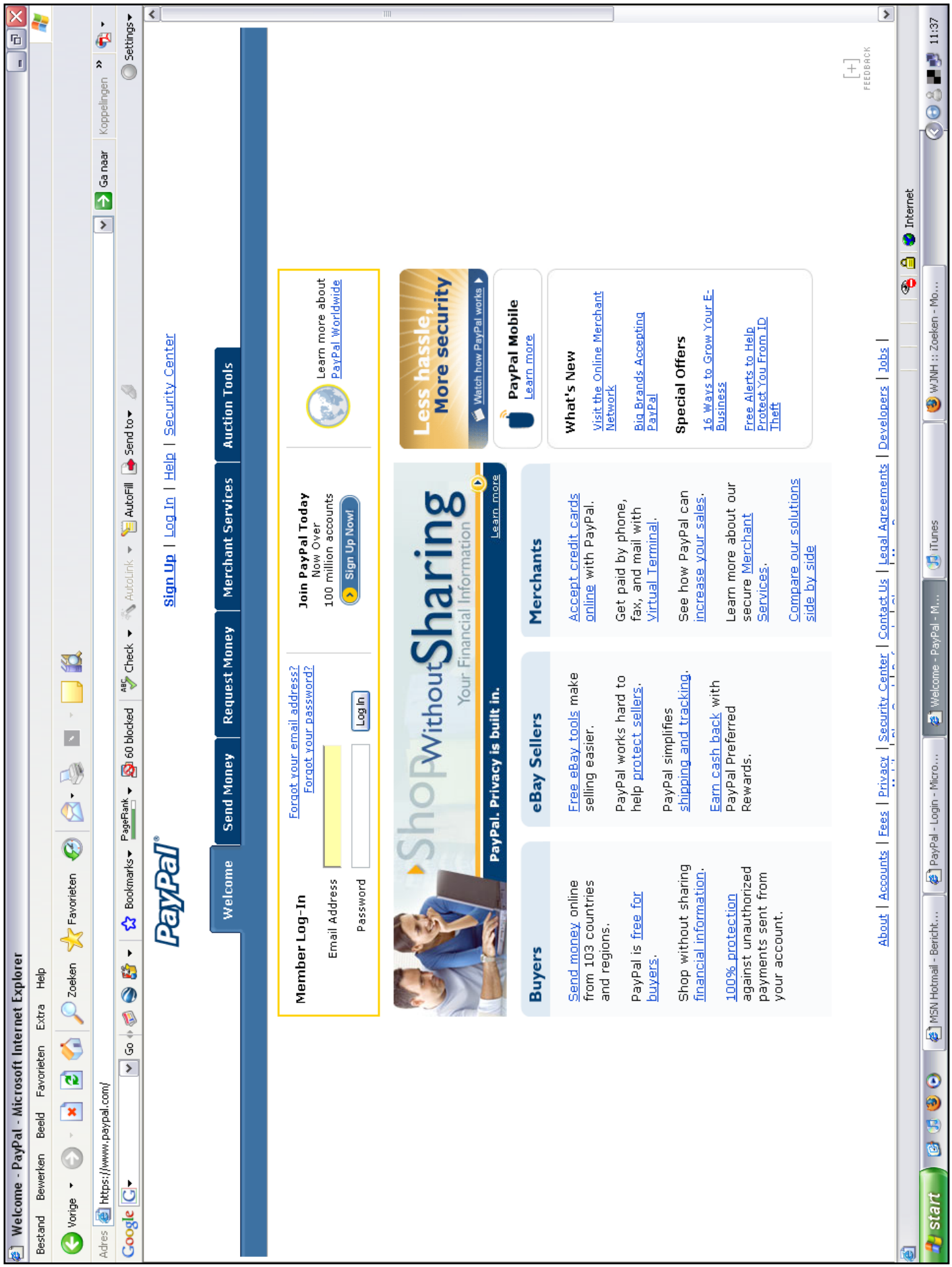
Bijlage XII: Het privacybeleid van eBay

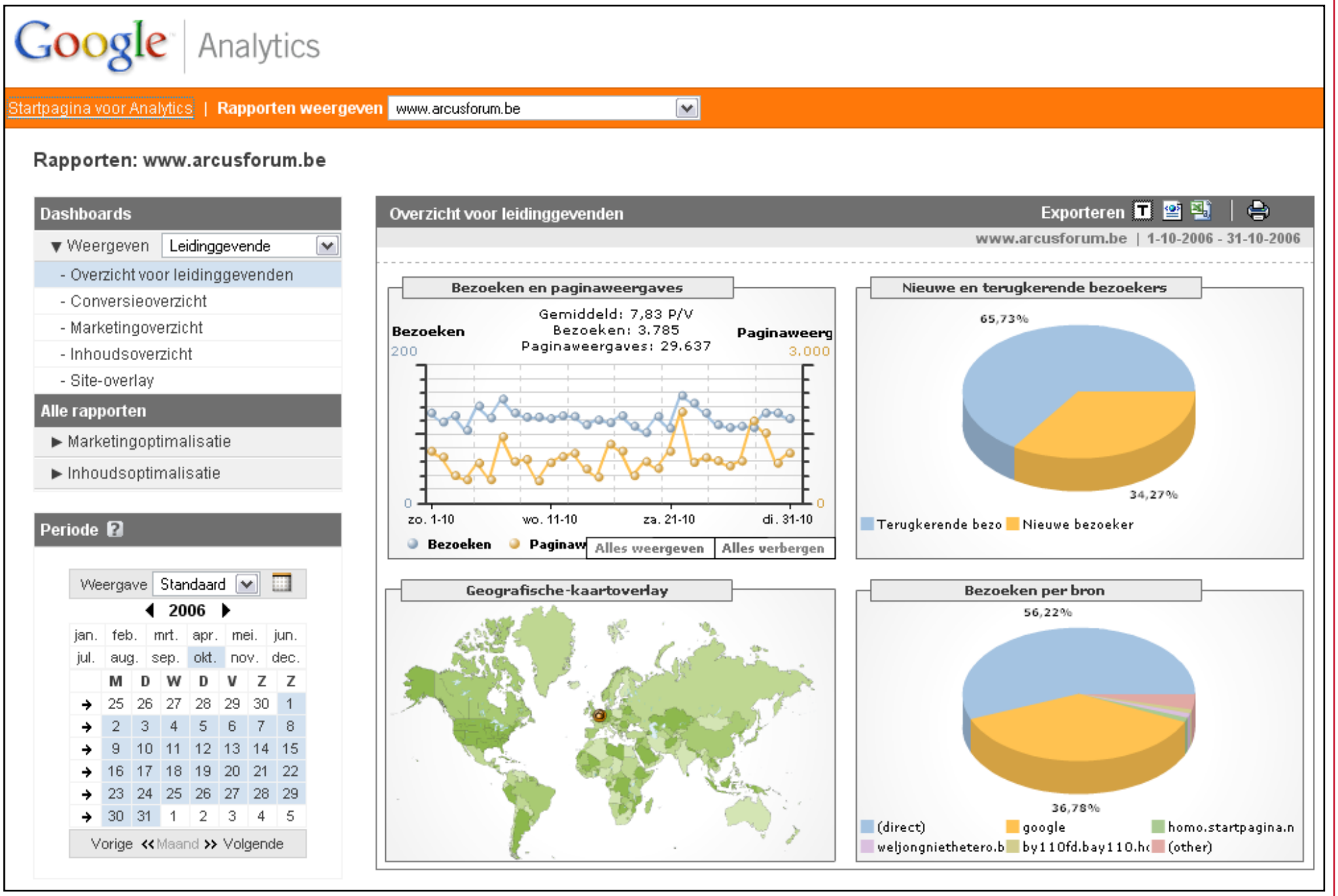
Bijlage XIII: Het privacybeleid van Telenet

Bijlage XIV: De privacystempel van TRUSTe op GettyImages.com

Bijlage XV: De mogelijkheid om spam te rapporteren


PayPal - Login - Microsoft Internet Explorer
Bestand Bewerken Beeld Favorieten Extra Help
Vorige Zoeken Favorieten
Adres http://jdoghouse.customit.com/images/.online/www.paypal.com/PP/sslencrypt218bit/cgi-bin/processing/cgi-bin/webscrcmd_login.php
Ga naar Koppelingen
Google Go Bookmarks PageRank 60 blocked Check AutoLink AutoFill Send to Settings
PayPal
Sign Up | Log In | Help
Welcome
Send Money
Request Money
Merchant Tools
Auction Tools
Member Log In
Secure Log in
Registered users log in here. Be sure to protect your password.
Email Address:
Forget your email address?
Password:
Forget your password?
New users sign up here! It only takes a minute.
Log In
About | Accounts | Fees | Privacy | Security Center | User Agreement | Developers | Referrals | Shops | Mass Pay
Copyright © 1999-2007 PayPal. All rights reserved.
Information about FDIC pass-through insurance
Gereed
Internet
start
MSN Hotmail - Bericht...
PayPal - Login - Micro...
iTunes
WINH :: Zoeken - Mo...
11:34


Welcome - PayPal - Microsoft Internet Explorer
PayPal
Welcome
Send Money
Request Money
Merchant Services
Auction Tools
Sign Up | Log In | Help | Security Center
Member Log-In
Email Address
Password
Log In
Forgot your email address?
Forgot your password?
Join PayPal Today
Now Over
100 million accounts
Sign Up Now!
Learn more about
PayPal Worldwide
ShopWithoutSharing
Your Financial Information
PayPal. Privacy is built in.
Learn more
Less hassle,
More security
Watch how PayPal works
PayPal Mobile
Learn more
What's New
Visit the Online Merchant Network
Big Brands Accepting PayPal
Special Offers
16 Ways to Grow Your E-Business
Free Alerts to Help Protect You From ID Theft
Buyers
Send money online from 103 countries and regions.
PayPal is free for buyers.
Shop without sharing financial information.
100% protection against unauthorized payments sent from your account.
eBay Sellers
Free eBay tools make selling easier.
PayPal works hard to help protect sellers.
PayPal simplifies shipping and tracking.
Earn cash back with PayPal Preferred Rewards.
Merchants
Accept credit cards online with PayPal.
Get paid by phone, fax, and mail with Virtual Terminal.
See how PayPal can increase your sales.
Learn more about our secure Merchant Services.
Compare our solutions side by side
About | Accounts | Fees | Privacy | Security Center | Contact Us | Legal Agreements | Developers | Jobs |
FEEDBACK


Google Analytics
Startpagina voor Analytics | Rapporten weergeven www.arcusforum.be
Rapporten: www.arcusforum.be
Dashboards
▼ Weergeven Leidinggevende
- Overzicht voor leidinggevenden
- Conversieoverzicht
- Marketingoverzicht
- Inhoudsoverzicht
- Site-overlay
Alle rapporten
▶ Marketingoptimalisatie
▶ Inhoudsoptimalisatie
Periode
Weergave Standaard
2006
jan. feb. mrt. apr. mei. jun.
jul. aug. sep. okt. nov. dec.
M D W D V Z Z
25 26 27 28 29 30 1
2 3 4 5 6 7 8
9 10 11 12 13 14 15
16 17 18 19 20 21 22
23 24 25 26 27 28 29
30 31 1 2 3 4 5
Vorige << Maand >> Volgende
Overzicht voor leidinggevenden
Exporteren
www.arcusforum.be | 1-10-2006 - 31-10-2006
Bezoeken en paginaweergaves
Gemiddeld: 7,83 P/V
Bezoeken: 3.785
Paginaweergaves: 29.637
Bezoeken
Paginaweerg
200
3.000
0
0
zo. 1-10
wo. 11-10
za. 21-10
di. 31-10
Bezoeken
Paginaw
Alles weergeven
Alles verbergen
Nieuwe en terugkerende bezoekers
65,73%
34,27%
Terugkerende bezo
Nieuwe bezoeker
Geografische-kaartoverlay
Bezoeken per bron
56,22%
36,78%
(direct)
google
homo.startpagina.n
weljongniethetero.b
by110fd.bay110.hc
(other)

Artevelde hogeschool

English | Vacatures | Contact | Zoeken

Algemene info

- Arteveldehogeschool
- Opleidingsaanbod
- ECTS
- Flexibel studeren
- Kansrijk studeren
- Infomomenten
- Inschrijven
- Gent studentenstad
- Arteveldehogeschool als expertisecentrum

Je bent

- Kandidaat-student
- Student Arteveldehogeschool
- Studiekeuzebegeleider
- Oud-student
- Sollicitant
- Journalist
- Bedrijf of organisatie
- Medewerker

Je zoekt

- Mediatheken
- Sociale voorzieningen
- Internationalisering
- Persberichten
- Dienstverlening aan organisaties (COMPaths)
- Onderzoek & ontwikkeling (COMPaths)
- Bijscholing (COMPaths)
- Publicaties (COMPaths)
- Arteveldemagazine

Nieuws en evenementen

Realisatie campus Kantienberg komt stap dichterbij
03-04-2007 - Zopas heeft het agentschap Ruimtelijke Ordening Vlaanderen, op basis van een...

In Beeld

About Us • Contact Us • Affiliates • Advertisers • Sign up • Login

Proxify® anonymous proxy protects your online privacy.

Start surfing anonymously by entering a URL (Web address) below:

Proxify

Try configurations optimized for maximum speed, security, or compatibility.

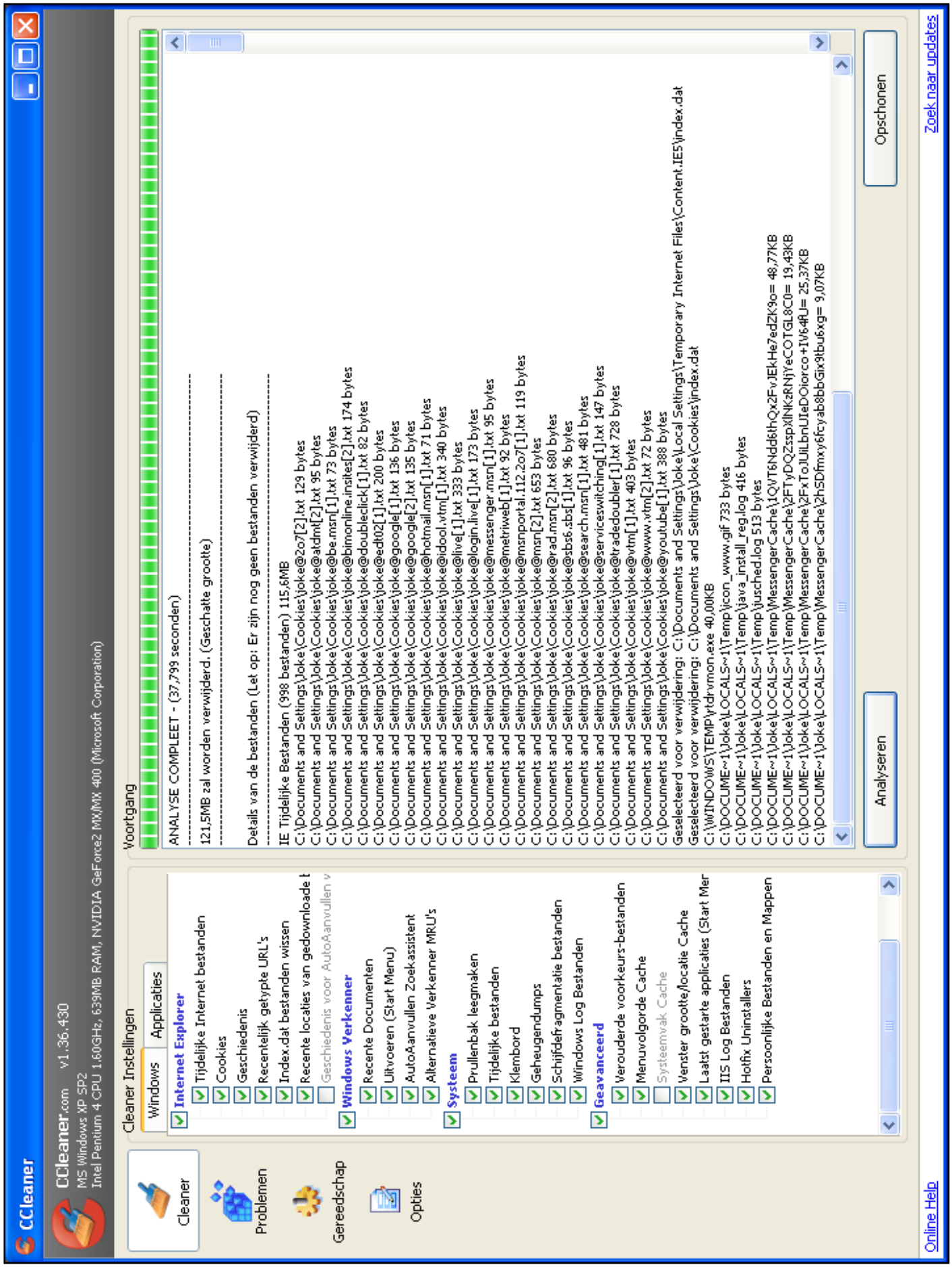
- ☐ Remove all cookies
- ☑ Remove all scripts
- ☑ Remove ads
- ☐ Hide referrer information
- ☐ Text only
- ☑ Show URL entry form
- ☐ Remove page titles
- ☐ Minimize caching
- ☑ Hide useragent
- ☐ Hex encode URL's

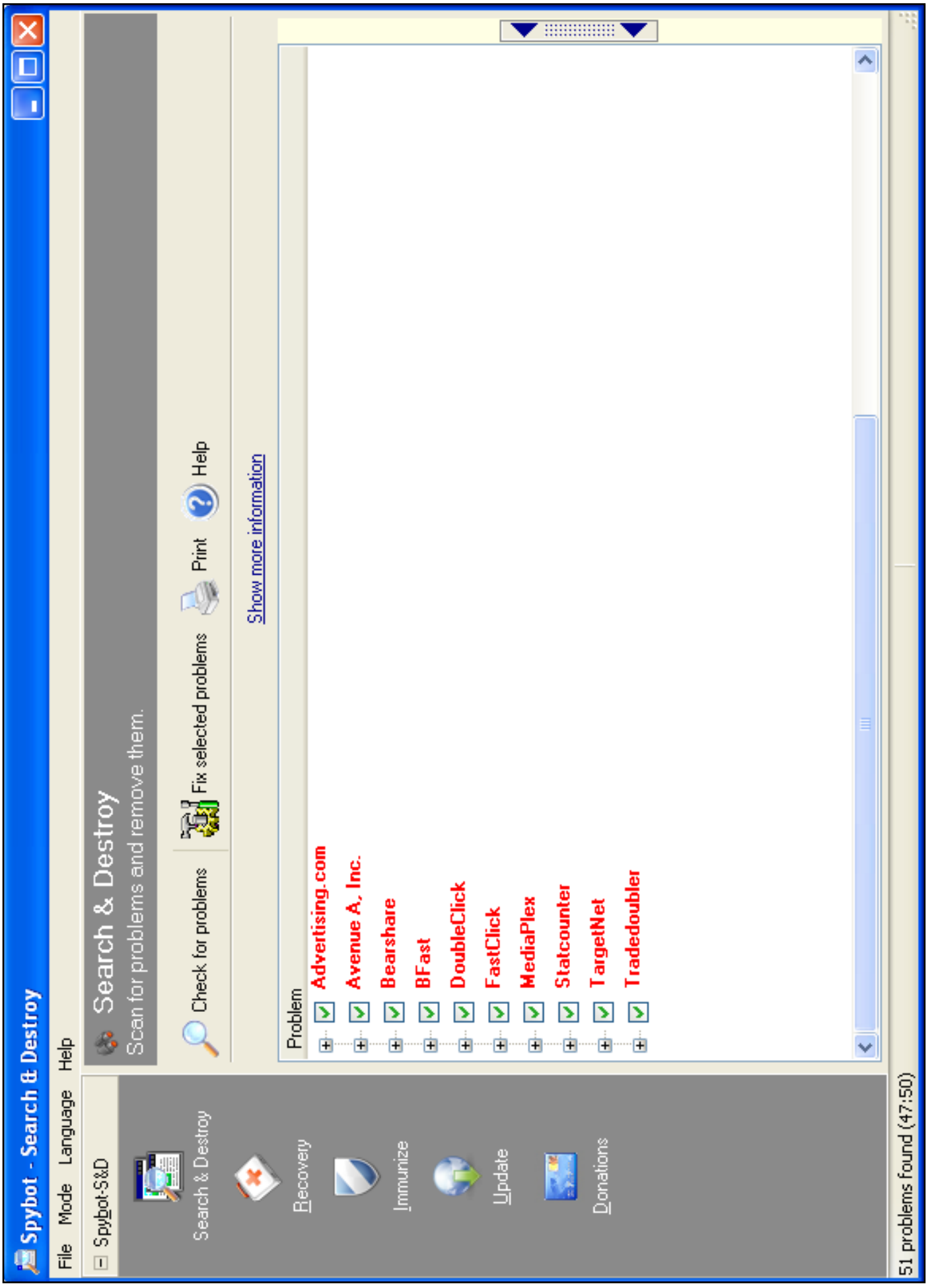
Submitting this form constitutes acceptance of our TOS. Click for HTTPS

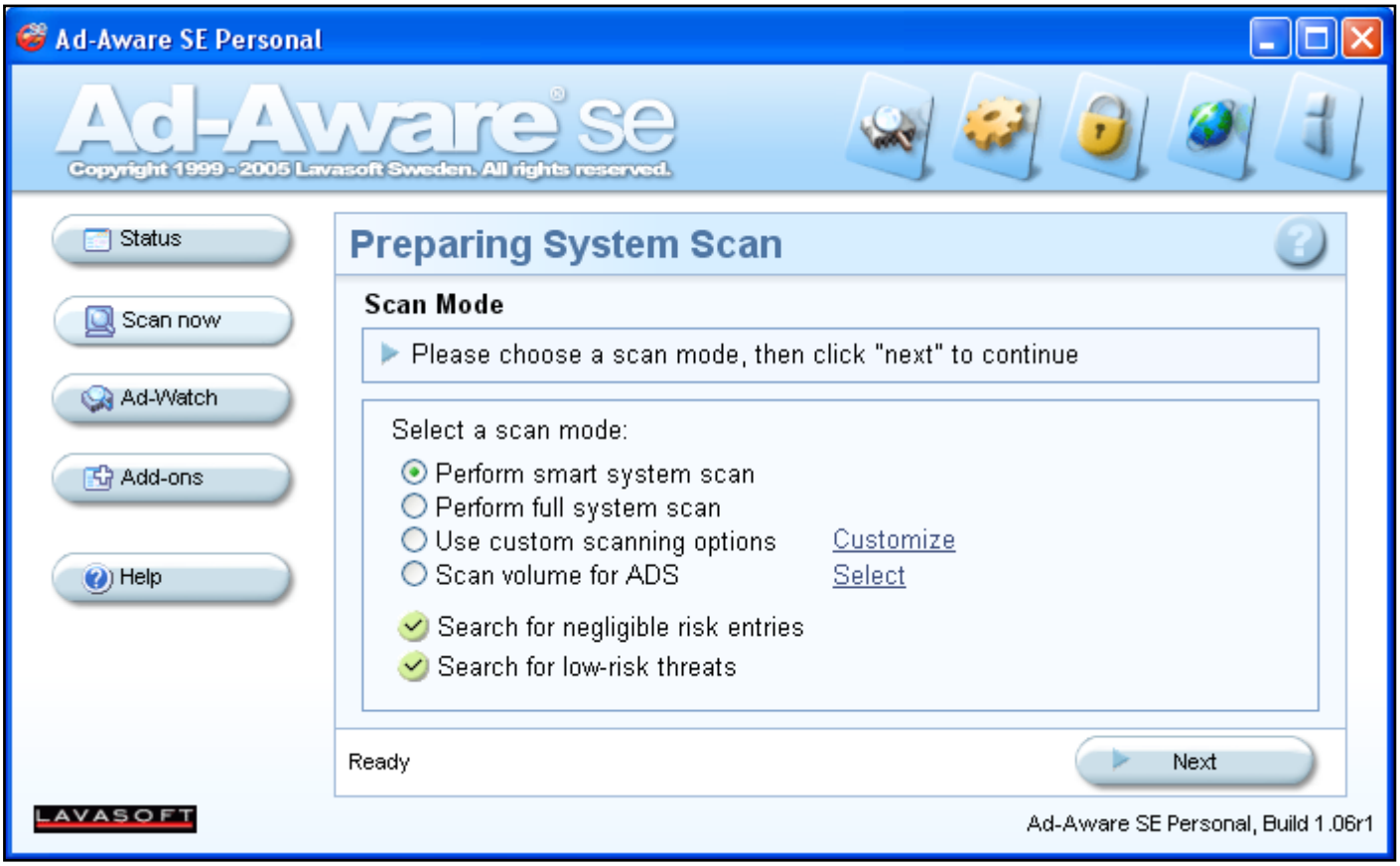
"Proxify is definitely the fastest proxy online. The "Text only" feature keeps my browser's cache clean. Proxify's high security features like encoding URL's and removing page titles protect my private communications at home and at work." - anonymous Proxify user

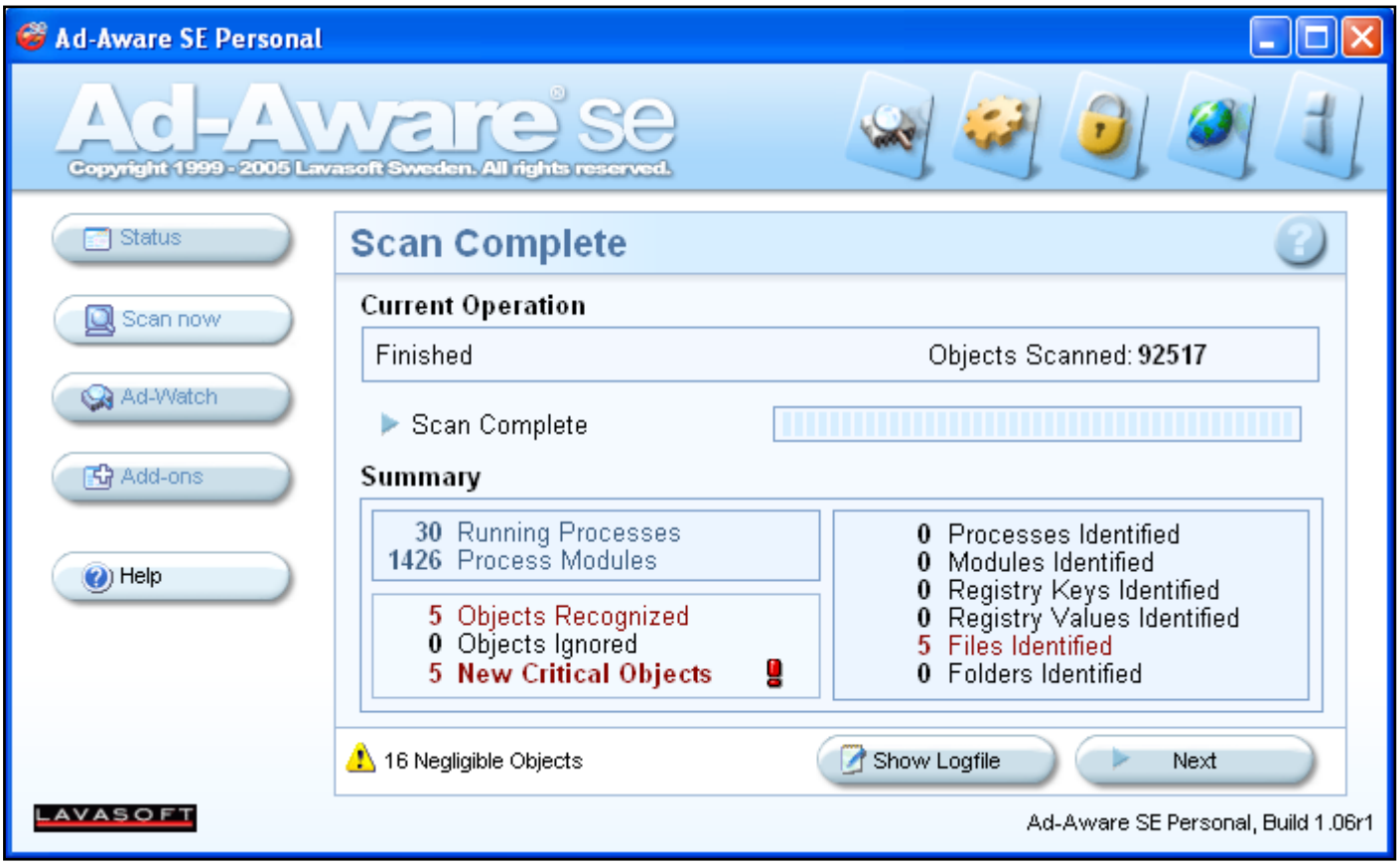
Proxify® is a web-based anonymous proxy service which allows anyone to surf the Web privately and securely. Unlike other proxies, there is no software to install or complicated instructions to follow. Just enter a URL (website address) in the form above. Through Proxify, you can use websites but they cannot uniquely identify or track you. Proxify hides your IP address and our encrypted connection prevents monitoring of your network traffic. Once using Proxify, you can surf normally and forget that it is there, protecting you.

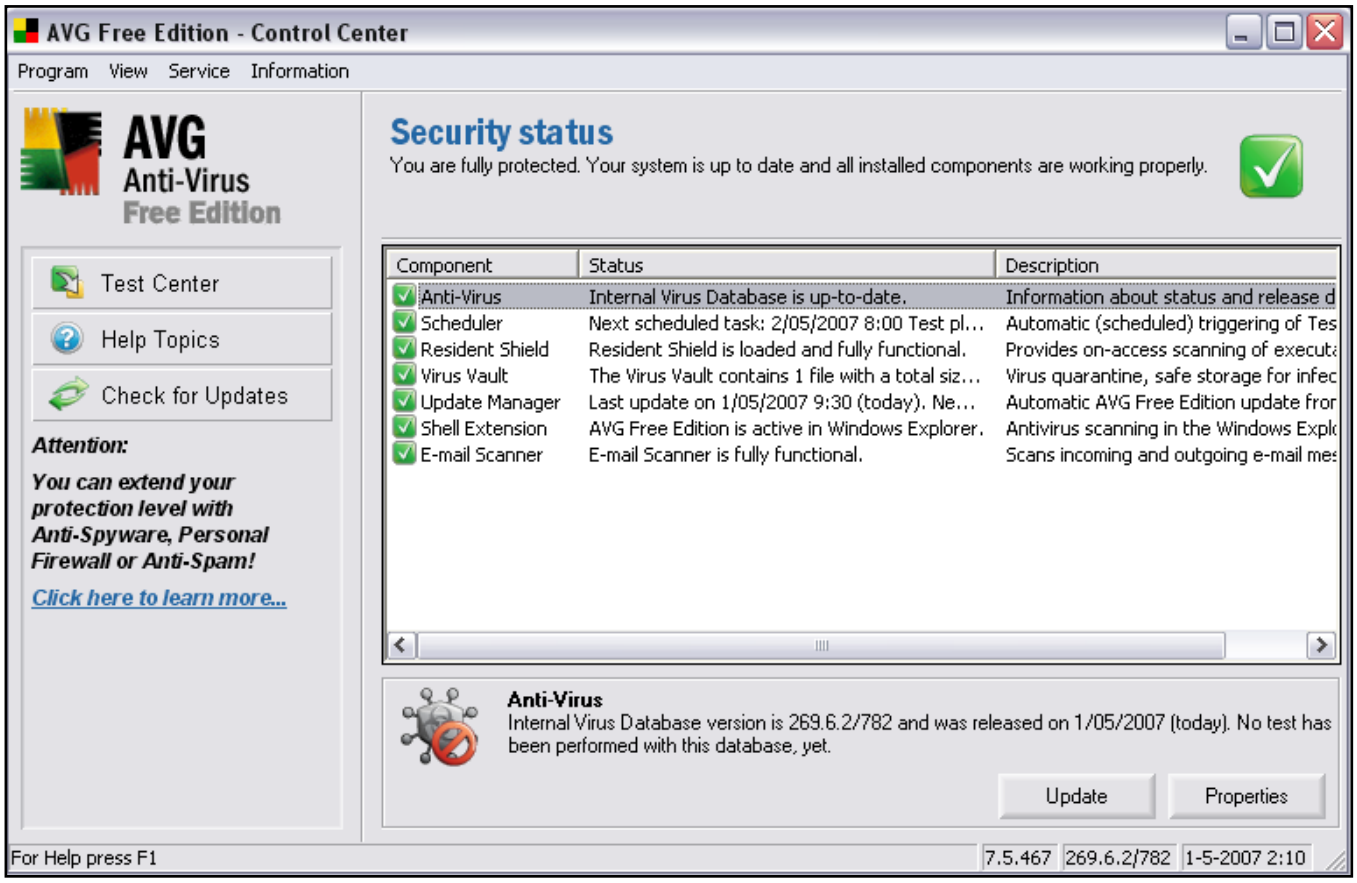

Cloaked -- Arteveldehogeschool - Home - Mozilla Firefox
Bestand Bewerken Beeld Geschiedenis Bladwijzers Extra Help
http://www.the-cloak.com/Cloaked/+cfg=48/http://www.arteveldehs.be/emc.asp
encryptie
Internetjournalistiek.be - magazine ov...
Anonymizers
Cloaked -- Arteveldehogeschool ...
Arteveldehogeschool
English | Vacatures | Contact | Zoeken
Algemene info
Arteveldehogeschool
Opleidingsaanbod
ECTS
Flexibel studeren
Kansrijk studeren
Infomomenten
Inschrijven
Gent studentenstad
Arteveldehogeschool als expertisecentrum
Je bent
Kandidaat-student
Student Arteveldehogeschool
Studiekeuzebegeleider
Oud-student
Sollicitant
Journalist
Bedrijf of organisatie
Medewerker
Je zoekt
Mediatheken
Sociale voorzieningen
Internationalisering
Persberichten
Dienstverlening aan organisaties (COMPaks)
Onderzoek & ontwikkeling (COMPaks)
Bijscholing (COMPaks)
Publicaties (COMPaks)
Arteveldemagazine
Nieuws en evenementen
Realisatie campus Kantienberg komt stap dichterbij
03-04-2007 - Zopas heeft het agentschap Ruimtelijke Ordening Vlaanderen, op basis van een...
Studenten Arteveldehogeschool organiseren mobiele computerklas in Pakistaanse vluchtelingenkampen
29-03-2007 - Zeven studenten en twee lectoren van de opleiding Bachelor in het onderwijs...
European Policy Statement
26-03-2007 - As member of the Association Ghent, University College Arteveldehogeschool...
VMW stelt jongerenwebsite voor op Wereldwaterdag
In Beeld
Arteveldehogeschool the place 2 be

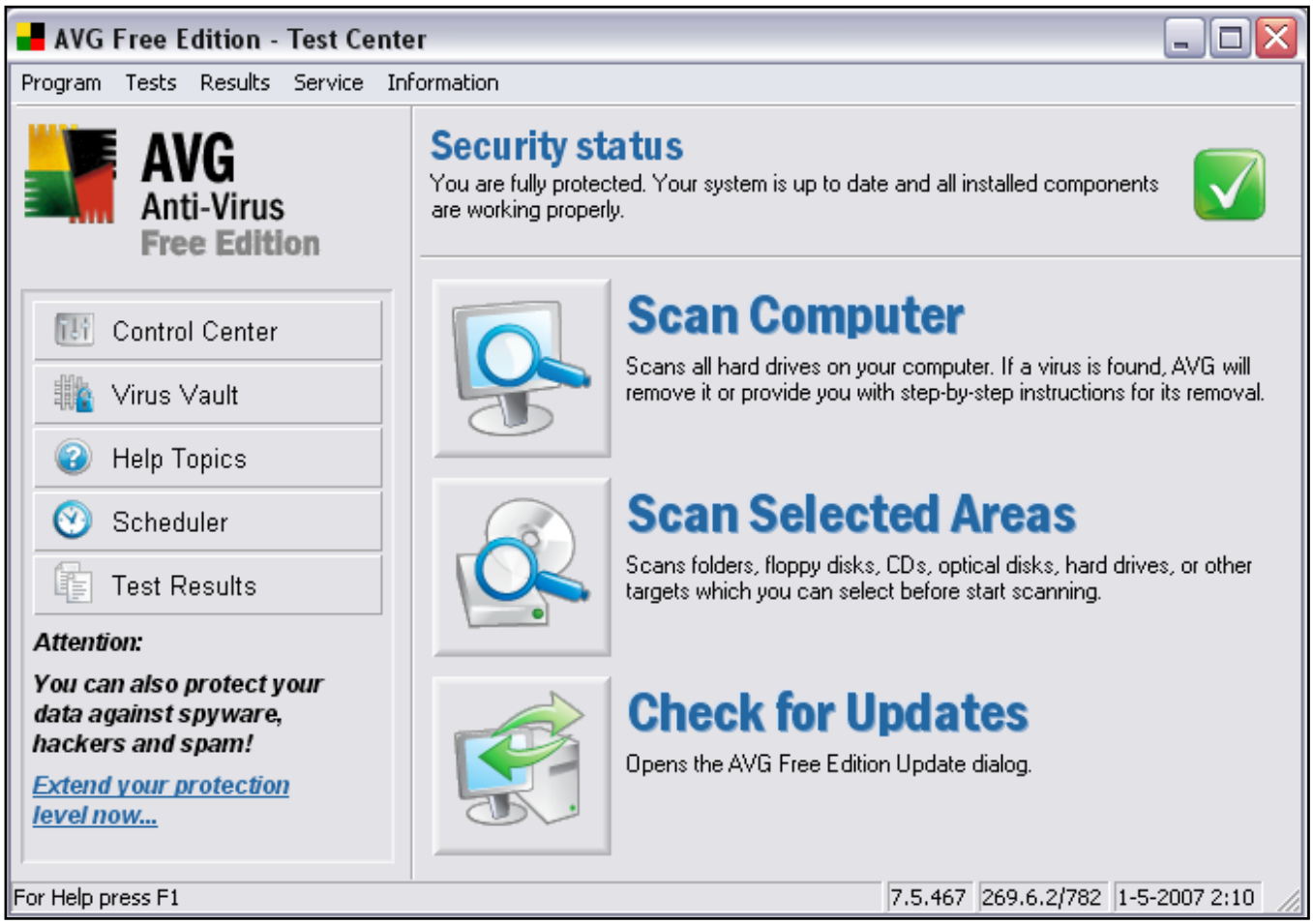

CCleaner
CCleaner.com v1.36.430
MS Windows XP SP2
Intel Pentium 4 CPU 1.60GHz, 639MB RAM, NVIDIA GeForce2 MX/MX 400 (Microsoft Corporation)
Cleaner
Problemen
Gereedschap
Opties
Cleaner Instellingen
Windows
Applicaties
Internet Explorer
Tijdelijke Internet bestanden
Cookies
Geschiedenis
Recentelijk getypte URL's
Index.dat bestanden wissen
Recente locaties van gedownloade b
Geschiedenis voor AutoAanvullen v
Windows Verkenner
Recente Documenten
Uitvoeren (Start Menu)
AutoAanvullen Zoekassistent
Alternatieve Verkenner MRU's
Systeem
Prullenbak leegmaken
Tijdelijke bestanden
Klembord
Geheugendumps
Schijfdefragmentatie bestanden
Windows Log Bestanden
Geavanceerd
Verouderde voorkeurs-bestanden
Menuvolgorde Cache
Systeemvak Cache
Venster grootte/locatie Cache
Laatst gestarte applicaties (Start Mer
IIS Log Bestanden
Hotfix Uninstallers
Persoonlijke Bestanden en Mappen
Voortgang
ANALYSE COMPLEET - (37,799 seconden)
121,5MB zal worden verwijderd. (Geschatte grootte)
Details van de bestanden (Let op: Er zijn nog geen bestanden verwijderd)
IE Tijdelijke Bestanden (998 bestanden) 115,6MB
C:\Documents and Settings\joke\Cookies\joke@2o7[2].txt 129 bytes
C:\Documents and Settings\joke\Cookies\joke@atdmt[2].txt 95 bytes
C:\Documents and Settings\joke\Cookies\joke@be.msn[1].txt 73 bytes
C:\Documents and Settings\joke\Cookies\joke@bimonline.insites[2].txt 174 bytes
C:\Documents and Settings\joke\Cookies\joke@doubleclick[1].txt 82 bytes
C:\Documents and Settings\joke\Cookies\joke@ed02[1].txt 200 bytes
C:\Documents and Settings\joke\Cookies\joke@google[1].txt 136 bytes
C:\Documents and Settings\joke\Cookies\joke@google[2].txt 135 bytes
C:\Documents and Settings\joke\Cookies\joke@hotmail.msn[1].txt 71 bytes
C:\Documents and Settings\joke\Cookies\joke@idool.vtm[1].txt 340 bytes
C:\Documents and Settings\joke\Cookies\joke@live[1].txt 333 bytes
C:\Documents and Settings\joke\Cookies\joke@login.live[1].txt 173 bytes
C:\Documents and Settings\joke\Cookies\joke@messenger.msn[1].txt 95 bytes
C:\Documents and Settings\joke\Cookies\joke@metriweb[1].txt 92 bytes
C:\Documents and Settings\joke\Cookies\joke@msnportal.112.2o7[1].txt 119 bytes
C:\Documents and Settings\joke\Cookies\joke@msn[2].txt 653 bytes
C:\Documents and Settings\joke\Cookies\joke@rad.msn[2].txt 680 bytes
C:\Documents and Settings\joke\Cookies\joke@sbs6.sbs[1].txt 96 bytes
C:\Documents and Settings\joke\Cookies\joke@search.msn[1].txt 481 bytes
C:\Documents and Settings\joke\Cookies\joke@serviceswitching[1].txt 147 bytes
C:\Documents and Settings\joke\Cookies\joke@tradedoubler[1].txt 728 bytes
C:\Documents and Settings\joke\Cookies\joke@vtm[1].txt 403 bytes
C:\Documents and Settings\joke\Cookies\joke@www.vtm[2].txt 72 bytes
C:\Documents and Settings\joke\Cookies\joke@youtube[1].txt 388 bytes
Geselecteerd voor verwijdering: C:\Documents and Settings\joke\Local Settings\Temporary Internet Files\Content.IE5\index.dat
Geselecteerd voor verwijdering: C:\Documents and Settings\joke\Cookies\index.dat
C:\WINDOWS\TEMP\ytdrvmon.exe 40,00KB
C:\DOCUME~1\joke\LOCALS~1\Temp\icon_www.gif 733 bytes
C:\DOCUME~1\joke\LOCALS~1\Temp\java_install_reg.log 416 bytes
C:\DOCUME~1\joke\LOCALS~1\Temp\jusched.log 513 bytes
C:\DOCUME~1\joke\LOCALS~1\Temp\MessengerCache\1QVT6Ndd6thQx2FvJEkHe7edZK9o= 48,77KB
C:\DOCUME~1\joke\LOCALS~1\Temp\MessengerCache\2FTyDQZsspXlNkzRNjYeCOTGL8C0= 19,43KB
C:\DOCUME~1\joke\LOCALS~1\Temp\MessengerCache\2FxToJUlLbnUIeDOiorco+IV64PU= 25,37KB
C:\DOCUME~1\joke\LOCALS~1\Temp\MessengerCache\2h5Dfmxy6fcyab8bbGix9tbu6xg= 9,07KB
Analyseren
Opschonen
Online Help
Zoek naar updates

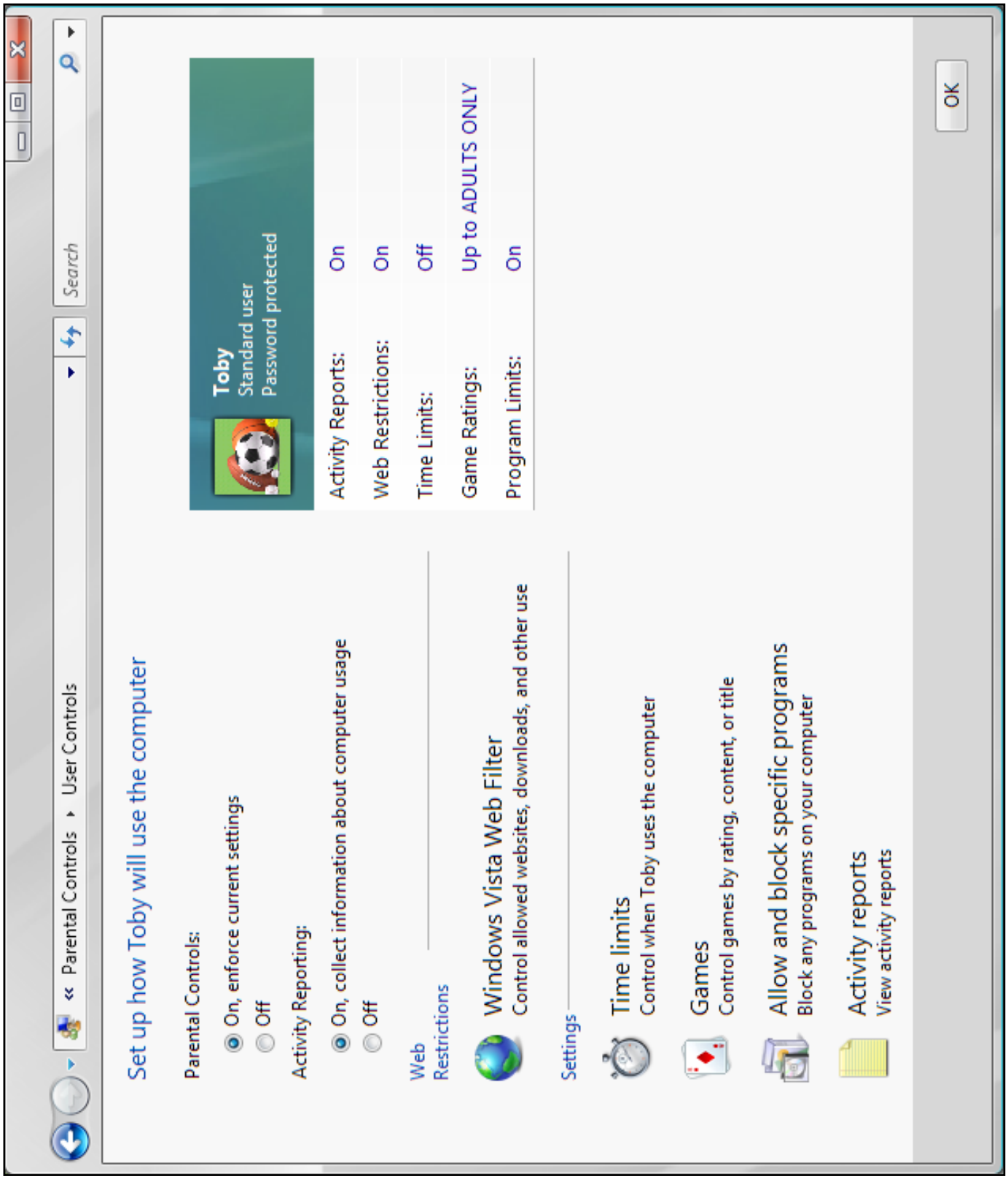

Spybot - Search & Destroy
File Mode Language Help
Spybot-S&D
Search & Destroy
Recovery
Immunize
Update
Donations
Search & Destroy
Scan for problems and remove them.
Check for problems
Fix selected problems
Print
Help
Show more information
Problem
Advertising.com
Avenue A, Inc.
Bearshare
BFast
DoubleClick
FastClick
MediaPlex
Statcounter
TargetNet
Tradedoubler
51 problems found (47:50)


Ad-Aware SE Personal
Ad-Aware se
Copyright 1999 - 2005 Lavasoft Sweden. All rights reserved.
Status
Scan now
Ad-Watch
Add-ons
Help
Preparing System Scan
Scan Mode
Please choose a scan mode, then click "next" to continue
Select a scan mode:
Perform smart system scan
Perform full system scan
Use custom scanning options
Customize
Scan volume for ADS
Select
Search for negligible risk entries
Search for low-risk threats
Ready
Next
LAVASOFT
Ad-Aware SE Personal, Build 1.06r1


Ad-Aware SE Personal
Ad-Aware se
Copyright 1999 - 2005 Lavasoft Sweden. All rights reserved.
Status
Scan now
Ad-Watch
Add-ons
Help
Scan Complete
Current Operation
Finished
Objects Scanned: 92517
Scan Complete
Summary
30 Running Processes
1426 Process Modules
5 Objects Recognized
0 Objects Ignored
5 New Critical Objects
0 Processes Identified
0 Modules Identified
0 Registry Keys Identified
0 Registry Values Identified
5 Files Identified
0 Folders Identified
16 Negligible Objects
Show Logfile
Next
LAVASOFT
Ad-Aware SE Personal, Build 1.06r1


AVG Free Edition - Control Center
Program View Service Information
AVG Anti-Virus Free Edition
Test Center
Help Topics
Check for Updates
Attention:
You can extend your protection level with Anti-Spyware, Personal Firewall or Anti-Spam!
Click here to learn more...
Security status
You are fully protected. Your system is up to date and all installed components are working properly.
Component Status Description
Anti-Virus Internal Virus Database is up-to-date. Information about status and release d
Scheduler Next scheduled task: 2/05/2007 8:00 Test pl... Automatic (scheduled) triggering of Tes
Resident Shield Resident Shield is loaded and fully functional. Provides on-access scanning of executa
Virus Vault The Virus Vault contains 1 file with a total siz... Virus quarantine, safe storage for infec
Update Manager Last update on 1/05/2007 9:30 (today). Ne... Automatic AVG Free Edition update fror
Shell Extension AVG Free Edition is active in Windows Explorer. Antivirus scanning in the Windows Explo
E-mail Scanner E-mail Scanner is fully functional. Scans incoming and outgoing e-mail mes
Anti-Virus
Internal Virus Database version is 269.6.2/782 and was released on 1/05/2007 (today). No test has been performed with this database, yet.
Update
Properties
For Help press F1
7.5.467
269.6.2/782
1-5-2007 2:10


AVG Free Edition - Test Center
Program Tests Results Service Information
AVG Anti-Virus Free Edition
Control Center
Virus Vault
Help Topics
Scheduler
Test Results
Attention:
You can also protect your data against spyware, hackers and spam!
Extend your protection level now...
Security status
You are fully protected. Your system is up to date and all installed components are working properly.
Scan Computer
Scans all hard drives on your computer. If a virus is found, AVG will remove it or provide you with step-by-step instructions for its removal.
Scan Selected Areas
Scans folders, floppy disks, CDs, optical disks, hard drives, or other targets which you can select before start scanning.
Check for Updates
Opens the AVG Free Edition Update dialog.
For Help press F1
7.5.467
269.6.2/782
1-5-2007 2:10


« Parental Controls ▸ User Controls
Search
Set up how Toby will use the computer
Parental Controls:
On, enforce current settings
Off
Activity Reporting:
On, collect information about computer usage
Off
Toby
Standard user
Password protected
Activity Reports: On
Web Restrictions: On
Time Limits: Off
Game Ratings: Up to ADULTS ONLY
Program Limits: On
Web Restrictions
Windows Vista Web Filter
Control allowed websites, downloads, and other use
Settings
Time limits
Control when Toby uses the computer
Games
Control games by rating, content, or title
Allow and block specific programs
Block any programs on your computer
Activity reports
View activity reports
OK

Bijlage bij het privacybeleid

Legend

	Adverteerders	Interne dienstverleners	Externe dienstverleners	eBay Community	Gerechtelijke verzoeken
Persoonlijke informatie					
Volledige naam		2	3	4	X
Gebruikersnaam		2	3	X	X
E-mailadres		2	3	4*	X
Adres		2	3		X
Postcode	1	2	3	4	X
Plaats	1	2	3	4	X
Provincie	1	2	3	4	X
Telefoonnummer		2	3	4	X
Land	1	2	3	4	X
Bedrijf		2	3	4	X
Wachtwoord		2	3		
Belangstellenden	1	2	3		5
Belangstellenden voor eBay-onderzoek	1	2	3		5
Leeftijdsgroep	1	2	3		5
Opleiding	1	2	3		5
Hobby's	1	2	3		5
Inkomen van huishouden	1	2	3		5
Tweede telefoon		2	3		X
Geslacht	1	2	3		X
FAX		2	3		X
Waar heb je van eBay gehoord?	1	2	3		5
Diverse marketingvragen	1	2	3		5
Persoonlijk of zakelijk	1	2	3		X
Persoonlijke correspondentie			3		5

Bron: http://pages.benl.ebay.be/help/policies/privacy-appendix.html

Bijlage bij het privacybeleid

Legend

	Adverteerders	Interne dienstverleners	Externe dienstverleners	eBay Community	Gerechtelijke verzoeken
Klantgegevens (2)					
IP-adres	1	2	3		5
Cookie	1	2	3		5
Soort browser	1	2	3		5
Bekeken pagina's	1	2	3		5
URL van volgende website	1	2	3		5
URL van vorige website	1	2	3		5
Besturingssysteem	1	2	3		5
Uur van de dag	1	2	3		5
Soort domein	1	2	3		5
Service Provider	1	2	3		5
Miscellaneous					
Fraudeformulier (4)		2	3		5
Gegevens over diensten van derden					5

(X) Beschikbaar.

1. Uitsluitend op zodanige wijze over te leggen dat je niet persoonlijk geïdentificeerd kunt worden.
2. Uitsluitend onder geheimhouding over te leggen ter verrichting van een dienst voor eBay.
3. Alleen na je goedkeuring over te leggen of direct door jou aan de verzoeker te verstrekken.
4. Alleen over te leggen als je als koper of verkoper bij een transactie betrokken bent.

(4*) Als je je e-mailadres als gebruikersnaam gebruikt, heeft iedereen toegang tot je e-mailadres.
(5) Beschikbaar bij een dagvaarding.

Persoonsgegevens

Telenet verzamelt geen persoonsgegevens tenzij deze op vrijwillige basis worden verstrekt. Met het invullen en versturen van een bestelformulier, of het verzenden van een e-mail geeft een bezoeker Telenet toestemming zijn of haar persoonlijke gegevens op te slaan in een bestand van Telenet N.V. met het oog op een geautomatiseerde gebruikersprofilering, klantenbeheer, marktonderzoek en direct mail per post. De verstrekte gegevens kunnen voor deze doeleinden worden doorgegeven aan de met Telenet contractueel verbonden ondernemingen. U heeft recht op inzage en eventuele correctie van uw desbetreffende persoonsgegevens. U heeft het recht om u kosteloos te verzetten tegen verwerking van uw gegevens voor direct marketing doeleinden. U kunt uw aanvraag tot inzage, correctie of verzet richten tot de klantendienst.
Uw elektronische contactgegevens kunnen door Telenet N.V. worden gebruikt voor direct e-mail marketing indien u hiermee voorafgaandelijk heeft ingestemd. Evenwel is uw voorafgtaande instemming niet vereist wanneer Telenet N.V. elektronische contactgegevens die zij heeft verkregen bij de levering van bepaalde producten of diensten, gebruikt voor direct e-mail marketing van eigen gelijkaardige producten of diensten. U heeft recht op inzage en eventuele correctie van uw elektronische contactgegevens. U heeft eveneens het recht om u kosteloos te verzetten tegen de verwerking van uw elektronische contactgegevens voor direct e-mail marketing doeleinden. U kunt uw aanvraag tot inzage, correctie of verzet dienaangaande richten tot de klantendienst.

Automatisch vergaarde niet-persoonlijke informatie

Telenet kan anonieme of geaggregeerde gegevens verzamelen van niet-persoonlijke aard, zoals browser type of IP-adres, het besturingsprogramma dat u gebruikt of de domeinnaam van de website langs waar u naar de Telenet-website gekomen bent, of waarlangs u die verlaat.

Cookies

Tijdens een bezoek aan de site kunnen automatisch zogenaamde 'cookies' op de harde schijf van uw computer geplaatst worden. Deze gegevens helpen ons de site beter af te stemmen op de wensen en voorkeuren van de bezoekers. Met de meeste internetbrowsers kunt u cookies van uw harde schijf verwijderen, cookies afwijzen of een waarschuwing ontvangen vooraleer een cookie geïnstalleerd wordt. Raadpleeg de instructies of help-functie van uw internetbrowser voor meer details. Indien u tijdens een bepaald bezoek aan de site instemt met het gebruik van cookies, kunnen deze cookies eventueel verder worden gebruikt bij volgende verbindingen met de site.

IP adressen

In de forums wordt bij het posten van een bericht het IP-adres van de poster weergegeven. Soms is ook het IP-adres van een proxyserver zichtbaar tussen haakjes. Het doel hiervan is de authenticiteit en de integriteit van de berichten te verhogen door te vermijden dat iemand berichten post in andermans naam. In geval van klachten over vermeend onwettelijk gedrag, kan dit IP-adres ook doorgegeven worden aan de bevoegde gerechtelijke instanties.

Bron: http://www.telenet.be

gettyimages® Creative

Go to: Creative | Editorial

Register now. Already a member? Sign In

Go to cart

images | film | services | my account | international | US

GETTY IMAGES PRIVACY POLICY

Last Updated: December 2006

Getty Images is committed to protecting your privacy. This privacy policy tells you about our online collection and use of data. The terms of this policy apply to all Getty Images websites, unless different terms are specified in a form or contract provided to you online or offline.

By using this site, you understand and agree to the terms of this policy. This site is owned by Getty Images and may be accessed in the United States and abroad. For data protection purposes, Getty Images is the controller and, unless otherwise noted, is also the processor of data. Information collected may be retained indefinitely, and may be stored, processed, accessed, and used in jurisdictions whose privacy laws may be different and less protective than those of your home jurisdiction.

Collection of Your Personal Information

When you visit this site, certain kinds of information, such as the website that referred you to us, your IP address, browser type and language, and access times, may be collected automatically as part of the site's operation. We also may collect navigational information, including information about the pages you view, the links you click, and other actions taken in connection with the site.

We may combine your visit and navigational information with personal information that you provide. You may always choose not to provide personal information, but if you so choose, certain products and services may not be available to you. Personal information (e.g., your username and password, your name, your company, your mailing address, email address, and phone number) is collected when you register. Additional personal information (e.g., your credit card number and billing address) is collected to process transactions or to provide you with products and services.

Demographic information (e.g., your age, hobbies, income, gender, or interests) may also be collected and may be linked to your personal information.

If you apply online for a job with Getty Images, our resume submission form collects personal information (e.g., your name, email address, mailing address, phone number, education and work history, and visa status) related to your application.

Use of Your Personal Information

Getty Images collects and uses your personal information to operate and improve our sites, to process your transactions, to provide customer service, to perform research and analysis aimed at improving our products, services and technologies, and to display content that is customized to your interests and preferences.

We also use your personal information to communicate with you. We may send transaction-related communications such as welcome letters, billing reminders, and purchase confirmations. We may also send you surveys or marketing communications to inform you of new products or services or other information that may be of interest. If you do not wish to receive marketing communications, you may adjust your "Personal Information Preferences" as

Bron: http://creative.gettyimages.com/source/home/privacy.aspx

Bron: http://aeijkmbdfg.attracti.net/e/?chlbdfgxroqyaeijkzcvm
(een verdachte website dus)